RESEARCH ARTICLE OPEN ACCESS

Application of Distributed Network Services Using SSO with Different Security Mechanism

Ms. Shreya B. Pandey *, Prof. S. P. Chhaware **, Ms. Antara Bhattacharya***
*(Dept. of computer science and engineering,
R. T. M. Nagpur University, Nagpur, India
pandeyshreya07@gmail.com)
**(Dept. of computer science and engineering,
R. T. M. Nagpur University, Nagpur, India
ct.sphiroj@pce.ltjss.net)
***(Dept. of computer science and engineering,
R. T. M. Nagpur University, Nagpur, India
antara.bhattacharya@raisoni.net)

ABSTRACT
A new authentication mechanism is SSO that helps to a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Security protocols and authentication mechanisms are integrated in a middleware. A Single sign-on mechanisms ensure the use of user credentials for accessing multiple resources that the user is requested to enter its credentials only once in the distributed system. It ensures a reduction of the number of passwords used which can significantly improve security of systems by minimizing the password being compromised. Communication between client applications and servers is done using secure channels based on security protocols. This paper provides different application of a distributed computer network using SSO.

Keywords **-** Algorithm, Security, Authenticity, single sign-on, authentication, security protocols, cryptography.

I. INTRODUCTION

Single sign-on mechanisms ensure the use of user credentials for accessing multiple resources where the user is requested to enter its credentials only once. This ensures a reduction of the number of passwords used which can significantly improve security of systems by minimizing the likelihood of a password being compromised [1].

Communication between client applications and servers is done using secure channels based on security protocols. The rest of the paper is structured as follows. the architecture of the middleware: the requirements, the software stack and the security protocols.

The user authentication plays a crucial role in distributed computer networks to verify the legacy of a user and then can be granted to access the services requested. To prevent unauthorized servers, users usually need to authenticate service providers. After authentication, a session key may be negotiated to keep the confidentiality of data exchanged between a user and a provider [4].

When users have to keep so much confidential information, security problems can occur and will increase the overhead for the networks. So, there are four important security problems that the user identification scheme must have to solve which is, it must determine whether users are legitimate or not and then service providers must be authenticated, Next is a common session key must be appropriately established. And finally the privacy of legal users must be ensured [3][5]. Aauthentications to a specialized infrastructure also enables the enforcement of a consistent authentication policy throughout the enterprise. SSO is the ability for a user to authenticate once to a single authentication authority and then access other protected resources without re-authenticating [6]. The Open Group defines SSO as the mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access authorization, without the need to enter multiple passwords [7].

The proposed secure single sign-on mechanism allow mobile users to use the unitary token to access multiple services. The mobile user can use the mobile device, e.g., a cell phone, with the unitary token to access multi services, such as download music, receive/reply electronic mails, order goods, or process online payment from different service providers in distributed computer networks. The main objective of the proposed system using ECC(Elliptic Curve Cryptography) is to enhance security for single sign-on solutions and eliminate the need for users to repeatedly prove their identities to different applications and to provides high security with smaller key sizes for battery limited devices.

II. RELATED WORKS

In 2000, Lee and Chang proposed a user identification scheme with key distribution maintaining user anonymity for distributed computer networks. The security of the scheme is based on the factoring problem and the one-way hash function. The scheme can only let the service provider identify the legal user and establish a session key with the user. Moreover, the scheme does not require any password table [1]. Latter, in 2004, Wu and Hsu showed that the Lee–Chang's scheme is insecure under server spoofing attack and the identity of the user can be exposed. By using server spoofing attack, an adversary can masquerade as a service provider to exchange a session key with a user. In addition, an adversary can reveal the identity of the user with session key [2]. Then, Wu and Hsu proposed more efficient user identification scheme with key distribution an improved. Unfortunately, Yang *et al.* demonstrated that Wu-Hsu's scheme is vulnerable to a compromising attack. It is possible for an adversary to derive the private keys of users who request services. Yang *et al.* also proposed an improvement of Wu–Hsu scheme to overcome the security leak and achieve the same security requirements. However, in 2006 Mangipudi and Katti have shown that Yang *et al.*'s scheme suffers from a Denial-of-Service (DoS) attack [3]. To withstand such a DoS attack, Mangipudi and Katti further proposed a secure identification and key agreement protocol with user anonymity (SIKA).In 2009 Hsu and Chuang demonstrated that both Yang *et al.*'s and Mangipudi–Katti'sschemes are vulnerable to identity disclosure attacks and proposed an improvement to prevent such attacks. Hsu–Chuang's scheme uses timestamps to avoid replay attacks , and, unfortunately, it is difficult to verify the timestamp when entities are located in different time zones or when there is a congested network environment that has unstable latency [4][7]. Therefore, additional time-synchronized mechanisms are needed to adjust the clock between the two parties. IN 2012 Chin-Chen Chang and Chia-Yin Lee, uses RSA and secure single sign-on mechanism to allow mobile users to use the unitary token to access multiple services [5][6].

III. ROLE OF SSO IN DISTRIBUTED NETWORK SERVICES

In Distributed Network Services SSO play an important role while providing different services and it work effectively for different security algorithm.

- ***Reduce the communication cost***

The proposed system focused on the computation cost on the client side. For each client, our scheme uses modular exponential operations, meaning that our scheme is more efficient and has lower energy consumption than the other schemes. With smaller key sizes processing speed is fast using ECC and reduces the communication cost.

- ***Provide the security with smaller key sizes***

Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem, in particular for mobile (i.e., wireless) environments.ECC offers equivalent security with smaller key sizes as compared to RSA. With smaller key size ECC require fewer resources of the device to perform the mathematical tasks.ECC keys require more time to break as compared to other algorithm.

- ***Useful for battery limited device***

Elliptic Curve Cryptography (ECC) has high efficiency with smaller key sizes useful for mobile devices that has limited power .In the proposed system using ECC the cryptographic operations will be performed with fewer processor cycles and operation can be performed much faster and thus reduced in power consumption.

IV. AUTOMATE APPLICATION OF DISTRIBUTED NETWORK SERVICES USING SSO

- Streamline application access with Single sign we can automate the management of password security. Single sign enables SSO for all applications- including client-server,

legacy, java and Web applications and allows you to manage passwords by enforcing password policy and changes passwords when required.

- Centralize compliance reporting. With the push of a button, administrators can produce a variety of reports - pre-built or customized - to show which users had which type of access to what type of data, at what time and from which location as well as the ability to see who is sharing passwords.
- Securely authenticate users. Single sign on offers native support for a range of strong user authentication options such as active and passive smart cards proximity cards, finger biometrics, ID tokens and USB tokens.
- Manage passwords more easily. Users need only log on to the network once to have full authorized access to all their applications. Password management includes the generating strong and secure passwords, changing them as needed to comply with password security policies, and enforcing password policy across the organization.

V. WORKING MODULE

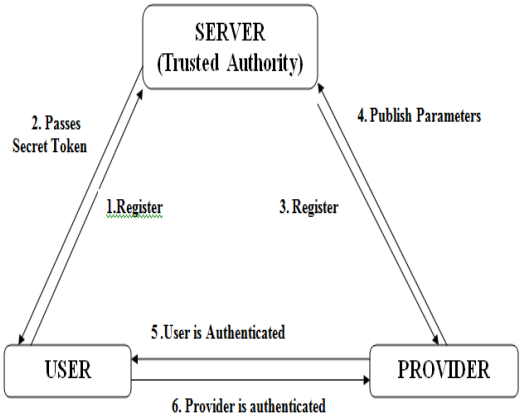

Figure 1: Working Module

- **System Initialization Module** => In this phase the trusted authority will be created

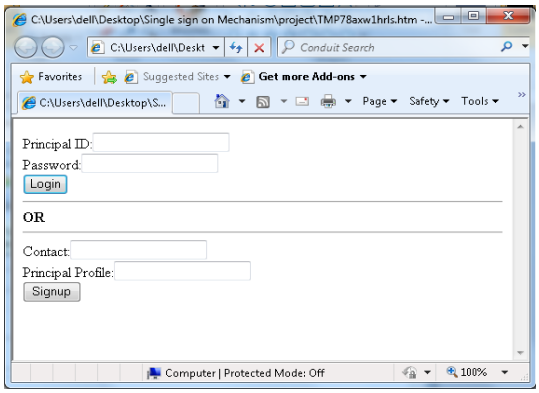

Figure 2: Login window

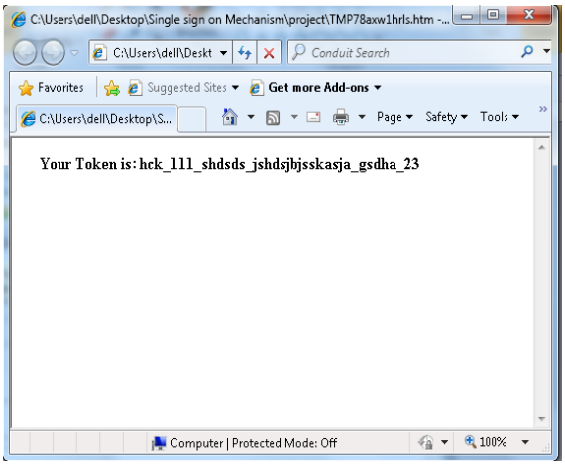

Figure 3: Token Generation

- **Registration Module** => User registers with unique identity to the trusted authority.

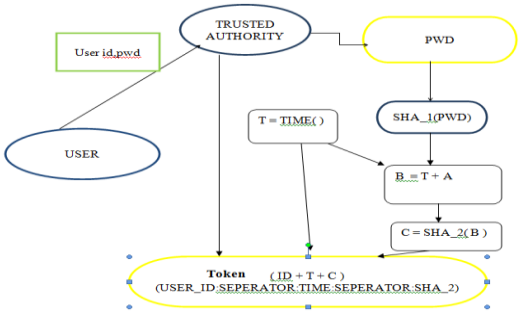

Figure 4 a: Token Generation Using Sha1

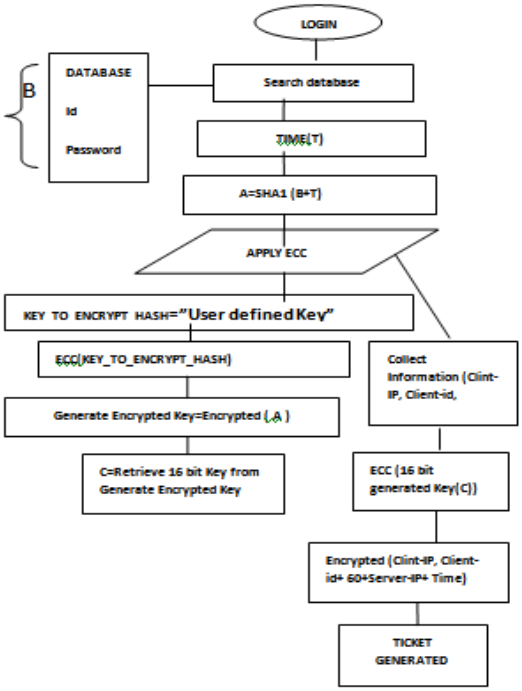

Figure 4 b: Ticket Generation Using ECC

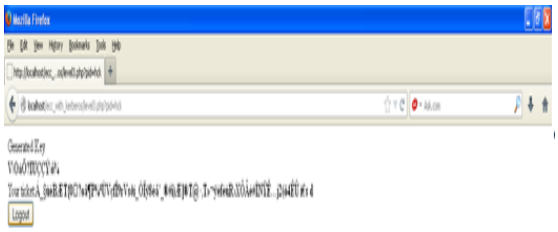

Fig 5: Generation of Key and Token Using ECC

VI. CONCLUSION

Single sign on benefits are having Ability to enforce uniform enterprise authentication and/or authorization policies across the enterprise. End to end user audit sessions to improve security reporting and auditing. SSO help for reducing computational cost and lower communication cost.

REFERENCES

[1] Kiran Mehta, Donggang Liu, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", *IEEE Transactions On Mobile Computing, Vol. 11, No. 2*, February 2012.

[2] Yun Li, Jian Ren," Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", *IEEE Transactions On Mobile Computing, Vol. 11, No. 2*, February 2012.

[3] Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, "Hardware implementation of RFID mutual authentication protocol," *IEEE Trans. Ind. Electron., vol. 57, no. 5*, pp. 1573–1582, May 2010.

[4] 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, Feb. 2010.

[5] Da-Zhi Sun, Jin-Peng Huai, Ji-Zhou Sun, Jian-Xin Li, Jia-Wan Zhang, Zhi-Yong Feng." Improvements of Juang *et al.*'s Password-Authenticated Key Agreement Scheme Using Smart Cards" *IEEE Transactions on industrial electronics, vol. 56, no. 6*, june 2009.

[6] Xiangxue Li, Weidong Qiu, Dong Zheng, Kefei Chen, and Jianhua Li ," Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards", *IEEE Transactions on industrial electronics, vol. 57, no. 2*, february 2010.

[7] K. Bouyoucef and K. Khorasani, "A Robust Distributed Congestion-Control Strategy for Differentiated Services Network", I*EEE Transactions on industrial electronics, vol. 56, no. 3*, march 2009.

[8] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," *Computer System .Sci. Eng., vol. 15, no. 4*, pp. 211–214, 2000.

[9] 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, Feb. 2009.

[10] Chin-Chen Chang, Fellow, IEEE, and Chia-Yin Lee," A Secure Single Sign-On Mechanism for Distributed Computer Networks", *IEEE transactions on industrial electronics, vol. 59, no. 1*, january 2012.