Multi-Domain Authentication Protocol Based on Dual-Signature

Zengyu Cai*1, Qikun Zhang1, Li Ming2, Yong Gan1, Junsong Zhang1, Xiaoke Su1
1 School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
2 PetroChina West East Gas Pipeline Company Guangxi Management Office, Nanning 530000, China
*Corresponding author, e-mail: mailczy@163.com

Abstract

Today most multi-domain networks authentication systems provide data security and mutual authentication with asymmetric and traditional public key cryptography. There exist some problems, such as the overhead of passing certificates, the more complexity of management certificates and network bottlenecks and so on. These schemes can't protect the safety of multi-domain interoperability in distributed network effectively. Aiming at these problems, the paper proposes an identity-based multi-domain authentication protocol among domains in large-scale distributed collaborative computing network. It adopts bilinear mapping and short signature technology to achieve mutual authentication between entities in different domains, which overcome the complexity of certificate transmission and bottlenecks in the scheme of PKI-based. Analyzed shows that this scheme has anonymity, security and supporting mutual anonymous authentication and it is suitable to use in security alliance authentication mechanism in large distributed network.

Keywords: multi-domain, bilinear map, signature, anonymity, elliptic curve

1. Introduction

Along with the rapid development of network application in all kinds of fields, network applications are more and more extensive. All sorts of businesses or activities, such as network-based searching, remote collaborative designs, remote medical treatments, resource sharing, remote control and intelligent houses, may have requirements of cross-domain authentication. There also have the problems of cross-domain work in new network application forms such as grid computing, cloud computing, Internet of things etc. The study of cross-domain authentication theory and technology has becoming an urgent problem.

Although some authentication services, such as Kerberos [1], 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 [2]-[4] introduced the use of lattice theory in cross-domain authentication, each of them used lattice to the construction of the network structure. They provided a better solution to the potential safety problems caused by the authentication from an independent privileged body. And they also solved the problems of network bottlenecks and single point crash in PKI authentication framework.

Reference [5] 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. 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. However, 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.

The other is authentication framework based on traditional PKI [6],[7]. The procedures of credentials under public key cryptography are heavy burdens. Specifically, the consumptions is caused by the construction of credential paths, the query of the status of credentials and transfer of credentials. It can also cause the network bottleneck of authentication center when under frequent cross-domain accesses. Reference [8] 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 [9],[10] adopt sign-cryption method to implement mutual authentication between entities, but it is only suitable for a single domain. Reference [11] 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 [12] 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 [13] presents a multi layer perception neural network-based method for network traffic identification.

Reference [14] 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 [15] 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 [16],[17]. 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 analyzed the advantages and disadvantages of traditional multi-domain authentication schemes. We propose a multi-domain authentication protocol based on dual-signature, which mainly solves the problem of the network bottleneck and key escrow in traditional PKI authentication protocols. The protocol also achieves the anonymity of the two-way entity authentication.

2. Preliminaries

2.1. Bilinear Group

Firstly, we give the definition of bilinear map, assuming that $G_1$ is additive group, $G_T$ is multiplicative group with same prime order $p$, $p \geq 2^k + 1$, $k$ is the security parameter, let $G_1 = \langle g_1 \rangle$ be generated by $g_1$ and the solution of discrete logarithm over the $G_1$ and $G_T$ is hard. And $e$ is a computable mapping, and $e : G_1 \times G_1 \rightarrow G_T$ has the following properties:

1) **Bilinearity:** For all $u, v \in G_1$, and $a, b \in Z_p^*$, there is $e(uv, ab) = e(u, v)^{ab}$;

2) **Non-degeneracy:** There exits $u, v \in G_1$, such that $e(v, u) \neq 1$;

3) **Computability:** For all $u, v \in G_1$, there exits an efficient way to calculate $e(v, u)$.

**Inference 1:** For all $u_1, u_2, v \in G_1$, there is $e(u_1 + u_2, v) = e(u_1, v)e(u_2, v)$.

**Definition 1 Discrete logarithm problem:** For given groups $G_1$, $G_2$ and $G_T$, $g_1, g_2$ are generators of $G_1$ and $G_2$ respectively. For the above definition we can define the following the difficult solution problems. Discrete logarithm problem: set $g_1, g_1' \in G_1$, look for an integer $a$ and make it to meet $g_1' = ag_1$.

**Definition 2 Bilinear Computational Diffie-Hellman Problem (BCDHP):** Suppose a triad $(g_1, ag_1, bg_1) \in G_1$, for all $a, b \in Z_p^*$, find the element $g_1^{ab} \in G_1$. We say that algorithm $A$ has advantage $E$ in solving CDH in $G_1$ if $Pr[A(g_1, ag_1, bg_1) = g_1^{ab}] \geq E$.

**Definition 3 Decisional Diffie-Hellman Problem (DDH):** Suppose a quad $(g_1, ag_1, bg_1, cg_1) \in G_1$, for all $a, b, c \in Z_p^*$, decides that is there $c = ab \mod p$. 

---

Multi-Domain Authentication Protocol Based on Dual-Signature (Zengyu Cai)
Definition 4 Gap Diffie-Hellman (GDH) group: The problem of CDH is difficult to solve but the DDHP is easy. With this feature group called for the GDH group.

Definition 5 \((t, \varepsilon) - CDH\) assumption: The \((t, \varepsilon) - CDH\) assumption holds in group \(G_t\) if no \(t\)–time adversary has advantage at least \(\varepsilon\) in solving CDH in \(G_t\).

2.2. Multi-linear Mapping

Multi-linear Diffie-hellman hypothesis: Firstly given the definition of multi-linear mapping. Suppose that the discrete logarithm problem of \(G_1\) and \(G_2\) is hard.

Let \(G_1, G_2\) be two groups of the same prime order \(p\). The mapping \(e_1 : G_1^m \rightarrow G_2^1\) is called \(m\) multi-linear mapping, if it satisfies the following properties:

1) Multi-linearity: For any of \(a_1, a_2, \ldots, a_m \in Z_p^1\) and any of \(g_1, g_2, \ldots, g_m \in G_1\), there is:
\[
e_1(a_1 g_1, a_2 g_2, \ldots, a_m g_m) = e_1(g_1, g_2, \ldots, g_m)^{a_1 a_2 \cdot \ldots \cdot a_m}.
\]

2) Non-degeneracy: If \(g \in G_1\) is a generator of \(G_1\), then \(e_1(g, g, \ldots, g)\) is also a generator of \(G_2\).

3) Computability: For all \(u_1, u_2, \ldots, u_m \in G_1\), there exists an efficient way to calculate \(e(u_1, u_2, \ldots, u_m)\).

Definition 6 Decisional Multi-linear Diffie-Hellman (DMDH) problem is that given \(g, a, g_1, a_1 g_1, a_2 g_2, \ldots, a_m g_m \in G_1\) and \(\forall z \in G_2\), it is to determine if there is \(z = e_1(g, g, \ldots, g)^{a_1 a_2 \cdot \ldots \cdot a_m}\).

Definition 7 Hypothesis of DMDH: Hypothesis of DMDH 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. Multi-Domain Authentication Based on Dual-Signature

In this section, a new multi-domain authentication protocol is designed. There are several steps will be described.

The system is composed by \(n\) domains. Each domain is independent and autonomous. Each domain consists of a \(KMC_i (1 \leq i \leq n)\) (key management center) and a number of members \(u_j (1 \leq j)\) within the domain. \(KMC_i\) distributes and manages some keys of their members within its domain.

3.1. Dual-Signature

(1) Setup phase: select an addition group \(G_1\) and a multiplicative group \(G_2\) with same large prime order \(p\), \(g_1\) is a generator of \(G_1\) and \(g_2\) is a generator of \(G_2\), \(e : G_1 \times G_1 \rightarrow G_2\) is an efficiently computable bilinear mapping, \(h_0 : \{0, 1\}^* \rightarrow Z_p^1\), \(h_1, h_2 : \{0, 1\}^* \rightarrow G_1^*\), \(h_3 : G_2 \rightarrow Z_p^1\) are hash function.

Each \(KMC_i (1 \leq i \leq n)\) selects a number \(s_i \in Z_p^1\) randomly, and calculates \(p_i = s_i g_1\), where \((s_i, p_i)\) are the public/private keys of \(KMC_i\). Similarly, each member \(u_i\) selects a number \(x_i \in Z_p^1\) randomly, and calculates \(y_i = x_i g_1\), where \((x_i, y_i)\) are the public/private keys of \(u_i\).

(2) Alliance-domain system keys agreement: All the \(KMC_i\) can negotiate an alliance public/private key pair \((a_{ik}, a_{pk})\) by multi-linear mapping, the process is as follows:
Each $KMC_i$ calculates the alliance private $a_{ik}$ with the private key $s_i$ and public keys of other members $KMC_j$ ($1 \leq j \leq n, i \neq j$).

\[
a_{ik} = a_{ij} = h_i(e_i(g_i, p_2, p_3, \ldots, p_n)^{v_i})
\]

\[
a_{ik} = h_i(e_i(p_1, g_i, p_3, \ldots, p_n)^{v_i})
\]

\[
\vdots
\]

\[
a_{ik} = h_i(e_i(p_1, p_2, \ldots, p_{n-1}, g_i)^{v_i})
\]

Each $KMC_i$ ($1 \leq i \leq n$) calculates the alliance corresponding alliance public key $a_{pk} = a_{ik}g_1$.

3. Dual-signature and register: Suppose there are $N$ numbers in the domain $D_i$. Using the set $IDSET = \{id_j | 1 \leq j \leq N\}$ expresses the identities set of these numbers, and $ID_i$ is the identity of $KMC_i$.

1) Each $KMC_i$ calculates $R_i = s_i h_0(id_i)$ and $\eta = R_i^{-1}g_1$, then sends $\eta$ to all the members in its domain.

2) Each member $u_j (1 \leq j \leq N)$ of the domain received the $\eta$, and calculates $r_j = x_j h_0(id_j)$, $\delta_j = r_j \eta$, and selects a number $m_j \in Z_p^*$ randomly, calculates $\Gamma_j = m_j p_i$, then sent $(\delta_j, y_j, id_j, \Gamma_j)$ to its $KMC_j$.

3) The $KMC_i$ received the message $(\delta_j, y_j, id_j, \Gamma_j)$ sent by $u_j$, then verifies equation $e(\delta_j, h_0(id_j)P_j) = e(h_0(id_j) y_j, g_1)$. If it is correct, $KMC_i$ can ensure that $\delta_j$ is sent by $u_j$, and $y_j$ is unique within that domain.

4) Then $KMC_i$ can compute, $\sigma_i = (h_0(id_i) (s_i + a_{ik}) s_i)^{-1} \Gamma_j$, then sends $\sigma_i$ to $u_j$.

5) After received the $\sigma_i$, each $u_j$ calculates $\varphi_j = m_j^{-1} \sigma_i$, and verifies the equation $e(\varphi_j, (P_j + a_{pk})) = e(h_0(id_i)^{-1} g_1, g_1)$, if it is correct, $u_j$ can ensure that $\sigma_i$ is sent by $KMC_i$.

6) Where the $\delta_j$ and $\varphi_j$ are dual-signature by user $u_j$ and $KMC_i$, because they include the secret information of $u_j$ and $KMC_j$, and they also can be verified by the public keys of $u_j$ and $KMC_i$.

3.2. Dual-Signature Authentication

To ensure the security, members from different domains need to be mutual authenticated when they access resources each other. To speed up the resource access and avoid the bottleneck problem during the authentication, this paper proposed a multi-domain alliance authentication protocol based on dual-signature, which enables any two members to direct authentication and does not need to transfer the ticket by the third party (the authentication center).

Let two domains in the alliance-domain system be $D_i$ and $D_j$ respectively, the public/private key pair of $KMC_j$ in domain $D_i$ is $(P_i, s_j)$, and the public/private key pair of $KAC_j$ in domain $D_j$ is $(P_j, s_j)$, where $(i \neq j)$, and the public/private key pair of alliance-domain system is $(a_{pk}, a_{sk})$. The members $u_i$ and $v_j$ are internal members of $D_i$ and $D_j$, respectively.
$x_i$ is the private key of $u_i$, and $y_i = x_i g_i$ is the public key of $u_i$. $x_j$ is the private key of $v_j$, and $y_j = x_j g_j$ is the public key of $v_j$. The public keys and the identities $ID_i$ of every one are public.

When $u_i$ want to access resource from $v_j$, the process of multi-domain authentication and session key agreement are described as follows:

1. $u_i$ in domain $D_i$ calculates $ui_{\text{sig}} = x_i y_j$ and $\phi_i = x_i \varphi_i$, then sends the public information $(ui_{\text{sig}}, \phi_i)$ to verify $v_j$, where $\varphi_i$ is a dual-signature that in 3.1 (6).

2. After receiving the messages $(ui_{\text{sig}}, \phi_i)$, $v_j$ with its private key $x_j$ to calculates $\text{ver}_j = (x_j^{-1} u_{\text{sig}})$, and verifies whether $e(\phi_j, (P_i + a_{sk})) = e(h_h(ID_i))^{-1} g_1, \text{ver}_j$ is satisfaction.

3. If $\text{ver}_j = (x_j^{-1} u_{\text{sig}}) = y_j$ and $e(\phi_j, (P_i + a_{sk})) = e(h_h(ID_i))^{-1} g_1, \text{ver}_j$, $v_j$ can ensure $(ui_{\text{sig}}, \phi_i)$ are sent by $u_i$ and $u_i$ is a member in the domain $D_i$, then $v_j$ calculates $uj_{\text{sig}} = x_j y_i$ and $\phi_j = x_j \varphi_j$, sends the public information $(uj_{\text{sig}}, \phi_j)$ to verifier $v_j$, where $\varphi_j$ is a dual-signature that in 3.1 (6).

4. After receiving the messages $(uj_{\text{sig}}, \phi_j)$, $u_i$ with its private key $x_i$ to calculates $\text{ver}_i = (x_i^{-1} u_{\text{sig}})$, and verifies whether $e(\phi_i, (P_j + a_{sk})) = e(h_h(ID_j))^{-1} g_1, \text{ver}_i$ is satisfaction.

5. If $\text{ver}_i = (x_i^{-1} u_{\text{sig}}) = y_i$ and $e(\phi_i, (P_j + a_{sk})) = e(h_h(ID_j))^{-1} g_1, \text{ver}_i$, $v_j$ can ensure $(uj_{\text{sig}}, \phi_j)$ are sent by $v_j$, and $v_j$ is a member in the domain $D_j$.

Because two-way can mutual verify by the dual-signature of their KMC and themselves, and signature message $ID_i$ is the identity of their KMC, which can be sure everyone belongs to which domains, the cross-domain authentication in the multi-domain system is successful.

4. Performance Analysis

4.1. Correctness Analysis.

Multi-domain authentication protocol of this paper is established based on dual-signature. In order to ensure the safe authentication when the domains access resources each other, the correctness of the dual-signature must be ensured for first time.

**Theory 1:** If everyone computes correction, the legal member can be verified.

**Proof:**

1. Since $ui_{\text{sig}} = x_i y_j$, if the $v_j$ computes correction, then

$$\text{ver}_j = (x_j^{-1} u_{\text{sig}})$$
$$= x_j^{-1} x_j x_j g_j$$
$$= x_j g_j = y_j$$

2. Since

$$\sigma_j = (h_h(ID_j)(s_j + a_{sk}))^{-1} \Gamma_j$$
$$= (h_h(ID_j)(s_j + a_{sk}))^{-1} m_j g_1$$
$$\varphi_j = m_j^{-1} \sigma_j = (h_h(ID_j)(s_j + a_{sk}))^{-1} g_1,$$

and the properties of the bilinear pairings, we have:
\[ e(\phi_i, (P_i + a_{pk})) = e(x, \varphi_i, (P_i + a_{pk})) \]
\[ = (x_i(h_0(ID_i)(s_i + a_{sk}))^{-1} g_1, (P_i + a_{pk})) \]
\[ = e(x_i(h_0(ID_i)(s_i + a_{sk}))^{-1} g_1, (s_i + a_{sk}) g_1) \]
\[ = e((h_0(ID_i))^{-1} g_1, g_1) \]
\[ = e((h_0(ID_i))^{-1} g_1, x_i g_i) \]
\[ = e((h_0(ID_i))^{-1} g_1, \text{ver}_j) \]

4.2. Anonymity Analysis

The paper proposes a two-way anonymity authentication protocol, which do not need the real identities of both entities when they do mutual authentication. Each member \( v_j \) verify the identity of \( u_i \) only by the equation \( e(\phi_i, (P_i + a_{pk})) = e((h_0(ID_i))^{-1} g_1, \text{ver}_j) \), therefore, \( v_j \) don’t know the identity of \( u_i \), it only know the identity \( ID_i \) of the \( KMC_j \) that \( u_i \) belong to the domain and the public key \( y_i \) of \( u_i \).

4.3. Security Analysis

The security of multi-domain anonymity authentication protocol is based on the security of the dual-signature. The security of the signature method proposed in this article relies on the BCDHP.

**Theory 2:** Under the above assumption BCDHP, the proposed multi-domain anonymity authentication protocol is secure. Any attacker cannot forge dual-signature by eavesdropping on messages transmitted over the public channel.

**Proof:**

According to the contradiction proof principle, assume that an attacker can use an efficient probabilistic polynomial algorithm \( A \) to forge dual-signature of the proposed protocol. We use the contradiction proof technique to prove that the proposed protocol is secure under the assumption BCDHP. We can use the algorithm \( A \) to construct another efficient algorithm \( A' \) to distinguish \( \beta \) from \( abg \) based on BCDHP.

(1) An adversary \( P \) tries to learn the signature by eavesdropping on messages transmitted over the public channel. The adversary can obtain the messages \((u_{i \text{sig}}, \phi_i)\) of \( u_i \) transmitted, where \( u_{i \text{sig}} = x_i v_j \) and \( \phi_i = x_i \varphi_i \). Here, assume that adversary cannot obtain the private key \( x_i \) of \( u_i \). Under this assume, we shall prove that:

\[ e(\phi_i, (P_i + a_{pk})) = e((h_0(ID_i))^{-1} g_1, \text{ver}_j) \]

are computationally indistinguishable, where \( \beta \) is a random value in \( G_1 \).

(2) Using the contradiction proof, assume that there is an efficient probabilistic polynomial algorithm \( A \) to distinguish \( e(\phi_i, (P_i + a_{pk})) = e((h_0(ID_i))^{-1} g_1, \text{ver}_j) \) and \( e(\beta, (P_i + a_{pk})) = e((h_0(ID_i))^{-1} g_1, \text{ver}_j) \).

Based on the algorithm \( A \). We can construct another polynomial algorithm \( A' \) to distinguish \((ag_1, abg_1, bg_1)\) and \((ag_1, abg_1, \beta)\), where \( \beta \) is a random number and \( \beta \in G_1 \), \( a, b \in Z_p^* \). First, take the value \( ag_1, abg_1 \) and \( \beta \) as the input of algorithm \( A' \). Let \( \varphi_i = ag_1 \), and \( \phi_i = \beta \varphi_i \). Then, algorithm \( A' \) randomly selects \( \lambda \) from \( Z_p^* \), Then, \( A' \) calls \( A \) with these values.
If \( e(\phi_i, (P_i + a_{pk})) = e(\beta \lambda^{-1} \phi_i, (P_i + a_{pk})) \), that means key \( \beta = hg_i \). Therefore, adversary \( P \) can use algorithm \( \Lambda' \) to distinguish \((ag_i, abg_i, hg_i)\) and \((ag_i, abg_i, \beta)\), which is a contradiction for the BCDHP. Thus, that our proposed protocol is secure under the assumption BCDHP.

Compared with the existing cross-domain authentication, our advantages are as follows:

1. Authentication protocol in communication and computation is smaller than SAP scheme, and the efficiency of the certification is higher than SAP scheme.
2. Our scheme greatly simplifies the system architecture compared with the traditional PKI-based authentication framework, and saves system cost.
3. Compare with the literature [18] in the certification framework, this paper proposed protocol can provide mutual authentication in different trust domains, and the application is broader, more in line with the actual needs of a distributed network environment.
4. This paper proposed authentication protocol has forward security, and in the Reference [16] the non-interactive authentication session key is static, if an attacker controls a user's private key, he can calculate the session key that between this user and any entity, it does not have forward security.

4.4. Computation and communication consumption Analysis

In this section, we compare our basic scheme with the prior schemes in the light of key size, communication overhead, processing complexity and their security. The consumption of computing and communication mainly reflect in modular exponentiation \( E \), bilinear operation \( pr \), multiplication over group \( pm \). In the protocols, any node calculates the path key of all its ancestors and other correlative computing, which can be pre-computed. So the consumption of computing about the signature certification would be negligible[19]. We compare our protocols with other corresponding authentication protocols in communication cost in Table 1. We use notations as follows:

- \( ep \): Modular exponentiation.
- \( pr \): Bilinear map.
- \( pm \): Multiplication over group.
- \( |G_i| \): The order of \( G_i \).
- \( |q| \): The length of \( q \).
- \( (P, V) \): Signing message and Verify signature.
- \( ES \): The algorithm to establish parameters.
- \( EX \): The algorithm to extract keys.

| Table 1. The Performance Comparison of Difference |
|------------------------------------------------|
| Reference [20] | Reference [21] | Our scheme |
| Computing      | ES : 0        | ES : 0        | ES : 0        |
|                | EX : \( ep + pr + 3pm \) | EX : \( 1pm \) | EX : \( 1pm + pm \) |
|                | \( (P, V) : 2ep + 2pr + 3pm \) | \( (P, V) : 2pr + 3pm \) | \( (P, V) : 2pr + 3pm \) |
| Communication  | \( (P, V) : 3|G_i| + |q| + 3|G_i| \) | \( (P, V) : 2|G_i| + |q| \) | \( (P, V) : 4|G_i| \) |
| Against active | Yes           | No            | Yes            |
| attacks        | Authentication | One-way authentication | One-way authentication | Two-way authentication |
| Anonymity/     | No            | No            | Yes            |
| traceability   |               |               |                |

As so in Table 1, our protocol is more efficient than Reference [20]'s protocol with respect to both computing and communication. The computing is similar to Reference [21]'s and the communication is larger than Reference [21]'s. 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 communicating.

5. Conclusion

Multi-domain alliance-authentication is required for security in multi-domain network environment. The scheme of anonymity authentication protocol purposed in this article can ensure the security while share the resource among multiple domains. The anonymity can protect the privacy of each entity, and each entity can access cross-domain resources needless the intervention of the key management 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. 61163017, 61272511, 61272038 and 61340059), Science and Technology Key Projects of He’nan Province (142102210081) and the PhD Research Fund of the Zhengzhou University of Light Industry (2013BSJ045).

References

[1] H Liu, P luo, D Wang. A scalable authentication model based on public keys. Journal of Network and Computer Application. 2008; 31(4): 375-386.
[2] Chang F, Dean J, Chemawat S, Hsieh WC, Wallach DA, Burrows M, Chandra T, Fikes A, Gruber RE. Bigtable: A distributed storage system for structured data. Proc. of the 7th USENIX Symp. on Operating Systems Design and Implementation. Berkeley. 2006: 205-218.
[3] Li D, Chen G, Zhang H. Analysis of Areas of Research Interest in Cloud Computing. ZTE COMMUNICATIONS. 2010; 16(4): 01-04.
[4] Ming Z, Rong Z, Wei X, Weining Q, Aoying Z. Security and Privacy in Cloud Computing: A Survey. Proc. of the 6th International Conference on Semantics, Knowledge and Grids. Beijing, China. 2010: 105-112.
[5] Shiping C, Surya N, Ren L. Secure Connectivity for Intra-Cloud and Inter-Cloud Communication. Proc. of the 2011 International Conference on Parallel Processing Workshops. Taipei. 2011: 154-159.
[6] Take your business to a Higher Level - Sun cloud computing technology scales your infrastructure to take advantage of new business opportunities. Available online: http://www.aeciberseguridad.es/descargas/categoria6/4612546.pdf. Accessed on 5 April 2014.
[7] Kevin C, Sean C, Mervyn A. Security issues in cloud computing. Elixir Network Engg. 2011; 38: 4069-4072.
[8] J Callas, et al. Open PGP message format, RFC 4880. IETF standard. 2007.
[9] T Dierks, E Rescorla. The Transport Layer Security (TLS) Protocol, RFC 5246. IETF standard. 2008.
[10] Miao F,Zhang Q. Cross-Domain Authentication Model Based on Lattice. Information Engineering (ICIE). Beidaihe, China. 2010; 1: 115-118.
[11] Zheng X. Cross-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. 2010; 5: 78-82.
[12] Kameswara R, Novel Shoulder Surfing Resistant Authentication Schemes using TextGraphical Passwords. International Journal of Information and Network Security. 2012; 1(3): 163-170
[13] Zhou D, Liu W, Zhou W, Dong S. Research on network traffic identification based on multi layer perceptron. TELKOMNIKA (Telecommunication, Computing, Electronics and Control). 2014; 12(1): 201-208
[14] Peng H. An identity-based authentication model for multi-momain. Journal of Computers. 2006; 29(8): 1271-1281.
[15] J Malone L. Identity-based signcryption. Available online: http://eprint.iacr.org/2002/098.pdf. Accessed on 25 November 2013.
[16] Wenbo, Hongqi Z, Bin Z, Yan Y. 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. 2008; 3: 165-169.
[17] Satria MH, Yunus J, Supriyanto E. Emergency prenatal telemonitoring system in wireless mesh network. TELKOMNIKA (Telecommunication, Computing, Electronics and Control). 2014; 12(2): 367-378
[18] Lu X, Feng D. An identity-based authentication model for multi-domain grids. Chinese Journal of Electronics. 2006; 34(4): 577-582.

[19] Freier AO, Karlton P, Kocher PC. The SSL Protocol Version 3.0. INTERNET DRAFT. IETF. 1996.

[20] Kim M, Kim K. A new identification scheme based on the bilinear Diffie-Hellman group. Proc. of the 7th Australasian Conference in Information Security and Privacy. Melbourne. 2002: 362-378.

[21] Shao J, Cao ZF, Lu RX. A new efficient identification scheme based on strong Diffie-Hellman assumption. ISFST2004. Available online: http://www.sea.jp/Events/isfst/ISFST2004/CDROM04/Presented04/1P2-T1/isfst2004_C161.pdf. Accessed on 25 March 2014.