NOVEL IMPLEMENTATION OF SECURE SINGLE LOGIN IN DISTRIBUTED COMPUTING NETWORKS USING ECC

[1]D.Mariammal, [2]P.Brundha

[1]PG Scholar, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli.

[2]Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu State, India.

ABSTRACT--**Single Sign On (SSO) is a new authentication mechanism in which legal user can authenticate with proper credential in a distributed computer networks which enables for multiple service provider. The existing scheme is insecure such that it has two attacks. One is malicious service provider. In another attack, an outsider can enjoy the network services freely without any valid credentials. The proposed SSO scheme known as ECC (Elliptic Curve Cryptography) are used .Unlike other algorithm such as RSA and DES, ECC provides more security with smaller key size, lower battery resource, less processing time and high speed. ECC is achieved credential privacy and soundness of authentication. It is widely used for mobile applications.**

Keywords-**Attacks, Single Sign On (SSO), Authentication, Credential Privacy.**

I. INTRODUCTION

In distributed computer networks, the user may access various network services that is given by service provider. The user authentication is very important to identify or verify whether the user is legal or not. Only the legal user can access the various network services through valid credentials. In the environment, one user cannot maintain distinct pair of identity or password for different service provider, so that, user and service provider should meet lot of problem during accessing or providing the network services. To overcome the above problem SSO mechanism is proposed. SSO is a new authentication scheme in which only legal users are allowed with valid credential to access various network services from multiple service providers.

In SSO mechanism, the user sign on only once, their detailed are verified and services are provided by the different service provider in distributed environment. The SSO should meet three basic security requirements.

1) Unforgeability
2) Credential privacy
3) Soundness.

Unforgeability means no one can forge a valid credential for a new user, except the trusted user. Credential Privacy means illegal service provider cannot get valid credential. Soundness means unregistered user cannot get the services from the service provider. Legal user only can access the services.

Benefits of SSO

1) No need to remember multiple password and identity.
2) Time reduced through single login with multiple service providers.
3) IT costs reduced.

RSA

It is a public key encryption algorithm. RSA provide security for system process. But the computation cost is very high because RSA taking very large bit values for encryption & decryption. RSA spent more time in process execution.

ECC (Elliptic Curve Cryptography)

It is also one of the public key encryption algorithms. ECC have smaller key size only. So computation costs are reduced and less storage time. Execution processing time is high. ECC provides more security when compared to RSA and DES.

II. PREVIOUS WORK

In previous work, Chang-Lee proposed new SSO scheme to provide security parameters in distributed computer network environment. Unfortunately their scheme is failed to meet credential privacy and authentication soundness.

Two types of attacks occurred in this scheme, o one is to allow malicious service provider and another type of attack is that the outsider can enjoy the network services without any valid credential. To overcome the above failure, the RSA - VES technique is proposed. Here security is provided as well as it is useful for mobile applications.

Disadvantages

1) Computation and Communication costs are very high.
2) It takes more time for processing and execution.
3) Bit size values are very large.

III.PROPOSED SCHEME

The proposed scheme is used to overcome the above previous work. Here, Elliptic Curve Cryptography (ECC) algorithm is implemented to provide more security compare than RSA-VES. Various phases in ECC are as follows:

1) Initiation Phase
2) Registration Phase
3) Authentication Phase

Initiation Phase

In this phase, the user gives two number p and q. From that, p value is calculated and similarly q value is calculated. p', q' values are calculated using p and q values. From the four values, the keys are generated after that public key and corresponding private key are created. Keys are stored in database. Each service provider have id, the service provider id and user keys are stored.

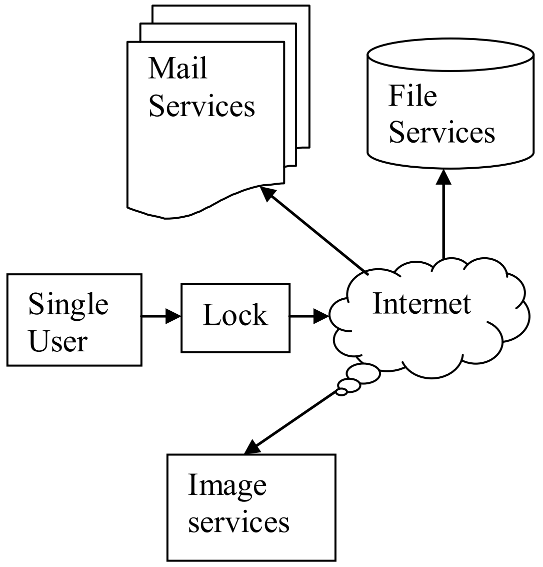

Fig: 1 Single User Sign-On to Multiple Services

Registration Phase

In this phase, user register their details like user name, age, mobile number etc, and then get id from smart card producing centre produce for user id, signature during the registration time. In this way each user registers their detail. Registration user only gets the services from the various service providers.

Authentication Phase

In this phase valid user only can enter. The service provider is used to verify the database, whether the user id and other user related information present in the database or not. If the user information is present in the database, particular user only get services from the service provider using smart card producing centre. After getting credential, the user gets authentication. Authentication is very important to access the network services. ECC scheme is more secure during communication. The computation cost is very low, also efficient for mobile application and many distributed computer networks.

Advantages

1)ECC have key size value are small
2)Computation cost and executing time is also reduced.
3)ECC deals with complex problems in distributed computer networks.

IV. RELATED WORKS

Single sign on is a new authentication mechanism that enables legal user can access the network services from multiple service provider with proper credentials. The Chang-Lee proposed a new SSO scheme to provide more security but their scheme become insecure. It contains two types of attacks.

1) Malicious Service Provider.
2) Outsider can forge the network services without any valid credentials.

To overcome the above attacks, RSA-VES technique is proposed to meet credential privacy and soundness of authentication. It is useful for mobile application, however this proposed scheme is inefficient and insecure [1].

GDC is used to provide user authentication for secure communication. GDC contains user's public information, digital drive license about user and digital birth certificate about the user etc. The GDC information is signed by trusted certificate authority. The GDC is useful for user authentication .Authentication are very important in distributed computer network .If user is authenticated, that particular user only prove that their private key corresponding public key. GDC have secret token for each user. Through this token, user knows about the detail of the digital certificate. GDC is much simpler than public key certificate. It is useful for secure communication [5].

Two parties can exchange their message in fair way during that time no one interrupts. A trusted third party as mediator was introduced by OFE. The mediator always should present the online while two parties exchange their digital items. Otherwise fault will occur. OFE is known as Off-line Fair Exchange. In this approach, there is no need for the mediator to present all the in online. When fault will occur between two parties that time only mediator gets invoked.OFE provide strong resolution ambiguity [2].

To create secure distributed information system, the user authentication and key agreement are more important security primitives. It provides identity privacy of users. Elliptic curve cryptography scheme supports for user authentication and key agreement. Proposed scheme consists five phases

1) Registration Phase
2) Login Phase
3) Precomputation Phase
4) Parameter Generation Phase
5) Password Changing Phase

This scheme has many merits.

1) Computation and Communication cost is low

2) User can change the password their convenient

3) No need password table.

4) It can prevent dictionary offline attack.

V.RESULT ANALYSIS

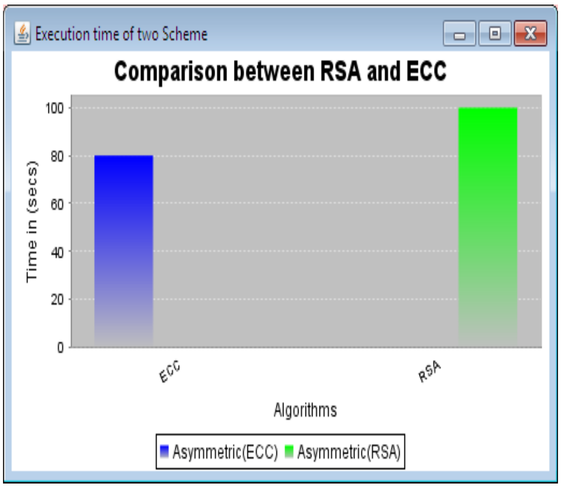

Fig: 2 Comparison of RSA and ECC

This graph shows the comparison between RSA and ECC. In the existing one, RSA algorithm is used. To overcome Chang-Lee scheme security attacks and also provides more security but in this scheme taking more time for execution process and taking very large size bit values. In this graph, ECC also a public key encryption like RSA in ECC provide more security as well as the process execution is high and it takes small bit size key value, so computation and communication cost also reduced. The value taken in X axis are indicated by algorithms and Y axis indicated by times in seconds.

VI.CONCLUSION

SSO scheme is a new authentication mechanism in which legal user only can access various network services from multiple service providers with proper credentials. But, this scheme is insecure and different types of attacks occurred. ECC technique is implemented in proposed scheme. ECC gives more security when compared to RSA and other algorithms. ECC is one of the public key algorithms. ECC uses smaller key sizes value only so that computation and communication costs are also reduced. Many IT concern can promote the progress of single sign in systems.

ACKNOWLEDGEMENT

First of all I thank the almighty for giving us the knowledge and courage to complete the research work successfully. Next I express my gratitude to our respected Assistant Professor Mrs.P.Brundha for following me to do research work effectively. Finally, I wish to express my gratitude to my family and my friends, for providing unending support in every aspect possible, to ease my path on this journey.

REFERENCES

[1] 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.

[2] N. Asokan, V. Shoup, and M. Waidner, 'Optimistic fair exchange of digital signatures'IEEE Trans J. Sel. Areas Commun., Vol. 18, No. 4, pp. 591–606 ,2010.

[3] Chin Chang and C.-Y. Lee , 'A secure single sign-on mechanism for distributed computer networks,' IEEE Trans. Ind. Et, Vol. 59,No. 1, pp. 629–637,2012.

[4] Cheminod, A. Pironti, and R. Sisto , 'Formal vulnerability analysis of a security system for remote field bus access,' IEEE Trans. Ind. Inf., Vol. 7, No. 1, pp. 30–40,2011.

[5] 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. 2372–2379,2011.

[6] C.L Hsu. and Y.-H. Chuang, 'A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,' Inf. Vol. 179, No. 4, pp. 422–429, 2009.

[7] 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. 2551–2556,2008.

[8] X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li , 'Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards,' IEEE Trans. Ind. Electron., Vol. 57, No. 2, pp. 793–800,2010.

[9] V.K Mangipudi and R. S. Katti , 'A secure identification and key agreement protocol with user anonymity (SIKA),' Comput. Security,Vol. 25, No. 6, pp. 420–425,2011.

[10] Sun, Y.-H. Chen, and Y.-H. Lin, 'oPass: A user authentication protocol resistant to a password stealing and password reuse attacks, 'IEEE Trans. Inf. Forensics Security, Vol.7, No 2, pp. 651–663, 2012.

AUTHOR(S) PROFILE

D.Mariammal is doing M.E Computer Science and Engineering in Francis Xavier Engineering College, Tirunelveli. She completed her B.E Computer Science and Engineering in Raja Rajeshwari Engineering College, Vanagaram, Chennai in the year of 2008. She published many Conference Papers. She is an active member in Computer Society of India. Her areas of interest are Network Security, Wireless communication and Mobile Technology.

Mrs. P. Brundha is working as an Assistant Professor, Department of Computer Science and Engineering in Francis Xavier Engineering College, Tirunelveli. She has completed her B.E Computer Science and Engineering from P.S.R Engineering College, Sivakasi and M.E Computer Science and Engineering from Manonmanium Sundaranar University in Tirunelveli.