Authentification of Certificate in Network by Using Unique Sign-on Algorithm

Dr.Venkatesan[1], Dr.Venkatramana[2], Dr.Karunakar Reddy[3], Dr.Sambasiva Rao[4]
[1,2,3,4] KITS for Women

Abstract- **A computer network is a special category of network, which make possible the users to use different network check which are provided by the check providers. In the distributed computer networks, user confirmation is an important process for protect. In the verification process, the choice is taken whether the user is authorized or illegitimate and subsequent to that allows the users to access the utilities in web. For that we are implemented new process of Single sign-on Mechanism (SSOM) is a new verification mechanism that facilitates an officially permitted user with a single sign in credential to be authenticated by many service providers in distributed computer networks. In additional to the service provider's verification, user verification is also important to avoid bogus servers. The data exchange between a user and a service provider in the completion of the user and service provider verification and a session key is provided to preserve the security in network; that security status has demonstratively shown in this proposal is actually insecure as it fails to convene credential confidentiality and reliability of confirmation. Specifically, we present two different steps of attacks in the system. Main one is attack access a malicious service provider in internet, different types of users may communicate twice in the system. Chang and Lee method is one of the single-sign on mechanism which is obtainable by Chang and Lee for providing security in the distributed computer networks. We recognize the flaws in their protection elements to explain why attacks are possible alongside their SSOM method. Our attacks also related to another SSOM method proposed by Chuang and Hsu, which motivate the design of Chang-Lee Methods. We support the learning of the reliability of authentication as one open problem.**

Index Terms- Distributed Systems, Authentication, Token, Attacks, Sign-On, and Credentials.

I. INTRODUCTION

In Distributed Computer Networks or any client – server networking architecture verifying the legal/authorized user for checking its credentials .In Distributed Computer Networks no use the security analysis mechanism (just like Single Sign On mechanism) That time the authorized user required to login to each application with authorized user id and password within that network . Suppose authorized user will first time login on to one application within a system in the Distributed Computer networks as well he want to access another application that time he again required to login. Due to that reason the authorized user required to login to each and every authentication with user id and password. So to avoid that type of problem there is one mechanism which is called as SSO. SSO mechanisms will allow the users to sign on only once and have their identities automatically verified by each application or service they want to access afterward. If unauthorized user will try to access to login to the account with same user id and password then it avoid that type of unauthorized user.

The Single Sign On (SSO) is one security mechanism by using that mechanism we can provide the facility to the authorized user to login to the system with some credential like authorized user id and password on the Distributed Computer networks. If the authorized user want to login to another system within that Distributed Computer networks that time authorized/unauthorized user got some message like authorized user is logged on to the different system. The authorized/unauthorized person cannot be login to another system till authorized users will first logout from the system where the authorized user was logged in to the previous system. The Single Sign On mechanism also provide some security to your account. Take an example such as one authorized user login to the system by using the Single Sign on mechanism in distributed computer networks. On the same time one unauthorized user is trying to login to the different system with same user id and password that time the authorized user will got message on his logging account is that the unauthorized user is trying to access your account and it will gives some information about the unauthorized user like IP address and name of the system where the unauthorized user is trying to access the authorized user account as well as he also provide the time when the unauthorized user will try for to access the account of the authorized user account.

The main advantages of the Single Sign On are first is Once the user is login to the system there is no need to provide user id and password for authentication of user account. The authorized user will use a single password for the system.

This mechanism will provide another facility like it give info about unauthorized user (like system IP address and system name and time) who is trying to access the authorized users account.

II. RELATED WORK

In distributed systems key exchange concept was introduced in the early years of 2000 for the security purpose in the network and to maintain the authorized people details for the future transaction. There are many attacks in the network; we can check it in any of distributed networks. So to overcome and to provide the security to the users information we are introduced RSA algorithm based content verification and key distribution process in Distributed network for a better security. To maintain number of accounts in network is too difficult for the users in network, in that situation security is main reason to the users so avoid that process and when the hacker or any other person had hacked our profile or the information in the network automatically it's a problem to the valid users to store any of their information in the network. Then they will try to create another account for the personal information and for the security in the network. So to avoid this process of single user maintaining the number of accounts in the network we are used this key sharing process in the network user benefits and as well as to reduce the number of duplicated accounts in the network.

To handle the multiple accounts we are proposed single sign on process to reduce the burden on server as well as for the user to fell his information was secured. Here in this system whenever user has login in account automatically hashing methodology will release a token for the each and every user in the system. Each token will be alive till the user sign out from the network. If user had not signed out on his system in online, he may not login again and single sign on technique will support to the token to keep alive that token till the user sign-out. At that time user can't login with the same credentials in another system, because for that user already a token has assigned and it's still alive in the server. So he has to logout from where he has sign-on in network or any system. That time user will be alert about his account, so wherever he checking his account then he will identify and he will re check his status. Is it alive or sign out from the distributed system?. So users will be alert about their information and accounts when they sign on.

Through the single sign on system user can maintain one authenticated profile in distributed networks. Here user credentials will obtain from the data base if the authentication of user is valid only. In general way security of single sign on mechanism is to provide the security to the user and if we check with the existing process there are two drawbacks they are

1) Sometimes outside users may try to attack and he can get the user valid credential details if he got the random value of the user password and security issues are very less

2) Time stamp has used in the existing system it has processed based on RSA. In general system it was not compatible to the all devices to use in distributed networks.

OPASS- User authentication Technique:

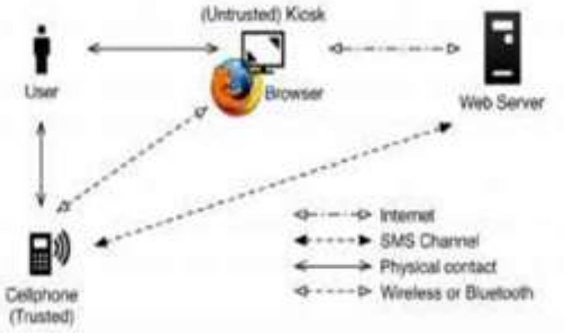

Fig1: User OPASS Authentication Architecture

To avoid the password guessing and hacking techniques in distributed system we are implemented this process. It will be utilized based on the user mobile phones and its authentication process. It will supports the user in the time of registration to provide the large amount of security key to the profiles. That time user will get the short message service on the process user to get his information in the network. Some of the situations we may login in public systems and we may not say exactly security is there for the users data so avoid that fear we are implemented this concept to provide the security to the users. And here we are given permission for the other user also as well as. For that user we are generation an automatic one time password for the user sign on. It will support only one time for the user after that he can enter that password and he can login without any problem in the network.

III. RESULTS

Single Sign-On Mechanism is a security system that provides access for the user as well as security for client-server networking. The main aim of the SSO is the Unauthorized person can't access the system that is present within distributed network .The main reason that why we are using this application is to protect the privacy of the user credential. Encryption and Decryption mechanism is used to transfer the data from the user to the provider (who wants to use). User credential plays a major role to access the control mechanism of the entire application. If one person login into the one system with his own credential then with the same credential the person can't login to the another PC, if the person want to access in to the other system then the authorized person should logout the first system and login to the next system. If the authorized login in one system and the person want to login in to the another system with the same credential then the system will be asking some

Load forecasting helps an electric usefulness to make important selection including selections on purchasing and generating electric load, load switching, and infrastructure development. The meaning of Load forecasting is to forecast the future demand with the help of historical load data available. Load forecasts are highly important for energy suppliers and other participator in electric energy generation, transmission, distribution and market. The accurate forecasting of the load is an essential element in power system security like one time password, or it generates some key at the authorized person if the authorized person provides that password which will receive to the authorized person's mobile number, then the other user can login to the other system. By using this SSO the user can generate only one password to access with the all applications and to avoid the problems from the hackers the authorized person should provide the strong (or) good password such that the hackers can't access the application and it should be very hard to crack and the application should have some time limit for the password to provide access to the provider .If the external person want to use the internal web application without having to add these users to your domain. There is one more major security that the person can know that IP address, System name and time (At what time the person is login and logout).

IV. CONCLUSION

In our daily society there are many applications that are used for our business purpose, so the application which we use in our daily life should be secure because we don't want the user to goes in any application the they need. So here we should have some security for the application here we use SSO. By using this SSO i.e., Single sign-on system web application can help the users to save the time and easy to access. Here only the one person can access the system if other person wants to access then the user should provide some password (or) key to other person to access the application. Finally, It's really complicate for hackers or to crack the password because every time the password is duplicated. This application is used in many areas like hospitals, colleges; software companies in order to reduce our time and that can be easy to access. Finally, I conclude that by using this single-son application we can provide security for the application as well as we can maintain single password for all the applications that reduces our time and increases our speed because only one password that can be shared to the providers to use the application and one of the major advantage is the user can know the IP address, time and name of the system from which system the person is accessing.

REFERENCES

[1] Weaver and M. W. Condtry,“Distributing Internet services to the network’s edge”, IEEE Trans. Ind. Electron., 50(3): 404-411, Jun. 2003.

[2] L. Barolli and F. Xhafa, “JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing”, IEEE Trans. Ind. Electron., 58(6): 2163-2172, Oct. 2010.

[3] L. Lamport, “Password authentication with insecure communication”,Commun. ACM, 24(11): 770-772, Nov. 1981.

[4] Chin-Chen Chang, “A secure single mechanism for distributed computer networks,” IEEE Trans. On Industrial Electronics,vol.59, no. 1, Jan 2012.

[5] W. B. Lee and C. C. Chang, “User identification and key distribution maintaining anonymity for distributed computer networks,”Computer Systems Science and Engineering, 15(4): 113-116, 2000.

[6] W. Juang, S. Chen, and H. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind.Electron.,15(6): 2551-2556, Jun. 2008.

CONFIRMATION CERTIFICATION IN NETWORK BY USING UNIQUE SIGN-ON METHODOLOGY

Author 1:

Chinnala Balakrishna M.Tech (CSE) from Madhira Institute of Technology and Science, JNTUH and B. Tech (IT) from Nagarjuna Institute of Technology and Science, JNTUH . He has more than 8 years of experience and guided UG & PG students, currently he is working as Asst Prof at SRTIST Engineering College. His research areas include, Computer Networks, Cloud computing, Network Security, Software Engineering.

Author 2:

Prabhakar Marry M.Tech from RRS College of Engineering, JNTU B.Tech IT from SRTIST Engineering College. He is having more than 8 years of experience has guided UG & PG students, currently he is working as Asst Prof at SRTIST Engineering College. His research areas include Software Engineering, Computer Networks, Cloud computing, Design Analysis of Algorithms, C & Data Structures.

Author 3:

Shepuri Srinivasulu M.Tech from IIT Madras B.Tech CSE from SRTIST Engineering College. He is having more than 3 years of experience has guided UG & PG students, currently he is working as Asst Prof at SRTIST Engineering College. His research areas include Software Engineering, Computer Networks, Cloud computing, Design Analysis of Algorithms, C &Data Structures.