International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.323-336
http://dx.doi.org/10.14257/ijsia.2015.9.8.29

Multi-domain Security Authentication Protocol for Hybrid Cloud

Zhang Qikun[1], Zhang Lei[2], Gan Yong[1], Duan zhaolei[1] and Zheng Jun[3]

1(Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)
2(Shengda Trade Economics & Management College of Zhengzhou, Zhengzhou 451191, China)
3(School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China)
zhangqikun04@163.com

Abstract

In recent years, with the high-speed development of cloud computing and its universal application, the cloud security technology is more and more important. In cloud computing, it is mainly through the resource sharing and collaborative action to meet the demand for an unlimited access speed, unlimited storage space and a reliable resource protection for users. For the secure access resources among different domains in cloud network, today most Cloud Computing Systems provide data security and mutual authentication with asymmetric and traditional public key cryptography. For these researches, the authentication process is cumbersome, and the certificate management is complex, which would bring some inconvenience for mutual authentication among servers or users in a Hybrid Cloud. This paper provides a security authentication protocol among multiple domains. It adopts the direct product decomposition and linear mapping technology of cyclic group to achieve mutual authentication between members in multi-domain systems or heterogeneous networks. Extensive security and performance analysis show that the proposed schemes have the advantages of in security, computation consumption and Communication consumption. It is suitable for safety authentication in large-scale Cloud computing environment.

Keywords: *multi-domain authentication; direct product decomposition; bilinear mapping; cloud computing*

1. Introduction

Cloud computing is a new mode of calculation. It is the development of distributed computing, parallel computing and the grid computing. Cloud computing has achieved two important goals of distributed computing, scalability and high availability. The Inter-Cloud [1] is instead a new perspective of cloud computing where clouds cooperate with other federated ones with the purpose to enlarge their computing and storage capabilities. There are mainly three types of clouds: private clouds, public clouds and hybrid clouds [2]. Private clouds, also called internal clouds, are the private networks that offer cloud computing services for a very restrictive set of users within internal network. Compared with a hybrid cloud, it is easy to assure the security of a private cloud or a public cloud, because both of them only have one service provider in the cloud. While there are multiple service providers in a hybrid cloud, it is much more difficult to assure its security for key distribution and mutual authentication. Also for users to access the services in a cloud, a user digital identity is needed for the servers of the cloud to manage the access control. While there are many different kinds of clouds

ISSN: 1738-9976 IJSIA

and each of them has its own identity management system in the whole cloud, therefore users who want to access services from different clouds need multiple digital identities in different clouds, which would bring inconvenience for users. With the multi-authentication, each user would have its unique digital identity and can access different services from different clouds with its identity. There are considerable technologies and protocols proposed to address similar issue [3, 4]. However, the existing technologies are not being developed for the dynamic and multi-party collaborations in the cloud-based environment, where service owners have no control of the underlying cloud infrastructures. Although there are many difficulties faced by researches, it is well believed that supporting multi-authentication would be critical important to the practical application of cloud security in homogeneous cloud or heterogeneous cloud environment.

In the environment of private cloud, the sensitive data must be protected by servers in cloud computing environment, all the servers can be accessed through internal connections rather than public internet connections, which make it easier to use existing security measures and standards. While in a hybrid cloud, it includes more than one domain, which will increase the difficulty of security provision, especially key management and mutual authentication. The domains in a hybrid cloud can be heterogeneous networks, hence there may be gaps among these networks that the different services providers. Though security can be well guaranteed in each private/public cloud, in a hybrid cloud with more than one kind of clouds that have different kinds of network conditions and different security policies, how to provide efficient security protection is much more difficult. For example, cross-domain authentication can be a problem in a hybrid cloud with different domains. Although some authentication services, such as Kerberos [5], can provide multi-domain authentication, the scheme is related with the complexity of symmetric key management and key consultations. If there are N Kerberos domains and each of them want to trust each other, the number of key exchanges is N(N-1)/2, and it cannot deal with the anonymous problem effectively. Reference [6-8] introduced the use of lattice theory in cross-domain authentication, each of them used lattice to the construction of the network structure, which provided a better solution to the potential safety problems caused by the authentication from an independent privileged body and the problem of network bottlenecks and single point crash in PKI authentication framework.

Reference [9] summarized the existing technologies of certification in grid environment, such as PKI in grid authentication infrastructure, the model of user privacy protection and role-based private authentication protocol. However, each of them was just for one problem in multi-domain authentication, they only solved the privacy of user's identity or the authentication mechanism, without considering all the factors as a whole, although, there are also problems of the difficulties in PKI certificate management and maintenance, the complexity of authentication path finding and the low utilization of network resources. Reference [10] has purposed an identity-based multi-domain authentication model, which the premise is that all the authorities must be mutual trust. Also, the scheme requires the key parameters of all domains to be same. It could not avoid the authority faking the members to cross-domain access resources. Reference [11,12] adopt signcryption method to implement mutual authentication between entities ,but it is only suitable for a single domain. Reference [13] extends the method, it enable the mutual authenticate of entities in multi domains, but the precondition of this scheme assumes that Private Key Generator (PKG) of each domain is honest. Because the PKG has the private keys of all the members within its domain, if PKG is malicious, the security of the users' private keys could not be guaranteed. At present, in the mutual authentication protocol, SSL/TLS authentication protocol (SAP) is the most popular protocol and has become standard protocol to

ensure Web security. Reference [14] propose two authentication schemes that support keyboard as well as graphical mouse-based input that map password characters to other regions of the password space. This shields the user's password from being known to the adversary thus deflecting shoulder-surfing and spyware attacks. Reference [15] presents a multi layer perceptron neural network-based method for network traffic identification.

Reference [16] assumes that all the entities in the network trust an authority agency, and this is not real, for in this condition the problems of bottleneck and the one point failure are too also heavy. Reference [17] presents a way to find the target trust center through a trust link. If the trust link is too long, the affection of cross-domain authentication will be too low. The issues with cross-domain authentication have been discussed in many papers. For example, both direct cross-domain authentication and transitive cross-domain authentication are supported in Kerberos [18-19]. By using transitive cross-domain authentication, a principal can access the resources in a remote domain by traversing multiple intermediate domains if there is no cross-domain key shared with the remote domain.

In this paper, we propose an efficient multi-authentication protocol for servers in the homogeneous cloud or heterogeneous cloud. Our contribution can be summarized as follows:

1) We have designed an authentication model for hybrid cloud network.
2) We have proposed a multi-authentication protocol among the cloud alliance system based on authentication model.
3) We have proved the security of our proposed protocol and justify the performance of our scheme through concrete implementation and comparisons with some similar schemes.

2. Basic Theory

2.1. Bilinear Group

The definition of bilinear map, if G_1 is an addition group, G_2 is multiplicative group and discrete logarithm problem of G_1 and G_2 is difficult.

Set G_1 and G_2 is a pair of bilinear group, $G_1 = \langle g_1 \rangle$ is generated by g_1, and $G_2 = \langle g_2 \rangle$ is generated by g_2. G_3 is a cyclic group. G_1, G_2 and G_3 are the same large order prime p, e is the mapping that can be calculated, $e: G_1 \times G_2 \to G_3$.

Nature1: bilinear, for all $u \in G_1$, $v \in G_2$ and $a, b \in Z$, there is $e(u^a, v^b) = e(u, v)^{ab}$.

Nature 2: Not degenerative, i.e. $e(g_1, g_2) \neq 1$

Definition1: For given groups G_1, G_2 and G_3, and g_1 is a generator of G_1, and g_2 is a generator of G_2. For the above definition we can define the following the difficult solution problems [13].

Discrete logarithm problem: set $g_1, g_1' \in G_1$, look for an integer a and make it to meet $g_1' = g_1^a$.

① Computational Diffe-Hellman problem (CDHP) Suppose a triad $(g_1, g_1^a, g_1^b) \in G_1$, for all $a, b \in Z_p$, find the element g_1^{ab}.

② Decisional Diffe-Hellman problem (DDHP): Suppose a quad $(g_1, g_1^a, g_1^b, g_1^c) \in G_1$, for all $a, b, c \in Z_p$, decides that is there $c = ab \bmod p$.

③ GapDiffe-Hellman group(GDH): The problem of CDH is difficult to solute but the problem of DDH is easy. With this feature group called for the GDH group.

2.2. Multi-linear Mapping

Multi-linear Diffie-hellman hypothesis: Firstly given the definition of multi-linear mapping[14]. Suppose that G_1 is a additive group, G_2 is a multiplicative group and the discrete logarithm problem of G_1 and G_2 is hard.

Definition 2: The mapping $e_1 : G_1^m \to G_2$ is called m multi-linear mapping, If it can meet the following properties:

(1) (1) G_1 and G_2 have the same primes order p ;

(2) For any of $a_1, a_2, ...a_m \in Z$ and any of $g_1, g_2, ...g_m \in G_1$, there is $e_1(a_1 g_1, a_2 g_2, ...a_m g_m) = e_1(g_1, g_2, ...g_m)^{a_1 a_2 ... a_m}$.

(3) The mapping e_1 is not degrading. If $g \in G_1$ is a generator of G_1 , $e_1(g, g, ...g)$ is also a generator of G_2.

Definition 3: Decisional multi-linear Diffie-Hellman problem (DMDH) is that given $e_1(g, a_1 g, a_2 g, ...a_{m+1} g)$ and $\forall z \in G_2$, it is to determine if there is $e_1(g, g, ...g)^{a_1 a_2 ... a_{m+1}}$.

Definition 4: Hypothesis of decisional multi-linear diffie-hellman is that solving decisional multi-linear diffie-hellman problem is difficult. That is to say that there cannot be a probability polynomial time algorithm which can solve Diffie-Hellman problem.

3. Problem Statement

The network architecture for hybrid cloud federation is illustrated in Fig. 1. There are some clouds composed a hybrid cloud federation and each cloud can be one of the three types of clouds: private clouds, public clouds and hybrid clouds.

Definition 5: we define single local cloud as a Cloud End, such as Cloud End A, Cloud End B and Cloud End C are Cloud Ends in Fig. 2.

Definition 6: we define one or more Cloud Computation Servers with its Clients as a domain.

Three different network entities in each Cloud End can be identified as follows:

1) Client(u_i): an entity, who need large data files from the cloud or relies on the cloud for data maintenance and computation, can be either individual consumers or organizations;
2) Cloud Computation Server (CCS): an entity, which is managed by Cloud Server Provider (CSP), has significant storage space and computation resource to maintain the clients' data, provides entities tracing services for the verifier that be accessed by the certifiers who have registered in the CCS;
3) Key Generation Center (KGC): an entity, which takes charge of generation and management the keys of Cloud End, may be provided by Third Party Auditor, is trusted to trace illegal entities to access resource on behalf of the rightful entities upon request, and provides entities tracing services for the verifier that be accessed by the certifiers who have registered in the KMC.

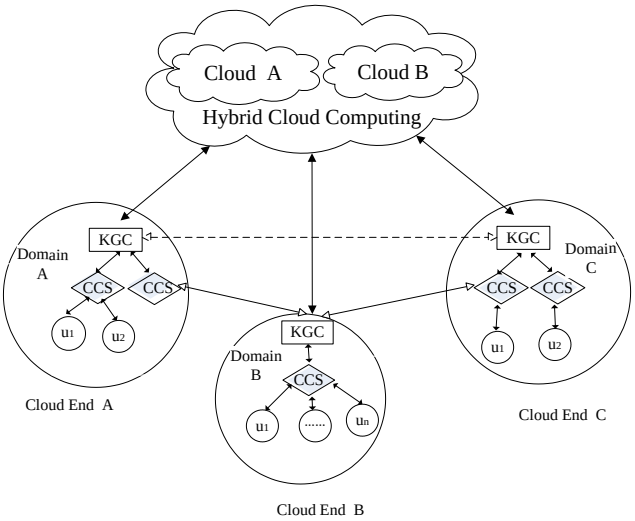

Figure 1. Network Architecture for Cloud Federation

In the federal cloud paradigm, each Cloud End is a tree-based model that is composed of only one KGC, some of CCSs and Clients. The KGC denotes a root node of the tree, and the CCSs denote the branch nodes of the tree, and the Clients denote the leaves nodes of the tree. Each branch of the tree can be a domain including some clients and CCSs, and each Cloud End is composed of some of domains. The Cloud End architecture is illustrated in Figure 2.

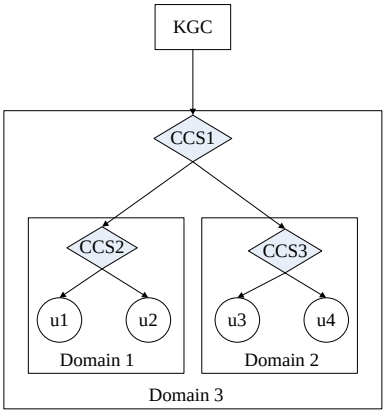

Figure 2. The Cloud End architecture

The root node KGC of a tree in each Cloud End manages the keys of whole entities in the Cloud End. The branch nodes CCSs ensure the security of its children in the domains with the help of the root. The security includes authentication, authorization, tracing entity, storage space, computation resource, access control et al. All the entities can share resources in the same Cloud End or in different Cloud Ends, if they have passed mutual authentication. In other words, a Client can share another Client's data cross domains or cross Cloud Ends.

4. The Multi-authentication for Hybrid Cloud

The number of cloud customers is large, and they are distributed widely. Once the data in cloud is under attack or tampered, the loss is inestimable; therefore, cloud security is particularly important. When a cloud is providing resources, it requires the

collaborative computing of multiple fields' servers, or a group of resource servers in a domain to mutual cooperate to accomplish. When a cloud access resources to cross other clouds or clouds access resources to each other, it needs authentication by certification to ensure safety, and this form cloud union certification. Each resource servers provides resources as individual form or groups form to participate. When it provides or access the resources as a group, the branch node can provide a unified the authentication or identity for their sub trees. When numbers in a group access resources to each other, it uses individual authentication. In the tree structure of the cloud network resources, each branch of the tree can be considered as a cloud of cloud union. Each of the root nodes of sub trees can be as an authentication interface for their children resources; the node is in charge of the key management.

4.1. The Key Generation of Nodes

The access authentication mechanism of cloud resources is built on the cryptosystem, this paper establish a flexible authentication system which can provide authentication by individuals or groups at any time. Groups or individuals can easily calculate that whether the access which is from external is legal entity.

Each entity has five keys, they are the private key, public key, blind key and path key and registration key. Establish the system parameters:

Set G_1 is a addition group, the generator is g_1, G_2 is a multiplicative group. They are with the same oder large prime q, $e_1 : G_1^m \to G_2$ is a Computational multi-linear mapping which is from G_1 to G_2, $h : \{0,1\}^* \to Z_p$ is a hash function and system parameters is (G_2, G_1, g_1, q).

The paper takes m binary tree as a example, each node of the tree is represented by $N_{<l,d>}$ (l represents the l th layer, d represents the d th node in a layer). Each node has a private key and corresponding public key, blind key and path keys. The private key of the node $N_{<l,d>}$ is $K_{<l,d>}$, corresponding public key is $P_{<l,d>} = K_{<l,d>} g_1$, and its' path key is $S_{<l,d>}$ and corresponding blind key is $BS_{<l,d>} = f(S_{<l,d>})$, $f(S_{<l,d>}) = S_{<l,d>} g_1$. Summary of keys in Table 1.

Table 1. Summary of Keys

Key	Description	Usage
$K_{<l,d>}$	the l-th layer and the d-th node's private key.	Encryption
$P_{<l,d>}$	the l-th layer and the d-th node's public key.	Verify the signature of the entity.
$S_{<l,d>}$	the l-th layer and the d-th node's path key.	Creation the entity's blind key.
$BS_{<l,d>}$	the l-th layer and the d-th node's blind key.	Verify the signature of the entity.
$R_{<l,d>}$	the l-th layer and the d-th node's register key.	For entity tracking.

Except the leaf nodes do not have path keys, the rest of the nodes' path key can calculate as follows:

Lemma1: Any non-leaf node's path key can be calculated by a child's path key and the rest of the children nodes' blind key. Proof:

For the m children of node $N_{<l,d>}$ that are the nodes $N_{<l+1,d>}$, $N_{<l+1,d+1>}$,....., $N_{<l+1,d+m>}$ and node $N_{<l+1,d>}$ uses the following formula to calculate its parent's path key and blind keys:

$$S_{<l,d>} = e_1(BS_{<l+1,d+1>}, BS_{<l+1,d+2>}, ..., BS_{<l+1,d+m-1>})^{S_{<l+1,d>}} = e_1(q,q,...,q)^{S_{<l+1,d>}S_{<l+1,d+2>}...S_{<l+1,d+m-1>}} \quad BS_{<l,d>} = S_{<l,d>}g_1$$

node $N_{<l+1,d+1>}$ uses the following formula to calculate its parent's path key and blind keys:

$$S_{<l,d>} = e_1(BS_{<l+1,d>}, BS_{<l+1,d+2>}, ..., BS_{<l+1,d+m-1>})^{S_{<l+1,d+1>}} = e_1(q,q,...,q)^{S_{<l+1,d>}S_{<l+1,d+2>}...S_{<l+1,d+m-1>}} \quad BS_{<l,d>} = S_{<l,d>}g_1$$

.....

node $N_{<l+1,d+m-1>}$ uses the following formula to calculate its parent's path key and blind keys:

$$S_{<l,d>} = e_1(BS_{<l+1,d>}, BS_{<l+1,d+2>}, ..., BS_{<l+1,d+m-2>})^{S_{<l+1,d+m-1>}} = e_1(q,q,...,q)^{S_{<l+1,d>}S_{<l+1,d+2>}...S_{<l+1,d+m-1>}} \quad BS_{<l,d>} = S_{<l,d>}g_1$$

In the above expressions, if a child node is empty, then its corresponding blind key will be replaced by left child node's blind key of its father.

Leaf node does not have a child node, namely the groups of the node is itself, and it is only one entity. The members of $N<l,d>$ can calculate the path keys of all fathers and grandfathers from $S_{<l,d>}$ to $S_{<0,0>}$.

4.2. The Alliance Key Generation of the Hybrid Cloud System

Set the number of entities in alliance cloud is n, any entity of the alliance cloud $u_i(i=1,2,...,n)$ chooses the $r_i \in_R Z_P^*$ randomly, and calculates its private key $K_i = r_i \bmod q$ and its public key $P_{u_i} = K_i g_1$, then it publish its public key to others. All the leaf nodes v_j choose $r_j \in_R Z_P^*$ randomly, and calculate its path key $S_i = r_j \bmod q$ and publish its corresponding blind key $BS_i = S_i g_1$.

Any leaf node of all the branches node $N_{<l,d>}$ calculates the path key $S_{<l-1,d>}$ of its father node $N_{<l-1,d>}$ by the blind key of its brother and its own path key, and uses its father node's public key $P_{<l-1,d>}$ to encrypt and gives it to his father node $N_{<l-1,d>}$. The node $N_{<l-1,d>}$ decrypts it and gets its own path key $S_{<l-1,d>}$, and calculate its corresponding blind key $BS_{<l-1,d>}$, and publishes it. Then its father node $N_{<l-2,d>}$'s path key $S_{<l-2,d>}$ can be calculated with its own path key $S_{<l-1,d>}$ and its brother's blind keys, and uses its father's public key to encrypt $S_{<l-2,d>}$, then return it to his father, and so on, till to the root node $N_{<0,0>}$. Now all nodes have four keys: private key, public key, blind key, path keys. The blind key and public key of every node are open and private key and path key are confidential.

4.3. The Registration of Nodes

Except the root node in the cloud tree, the father node u_i of any node $u_j(1 \le j \le m)$ calculates $Y_i = (1/(K_i + S_i))g_1$ with its own private key K_i and path key S_i, and passes the result Y_i to its child node $u_j(1 \le j \le m)$. The child node u_j receives the message and

calculates its own registration key $R_j = K_j Y = (K_j / (K_i + S_i)) g_1$ $(1 \le j \le m)$,and pass register keys R_j and their public keys to their father u_i to register identities for entity tracking.

4.4. Multi-domain Authentication in Hybrid Cloud

In order to convenience and safety authentication in this huge cloud network, this paper designs an multi-domain authentication scheme which is suitable for two-way entities mutual authentication in the same domain, and also suitable for two-way entities mutual authentication from different domain in hybrid cloud network.

Lemma 2: Any of authorized members in cloud can compute blind key and path key of any node which is tend to the root node with its own key and blind key of the corresponding bypath and here the bypath means the nodes muster which consist of the brother nodes of path nodes. Proof:

Any node $N_{<l+1,d>}$ can calculate the blind keys and path keys of its ancestor's nodes $N_{<l,d>}$、$N_{<l-1,d>}$、.....、$N_{<1,1>}$ .proof as follows:

$$S_{<l,d>} = e_1(BS_{<l+1,d+1>}, BS_{<l+1,d+2>}, ..., BS_{<l+1,d+m-1>})^{S_{<l+1,d>}}$$

$$BS_{<l,d>} = S_{<l,d>} g_1$$

$$S_{<l-1,d>} = e_1(BS_{<l,d+1>}, BS_{<l,d+2>}, ..., BS_{<l,d+m-1>})^{S_{<l,d>}}$$

$$BS_{<l-1,d>} = S_{<l-1,d>} g_1$$

.....

$$S_{<1,1>} = e_1(BS_{<2,d+1>}, BS_{<2,d+2>}, ..., BS_{<2,d+m-1>})^{S_{<2,d>}}$$

$$BS_{<1,1>} = S_{<1,1>} g_1$$

In the above expressions, if a grandfather node $N_{<i,j>}$ of node $N_{<i-2,j>}$ is empty, its corresponding blind key will be replaced by left child node's blind key of the father node $N_{<i-1,j>}$ of the node $N_{<i-2,j>}$.

Each branch node in cloud tree can provide resource service and also can provide resources authentication for his sub tree. The whole cloud network is a resource system and is also a certification alliance.

Assume D_1 and D_2 are two nodes that in different domains, and D_1 want to access the resource from D_2. For security, D_1 need to provide its own identity to the verifier D_2 for authentication. Let the private key of D_1 is K_{D_1}, its public key is $P_{D_1} = K_{D_1} g_1$, its register key is R_{D_1}, its path key is S_{D_1}, the blind key and the public key of its father node are $BS_D = S_D g_1$ and $PS_D = K_D g_1$ respectively, and the blind key of the nearest common ancestor of D_1 and D_2 is $BS_{D_1D_2}$. The process of authentication is as follows:

(1) D_1 calculates the path key $S_{D_1D_2}$ of the common ancestor of D_1 and D_2 with its own path key and blind keys of the rest of the bypath nodes and calculates $Q_{D_1} = S_{D_1D_2} R_{D_1}$.

(2) D_1 Choose $x \in_R Z_P^*$ randomly and calculates $T_1 \leftarrow x g_1$.

$$D_1 \xrightarrow{P_{D_1}, Q_{D_1}, BS_D, PS_D, BS_{D_1D_2}, T_1} D_2$$

(3) D_2 verifies $e(Q_{D_1}, (BS_D + PS_D)) \stackrel{?}{=} e(BS_{D_1D_2}, P_{D_1})$, if their equal ,then chooses a message $mes \in \{0,1\}^*$ for signature and calculates the questioned value $c \leftarrow h(T_1, mes)$.

$$D_1 \xleftarrow{c} D_2$$

(4) D_1 calculates $b_1 \leftarrow x + cK_{D_1}$.

$$D_1 \xrightarrow{b_1} D_2$$

(5) D_2 verifies the signature.

$$b_1 g_1 \stackrel{?}{=} T_1 + cP_{D_1}$$

Receive effective verification, only if the establishment of the equation of the expression (3) and (5).

If it is verified, D_2 can verify that D_1 is a child nodes of a member whose blind key is $BS_{D_1D_2}$,and also can verify D_1 is an internal member whose blind key is BS_{D_1} .Namely, it has achieved across multiple domains to authenticate.

5. Performance and Safety Analysis

Cloud resources are distribute in broad areas, in order to providing infinite information and service resources to outside ,the resource domains within the cloud need to mutual coordinate. To ensure the legal resources to exchange conveniently, and also to prevent illegal users to access resources, the security management of cloud computing is necessary.

5.1. Correctness Analysis

The correctness is that when the legal members in cloud alliance have their autographed, they can pass the signature verification to achieve their effect identity authentication. The scheme proposed can satisfy correctness.

Theorem 1: All registered members of the key tree are able to compute the blind key and the path key of ancestors' node, for the blind signature calculation.

The proof in above lemma 2.

Theorem 2: All legal members of the model can pass the signature certification ,if their calculation is correct.

Proof:

1)

$$\begin{aligned}
&e_1(Q_{D_1}, (BS_D + PS_D)) \\
&= e_1(S_{D_1D_2} R_{D_1}, (S_D g_1 + K_D g_1)) \\
&= e_1((S_{D_1D_2} K_{D_1} / (S_D + K_D)) g_1, (S_D g_1 + K_D g_1)) \\
&= e_1(g_1, g_1)^{S_{D_1D_2} K_{D_1}} \\
&= e_1(S_{D_1D_2} g_1, K_{D_1} g_1) \\
&= e_1(BS_{D_1D_2}, P_{D_1})
\end{aligned}$$

2) $b_1 g_1 = (x + cK_{D_1}) g_1 = xg_1 + cK_{D_1} = T_1 + cP_{D_1}$

Therefore, any legal member calculates correctly, it can pass the authentication.

5.2 The Safety Analysis

In this paper the authentication protocol goal is to realize two-way entity authentication and key agreement, and the safety of the protocol is based on the safety of cryptographic algorithm. The safety of the certification protocol based on two aspects: one is the safety of inter-domain signcryption, the other is the safety of authentication protocol. The safety of signcryption is attributed to the discrete logarithm problem of $DBDH$ and $MBDH$ over G_1 and G_2.

The security analysis of authentication protocol between clouds, as follows:

(1) Unforgeability: any member that is out of cloud alliance or in cloud alliance can not fake other member's identity to access resource in cloud alliance.

①Assuming the illegal user D_1 of the external clouds want to access cloud resources, for it dose not register in cloud tree, so it dose not have the corresponding registration key R_{D_1}, then the followed authentication $e_1(Q_{D_1},(BS_D+PS_D))=e_1(BS_{D_1D_2},P_{D_1})$ is false.

②Assuming that the branch node D_i of the cloud tree allies with its grandson node D_j to pretend its child D_k to access resources, D_i can calculate the path key of its child node D_k from its grandson node D_j ,and get register key of D_k , it can pass verification $e_1(Q_{D_1},(BS_D+PS_D))=e_1(BS_{D_1D_2},P_{D_1})$,but D_i does not have the private key K_{D_k} of node D_k, so it is not pass the signature verification $b_1g_1=T1+cP_{D_1}$.

(2) Traceability: In this huge cloud network system, to make every resource server register all cloud members is great cost and unnecessary. This paper proposed that the cloud members in the network can access resources, only it can be verified, for any individual node has registered in his father node, so that it can trace individual nodes when dispute is occurred by verifying $e_1(Q_{D_1},(BS_D+PS_D))=e_1(BS_{D_1D_2},P_{D_1})$, it can track its respective fields, then trace back to itself.

(4) Anti-attack: ①Against $MITM$: Assuming that D_1 and D_2 attempt to communication, mediator $D_j(j\neq 1,2)$ is attacking to this protocol. Firstly, D_j can not achieve the consistency session key to D_1 or D_2, because D_j does not have the private key K_{D_1} of D_1, and he can not compute $y_1=x_2g_1$ when $D_2\rightarrow D_1:(P_{D_2},x_2P_{D_1})$. Obviously he also can not compute $y_2=x_1g_1$, and finally D_j and D_1 or D_j and D_2 are impossible to calculate consistent temporary session key $P_{D_1D_2}=e_1(y_1,y_2)=e(g_1,g_1)^{x_1x_2}$. ②Against replay attack: The secret communication between arbitrary groups, individuals and clouds of cloud alliance network, they used the temporary one-time session keys, and thus it can defense replay attack.

5.3 The Consumption of Computation and Communication

In this section, we compare our basic scheme with the prior schemes on the computation overhead in the light of key size, communication overhead, processing complexity and their security. The consumption of computing and communication of the mutual authentication protocol in cloud computing is mainly reflected in modular exponentiation ep , bilinear operation pr , multiplication over group pm . In the protocols, any node calculates the path key of all its ancestors and correlative computing can be pre-computed, so in signature certification process it's computing would be negligible. We now compare our protocol's communication cost with other previously constant authentication protocols in Table 1.

Table 1. The Consumption of Communication

	Reference[20]	Reference[21]	Our scheme
computing	$(\mathrm{P},\mathrm{V}):2ep+2pr+3pm$	$(\mathrm{P},\mathrm{V}):2pr+3pm$	$(\mathrm{P},\mathrm{V}):2pr+5pm$
communication	$(\mathrm{P},\mathrm{V}):\ 3\lvert G_1\rvert+\lvert q\rvert+3\lvert G_2\rvert$	$(\mathrm{P},\mathrm{V}):\ 2\lvert G_1\rvert+\lvert q\rvert$	$(\mathrm{P},\mathrm{V}):\ 5\lvert G_1\rvert+3\lvert q\rvert$
security	against active attacks	no-against active attacks	against active attacks
	One-way authentication	One-way authentication	Two-way authentication

ep Modular exponentiation, pr Bilinear map, pm Multiplication over group , $\lvert G_i\rvert$ The order of G_i , $\lvert q\rvert$ The length of q , (P,V) Signing message and Verify signature.

We perform the total energy consumption cost analysis of performing GKA using the data provided in Tan *et al.* [22] is presented, The total energy cost of each GKA protocol is simply the sum of the computation and communication cost, according to Tan et al., a 133 MHz"Strong ARM" microprocessor consumes 9.1 mJ for performing a modular exponentiation, 8.8 mJ for performing a scalar multiplication , 47.0 mJ for a Tate pairing, 8.8 mJ for performing a Elliptic Curve Digital Signature Algorithm and 10.9 mJ for performing a Elliptic Curve Digital Signature Verify Algorithm . As for the communication energy cost, according again to (Tan), an IEEE 802.11 Spectrum24 WLAN card consumes 0.66 mJ for the transmission of 1 bit and 0.31 mJ for the reception of 1 bit. The abovementioned energy costs will be used for the performance evaluation of the examined GKA protocols and are summarized in Table 2.

Table 2. Energy Costs for Computation and Communication

Type of Communication	Energy Costs/mJ
Computation cost of Modular Exponentiation (ep)	9.1
Computation cost of Scalar Multiplication (pm)	8.8
Computation cost of Tate Pairing (pr)	47.0
Communication cost for transmitting a bit	0.00066
Communication cost for receiving a bit	0.00031

As so in Figure 3, our protocol is similar to the reference [20]'s protocol with respect to both computing and communication. The computing is more than reference [21]'s protocol. However, our protocol is the more secure than reference [21]'s and our scheme can achieve to two-way authentication, so both sides are unforgeable when their communication. The advantage of ours scheme is that any two entities can mutual authenticate and do key agreement directly, so it needn't the third-party to take part in. The cross-domain authentication scheme in reference [20] and reference [21] when an entity wants to access resources from another entity in different domain it must be checked by the third-party, so it is very complex.

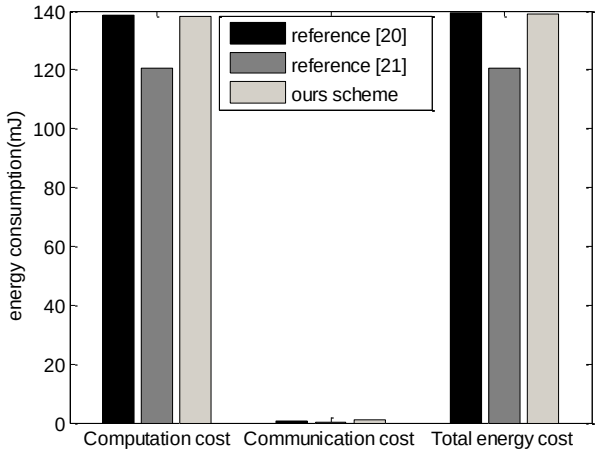

Figure 3. Energy Consumption

Analysis shows that this protocol is correct and can defense attack effectively and is not to need to know the identity of each other, which can achieve the effective authentication and good anonymous. The entity can be tracked when there have dispute occurs. The computation and communication overhead is relatively low. It has a good security.

6. Conclusion

Multi-domain authentication is a security requirement for sharing resources in hybrid cloud network environment. The paper proposed a multi-domain authentication protocol in hybrid cloud network environment, which ensure the security mutual authentication among entities that from different cloud networks or different domains. Each entity can access cross-domain resources needless the intervention of the key authentication center, which provide good flexibility. It can avoid the bottleneck problem and the complexity of the transfer tickets of the traditional pattern based on PKI. It is safe and practical.

Acknowledgements

This work is supported by National Natural Science Foundation of China (under Grant No. 61272511 and 61272038), Science and Technology Key Projects of He'nan Province (142102210081), the Science and Technique Research Program of Henan Educational Committee (No. 15A520032， 14A520022), the PhD Research Fund of the Zhengzhou University of Light Industry and National High-tech R&D Program of China (863 Program) (Grant No. 2013AA01A212).

References

[1] Sun Microsystems Take your business to a Higher Level - Sun cloud computing technology scales your infrastructure to take advantage of new business opportunities, guide, **(2009).**
[2] K. Curran, S. Carlin and M. Adams, "Security issues in cloud computing [J]", Elixir Network Engg., vol. 38, **(2011)**, pp. 4069-4072.
[3] J. Callas, "OpenPGP message format", RFC 4880, **(2007)**.
[4] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", RFC 5246, **(2008)**.
[5] H. Liu, P. Luo and D. Wang, "A scalable authentication model based on public keys", Journal of Network and Computer Application, vol. 31, no. 4, **(2008)**, pp. 375-386.
[6] F. Chang, J. Dean, S. Ghemawat, WC. Hsieh, DA. Wallach, M. Burrows, T. Chandra, A. Fikes and RE. Gruber, "Bigtable: A distributed storage system for structured data", Proc. of the 7th USENIX Symp. on Operating Systems Design and Implementation. Berkeley, **(2006)**, pp. 205-218.
[7] D. Li, G. Chen and H. Zhang, "Analysis of Areas of Research Interest in Cloud Computing", ZTE COMMUNICATIONS, vol. 16, no. 4, **(2010)**, pp. 1-04.
[8] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security and Privacy in Cloud Computing: A Survey", Proc. of the 6th International Conference on Semantics, Knowledge and Grids. Beijing, China, **(2010)**, pp. 105-112.
[9] S. Chen, S. Nepal and R. Liu, "Secure Connectivity for Intra-Cloud and Inter-Cloud Communication", Proc. of the 2011 International Conference on Parallel Processing Workshops. Taipei, **(2011)**, pp. 154-159.
[10] J. Callas, "OpenPGP message format", RFC 4880. IETF standard, (**2007**), November.
[11] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", RFC 5246. IETF standard, August, **(2008)**.
[12] Q.-Y. Zhang, "Cross-Domain Authentication Model Based on Lattice. Information Engineering (ICIE)", Beidaihe, China, vol. 1, **(2010)**, pp. 115-118.
[13] X. Zheng, "ross-Domain Authentication Model in SOA based on Enterprise Service Bus", Proc. of the 2010 2nd International Conference on Computer Engineering and Technology (ICCET), Chengdu, China, vol. 5, **(2010)**, pp. 78-82.
[14] K. Rao, "Novel Shoulder Surfing Resistant Authentication Schemes using TextGraphical Passwords [J]", International Journal of Information and Network Security, vol. 1, no. 3, **(2012)**, pp. 163-170.
[15] D. Zhou, W. Liu, W. Zhou and S. Dong, "Research on network traffic identification based on multi layer perceptron", Telecommunication Computing Electronics and Control, vol. 12, no. 1, **(2014)**, pp. 201-208.
[16] P. Huaxi, "An identity-based authentication model for multi-momain", Journal of Computers, vol. 29, no. 8, **(2006)**, pp. 1271-1281.
[17] J. Malone-Lee, "Identity-based signcryption", Available online: http://eprint.iacr.org/2002/098.pdf. **(2013)**.
[18] W. Zhang, H. Zhang, B. Zhang and Y. Yang, "An Identity-Based Authentication Model for Multi-domain in Grid Environment", Proc. of the 2008 International Conference on Computer Science and Software Engineering, Wuhan, Hubei, vol. 3, **(2008)**, pp. 165-169.
[19] S. M. Haikal, Y. J. Bin and S. Eko, "Emergency prenatal telemonitoring system in wireless mesh networ k [J]", Telecommunication Computing Electronics and Control, vol. 12, no. 2, **(2014)**, pp. 367-378.
[20] X. Lu and D. Feng, "An Identity-based Authentication Model for Multi-domain Grids", Chinese Journal of Electronics, vol. 34, no. 4, **(2006)**, pp. 577-582.

[21] C.-y. Luo, S.-w. Huo and H.-z. Xing, "Identity-based Cross-domain Authentication Scheme in Pervasive Computing Environments [J]", Journal on Communications, vol. 32, no. 9, **(2011)**, pp. 111-122.
[22] C. H. Tan and J. C. M. Teo, "Energy-efficient ID-based group key agreement protocols for wireless networks[C]", In: 20th International Parallel and Distributed Processing Symposium, 2006-IPDPS, DC, USA, **(2006)**, pp. 25-29.

Author

Zhang Qikun, Ph.D. Zhengzhou University of Light Industry, Zhengzhou. China. His research interests include information security and cryptography