ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 143-147 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Presumable Study of Single Sign-on Technique for Distributed Network Systems

GurralaVenkataMohana Sai[1]Dr P.Harini[2]

[1]M.Tech Student, Dept of CSE, St. Ann's College of Engineering Technology, Chirala, PrakasamDist, A.P, India

[2]Professor&HOD, Dept of CSE, St. Ann's College of Engineering Technology, Chirala, PrakasamDist, A.P, India

Abstract: - **In this paper we are impediment-ed a new concept for the network users and all the people to providing the security in there networking sites and there organization as well as now even we are pen our network some one in that place may try to hack our details with the same name of the user so to stop that process we are involved a new concept that is Presumable Study of Single Sign-on Technique for Distributed Network Systems so through this method we may can stop these type of issues in further and if in-case we are forgot to gout in the website it intimates us to log-out first where are log-in and then we can simply recognize where we forgot t log-out and we may educe the hacking chances and stop the others may not done miss usage with the same credentials f users. Here we have two types of problems are there in normal system i.e, "Credential Recovering Attack" and"Impersonation Attack without Credentials" so in this paper we can solve these both problems and after log in user also we are providing a signature to the user based on that signature only user can send and receive the files and messages when he sending to the someone else in that network area**

Keywords: - *c*redentials, networking, authentication.

I INTRODUCTION

We are employing a new way of mechanism that is the single sign in for the distributed systems we are implemented. We are analysis that the users facing problems in social network for the authentication in general many users are facing the problem how to protect their data from an un authorized persons in social networks and they are facing the attacks mainly two types that has described in as follows and they are trying to get new accounts because of that information was know by the others and trying to change password every time like this things users facing and after that also they are facing the security to their data Now a days users have the many ways of accessing of network and users may not know where to access the data and with the which credential users using also for all that of the user interface transaction of data and modification process of thing are done in wild area of network and some of the times users may forgot the thing to sign-out like the things in some f the areas so to avoid this we make it as a single log-in process so that all the things has described as below and we are provided security to the users data an authentication signature for every user when he will register in network and how ever we are checking in network areas and for the protection users data in network we need basically three types of the credentials they are as follows one is instance name and second is credential privacy in network and finally soundness through these we are providing security to the users and as well as we are maintaining their details in a secured manner.

In previous it was started as an SSO scheme with user anonymity. Later, it mentioned as a pointed out that in first implementation there was a problem from masquerading attack and identifying disclosure attacks. In Meanwhile, Yang showed that how we cannot preserve credential privacy and either since a malicious services also can recover the users credentials, and then we proposed and implemented to overcome this limitation. And that can be described on this page for the better performance of user details and data security demonstrated schemes have not provided user anonymity since their schemes are vulnerable to identity disclosure attacks. To prevent such attacks,

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 143-147 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

this can help the users and simply the usage of networks instead of using the multiple user-id and password in the network areas so this application can move friendly with the users

In this paper we present a normal model to define authenticated single key exchange of single sign-on scheme and its requirement is security mainly. and we list the components of data as well as define correctness, and describe an adversary model for the formally specify of security properties, including the secure credential of user authentication details , secure credential services provider authentication details, and finally session key security.

In the authentication process we are using a session password and a session of user signature details mainly this signature can perform main role and it's a unique to every user and through this we are implementing the security process and generating key t the use data whenever he is sending some information to the users and his fellow relation people. The main disadvantage in previous system is The above definition mainly focuses on public key it's based on AKESSO with the non-interactive proofs of users. And it could be extended to support the interactive proofs, where as we are generation persona key and signature like. However, the defining symmetric key is based on AKESSO rule and it will be another story to do farther implementation

In the present architecture if we check then the problem that we can see that the encryption technique used for securing log-in credentials of the user is through the mechanism of symmetric key algorithms where in the problem will not get solved completely there could be a chance that the intruders can try to decode the data and reveal the credentials of the user which is not being a secure system. Apart from this there is a one more problem in the existing system which is that a intruder can log-in to the application even without the credentials which actually refers to the SQL Injection.

In this paper we are introduced a key change ex changer and secured single sign-in manner for to providing the security to the users data and information and maintaining it's as a unique data.

II. PROPOSED WORK

In this system which is being designed will overcome the two problems that an existing system has in it i.e. first being the credentials of the user being accessed even though the encryption technique is used and second being the problem of accessing the user data even without the proper log-on credentials of the user. So in the proposed system we are going to employ the technique of Random 4 encryption technique to provide security to the user data and to the application. Secondly we are going to overcome the problem of SQL Injection in the designed application means that we are going to design the system where if the user tries to access the data from the application without proper credentials the user cannot access it's in this paper we present a normal model to define authenticated single key exchange of single sign-on scheme and its requirement is security mainly. and we list the components of data as well as define correctness, and describe an adversary model for the formally specify of security properties, including the secure credential of user authentication details , secure credential services provider authentication details, and finally session key security.

In this session we presents a single sign-in system for user anonymous for the remote user authentication in networking systems. Here we are using signature it helps the users to get information and details about another person and in previous system it doesn't have any user credential information viewing to the others and it doesn't have any sign and sound signature for the providing information. But here in proposed system it have a single private key to every user who ever registered in distributed networking systems and it helps the user after the registration and to send messages or files to the other users after signing to there profile it should have minimum number of fixed key it will generate a key to protect the users data and to send an encrypted data to the receiver when we send an encrypted data to the other user and in this place we are providing security to the uses data and all the information whatever send by the sender it will send an encrypted format after message reaches to the receiver he should need to enter the users personal key if he enter only the message can be visible to the recover otherwise it's can't be shown the receiver then we can identify

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 143-147 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

that the user and as well as we can provide the security the user data if he/her is an authenticated person they can open it and they can access the data without any doubt if he/her is not an authenticated that message should be in a protection mode like this we are providing the security to the users data from the attacks like this we are providing the security to the users data form an UN-authorized persons to save the user information for this we are using the DES algorithm to encrypt in-sender side and as well as in receiver side. In this the session key will generate by the time of sending a message to the others and information

Data Encryption Standard (DES) is a cryptographic standard that was proposed as the algorithm for the secure and secret items in 1970 and was adopted as an American federal standard by National Bureau of Standards is in 1973. DES is a block cipher text mode, which means that has work in during the process of encryption, the plain-text is broken into fixed length of blocks and each block is encrypted at the same time of block division. Normally it takes the 64-bit input plain text and it's key be 64-bits (here we are using 56 bits for the conversion process and reaming bits are used for the parity checking process) and it produces a 64-bit cipher text by encryption form and which can be decrypted to get the message using same key. Additionally, here we must highlight that of four standardized modes we have in DES operation: ECB (electronic code**b**ook mode), CBC (cipher block chaining mode), CFB (**C**ipher **F**eed-**b**ack mode) and OFB (**O**utput **F**eed-**b**ack mode). The normal depiction of DES encryption algorithm is which consists the initial permutation of the 64 bit plain text and then goes through 4 rounds, where each round consists permutation and substitution of the text bit and the inputted key must be in bits format, and at final it goes in a inverse initial permutations to gets the 64 bit key cipher text.

By using this we are providing security to the users data and as well as we are generating a new key for the shared no other one else and that key will generate based on the user signature it will randomly generate the key it will helps the users to get the information about content. For the process mainly we have two theorems it will described in bellow, through that we can clear all the doubts of this page.

Theorem1. (Secure Services Provider Authentication) In proposed system, if there is any PPT adversary for who has a non-negligible advantaged AdvSSPA(AO) as we declared in above definition session then signature of an employee by the service providers is existentially forgo-table under UFCM Attacks defined in this paper.

Proof: Since the previous session we know that the key will generate autocratically but here we are proposed a new a way of making a signature in the sight of users when ever they register in to the distributed systems and to apply that signature we are using to generate the key and to implement the process of implementing and providing the security to the users data and encrypted information also it will support based on the above definition.

Theorem2. According to Definition the proposed AKESSO scheme is secure under the assumption that all digital signatures employed in the scheme are existentially Unforeseeable against UFCMA attacks as specified in above.

Proof: In this above part we are discussed about how we are providing the security to the data and how we are creating key to t the data that everything is based on total we are considered from the above theorem we are discussed and introduced that methods we are followed to impairment the bases of that definitions. Through that we are implementing and providing the security to the data what were user sharing and sending to the other persons and how it all that things are implemented in this definition.

In this paper by using this theorems we are implemented it's as a user friendly and to providing security from the two attacks users mainly facing in general situations in the networking sites and after in the final user can get the key from the person by using the sender signature

III. RESULTS

In this application which is being designed will overcome the two problems that an existing system has in it i.e. first being the credentials of the user being accessed even though the encryption technique is used and second being the problem of accessing the user data even without the proper log-on credentials of the user. So here in this

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 143-147 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

application we are implemented a new technique to over come these problem and we are getting the users whoever registered in that site and we can send any information to the users whom we want to send and as that of the process we are encrypting and sending the data for to view the data whatever sender send to receiver he need the signature of the user if he don't know the signature he can't git that message or file data after enter the sender signature only receiver can get the original content file which and one more technique we are implemented as if the user log-in any one of the system in network area if he forgot to log-out that and again he came to log-in another system it's not possible to the users or if user log-in one system at that time if some one try to hack and if he try to open others profile he can't able to open that page like that we are providing security to the users based on their profile credential details and that networking IP addresses based through these ways we are providing security to the users data and as well as their cred-entail information through this we can stop the users may not need more user-id and more accounts in network areas and through this users can stay freely and without tension and no more of attacks in network location and as well as the security to the data whatever user send to receiver like this all things we are provided in this paper for the user to get more closer in the network.

CONCLUSION

In this paper we implemented a concept of single sign-on for the network users and here we are provided a security to the users and in this we are implemented a new way of stopping the attacks in the network area and to provide the user friendly in networking systems here we are implemented a network IP address basing concept and so in that if the user had forgot to log-out in that network area he cont able to log-in again in that same area and we are given a credentials of user authentication process of key generating based on the signature and communication between the both users by implementation of the user signature based on the user identification of signature and user profile information we are implemented the process and we are stopping the other users to log-in and miss use f user data like these security we are providing in this paper. And as well as we are provided security the user data whatever he send to another person in network location and that has to be send an encryption form then after receiver receives the message from the sender he must need the signature of the user by a normal communication way like if he doesn't know it can't be download and like this we are providing in a two ways systems in this application for the user comparable and security in network

REFERENCES

[1] A. C. Weaver and M. W. Condtry, "Distributing Internet

Services to The Networks Edge", IEEE Trans. Ind. Electron.,

vol. 50, no. 3, pp. 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., vol. 58, no. 6, pp. 2163-2172, Oct. 2010.

[3] L. Lamport, "Password Authentication with Insecure Communication", Commun. ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.

[4] F. Bao, R. H. Deng, "Privacy Protection for Transactions of Digital Goods", Proceedings of the Third International Conference on Information and Communications Security (ICICS '01), Springer-Verlag, London, UK, pp. 202-213.

[5] G. Wang, J. Yu, and Q. Xie, "Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks", IACR Cryptology ePrint Archive, Report 2012/107, http://eprint.iacr.org/2012/107.

[6] W. B. Lee and C. C. Chang, "User Identification and Key Distribution Maintaining Anonymity for Distributed Computer Networks", Computer Systems Science and Engineering, vol. 15, no. 4, pp. 113-116, 2000.

[7] T.-S.Wu and C.-L. Hsu, "Efficient User Identification Scheme with Key Distribution Preserving Anonymity for Distributed Computer Networks", Computers and Security, vol. 23, no. 2, pp. 120-125, 2004.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 143-147 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

GurralaVenkataMohana Sai received the **B.Tech(CSE)** from JNTU Kakinada, in 2012 & pursuing his M.Tech in Computer Science & Engineering from JNTU Kakinada.

Dr. P. Hariniis presently working as a professor and HOD, Dept of Computer Science and Engineering, in St.Ann's College of Engineering and Technology, Chirala.She obtained **Ph.D.** in distributed and MobileComputing from JNTUA, She Guided Many UG and PG Students. She has More than **18** Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and **25** Research Oriented Papers in Various Areas. She was awarded **Certificate of Merit** by JNTUK Kakinada on the University Formation Day on 21 - August - 2012