SSO Mechanism For Providing The Authentication Against The Faulty Users

Ms. Vandana N S, Assistant Professor, EPCET, Bangalore, India, vanduvandana1992@gmail.com

Ms. Indumathi S , Assistant Professor, EPCET, Bangalore, India, indusrinivasa@gmail.com

Mrs. Bindiya A J, Assistant Professor, EPCET, Bangalore, India, bindiyaaj@gmail.com

Abstract- Introducing authentication mechanism for proper access of the data from websites or any official accounts have become very hectic in recent days. In this paper we are using a single sign-on(SSO) mechanism to provide the authentication proof for the users who log-in, by providing proper user name and passwords. If the user is not member of particular website, firstly he need to register then he need to log-in and access content. Here SSO produces secrete key where this key will be sent to users mobile number or users mail id and then user can access his content. Adopting this mechanism prevents entry of illegal users, there by increasing more privacy, credentiality, enforgeability and soundness. This mechanism can be done offline.

Keywords* — *SSO, security, SCPC

I . INTRODUCTION

Because of not providing the authentication , many companies have under gone information leakage problem, there by loosing the capital which is invested. This SSO can be one of mechanism to provide better authentication to protect data against un-trusted victims. Mainly we follow some criteria.

1)If the user is not registered he need to register by giving his user name and set his password, and also have to fill the some necessary blocks such as phone number, email-id, address etc.

2) If the user is already a member of particular website, once user tries to login with his own details, a 10 digit digital signature will be produced by SSO and will be sent to users mobile number or mail.

3) If signature matches exactly with SSO generated one, then users are eligible to access the contents.

4) SSO means Single-sign-on, i.e once logged in by users, can access multiple contents at single attempt.

5) SSO supports FTP and Email, where both are offline mechanisms.

6) With single attempt the user can access any of the service that is provided.

In SSO we mainly have involvement of following.

1. User
2. SCPC
3. Server
4. User profileBy discussing five different levels, we can provide proof how SSO stands to provide security.

LEVEL 1: User will the request to server for registration purpose, server accepts that and produces digital signature and sends back to user. User enters the signature and this will fall with third party called SCPC.

LEVEL 2: SCPC receives the signature sent by user and verifies it with server. If it is correct then SCPC shows user profile.

LEVEL 3: User profile have capacity to choose FTP or Email . Once selected it is again sent to SCPC for verification. SCPC internally cross verifies with server and takes the acknowledgment and returns the user choice.

LEVEL 4: Once signature is verified by SCPC, user can interact directly with server.

LEVEL 5: User will interact directly with server and can access data from server or user can upload the data to server.

So the brief representation of all levels can be shown in the below diagram.

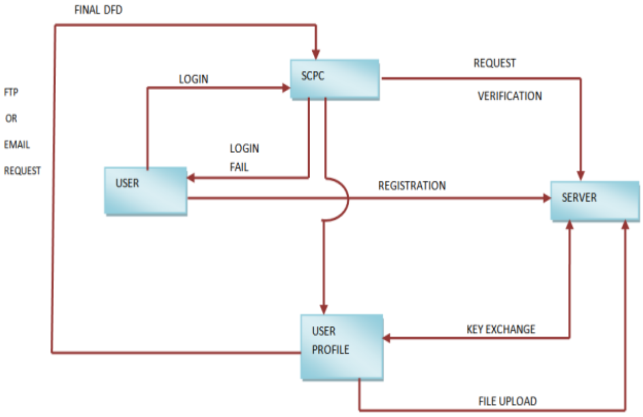

Figure: Summary of SSO working.

II. LITERATURE SURVEY

- In 2000, Lee and Chang proposed a mechanism called user identification and key distribution scheme.
- There was few mistakes which was identified by Wu and Hsu that the Lee–Chang scheme is insecure against both impersonation attacks and identity disclosure attacks. The attacker has capacity to forge the signature if it is displayed on the same working platform. It also denied the synchronization of time stamp.
- Then Yang-et al identified a weakness in the Wu–Hsu scheme and proposed an improvement.
- In 2006, however, Mangipudi and Katti pointed out that Yang et al.'s scheme suffers from Deniable of Service (DoS) attacks and presented a new scheme.
- In 2009, Hsu and Chang showed that the schemes of both Yang et al. and Mangipudi–Katti were insecure for identifying disclousre attack and proposed an RSA-based user identification scheme to overcome this weakness.

III. OBJECTIVES

1. Unforgeability
2. Credential privacy
3. Soundness

Unforgeability: Except valid users no one can access the data including the company members.

Credential privacy: Preventing dishonest persons to access the data there by avoiding the loss of company reputation .

Soundness : Unregestered user also cannot the data.

IV. IMPLEMENTATION

Two main algorithms are used for building the SSO mechanism.

A. *RSA algorithm for encryption and decryption.*

Sample code for key generation.

- **Key generation**
- ❑ Choose two distinct prime numbers u and v.
- ❑ caluculate n = u * v.
- ❑ Compute φ(n) = φ(u)φ(v) = (u − 1)(v − 1).
- ❑ Choose an integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1

Determine d ≡(d*e)modn

B. *Diffie Hellman Algorithm*

The production of secrete key at output stage must be same irrespective of the input passed by Alice and Bob. The below figure shows the working of this algorithm. Consider an eg, Let Alice = a and Bob=b.

Step1: Common color a=10 ,b=7.

Step2: Secrete color a=2, b=5.

Step 3: combine common color of Alice + secrete color of Bob. A=10+2=12

B=7+5=12

Step 4: Exchange secret keys of Alice and Bob.

Now secret key of a=5 and secret key of b=2.

Step 5: Add this secret keys with common key's. (common keys is a=10, b=10)

Alice a= common key of b + exchanged secret key of Bob.

Bob b= common key of a + exchanged secret key Alice.

There fore a= 7+5= 12

b= 10+2=12

Step 6 : A = B// matches

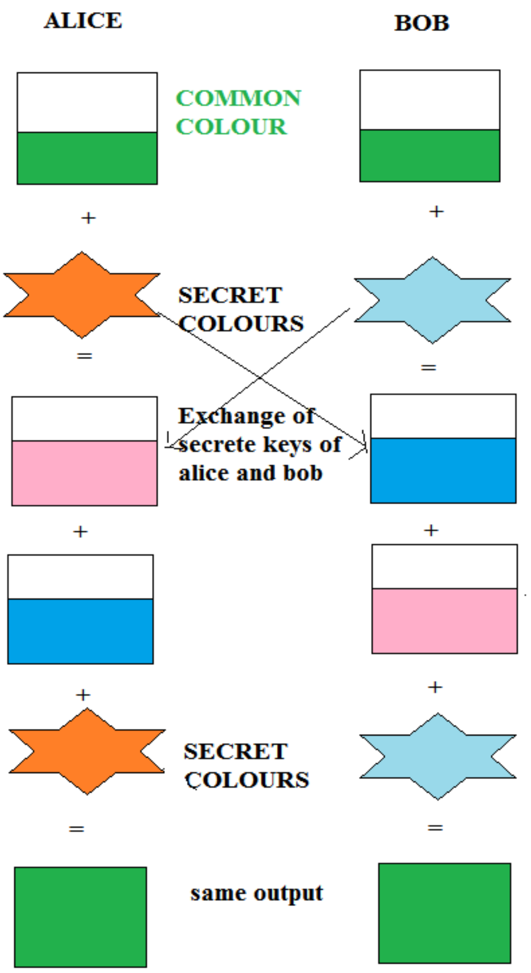

Figure 2: Diffie Hellman Algorithm working.

DOI : 10.18231/2454-9150.2019.0597

V. PSEUDOCODE

```
User sends request to  server for registration
    //the user will enter user name and password and selects the services if  it correct  the user will get registered with server
If(registration==success)
{
 server gives digital signature to user and scpc
Else
User name and password is invalid
}
//If the user want to access with same username and password , he can sign in with out registration  but services cannot be accessed.
If(login)
{
enter user name ,password, digital signature
Else
invalid user name ,password, digital signature
}
User needs to access either FTP or MAIL
If(Key exchange==success)
{
user may access ftp or mail
Else
    error
}
```

VI. CONCLUSION AND FUTURE ENHANCEMENT

We have briefly studied how SSO mechanism helps to gain all the objectives that we have discussed and also different algorithms have been implemented in order to provide proper authentication, soundness and privacy. As a future work it is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed.

REFERENCES

[1] L. Lamport, “Password authentication with insecure communication,” Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[2] W. B. Lee and C. C. Chang, “User identification and key distribution maintaining anonymity for distributed computer networks,” Comput. Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116, 2015.

[3] L. Lamport, “Password authentication with insecure communication,”Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 2014.

[4] W. B. Lee and C. C. Chang, “User identification and key distribution maintaining anonymity for distributed computer networks,” Comput.Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116, 2016.

[5] 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. 2014.

[6] 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.

[7] M. Cheminod, A. Pironti, and R. Sisto, “Formal vulnerability analysis of a security system for remote fieldbus access,” IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 30–40, Feb. 2012.

DOI : 10.18231/2454-9150.2019.0597