Security Enhancement of a Single Sign-On Mechanism based on ECC based Verifiable Encryption of Credential

Arul Princy.A[1], Vairachilai.S[2]
PG Student[1], Assistant Professor[2] , Department of CSE
NPR college of Engineering and Technology, TamilNadu, India

Abstract*- Single Sign-On (SSO) is a new method for authentication that enables a user to login once by using a single credential and allow the authenticated user to access the services provided by various providers. Few years back, Chang-Lee presented a new method for single user login and provided some security schemes without having any proof. Their scheme is not secure, because the two types of impersonation attacks are identified. To address this problem, the efficient RSA based verifiable encryption of signatures is introduced. The problem in using RSA is its increased key length for secure RSA, which creates a heavier processing load on the applications using RSA. To tackle this drawback and also for enforcing the security to the single user sign-on mechanism we proposed the new technique called "Elliptic –curve cryptography (ECC) based encryption scheme", which provides the strong security for multiple service authentications. As a result , the both attacks in the Chang-Lee mechanisms are detected and avoided. Hence, the proposed ECC based Verifiable Encryption of Credential is more efficient and it will provide high security to the single user sign-on mechanism.

***Index Terms*— Single sign-on (SSO), RSA-VES, ECC-VEC , authentication , security methods, credential.**

1. INTRODUCTION

Single Sign-On mechanism allows the individual user to login only once by using a single credential in order to access multiple resources. Here, their identities are verified automatically by each application they wish to access after wards. There are several secure sign-on models. Now-a-days, the most of the application requires the user to maintain the various kinds of credentials such as username, password or tokens for each service the user wish to access.

More than that, the user have to memorize the different credentials and they have to remember the appropriate credential while accessing the services from that particular application. By analyzing the practical situation, this method is very difficult for a user to maintain the various set of credential for various service providers. This will increase the processing workload of both the users and the service providers. To overcome this problem, the Single Sign-On scheme is introduced.

In distributed systems and networks, the user authentication plays an important role. Authentication is nothing but giving assurance that the two communicating parties such as the user; who is getting the resources and the resource provider; who is providing the resources, are authentic. The mutual authentication should be established between the two communicating entities such as the user and the service provider. This could avoid the illegal servers to access the services.

The mutual authentication will enables the communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys. These exchanged session keys should be eliminated after the successful communication .This could be done in order to provide the security and to maintain the confidentiality for the exchanged data between the two entities.

Once the user is authenticated, they can access multiple resources. The problem is, if the credentials are available to the other persons and if there is any misbehavior means, it will increase the negative impact. So that, the Single Sign-On requires a high focus for protecting the user credential from the other persons. Hence the strong security methods have to be employed. Few years back, Chang-Lee presented a new method for single user login and provided some security schemes without having any proof. Their scheme is not secure because, the two types of impersonation attacks are identified.

The first attack is the "credential recovering attack", where the malicious service provider will communicate with the user to obtain their credential and that malicious service provider will act as the user to access the services provided by the other service providers. The second attack is the "impersonation attack without credential", where the attackers can successfully act as the user without obtaining the credential from the user. The second attack is much similar to hacking.

Due to the lack of security, the existing method fails to meet the credential privacy and authentication during communication. To address these problems, the efficient RSA based verifiable encryption of signatures is introduced. Employing the RSA-VES technique in Single Sign-On scheme will encrypt the user credential in a highly secure manner. Hence, the above mentioned attacks are detected and avoided.

These attacks can be avoided by giving the users with dynamic credentials and each user is allocated with a particular session. So that once the process is closed, that session will be terminated. The problem in using RSA is its increased key length, which creates a heavier processing load on the applications using RSA.

To tackle this problem and in order to enforce more security to the Single Sign-On scheme, we proposed the new technique called "Elliptic-Curve Cryptography (ECC) based encryption scheme", which provides the strong security for multiple service authentications. When compared to RSA, the ECC will offer equal security for a far smaller key size, which also reduces the processing overhead. As a result, the both attacks mentioned above are detected and avoided. Hence the proposed ECC based Verifiable Encryption of Credential (VEC) is more efficient and ECC-VEC will also provide high security to the single user sign-on mechanism.

The rest of this paper is organized as follows. In the next section, we presented the related work. In section 3, we proposed our solution. In section 4, we describe our contribution. In Section 5, we analyze the security of our proposed scheme. Finally, we make a conclusion in section 6 and future enhancements in section 7.

2. RELATED WORKS

In [1] Lein Harn et al. described a technique called Generalized Digital Certificate (GDC) which is used to provide user authentication and key agreement. The GDC contains only user's public information. It does not have any user's public key. Here, the digital signature of the GDC is used as a secret token that will never be made public and the secret token will not be given to the verifier. Instead of that, the owner of the secret token will proves to the verifier that he has the knowledge of the signature. Hence, the digital certificate based on this technique is much easier to manage than the X.509 public-key digital certificates.

In [2] Chin-Chen Chang et al. introduced the new mechanism called Single Sign-On (SSO), which is mainly used for user identification scheme. The concept of SSO can permit the legitimate users to use the unique credential to access different service providers in the distributed systems and networks. They use one-way hash functions with random nonces and Data Encryption Standards (DES) for user identification scheme. Hence, the technique is more suitable and efficient for mobile devices. It also provides high security among the mobile users.

In [3] Jiangshan Yu et al. pointed out a most commonly applied technique for distributed systems and networks is the Single Sign-On (SSO), which is an authentication method that allows a user with single login and provides a user with unique token to access various services where the user has access permissions. Here, they formed the security model with authenticated key exchange, where the security method have been proved formally in order to satisfy the basic security requirements. Hence, the technique is very efficient and it is suitable for mobile devices.

In [4] Guilin Wang et al. suggested a Single Sign-On technique as a access control method, that allows a user to login once and enables a user with a unique credential to be authenticated by multiple service providers. Here, Guilin Wang et al. identify that the Chang-Lee scheme suffers from two impersonation attacks. Hence, there arises a security flaws. To address this problem, Guilin Wang et al. proposed the new security method based on the verifiable encryption of RSA signatures. The generation of keys and the encryption of signatures are based on the RSA algorithm. Hence, the more secured mutual authentication is achieved.

3. OUR SOLUTION

There exists a mechanism called Single Sign-On, which provides single token for a single user to access the various services from the different service providers. The variety of security methods were provided to make the scheme more secure. The existing methods suffer from various types of attacks and the several security flaws are identified. To address these problems, we present a more secure scheme by using the Elliptic Curve Cryptography based Verifiable Encryption of Credentials (ECC-VEC).

In Single Sign-On scheme, the generation of keys and the encryption of user credential are done based on the elliptic curve cryptography. The Figure-1 shows the overall proposed system design.

First, the trusted authority will generate the keys based on ECC algorithm. Each user has to register with the trusted authority for getting the unique identity and the signature. By using that unique identity, the user can login.

Now, the ECC based verifiable encryption of credential is done by analyzing the mutual authentication between the user request and the service provider. The user will send the message (msg_1) to the service provider for authentication.

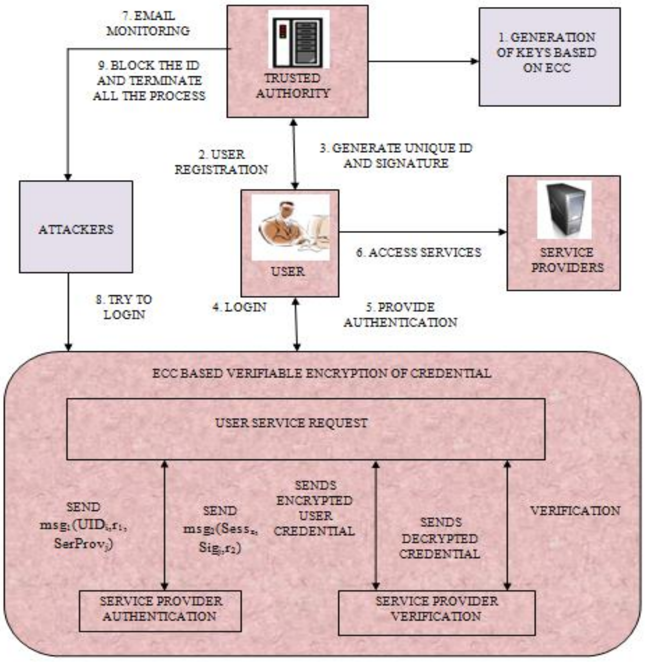
7. EMAIL MONITORING
9. BLOCK THE ID AND TERMINATE ALL THE PROCESS
TRUSTED AUTHORITY
1. GENERATION OF KEYS BASED ON ECC
2. USER REGISTRATION
3. GENERATE UNIQUE ID AND SIGNATURE
ATTACKERS
USER
6. ACCESS SERVICES
SERVICE PROVIDERS
8. TRY TO LOGIN
4. LOGIN
5. PROVIDE AUTHENTICATION
ECC BASED VERIFIABLE ENCRYPTION OF CREDENTIAL
USER SERVICE REQUEST
SEND msg₁(UIDᵢ,r₁, SerProvⱼ)
SEND msg₂(Sessₓ, Sigⱼ,r₂)
SENDS ENCRYPTED USER CREDENTIAL
SENDS DECRYPTED CREDENTIAL
VERIFICATION
SERVICE PROVIDER AUTHENTICATION
SERVICE PROVIDER VERIFICATION

Fig-1 Architectural Model

The service provider will receive the message (msg_1) and sends the message (msg_2) to the user. By processing the messages msg_1 and msg_2 the user will generate their credential and encrypt that credential based on ECC algorithm. That encrypted user credential will be send to the service provider for verification. The service provider will decrypt and sends the decrypted credential to the user.

Finally, the verification is done between the user and the service provider to identify that the session key shared between each other is same. If there is match exists between the user credential and the decrypted credential, then the user is provided with the authentication. As a result, the user can access the various services from the service provider.

The trusted authority is also responsible for monitoring the malicious users (attackers) via E-mail. If the attacker tries to login by hacking the original user ID before the session of that particular user is completed, the trusted authority will block the current user ID and it will terminate all the process. So that, the attackers cannot be able to access the services. Hence, the proposed system will provide more security against the attackers.

4. OUR CONTRIBUTION

We now present a high level overview of our mechanism and security analysis of the mechanism. The modules in our project are: Initialization Phase; user registration phase; user identification and secure signature generation; and secure ECC-VEC scheme for authentication.

4.1 Initialization Phase

The initialization phase is mainly used for key generation. The generation of secret key is based on the Elliptic Curve Cryptography algorithm. The key generation is done during the system initialization process. The secure large prime numbers are generated based on the user limits. Here, the user will select the private key and the public key is calculated by the user. The key generation process based on Elliptic Curve Cryptography will provide the key size of 160-bits which provides equal security with smaller key size when compared to RSA having 1024-bits key.

4.2 User registration Phase

In User registration phase, the user ($user_i$) needs to specify their personnel details for registering with the trusted authority. The trusted authority will receive the register request form the user and it will generate the Unique Identity (UID_i) and the signature (sig_i) . That UID_i and sig_i is issued to the user. Now, the user can login by using their unique identity UID_i. Each service provider ($serprov_j$) will also have the Identity (SID_j), throughout the process. The service providers with unique identity must maintain a pair of signing/verifying keys for secure signature scheme.

4.3 User identification and secure signature generation

The user is responsible to send the request to the service provider for accessing the resources. The user request is processed at the service provider environment for validation. First, the user will send the service request message msg_1 to the service provider. The message (msg_1) includes the user identity (UID_i),a random number(r_1) and the service provider to whom the user wish to communicate($serprov_j$).

The service provider will receive the message (msg_1) and sends the message (msg_2) to the user. The message (msg_2) includes the session key($sess_z$),the signature(sig_j) and the random number(r_2) selected by the service provider. During the secure signature generation, the user and the service provider will generate their own signature for secure sign on.

The user will generate their credential by processing the messages msg_1 and msg_2.This user credential will be encrypted based on the ECC encryption technique. That encrypted user credential is send to the service provider. The service provider will use that encrypted user credential and they will generate the cipher credential. That cipher credential will be send to the user.

4.4 Secure ECC-VEC Scheme for Authentication

The user will verify that the decrypted credential send by the service provider is equal to the original user credential. If there is a match exists between these credentials then it is concluded that the session key shared by both the user and the service provider is the same. Hence, the process is termed as the ECC based verifiable encryption of credential (ECC-VEC), which is employed to authenticate the user. After verification, the user will be authenticated to access the services from the service provider. Here, the service provider authenticates the user based on the ECC-VEC scheme in-order to access the various services.

4.5 Blocking the misbehaving users

The trusted authority is responsible for monitoring all the persons entering into the system in order to access the various services offered by different service providers. The trusted authority also responsible for monitoring the malicious users (attackers) via E-mail. Each user must register with the trusted authority to get the login ID and the signature. After getting the login ID, the user can access the system. If the attacker tries to login by hacking the original user ID before the session of that particular user is completed, the trusted authority will block the current user ID and terminate all the process completely. So that, the attackers cannot be able to access the services. Hence, the proposed system will provide strong security against the attackers.

5. IMPLEMENATION RESULTS

As a result, the Elliptic Curve Cryptography based Verifiable Encryption of Credential will provide strong security to the Single Sign-On scheme. When compared to RSA-VES, the ECC-VEC will provide several advantages. They are, the ECC and RSA provides equal security for various credential size which is shown in the Fig.2, the execution time of ECC is minimum than RSA which is shown in Fig.3 and the processing memory of ECC is lesser than RSA which is shown in Fig.4.

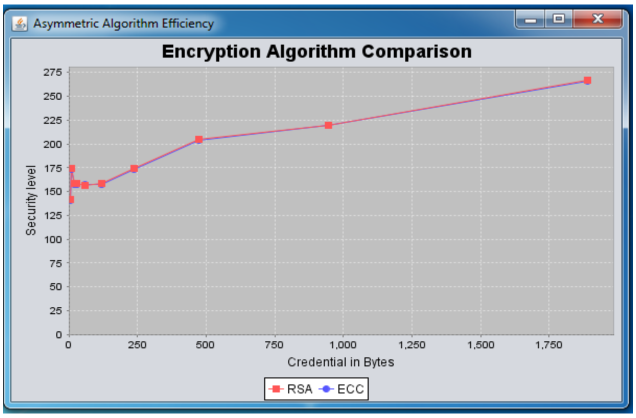

Fig.2 ECC and RSA provides equal security

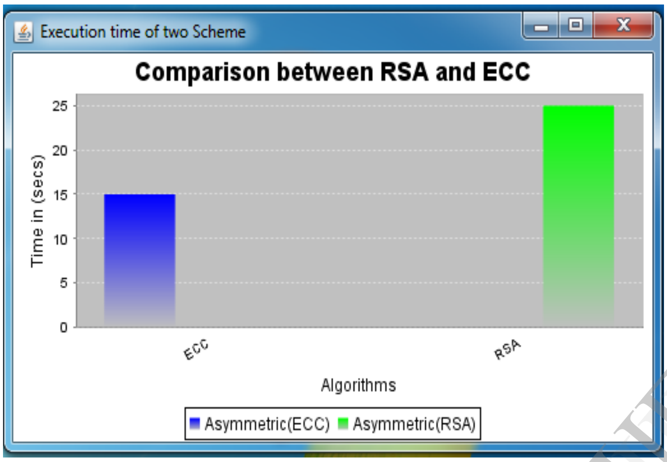

Fig.3 Minimum Execution Time

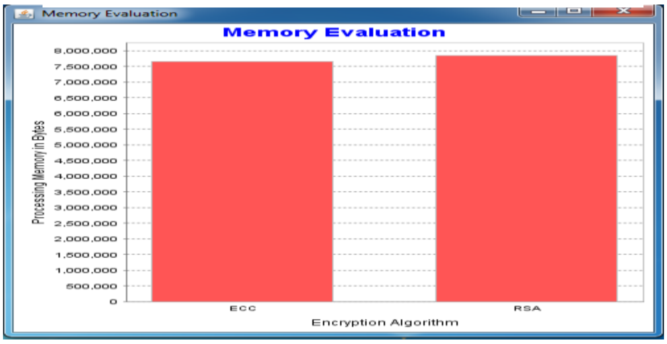

Fig.4 Less Processing Memory

We have implemented the project, "Enforcing Security of a Single Sign-On Mechanism for Multiple Service Authentications" with strong security. The main advantage of the project is that the entire credential as well as the exchanged data can be made highly secured. Using the elliptic curve cryptography in the single sign-on mechanism will provide the double security for the credential by encrypting it based on the ECC encryption algorithm. When compared to RSA, the proposed scheme offers high security for a far smaller key size, which reduces the processing overhead. Thus we have proposed the new technique called ECC based Verifiable Encryption of Credential (ECC-VEC), which enforce the strong security to the Single Sign-On scheme. The proposed scheme also detects and avoids the attacks in the existing method. We hope that our work is more efficient as well as it increased the security of the Single Sign-On scheme.

7. FUTURE ENHANCEMENTS

(i) With further modifications, the ECC-VEC technique can be implemented in the social networks for providing security to the personal data. The elliptic curve cryptography based verifiable encryption of credentials can be applied in the personal applications for securing the privacy of the data.

(ii) The security model can be formalized with authenticated key exchange. The user is provided with the private environment. So that, after user login, their credential is send to the user's private environment. For further process, the user has to know their credential from their private environment. The security can also be provided by using this method.

8. REFERENCES

[1] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2372–2379, Jul. 2011.

[2] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," *IEEE Trans. Ind. Electron.*, vol. 59, no. 1, pp. 629–637, Jan. 2012.

[3] J. Yu, G.Wang, and Y.Mu, "Provably secure single sign-on scheme in distributed systems and networks," in *Proc. 11th IEEE TrustCom*, Jun.2012, pp. 271–278.

[4] Guilin Wang,Jiangshan Yu, and Qi,"Security analysis of a single sign-on mechanism for distributed computer networks,"*IEEE Trans. Industrial Informatics*.,vol. 9,no. 1,Feb 2013.

[5] N. Asokan, Member, IEEE, Victor Shoup, Member,IEEE, and Michael Waidner, Member,IEEE, "Optimistic Fair Exchange of Digital Signatures",*IEEE Journal on selected areas in communications*,vol. 18,no.4,April 2000.

[6] Bismin V Sherif, Andrews Jose,"Secure Communication Using Generalized Digital Certificate"*International Journal of Computer Applications Technology and Research*,vol. 2,Issue 4, 396-399, 2013.

[7] T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," *Comput. Security*, vol. 23, no. 2, pp. 120–125, 2004.

[8] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 15, no. 6, pp. 2551–2556, Jun. 2008.

[9] The Open Group, "Security Forum on Single Sign-on", http://www.opengroup.org/security/l2-sso.html.

[10] C.-L. Hsu and Y.-H. Chuang, "A Novel User Identification Scheme with Key Distribution Preserving User Anonymity for Distributed Computer Networks", *Inf. Sci.*, vol. 179, no. 4, pp. 422-429, 2009.

[11] C.P. Schnorr, "Efficient Signature Generation by Smart Cards", *J. Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

[12] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," *Comput. Secur.*, vol. 24, no. 8, pp. 619–628, Nov. 2005.

[13] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes Cryptogr.*, vol. 19, no. 2/3, pp. 173–193, Mar. 2000.

[14] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, pp. 120–126, 1978.

[15] C. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, pp. 161–174, 1991.

[16] Lee WB, Chang CC. User identification and key distribution maintaining anonymity for distributed computer network. Comput Syst Sci Eng 2000;15(4):211e4.

[17] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *Wireless Commun.*, vol. 11, no. 1, pp. 62–67, Feb. 2004.