International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (Apr-23)

http://dx.doi.org/10.12785/ijcds/130160

Ciphertext-Policy Attribute-Based Encryption Scheme for Secure Organizations' Bitcoin Wallet Access

Fatty M. Salem[1], **Shereen M. Mahgoub**[1] **and I. I. Ibrahim**[1]

[1] *Department of Electronics and Communications Engineering, Faculty of Engineering, Helwan University, Helwan, Cairo, Egypt*

Received 5 Mar. 2022, Revised 18 Jul. 2022, Accepted 19 Dec. 2022, Published 16 Apr. 2023

Abstract: Bitcoin is a totally decentralized digital cryptocurrency stored in a wallet managed by the user using his private key. In organizations, to allow the employees to access organization wallet, bitcoins need to be managed based on each department's or team's budget. Organization's hierarchy need each department to have its bitcoins independently and control the wallet by employee's attributes as his position, email, and department to make the access more realistic and flexible. In this paper, the organization's wallet (superwallet) is divided into subwallets; a subwallet is assigned for each department based on this department's budget. This paper introduces a ciphertext-policy attributed-based encryption (CP-ABE) to control the access of organization's bitcoin subwallets. In the proposed CP-ABE scheme, a tree-based access structure will be used including AND, OR, and threshold gates with a flexible and secure access structure model. Therefore, the proposed scheme can keep the structures of organizations. Moreover, security of the proposed scheme has been analyzed.

Keywords: Bitcoin, Wallet, Organizations, Access Control, Ciphertext-policy attribute-based encryption

1. INTRODUCTION

Traditional banking [1] is totally centralized, has transaction limit, system carries the same user's name for multiple transactions, transaction fee is from 0.5% to 5% for each transaction made, and inflation can affect traditional banking system. On the other hand, bitcoin transaction [2] can be of any size, fully automated, authorized with a digital signature, users transact with different addresses can be made which makes them pseudonym, negligible cost, and inflation doesn't affect the system at all. Organizations sometimes need to produce accounting to prove about their activity. Using bitcoin offers the needed transparency to get and verify all transactions through the blockchain.

Bitcoin is created electronically by using internet connection [3]. Wallet consists of addresses with defined policy; this policy under which the bitcoins will be spent. Bitcoin wallet is divided into hot wallet and cold wallet based on how we save and spend wallet bitcoins. Hot wallet can be accessed directly from a network available device where the private keys are stored; on the other hand, cold wallet couldn't be accessed without accessing cold storage where keys are stored offline.

Organization structure [4] may be hierarchical, functional, horizontal, matrix, team based and network organization structure. As a simple example of organization team based structure, Figure 1 shows an organization consisting of some branches as operation, finance, human resource (HR), and marketing all under Chief Executive Officer (CEO) management. The existing signature schemes for bitcoins' wallet access control are not supportive for organization' hierarchy as it requires each department to access its own budget, and the financial department must prove each department budget before allowing access to wallet.

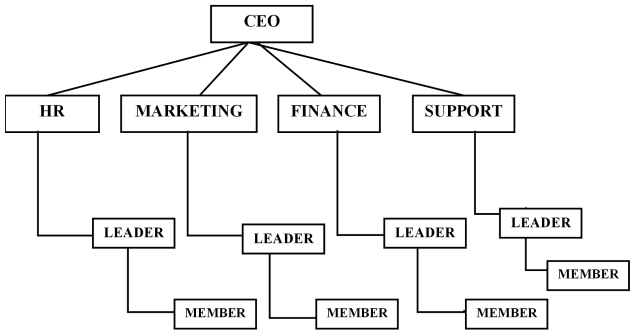

Figure 1. Example of organization hierarchy

E-mail address: faty_ahmed@h-eng.helwan.edu.eg, shry_m84@hotmail.com, iiibrahim1953@gmail.com

A. Problem Statement

When organization needs to use cryptocurrency as bitcoin, this will be different from usual currency transfer using bank. Bank or any third party has part of responsibility and management rules for organization money transfer and under government policy. In bitcoin, transaction third party doesn't exist and transaction cannot be reversed; hence, it needs more management and security. If an illegal party can access the full private keys, it can manage the wallet and make unpermitted transfers. There are two issues raised when using bitcoin wallet for organizations; First: who can access the wallet and with which budget; Second: in case of losing full wallet or losing the wallet keys, the amount of lost bitcoin must be minimized.

B. Related Work

Bitcoin transaction needs a private key for signing [5], and the value to be transferred. A new generated address is needed for each transaction where the output of this transaction will be the input of the next one. An alphanumeric sequence represents the private key which is used to unlock and sign wallet transaction.

Adding a transaction to block needs miners for validation process which uses proof of work mathematical problem to manage and prevent double spending attack [6], [7]. To secure bitcoin wallet, there are a lot of methods like authentication, digital signature schemes, two-factor authentication scheme [8] which uses password, and another authentication step like email, or messaging on phones, and three-factor authentication schemes [9], [10] which add biometrics in the authentication process.

Threshold signature schemes [11] - [12] use secret sharing by distributing a secret value share to different players. In [13], the author proposed a scheme to distribute secret keys based on the weight /priority of the user. Multi signature validation for transaction based on wallet policy is provided by bitcoin multi signature schemes [14], [15]. To reduce the bitcoin blockchain size, a new multi-signature scheme has been proposed by Ohta and Okamoto in [16]. However, to generate a short joint signature on a common message, Schnorr-based multi-signature scheme has been proposed in [17].

The author in [18] proposed an Advance Encryption Standard (AES)-based scheme to encrypt bitcoin wallet database. The authors in [19] made a comparison between different types of bitcoin key management approaches. Recently, the authors presented an encapsulated operation signature [20] in which a team member's signs from the lower to the higher priority member, until the last signer of the team.

There are many methods to control user access; traditionally using access control list (ACL) as in [21], [22] and by using role-based access control (RBAC) as proposed in [23], [24]. The author in [25] uses RBAC relying on the hierarchical identity-based encryption scheme and the challenge-response authentication protocol to gain security and flexibility and to provide additional properties in the cyber world. In [26], authors introduced many-to-many ciphertexts and user keys relation as the first ABE scheme. Attribute-based access control is introduced in [27] where access decision depends on user attributes. Access control and ABE support many applications as web access, oblivious transfer, vehicular ad-hoc network, and cloud computing [28], [29], [30], [31], [32] which may use biometric based application or threshold access control system.

Key-Policy Attributed-Based Encryption (KP-ABE) [33] allows tree-based access structure; however, key-issuer must be trusted to issue the suitable keys to accept or deny access to the defined users. KP-ABE schemes [34], [35], [36], [37] are used for one-to-many relation. In KP-ABE, attributes' set can identify ciphertexts and private keys that are compatible with the access tree that determines which ciphertexts the user can decrypt.

Ciphertext-Policy Attributed-Based Encryption (CP-ABE) is another ABE form introduced in [38], [39], [40], [41]; it proceeds in different manner by assigning attributes set to private keys and allowing senders to define the policy. A user could decrypt a specific ciphertext only if the defined attributes related to his private key gets the policy associated with this ciphertext. In CP-ABE schemes [42], [43], [44], every ciphertext is defined by access policy on attributes. In [45], the author has introduced a dual-encryption to prove a full security definition for CP-ABE. The authors in [46] have used composite bilinear groups to prove security of functional encryption schemes, and CP-ABE by dual bases vector spaces has been proposed in [47]. In [48], the authors use constant size secret key based on elliptic curve cryptography. In [49], the authors specified their work for law energy devices. Based on bilinear maps, the schemes [41], [50] have been introduced.

The authors in [51] have proposed two CP-ABE schemes in which authorization is determined using AND-gate with wildcard. While the authors in [52] have analyzed the relations between particular data objects, introduced the critical data constraint concept, and proposed a CP-ABE for the critical data compliance with hidden attributes. The policy is hidden where attribute's names cannot be exposed; to do so, the authors in [53] advocated not delivering the access matrix with the ciphertext.

Blockchain-based Distributed ABE (BDABE) scheme has been proposed in [54] as a collaborative attribute management method for CP-ABE. In [55], the authors have proposed a system that uses bitcoin technology to realize a trans-organizational role-based access control. The proposed system in [55] is based on providing incontrovertible confirmation of a user's position/role issued by an organization by using the bitcoin blockchain to verify the user's link to the organization. A challenge-response protocol can be used by the service provider to validate this role; if an unknown user gets access to the transaction's output address, he can't get the coins.

The superwallet subwallet idea has been proposed in [56], it is a fair exchange protocol in which bitcoins are stored in a personal bank, and subsequently distributed between numerous computing devices utilizing threshold approaches to create a small subwallet on a smartphone. Hence, in

case of smartphone loss or hacking by adversary, the user only loses the little quantity of money in his wallet, not the money in his personal bank.

C. Contributions

This paper provids important contributions in bitcoin wallet access control:

- Designing a secure organizations' bitcoin wallet access scheme based on CP-ABE.
- Offering secure wallet and limiting the access of each team to its budget.
- Minimizing the number of lost bitcoins in case of losing the full wallet or wallet keys.
- Keeping the structures of organizations.
- Providing security proof of the proposed scheme.

There are a lot of crypto currencies as bitcoin, Ethereum, altcoin.... etc. For example, Ethereum and bitcoin operate on blockchain technology; both of them have wallets with no third-party control. The different is in the consensus system, the ledger version, and the currency type (Ethereum, bitcoin, altcoin), but both have wallet with private keys that can be divided using our solution. We choose to work on bitcoin as it is the most popular digital token.

D. Road Map of the Paper

The rest of the paper is organized as follows: Section 2 presents the system model and access structure. Section 3 revises the preliminary work. The suggested CP-ABE access control method is introduced in Section 4. The proposed scheme's security is proved in Section 5. The performance of the proposed scheme is compared with other related schemes in Section 6. Lastly, the paper is concluded in Section 7.

2. SYSTEM MODEL AND ACCESS STRUCTURE

The organization system model and the organization wallet access structure will be described in this section.

A. System Model

For wallet access, the organization will be divided into two branches: operating branches and finance branches. Except for the financial department, any department in the organization can be classified as an operation branch. Financial department team is responsible for determining each operation team bitcoins budget and encrypting it for operation team in subwallet. Financial department team can manage and use all bitcoin subwallets for any critical or needed case by using its superwallet.
In our model, superwallet subwallet will be used in a different manner. The superwallet is the organization wallet which contains all bitcoins that will be under control of financial team and CEO Head; however, subwallets are the budget of the operation teams. As shown in Figure 2, wallet contains all coin (superwallet) will be divided into smaller subwallets for each team who needs his own budget. This will simplify organization money control as each team can access only his budget, but he can't get access to other teams' bitcoins.

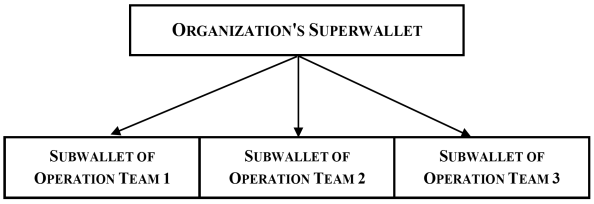

Figure 2. Organization superwallet subwallet

We mention that company has a definition of roles and sectors, but in real money, there is a third party as a bank, the bank has the role and policy for the company money as a limit to transfer, who can transfer and when. This is not clear in cryptocurrency which needs more control. We proposed a solution to manage wallet access and divide it to smaller sectors. It is not alternative to internal cost sector as this sector is the main part of our solution.
By dividing organization wallet, we can achieve the following benefits: managing each part of wallet separately, knowing the data of each part, and for any reason if you lost a part of your wallet, it won't affect other parts. Bitcoin is irreversible transaction; hence, if it is used with a huge scale in organization, it needs more security and careful saving. Meanwhile this also makes wallet accessed by more than one member together to save wallet. Also, if we made different project subwallets, we could make different members team to manage different subwallets.
Wallet needs to be divided into smaller budget parts, and each part will be accessed by its own operation department. Each department team will access the wallet due to organization role. Financial team can access all wallets to transfer money or to cancel the department budget for any reason. Moreover, financial team can transfer wallet money to other wallet address. CEO Head will be given also full control to access wallet. This access policy may differ from organization to another based on its policy and structure.

B. Access Structure

The access structures in the proposed system are carried out using an access tree in which each leaf node is labelled with an attribute and the internal nodes in non-leaf nodes of the access tree are And, OR, and threshold gates. Using the access tree, the access privileges of each employee can be defined. Using ABE scheme, we can use monotonic gates access structures [57], but we can't represent negative or non-monotonic gates [58]. Our idea consists of creating an aggregate access tree to permit a multi-level access of the wallet.
Our proposed organization tree-based access structure is depicted in Figure 3. At non-leaf nodes of the access structure, there are logical gates AND, OR, and threshold gates. Each subwallet will be decrypted by authorized department or teams' attributes which described in leaf node.

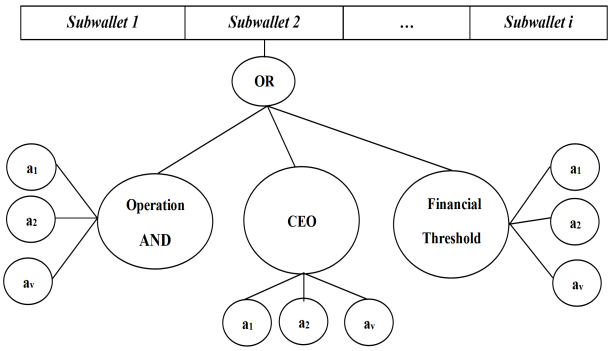

Figure 3. The proposed organization access tree-based structure

At the leaf nodes, the access comprises attributes which represents employee authorization. Employee's attributes can be name, team, position, or age of the employee; these attributes will be represented as $\{a_1, \ldots\ldots, a_v\}$ for each authorized department. Financial team can decrypt any subwallet, if needed, which allows full wallet control and bitcoins recovery. Each member is described using some attributes and each subwallet can be accessed by CEO, or threshold of financial team, or all the predetermined operation team.

C. Model Assumption

Following are the assumptions in our system model:

- ***Key Generation Center (KGC):*** Organization needs a fully trusted authority or KGC to generate the public and secret parameters for CP-ABE; KGC is responsible for generating the master secret key. Additionally, KGC contains data issues and revokes attribute keys to authorized users. It is responsible for issuing, revoking, and updating attribute keys for employees. It provides varied access rights to each user according to their attributes.
- ***Chief Executive Officer (CEO):*** It is an entity responsible for managing the overall operations and resources of a company. In addition, CEO Head will be given full control to access wallet.
- ***Financial Department:*** It is an entity responsible for putting each subwallet limit and its subwallet operation team attributes and gives these attributes to KGC.
- ***Employee (Operation Teams):*** It is an entity who aims to gain access to the encrypted bitcoins wallet.
- Providing security proof of the proposed scheme.

3. PRELIMINARIES

The preliminaries for the proposed CP-ABE scheme will be illustrated in this section.

A. Bilinear Mapping

We consider two cyclic groups of prime order q, namely $(G_T, +)$ and $(G_T,)$. $(G_T, +)$ is an additive cyclic group whereas $(G_T,)$ is a multiplicative group. The properties of bilinear mapping e $GG\text{ß}G_T$ are as follows:

1 Bilinearity: For any X, YG and p, qZ_y^*, it has $e(pX, qY) = e(X, Y)^{pq}$.
2 Non-degeneracy: For any X, YG, it must satisfy $e(X, Y)1_{GT}$.
3 Computability: For any X, YG, it is easy to compute $e(X, Y)$.

B. CP-ABE Security Definition

The security of the proposed scheme depends on the discrete logarithmic problem (DLP) and the computational bilinear Diffie-Hellman problem; these problems are defined as: DLP: Given X, YG, it is infeasible to get an integer n where Y = nX. Computational Bilinear Diffie Hellman (CBDH): Given $X, A = pX, B = qX, C = bXG$, and bilinear mapping $eGG\text{ß}G_T$, it is infeasible to find $e(X, X)^{pqb}$.

The security of a fully secure CP-ABE is based on the following indistinguishable game:

1 Setup: The challenger C starts Setup $(s, attr_{un})$, produces the public and master keys P_K and SK_M. Then, C hands out P_K to the adversary A while keeping the secret SK_M for himself.
2 Phase 1: A is the adversary who sends q requests for secret key to C for sets of parties' attributes $X_1, \ldots, X_Q$. For each $i - th$ query, C runs KeyGen (SK_M, P_K, X_i) to produce the secret key SK_{Xi} and gives SK_{Xi} to A.
3 Challenge: A gives messages M_0, M_1 with same size and a challenge structure β^* to the challenger. β^* is constrained with none queried attribute sets, and the set of attributes $X_1, \ldots, X_i$ as the authorized set in β^*. The challenger C guesses a binary coin b and runs Encrypt (P_K, M_b, β^*) and gives C to A.
4 Phase 1, for $X_{(i+1)}, \ldots, X_l$ which is none authorized set in β^*.
5 Finally, A guesses b and outputs b'; A wins if $b = b'$. The game advantage for A is: $Adv_{Gamereal_l}^{A} = |Pr[b = b'] - \frac{1}{2}|$. Definition. A CP-ABE scheme is considered to be fully secure if any polynomial time attacker has $Adv_{Game_{real}} \leq \varepsilon$ where ε represents a negligible function.

C. Threat Model and Goals

The proposed model addresses threats as follows:

- Wallet loss threat: It defines threat of losing the wallet due to unreversible wallet property and any authorized user having full access to it.
- Access policy threat: It defines a malicious employee whose aim is to access the wallet and gain the wallet coins.
- Private keys loss threat: It defines the full private keys access without deviation which means the wallet full loss or full access threat.

We need to achieve some objectives against the above-mentioned threats.

- Access Management: Access policy can be managed by keys encryption to gain wallet access control depending on employee attributes using CP-ABE.
- Data Confidentiality: The secrecy of encrypted data must be protected against malicious users as only authorized user can access the wallet.
- Detection: Detecting fraudulent transaction is a must using malicious user privates and attributes. Each operation team can access only his budget from wallet, and the budget limit is defined by financial team.
- Functional Separation of Duties: Each organization branch and each employee can access his budget based on his position in the organization hierarchy.
- Authorization: Authorized employee only should be able to access wallet bitcoins.
- Multi-layer Wallet Protection: The wallet access can be protected using ABE in addition to internal wallet signing roles.

4. THE PROPOSED CP-APE ACCESS CONTROL SCHEME

In this section, the proposed CP-ABE access control scheme is introduced for securing organizations' bitcoin wallet access using tree-based access structure to grant more flexible and secure access. As illustrated in Figure 4, the scheme proceeds briefly as follows:

1 Financial department gives attribute universe description n and attribute sets X_i of organization to KGC.
2 KGC generates bilinear group generator value, the public parameter P_K and the master secret key SK_M and uses the key generation algorithm to generate the employees' secrets SK_{Xi} and sends the corresponding secret key to each employee through a secure channel.
3 KGC decrypts each subwallet .dat file based on financial defined budget.
4 Finally, employees can use their keys and attributes to access their own subwallet, only their own wallet address or their own project budget.

The proposed CP-ABE access control scheme comprises of 5 algorithms: Setup, Key generation, Key distribution, Encryption, and Decryption. These five algorithms are defined as follows:

A. Setup

department gives attribute (n, X_i) of organizations to KGC after adjusting each subwallet limits and determining who can access. KGC uses collected information from financial team to generate the P_K and SK_M.

- Setup algorithm Setup(sec,n): KGC runs G_e =($N = p_1p_2p_3, G, G_T, e$) $\leftarrow$ $Gen(sec)$, where $Gen(sec)$ is a composite bilinear group's generator which outputs is G_e. Next, it chooses randomly $\{\gamma, s, k_0, \ldots, k_n, l_0, \ldots, l_n\} \leftarrow Z_N$, $gG_{p1}, and g_3G_{p3}$. It lets $Q = 0, \ldots\ldots, n$, and sets a function to compute Lagrange coefficient as:

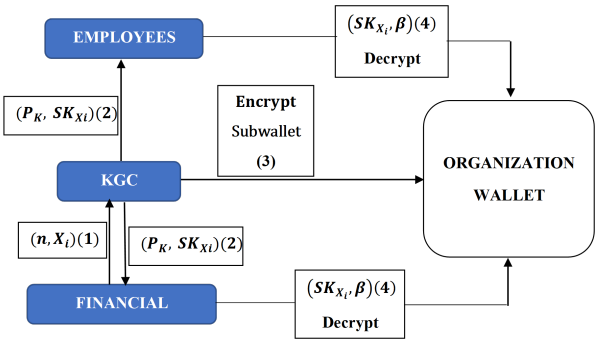

Figure 4. Procedures of the proposed scheme

$$(i, Q)(x) = {}_{jQ,ji} \frac{(x-j)}{(i-j)} \tag{1}$$

The setup algorithm entails setting up two public functions K: $Z_N \rightarrow G_{p1} and L : Z_N \rightarrow G_{p1}$ as:

$$K(x) = g^{s\,x}_{i=0}{}^{n} g^{k_{ii}, Q(x)} \tag{2}$$

$$L(x) = g^{s_{0,Q}(x)n}_{i=1} g^{l_{ii,Q}(x)} \tag{3}$$

Finally, Setup (sec, n) returns the public parameters P_K as $P_K = \{G_e, g, g^s, g^{l_o}, \ldots..,g^{l_n}, g^{k_0}, \ldots\ldots..,g^{k_n}, e(g,g)^{\gamma}\}$, while the master secret key SK_M is determined by: $SK_M = \{\gamma, g_3\}$.

B. Key Generation (SK_M, P_K, X_i)

KGC uses the key generation algorithm KeyGen (SK_M, P_k, X_i) and parses X_i as $x_{i1}, \ldots., x_{iv}$ where v is the size of X_i which represents department attributes.

At first, it selects randomly $u \leftarrow Z_N$ and $\{R, R', R_1, \ldots, R_v, R'_1, \ldots, R'_v\} \leftarrow G_{p3}$. Then, it returns SK_{Xi} for ith subwallet where X_i is department attribute.

$$SK_{X_i} = \{X_i, V = g^{\gamma}\, g^{su} R', W = g^u R', \{V_i = K x_i{}^u R_i, W_i = L x_i{}^u R'_i\}_{i=1,\ldots,v}\} \tag{4}$$

C. Key Distribution

The total wallet .dat file (super wallet) will be divided into smaller part for each team or project (subwallet) to be encrypted. As shown previously in Figure 3, with huge number of employees' access, the whole superwallet is divided as subwallets. Subwallet 2 will be accessed by a specific operation team, the financial team, or CEO. We assumed using AND gate for the specified operation team employees while financial team will access all subwallets using threshold gates, and finally CEO head has full wallet control.

Root is non-leaf node in β, andd$_{swi}$ is a secret of subwallet i for operation team, financial team, and CEO. KGC randomly chooses $d_{swi} \in Z_N$ and calls Secret Share $(Root, d_{swi})$ where d_{swi} is the subwallet secret share for each department who can access this subwallet as follows:

- Operation team shares are generated as follows: For $j = 1, \ldots\ldots$,v−1, where v is the number of operation team attributes:

$$\lambda_v = d_{sw_i} - \sum_{j=1}^{v-1} \lambda_j \tag{5}$$

- CEO will have d_{swi} with full control, and its shares λ_v for attributes will be as in equation (5).
- Financial team shares are generated as follows: The d_{swi} will be shared for financial team as follows: For $\rho = 1, \ldots\ldots, t-1$ and $a_\rho \leftarrow Z_N$:

$$q(x) = d_{sw_i} + a_1 x + + a_{t-1} x^{t-1} \tag{6}$$

For $k = 1, \ldots\ldots, v$, where v is number of financial team attributes:

$$\lambda_k = q(k) \tag{7}$$

Return: $\lambda_1, \ldots, \lambda_v$ which are the shares for daughter nodes in the Root.

D. Encryption(P_K, M, β):

Encryption algorithm (EA) takes as inputs: the public value P_K, a message M which is the related subwallet bitcoin wallet .dat file, and an access structure β, and it returns a ciphertext C. Let P is a set of all leaf nodes in β which requires X satisfying β. KGC randomly chooses $r_{att} \in Z_N$ for all $att \in$P where P represents different department attributes. If λ_{att} is a secret share for a leaf node $att \in P$, then the (EA) creates the subwallet ciphertext as follows:

$$\begin{aligned} C_{sw} = \{\beta, C = Me(g,g)^{\gamma d_{sw_i}}, C_1 = g^{d_{sw_i}}, D_{att} = g^{r_{att}} \\ C_{att} = g^{s\lambda_{att}} K(X(att))^{r_{att}}\} \end{aligned} \tag{8}$$

E. Decryption(SK_{X_i}, C_{sw}) :

Decryption algorithm (DA) takes as inputs: the subwallet ciphertext C_{sw} and the private key SK_{X_i}. Then, it outputs M if $\beta \in X_i$ where X_i represents the department attributes; otherwise, it outputs nothing. If $\beta \in X_i$, the (DA) calculates the secret share of β from bottom leaf nodes to root node. The decryption algorithm computes:

$$\begin{aligned} A_{att} = \frac{e(C_x, W)}{e(D_x, V_x)} = \\ \frac{e(g^{s\lambda_{att}} K(x)^{r_{dep}}, g^u R'))}{e(g^{r_{att}}, K(x)^u R')} = e(g,g)^{su\lambda_{att}} \end{aligned} \tag{9}$$

And compute for operation leaf node:

$$A_{op} = \prod_{Root} e(g,g)^{su\lambda_{Root}} = e(g,g)^{sud_{sw_i}} \tag{10}$$

The same for CEO leaf node:

$$A_{CEO} = \prod_{Root'} e(g,g)^{su\lambda_{Root'}, \Delta_{index(Root),I(0)}} = e(g,g)^{sud_{sw_i}} \tag{11}$$

Then compute for financial leaf node:

$$A_F = \prod_{Root'} e(g,g)^{su\lambda_{Root'}, \Delta_{index(Root),I(0)}} = e(g,g)^{sud_{sw_i}} \tag{12}$$

Finally, decryption algorithm can recover the message as:

$$\frac{C}{e(C_1, V)/A_{Root}} = \frac{Me(g,g)^{\gamma d_{sw_i}}}{e(g^{d_{sw_i}}, g^\gamma g^{su} R)/e(g,g)^{sud_{sw_i}}} = M \tag{13}$$

Where $e(g^{d_{sw_i}}, g^\gamma g^{su} R)/e(g,g)^{sud_{sw_i}} = e(g^{d_{sw_i}}, R).e(g,g)^{\gamma d_{sw_i}} . \frac{e(g,g)^{sud_{sw_i}}}{e(g,g)^{sud_{sw_i}}} = e(g,g)^{\gamma d_{sw_i}}$ as $e(g^{d_{sw_i}}, R) = 1$ due to the orthogonality. The decryption algorithm returns the message M if X has validated as an authorized set in the access structure β.

The proposed solution is mainly proposed for organizations to control the wallet and divid it to smaller parts. It controls organization pudget limit based on its projects or department limit. We solve the problem of losing the full wallet or make it under specific party control as the action is unreversable in bitcoin network. This system is applied for organization with large wallet and huge number of departments. The advantage is to control and save the wallet, while the disadvantage is the system cost that is nothing comparing with losing wallet.

5. SECURITY PROOF

We use the assumptions in [59] for our proof; this assumption uses some games that depend on semi-functional private key. We have three assumptions defined as follows:

Assumption 1. $|pr[A(D, T_1)] - pr[A(D, T_2)] = 1| < \varepsilon$, ε is a negligible function. Where $Gen(sec)$ is a composite bilinear groups generator which outputs $BLG = (N = P_1 P_2 P_3, G, G_T, e)$. Let $Y_1 \leftarrow G_{P_1}, g_3 \leftarrow G_{P_2}, T_1 \leftarrow G_{P_1}$ and $T_2 \leftarrow G_{P_1 P_2}$ all randomly selected. Using these elements, we set $D = (BLG, Y_1, g_3)$, all these parameters are used for assumption 1 satisfaction.

Assumption 2. $|pr[A(D, T_1)] - pr[A(D, T_2)] = 1| < \varepsilon$, ε is a negligible function. Where $Gen(sec)$ is a composite bilinear groups generator which outputs $BLG = (N = P_1 P_2 P_3, G, G_T, e)$. Let $X_1, Y_1 \leftarrow G_{P_1}, Y_2, Z_2, X_2 \leftarrow G_{P_2}, Y_3, g_3 \leftarrow G_{P_3}, T_1 \leftarrow G_{P_1 P_2 P_3}$ and $T_2 \leftarrow G_{P_1 P_3}$ all randomly selected. Using these elements, we set $D = (BLG, Y_1, Y_1^\alpha X_2, g_3)$, all these parameters are used for assumption 2 satisfaction.

Assumption 3. $|pr[A(D, T_1)] - pr[A(D, T_2)] = 1| < \varepsilon$, ε is a negligible function. Where $Gen(sec)$ is a composite bilinear groups generator which outputs $BLG = (N =$

$P_1P_2P_3, G, G_T, e$). Let $\alpha, S \leftarrow Z_N, X_2, Y_2 \leftarrow G_{P_2}, Y_3, g_3 \leftarrow G_{P_3}, T_1 = e(g,g)^{\alpha,s}$ and $T_2 \leftarrow G_T$ all randomly selected. Using these elements, we set $D = (BLG, Y_1, Y_1^{\alpha} X_2, g_3)$, all these parameters are used for assumption 3 satisfaction.

Semi-Functional Generation (SFG): First starting by compute a Semi-functional ciphertexts (SFC), secret keys and the two public functions $K : Z_N \rightarrow G_{P_1}$ and $L : Z_N \rightarrow G_{P_1}$. We use following equations:

$$K_{sf}(x) = g_2^{bx} \prod_{i=0}^{n} g_2^{q_i \Delta_i, Q(x)} \tag{14}$$

$$L_{sf}(x) = g_2^{L\Delta_o, Q(x)} \prod_{i=0}^{n} g_2^{l_i \Delta_i, Q(x)} \tag{15}$$

Where $\{b, q_0, ..., q_n, I_0, ..., I_n\} \leftarrow Z_N$ and $Q = \{0, ..., n\}$. A generator algorithm computes a normal ciphertext as:

$$C'_{sw} = \{Att, C' = Me(g,g)^{\gamma d_{sw_i}}, C'_1 = g^{d_{sw_i}}, D'_y = g^{r_y}, \\ C'_y = g^{d_{sw_i} \lambda_y} K(att(y))^{r_y}\} \tag{16}$$

The algorithm randomly chooses $c \in Z_n$. Then, it computes the secret share for c in the A^* . Suppose for all nodes $y \in A^*$, it has μ_y as y share; then, it randomly picks $\alpha_y \in Z_n$ and calculates the (SFC):

$$C_{sw_{sf}} = \left\{A^*, C', C_1 g_2^c, D_y = D'_y g_2^{\alpha_y}, C_y = C'_y g^{b\mu_y} K_{sf}(att(y))^{\alpha_y}\right\} \tag{17}$$

The algorithm randomly chooses $h, f \in Z_n$, then, uses normal key generation, and computes a normal secret key $SK'_x = \left\{d, V', W' \left\{V'_i, W'_i\right\}_{i=1,...,l}\right\}$. There are two semi-functional secret keys (SFS):

(SFS1):

$$SK_{sf1} = \left\{X, V = V' g_2^f, W = W' g_2^h, \right. \\ \left. \left\{V_i = K_{sf}(X_i)^h V'_i, W_i = L_{sf}(x_i)^h W'_i\right\}_{i=1,...,l}\right. \tag{18}$$

(SFS2):

$$SK_{sf2} = \left\{X, V = V' g_2^f, W = W', \right. \\ \left. \{V_i = V'_i, W = W'_i\}_{i=1,...,l}\right. \tag{19}$$

By decrypting a SFC, $C_{sw_{sf,A}}$ by 1 $SK_{sf1,x}$ when $X \in A$ yields:

$$Me(g_2, g_2)^{c(bh-f)} \tag{20}$$

When $h = f mod p_2$, the (DA) can resolve M. By that, we get nominal (SFS1). In contrast, if the decryption of $CT_{sf,A}$ by $SK_{sf2,x}$ for $X \in A$ yields:

$$Me(g_2, g_2)^{-cf} \tag{21}$$

As a result, the decryption will fail with very high probability. For the security proof of our proposed scheme, we will use five security games defined as follows:

1. $Game_{real}$ is a real security game as definition 1.
2. $Game_0$ is like $Game_{real}$ but the challenger returns SFC CT_{sf,A^*} for challenge phase.
3. $Game_{k,1}$ is like $Game_0$ but the $i-th$ secret key query in phase 1 or phase 2. The challenger returns as SK_{sf_2,x_i} if $i < k, SK_{sf_1,X_i}$ if $i = k$; otherwise it returns SK_{X1}
4. $Game_{k,2}$ is like $Game_0$ but for $i - th$ secret key query phase the challenger returns $SK_{sf2,Xi}$ if $i \leq k$; otherwise, it returns a normal key SK_{X_i}.
5. $Game_{final}$ is like $Game_{2q,2}$ where it returns SK_{sf2}. Except element C' in A^*, C_{sf,A^*} is a random element from G_T.

Hence, any PPT algorithm cannot distinguish between $Game_{real}$ and $Game_{final}$ as $Game_{real} \approx Game_0$ in Lemma 1, $Game_{k,1} \approx Game_{k-1,2}$ in Lemma 2, $Game_{k-1,2} \approx Game_{k,2}$ in Lemma 3, and $Game_{2q,2} \approx Game_{final}$ in Lemma 4.

Lemma 1. If $|Adv_{Game^A_{real}} - Adv^A_{Game_0}| \in \varepsilon$ for algorithm A exists; we can make an algorithm B with advantage which breaks Assumption 1. Proof. First, B is a challenger in our indistinguishable game. $D = (BLGD, Y_1, g_3)$ and T are given by Assumption 1. Started by the setup phase, B sets $g = Y_1$ and starts by setup algorithm to produces P_K as $P_K = \left\{BLG, g, g^s, g^{l_0}, \ldots, g^{l_n}, g^{k_0}, \ldots\ldots, g^{k_n}, e(g,g)^{\gamma}\right\}$. B sends P_K to an adversary A, while the private (γ, g_3) are kept secret.

Secondly, the game start key generation round which have two phases and B will reply to all secret key queries from A as it knows (γ, g_3).

Challenge phase, when B receives M_0, M_1, A^* from A, algorithm B flips a binary coin b, and randomly chooses r'_y for $\forall y \in p$ where p is all leaf nodes in $A*$. B then starts calculating secret sharing: Secret Share (Root, 1) Root of challenger $A*$, and λ'_y is a secret share for $y \in P$, so B sets the challenge ciphertext:

$$CT_{A^*} = \left\{A^*, C = M_b e(g,T)^{\gamma}, C_1 = T, \right. \\ \left. C_y = T^{s\lambda'_y} (T^{satt(y)} \prod_{i=1}^{n} T^{k_i \Delta_{i,Q}(att(y))})^{r'_y}, D_y = T^{r'_y}\right\} \tag{22}$$

Finally guess phase, where A generates b' as a guess for B, then uses $b' = b$ to break Assumption 1. If $b' = b$, algorithm B guesses $T = T_1$; otherwise, $T = T_2$.

Analyzing the game, if $T = G_{p1}$, B computes $T = g^{d_{swi}}$ and calculates $r_y = d_{sw_i} r'_y$ and $\lambda_y = d_{sw_i} \lambda'_y$. Hence, the challenge ciphertext CT_{A^*} has the same distribution as a

normal one; by that, B simulates $Game_{real}$ perfectly. But when $T \in G_{p_1p_2}$, B computes $T \in g^{d_{sw_i}} g_2^c$ and implicitly yields $r_y = d_{sw_i} r'_y \ mod\ p_1$ and $\lambda_y = d_{sw_i}\lambda'_y \ mod\ p_1$. B also computes $\alpha_y = cr'_y$, $\mu_y = c\lambda'_y$, $b = s$, $q_0 = k_0 \ldots, q_n = k_n, I_0 = l_0, \ldots..I_n = l_n$ in $mod\ p_2$. Although we used r'_y,λ'_y, $s, k_0, \ldots, k_n$, and $l_0, \ldots, l_n$ their values in $mod\ p_2$ are not equal to their values in $mod\ p_1$. Notice that challenge ciphertext CT^*_A has the same distribution as SFC. By that, B perfectly simulates $Game_0$.

Lemma 2. If $|Adv^A_{Game_{real}} - Adv^A_{Game_0}| = \varepsilon$ for algorithm A exists, we can make an algorithm B by ε as advantage which breaks Assumption 2. Proof. The challenger B in the game is given $D(BLGD, Y_1, X_1X_2, Y_2Y_3, g_3)$ and T from Assumption 2.

Started by the setup phase, A sets $g = Y_1$, and randomly chooses $\gamma, s, k_0, \ldots, k_n, l_0, \ldots, l_n \leftarrow Z_N$, then defines two functions $K(X)$ and $L(X)$, and P_k as shown above. B gives P_k to the adversary A.

Secondly, the game start key generation round, there are two phases, phase 1, 2, with 3 cases where B answers $i-th$ key query for a set of X_i.

Case 1. When $i < k$, B answers the key query with SFK2. First, B chooses $u', r_1, r_2, r_{3,1}, \ldots, r_{3,n}, r_{4,1} \ldots, r_{4,n} \leftarrow Z_N$ randomly. Then, B computes SK_{X_i} using the following equation and sends it to A. In this case, B computes a SFK2 with $u = u'$ and $g_2^f = Y_2^{r_1}$:

$$SK_{x_i} = \{X_i, V = g^{\gamma} g^{su'} (Y_2Y_3)^{r_1}, W = g^{u'} X_3^{r_2}, \{V_j = K(x_j)^w g_3^{r_{3,j}}, W_j = L(X_j)^{u'} X_3^{r_{4,j}}\}_{j=1,\ldots n}\} \tag{23}$$

Case 2. When $i > k$, B answers key query for attributes X_i with normal key SK_{X_i} as B knows (γ, g_3).

Case 3. When $i = k$, B takes T from assumption 2 to answer key query for a set of attributes X_i using:

$$SK_{X_k} = \{X_k, V = g^{\gamma} T^s, W = T, \{V_j = T^{\gamma x_j} \prod_{i=0}^{n} T^{K_i \Delta_{i,q}(x_j)}, W_j = T^{s\Delta_{i,Q}(x_j)_j} \prod_{i=0}^{n} T^{l_i \Delta_{i,Q}(x)}\}_{j=1,\ldots n}\} \tag{24}$$

Challenge phase, when B receives $M_0, M_1, A*$ from A, B flips a binary coin b and chooses randomly r'_y for $\forall y \in p$, B starts secret sharing (Root, a). B challenge ciphertext:

$$CT_{A^*} = \{A^*, C = M_b e(g, X_1X_2)^{\gamma}, C_1 = X_1X_2, C_y = (X_1X_2)^{\lambda'_y} ((X_1X_2)^{satt(y)} * \prod_{i=0}^{n} (X_1X_2)^{K_i \Delta_{i,Q}(att(y))})^{r'_y}, D_y = (X_1X_2)^{r'_y}\} \tag{25}$$

where λ'_y is a secret share. This challenge ciphertext has distribution similar to a semi-functional one $C_{sw_{sf}}$. The Algorithm B puts $X_1X_2 = g^{d_{sw_i}} g_2^c$ and sets $r_y = dr'_y \ mod p_1$, $\lambda_y = ds^{-1}\lambda'_y \ mod p_1$, $\alpha_y = cr'_y \ mod p_2$, and $\mu_y = c\lambda'_y \ mod p_2$. Note that B also computes $b = s \ mod p_2, q_0 = k_0 \ldots, q_n = k_n$, and $I_0 = l_0, \ldots I_n = l_n$ all in $mod p_2$.

Finally guess phase, A outputs b' as a guess for b. Algorithm B makes $b' = b$ to break Assumption 2. Analyzing the game: by $T \in G$, so B puts $T = g^u g_2^h R'$ and computes parameters from G_{p_3}:

$$R = (R')^s, R_j = (R')^{sx_i + \sum_{i=1}^{n} k_i \Delta_{i,Q}(x_j)}, R'_j = (R')^{s, \Delta_{i,Q} + \sum_{i=1}^{n} l_i \Delta_{i,Q}(x_j)} \tag{26}$$

B computes $f = hs \ mod\ p_2$, $b = s \ mod\ p_2$, $q_0 = k_0 \ldots, q_n = k_n$, and $r_0 = w_0, \ldots r_n = w_n$ where $T \in G_{p_1p_2}$, and puts $T \in g^u R'$. In same manner, B finds $k-th$ secret key SK_{X_k} with the same distribution as a normal secret key. Hence, B perfectly simulates $Game_{k-1,2}$. B can't perform the test if SK_X is a semifunctional secret key 1 ($T \in G$) or a normal key ($T \in G_{p_1p_2}$) where both can decrypt the SFC,C_{sf,A^*} where $A*$ is the access structure that satisfied attributes X_k. When C_{sf,A^*} decrypted by the nominal SFS1, so B can reveal c (the secret share in G_p2) since $f = bh$. Therefore, the proof is completed.

Lemma 3. If a polynomial time $AlgorithmA$ exists with a property $|Adv_{Game(k,1))^A} - Adv_{Game(k,2))^A}| = \varepsilon$, $AlgorithmB$ can be built with advantage ε for breaking Assumption 2.

Proof. Same process to the previous proof for Lemma 2 except when A makes $k-th$ query, B answers the query with $K\ SK_{X_k}$.

$$SK_{X_k} = \{X_k, V = g^{\gamma} T^s (Y_2Y_3)^o, W = T, \{V_j = T^{sx_j} \prod_{i=0}^{n} T^{L_i \Delta_{i,Q}(x_j)}, W_j = T^{s\Delta_{i,Q}(x_j)} \prod_{i=0}^{n} T^{l_i \Delta_{i,Q}(x_j)}\}_{j=1,\ldots,n}\} \tag{27}$$

Where oZ_N is selected randomly. When TG, B calculates $T = g^u g_2^h R'$, and computes:

$$g_2^f = g_2^{hs} Y_2^o, R = (R')^s Y_3^o, \{R_j\}_{j=1,\ldots,n}, and \{R'_j\}_{j=1,\ldots,n} \tag{28}$$

$$R_3 = (R')^s, R = (R')^{sx_i + \sum_{i=1}^{n} K_i \Delta_{i,Q}(x_j)}, R'_j = (R')^{s_{i,Q} + \sum_{i=1}^{n} l_i \Delta_{i,Q})(x_j)} \tag{29}$$

For all $\{V_j, W_j\}_{j=1,\ldots,n}$, they have an element from G_{P_2} with distribution similar to SFS1. Hence, $AlgorithmB$ gets with

a SFS1 for SK_{x_k}. By this, *AlgorithmB* simulates $Game_{k,1}$ perfectly. Hence, when $T \in G_{p_1p3}$, B puts $T = g^u R'$ and $g_2^f = Y_2^o$. Note that only K in SK_{x_k} is having elements from G_{p_2} and G_{p_1} for some elements in SK_{X_k} which has same distribution as normal secret key. Also, B replies with the $k-th$ key query with a SFS2. Hence, Algorithm B simulates $Game_{k,2}$ in perfect way. *AlgorithmB* can't make a self-testing to know if SK_{X_k} is a SFS1 or 2 as both cases preventing the decryption. When SK_{X_k} is a SFS1, it is a non-nominal since it has un-cancelable part Y_2^o in V. When $K_{SK_{X_k}}$ is a SFS2 the decryption will fail.

Lemma 4. If a polynomial time *AlgorithmA* found with a property $|Adv_{Game^A_{2q,2}} - Adv_{Game^A_{final}}| = \varepsilon$; thus, build *AlgorithmB* with advantage ε to break Assumption 3. Proof. First, B takes $D = (BLG, Y_1, Y_1^\gamma X_2, g_3, Y_1^{d_{swi}} Y_2, Z_2)$ and T from Assumption 3. Starting by the setup phase, B puts $g = Y_1$, chooses $s, k_0, ..., k_n, l_0, ..., l_n \leftarrow Z_N$ randomly, and calculates $K(X)$ and $L(X)$ as follows:

$$K(x) = g^{sx} \prod_{i=0}^{n} g^{k_i \Delta_{i,Q}(x)} \tag{30}$$

$$L(x) = g^{s\Delta_{0,Q}(x)} \prod_{i=1}^{n} g^{l_i \Delta_{i,Q}(x)} \tag{31}$$

B makes the public parameters P_K as follows:

$$P_k = \left\{BLG, g, g^s, g^{k_0}, ..., g^{k_n}, g^{l_1}, ..., g^{l_n}, e(g, Y_1^\gamma X_2)\right\} \tag{32}$$

Secondly, the game start key generation round, B answers all secret key queries with SFS2. For each query, B chooses $o, t', r_1, r_2, r_{3,1}, ..., r_{3,n}, r_{4,1}, ..., r_{4,n} \leftarrow Z_N$ randomly, and computes SK_{X_i} as follows:

$$\begin{aligned} &SK_{x_k} = \\ &\{X_i, V = (Y_1^\gamma X_2) g^{su'} Z_2^o X_3^{r_1}, W = g^{u'} g_3^{r_2}, \\ &\{V_j = K(X_j)^{u'} g_3^{r_{3,j}}, W_j = L(x_j)^{t'} g_3^{r_{4,j}} \\ &\}_{j=1,...,n}, \} \end{aligned} \tag{33}$$

B computes $g_2^f = X_2 Z_2{}^o$, where SK_{X_i} and SFS2 has similar distribution.

Challenge phase, B receives $(M_0, M_1, A*)$ from A, B flips a binary coin b and chooses r_y' for $\forall y \in P$ in a random way where P is leaf nodes in A^*. B computes secret sharing λ_y' for $\forall y \in P$ for access structure A^*. B calculates the challenge ciphertext as:

$$\begin{aligned} &CT_{A^*} = \\ &\{A^*, C = M_b T, C_1 = X_1 X_2, \\ &\{C_y = Y_1^{d_{swi}} Y2^{s\lambda_y'} ((Y_1^s Y_2)^{satt(y)} \\ &* \prod_{i=0}^{n} (Y_1^{d_{swi}} Y_2)^{k_i \Delta_{i,Q}(att(y))})^{r_y'}, D_y (Y_1^{d_{swi}} Y_2)^{r_y'}\}\} \end{aligned} \tag{34}$$

B computes $X_1 X_2 = g^{d_{swi}} g_2^c$ and puts $r_y = dr_y'\ mod\ p_1$, $\mu_y = d_{swi} \lambda_y'\ mod\ p_1$, $b = s\ mod\ p_2$, $q_0 = k_0, ..., q_n = k_n, I_0 = l_0, ..., I_n = l_n, \alpha_y = cr_y' \text{mod} p_2$, and $\mu_y = c\lambda_y'$.

Finally guess phase, A generates b' as a guess for b and uses $b' = b$ to break Assumption 3. As shown, when $T = e(g,g)^{\gamma d_{swi}}$, CT_A^* and SFC has similar distribution. Hence, *AlgorithmB* simulates $Game_{2q,1}$ perfectly. B simulates $Game_{Final}$ perfectly and our proof is completed.
Theorem 1. CP-ABE algorithm is secure if Assumption 1, 2 and 3 hold.
Proof. If Assumption 1 and 2 hold, then $Game_{real}$ is indistinguishable with $Game_{2q,2}$ by Lemma 1,2 and 3. $Game_{2q,2}$ is assumed to be indistinguishable with $Game_{final}$ if Assumption 3 holds. Hence, advantage of $Game_{real}$ is assumed to be negligible for breaking our CP-ABE scheme.

6. PERFORMANCE ANALYSIS

The performance of the proposed scheme is compared with various CP-ABE access structures in Table I . The memory requirement is represented by ciphertext length $|CT|$ and secret key length $|SK|$. Where X is the set of attributes, Y is polynomial time algorithm, n is attribute universe, $|M|$ is the message length, G_c and G_{Tc} are the composite order of pairing groups, $O(P)$ is the order of the base point that is assumed to be 160-bit integer in Z_p. In the proposed scheme, it doesn't depend on the size of attributes as the other scheme which allows large attribute universe in the proposed scheme. Additionally, it doesn't depend on the number of employees in the organization; hence, scalability is achieved in the proposed scheme. The scheme in [50] works better with shorter secret keys with an expressive AND gate access structure. The scheme in [41] provides variant secret keys size for the users which is not suitable for mobile device deployment.

7. CONCLUSION

Organizations may need to make a document about their budget activities; bitcoin offers transparency as most of signed distributed ledger or blockchain solution by providing information about balances in which all transactions saved on blockchain. A CP-ABE access control scheme has been proposed in this study. Organizations can manage their wallet access based on their policies. In addition, a smooth way has been provided for organizations to handle bitcoin requests based on team's or project's budget. We have presented superwallet-subwallet for a fully using And, OR, and threshold gates for large attributes space. By dividing the organization's wallet into subwallets, if the organization loses for any reason a part of its wallet, it won't affect other parts. We have used bilinear decisional Diffie-Hellman problem for our security proof. We have also proved that any polynomial time attacker cannot distinguish the distribution in a real game and in a final game. Finally, the challenger receives a SFK2 version of secret key or ciphertext; hence, the challenger cannot decrypt the challenge ciphertext using the queried secret key even though he has the secret key which satisfies the challenge access

structure. These advantages exhibit the high-level security provided by the proposed scheme which make it convenient for implementation in organizations' bitcoin wallet access.

References

[1] A. Rejeb, K. Rejeb, and J. G. Keogh, "Centralized vs. decentralized ledgers in the money supply process: a SWOT analysis," *Quantitative Finance and Economics*, vol. 5, no. 1, pp. 40–66, 2021.

[2] D. He, K. F. Habermeier, R. B. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, T. S. Sedik, N. Stetsenko *et al.*, *Virtual currencies and beyond: initial considerations*. International Monetary Fund, 2016.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[4] https://www.lucidchart.com/blog/types-of-organizational-structures#team-based, Accessed March 2022.

[5] M. E. Smid and D. K. Branstad, "Response to comments on the NIST proposed digital signature standard," in *Annual International Cryptology Conference*. Springer, 1992, pp. 76–88.

[6] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, pp. 1–32, 2015.

[7] I. D. Rubasinghe and T. De Zoysa, "Transaction verification model over double spending for peer-to-peer digital currency transactions based on blockchain architecture," *International Journal of Computer Applications*, vol. 975, p. 8887, 2012.

[8] https://en.bitcoin.it/wiki/Transaction, Accessed March 2022.

[9] J. Mayan, T. Latha, and K. Sinha, "Security analysis of three factor authentication schemes for banking," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 8, pp. 3504–3509, 2015.

[10] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390–1397, 2010.

[11] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll, E. W. Felten, and A. Narayanan, "Securing bitcoin wallets via a new DSA/ECDSA threshold signature scheme," 2015.

[12] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[13] P. Dikshit and K. Singh, "Efficient weighted threshold ECDSA for securing bitcoin wallet," in *2017 ISEA Asia Security and Privacy (ISEASP)*. IEEE, 2017, pp. 1–9.

[14] K. Ohta and T. Okamoto, "Multi-signature schemes secure against active insider attacks," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 82, no. 1, pp. 21–31, 1999.

[15] G. Andresen, "Bitcoin improvement proposal 11: M-of n standard transactions," https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki, Last accessed: March 2022.

[16] K. Ohta and T. Okamoto, "A digital multisignature scheme based on the fiat-shamir scheme," in *International Conference on the Theory and Application of Cryptology*. Springer, 1991, pp. 139–148.

[17] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple schnorr multi-signatures with applications to bitcoin," *Designs, Codes and Cryptography*, vol. 87, no. 9, pp. 2139–2164, 2019.

[18] O. A. Dawood, O. Hammadi, and F. Mohammed, "Secure symmetric block cipher design for encrypting the bitcoin wallets in cryptocurrencies applications," *Journal of Computer Science*, vol. 15, no. 5, pp. 758–768, 2019.

[19] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," *arXiv preprint arXiv:1802.04351*, 2018.

[20] S. M. Mahgoub, F. M. Salem, and I. I. Ibrahim, "An efficient organizations' bitcoin wallet signature scheme," in *International Conference on Advanced Intelligent Systems and Informatics*. Springer, 2019, pp. 194–203.

[21] S. Kaushik, A. Tomar, and Poonam, "Access control list implementation in a private network," *International Journal of Information & Computation Technology*, vol. 4, no. 14, pp. 1361–1366, 2014.

[22] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[23] R. S. Sandhu, "Role-based access control," in *Advances in Computers*. Elsevier, 1998, vol. 46, pp. 237–286.

[24] C. Bellettini, E. Bertino, and E. Ferrari, "Role based access control models," *Information Security Technical Report*, vol. 2, no. 6, pp. 21–29, 2001.

[25] J. P. Cruz and Y. Kaji, "Trans-organizational role-based access control in android: Secure mechanism for verifying user-role assignments of organizations," in *The Fourth International Conference on Advanced Communications and Computation (INFOCOMP)*, 2014, pp. 114–119.

[26] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 457–473.

[27] J.-J. Hwang, K.-C. Wu, and D.-R. Liu, "Access control with role attribute certificates," *Computer Standards & Interfaces*, vol. 22, no. 1, pp. 43–53, 2000.

[28] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Computers & Security*, vol. 30, no. 5, pp. 320–331, 2011.

[29] R. Mythili, R. Venkataraman, and T. Sai Raj, "An attribute-based lightweight cloud data access control using hypergraph structure," *The Journal of Supercomputing*, vol. 76, no. 8, pp. 6040–6064, 2020.

[30] D. Vadlamudi, S. Garlapati, Q. Syed, and K. Nunna, "Secure access control for cloud data using attribute based encryption schemes," *International Journal of Recent Technology and Engineering*, vol. 7, pp. 668–673, March 2019.

[31] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1526–1535, 2009.

TABLE I. Performance comparison

Ref.	Access Structure	$\|SK\|$	$\|CT\|$
[39]	AND gate-Multivalued	$(n+1)\|G\|$	$2G + G_T$
[40]	AND gate	$2G$	$3G + \|M\|$
[41]	Linear secret-sharing scheme	$(\|n\|+3)\|G_c\|$	$(2\|P\|+2)\|G_C\| + G_{Tc}$
[45]	Linear secret-sharing scheme	$(\|n\|+2)\|G\|$	$(2\|P\|+1)\|G\| + G_T$
[48]	AND gates	$2O(P)$	$(n-\|P\|+3)G + \|M\|$
[49]	AND±	$(n+1)G$	$2G + G_T$
[50]	AND gates	$2G$	$(n-\|P\|+2)G + G_T + \|M\|$
Ours	Full monotonic	$(2\|X\|+2)\|G\|$	$(2\|Y\|+1)\|G\| + \|G_T\|$

[32] H. Cui, R. H. Deng, and G. Wang, "An attribute-based framework for secure communications in vehicular ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 721–733, 2019.

[33] V. Goyal, A. Pandey, O and. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *13th ACM Conference on Computer and Communications Security, New York, NY, USA*. ACM, 2006, pp. 89–98.

[34] H. R. Hassen, A. Bouabdallah, H. Bettahar, and Y. Challal, "Key management for content access control in a hierarchy," *Computer Networks*, vol. 51, no. 11, pp. 3197–3219, 2007.

[35] C. Wang and J. Luo, "An efficient key-policy attribute-based encryption scheme with constant ciphertext length," *Hindawi Publishing Corporation Mathematical Problems in Engineering*, 2013, Article ID 810969.

[36] H. Yin, Y. Xiong, J. Zhang, L. Ou, S. Liao, and Z. Qin, "A key-policy searchable attribute-based encryption scheme for efficient keyword search and fine-grained access control over encrypted data," *Electronics*, no. 3, 2019.

[37] U. Hijawi, D. Unal, R. Hamila, A. Gastli, and O. Ellabban, "Performance evaluation of no-pairing ECC-based KPABE on IoT platforms," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 225–230.

[38] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 321–334.

[39] N. Doshi and D. C. Jinwala, "Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption," *Security and Communication Networks*, vol. 7, no. 11, p. 1988–2002, 2014.

[40] V. Odelu, A. K. Das, M. Khurram 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.

[41] B. W. A. Lewko, "New proof methods for attribute-based encryption: achieving full security through selective techniques," in *32nd International Conference on Cryptology (CRYPTO 2012)*. Springer, 2012, pp. 180–198.

[42] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in *14th ACM conference on Computer and communications security*. ACM, 2007, p. 456–465.

[43] O. P. V. Goyal, A. Jain and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *35th international colloquium on Automata, Languages and Programming*. Springer, 2008, p. 579–591.

[44] P. H. L. Ibraimi, Q. Tang and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," in *5th International Conference on Information Security Practice and Experience*. Springer, 2009, pp. 1–12.

[45] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *14th international conference on Practice and theory in public key cryptography conference on public key cryptography*. Springer, 2011, p. 53–70.

[46] W. S. D. X. K. R. Jin Li, Man Hu Au, "Attribute-based signature and its applications," in *5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10)*. ACM, 2010, pp. 60–69.

[47] T. Okamoto and K. Takashima, "Efficient attribute-based signatures for non-monotone predicates in the standard model," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 409–421, 2014.

[48] A. K. V.Odelu1, "Design of a new cp-abe with constant-size secret keys for lightweight devices using elliptic curve cryptography," *Security and Communication Networks*, vol. 9, no. 17, pp. 4048–4059, 2018.

[49] X. C. Y. Zhang, D. Zheng, "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in *8th International Conference on Provable Security (ProvSec 2014)*. Springer, 2014, p. 259–273.

[50] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "Cp-abe with constant-size keys for lightweight devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763–771, 2014.

[51] T. V. X. Phuong, G. Yang, and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 35–45, 2016.

[52] K. R. N. Helil, "CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy," *Security and Communication Networks*, vol. 2017, 2017.

[53] F. Khan, H. Li, L. Zhang, and J. Shen, "An expressive hidden access policy CP-ABE," in *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, 2017, pp. 178–186.

[54] G. Bramm, M. Gall, and J. Schutte, "BDABE - blockchain-based distributed attribute based encryption," in *ICETE*, 2018, pp. 99–110.

[55] J. Paul and K. Yuichi, "The bitcoin network as platform for trans-organizational attribute authentication," *IPSJ SIG Notes*, vol. 2015, no. 12, pp. 1–6, 2015.

[56] B. X. S. E. Barber, Simon and E. Uzun, "Bitter to better — how to make bitcoin a better currency," in *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2012, pp. 399–414.

[57] M. Srivatsa and L. Liu, "Key derivation algorithms for monotone access structures in cryptographic file systems," in *Computer Security – ESORICS 2006*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 347–361.

[58] A. S. R. Ostrovsky and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *14th ACM Conference on Computer and Communications Security*. ACM, 2007, pp. 195–203.

[59] B. Waters, "Dual system encryption: realizing fully secure ibe and hibe under simple assumptions," in *29th Annual International Cryptology Conference on Advances in Cryptology*. Springer, 2009, p. 619–636.

Fatty M. Salem received her B.Sc. degree in Electronics, Communications and Computers Engineering from Helwan University, Cairo, Egypt, in 2007. She received her M.Sc. and PhD degree in network security from Helwan University, in 2010 and 2014 respectively. Currently, she is an Associate Professor in the department of Electronics and Communications, Faculty of Engineering, Helwan University, Egypt. Her research interests include authentication, privacy, access control, applied cryptography, blockchain, bitcoins, and mobile security.

Shereen M. Mahgoub received her B.Sc. degree in Electronics, Communications, and Computers Engineering from Helwan University, Cairo, Egypt, in 2007. She received her M.Sc. degree in network security from Helwan University, in 2013. She is currently pursuing the Ph.D. degree in cryptography and network security with Helwan University, Cairo, Egypt. She is now a network engineer in Egyptian Radio Television Union. Her research interests include authentication, digital signature, access control, blockchain, and bitcoins.

I. I. Ibrahim Received his B.Sc. degree with honor in communications engineering from Helwan University, Cairo, Egypt, in 1976. He received his M.Sc. in communications from Cairo University, Cairo, Egypt in 1983 and PhD in communications from Queen University, Belfast, UK in 1987. He is a professor of wireless communications with the Faculty of Engineering, Helwan University. His current research interests include wireless communications, Internet of Things, device-to-device communications, and network security.