International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 17 Issue 2 – SEPTEMBER 2015.

A PRIVACY ENHANCED SECURITY STUDY OF A SOLITARY SIGN ON MECHANISM FOR DISTRIBUTED COMPUTER NETWORKS

[#1] P.Venugopal, [*2] S.Sravani

[#1]*PG Student, Dept. of CSE, St.Mark Educational Institution Society Group of Institution, Affiliated to JNTUA , Andhra Pradesh, India*
[*2]*Assistant Prof , Dept. of CSE, St.Mark Educational Institution Society Group of Institution, Affiliated to JNTUA, Andhra Pradesh, India*

***Abstract* —Credential of the technology is missing in the recent system. So, to improve the authentication of the distributed networks or multiple applications we are making use of a single sign on mechanism. Previously, users were using n number of usernames and passwords to access different applications on network. This would lead to higher expense for the administrator as each and every account of the organization will be handled with their particular username and password. But, now user needs to remember just single secure credential to access the multiple service providers in a distributed network by using single sign-on mechanism. However, most existing systems which are using this mechanism have some disadvantage regarding security requirements. So through this paper we will discuss about the development of security from earlier stage to present stage. And also discuss about the structure of the mechanism's working strategy.**

Keywords: Single sign-on, Distributed system and Privacy.

I. INTRODUCTION

User identification plays key role in distributed networks to verify the user is legal or not and can therefore grant access to distributed service providers . To avoid illegal user accessibility to the services we need proper user authentication . After mutual authentication between the user and the service providers, a session key should be negotiated to keep privacy of the data have exchanged. It is difficult to remember the password with user identity which is required to access each service provider in the network. Hence, Single sign-on mechanism was proposed so that user with single credential can be authenticated by multiple service providers. Single sign-on mechanism should meet two basic security requirements that is, credential privacy and soundness. Credential privacy guarantees that illegal service provider should not be able to fully recover a user's credential and then impersonate the user to login other service providers. Soundness means that unregistered user should not be able to access the services provided by the service providers . This paper aims to provide the enhanced security from the previous stage to present stage. The Distributed Computer Network several users and several service providers. It allows all users to access multiple services provided by service providers. User authentication isb also play important role in the Distributed System for identifying legal user and provides service to them. To avoid non-existent user or malicious servers we need authenticate the service providers. After authentication, session key play important role to keep data confidentiality

when data transaction in between user and service provider. In that process legal user anonymity is impotent to protected. Usually, it is not practical a user maintain different identity and password for multiple services that is increasing `workload of users and service providers. To overcome this problem, the single sign-on mechanism has been proposed so that, after receiving a credential from a trusted authority.

In this paper, System implementing the Chang–Lee scheme are insecure by proposing two types attacks, first one is credential recovering and second one is malicious user without credentials.
In first one, a malicious service provider who communicates with the user twice can recover the credential of that user and user this credential to access services and resources behalf of user. The second one is non-existent user impersonate legal user and act as user, since without having valid credential access the services and resources. These attacks that mean the Chang–Lee Single Sign On scheme failure to provide credential privacy and soundness, which are important requirements of SSO scheme. To implement these disadvantage of SSO, we propose enhance scheme for user authentication. We employ RSA with the encryption of signatures to verifiably encrypt credential. Signature with the RSA enhances the security. On the other side, it is usually not practical by asking one user to maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, the single sign-on (SSO) mechanism as been introduced so that, after

obtaining a credential from a trusted authority for a short period (say one day), each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., *unforgeability*, *credential privacy*, and *soundness*.Unforgeability demands that, except the trusted authority, even a collusion of users and service providers are not able to f valid credential for a new user. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Formal security definitions of unforgeability and credential privacy.

II. RELATED WORK

In 2000, Lee and Chang proposed a user identification and key distribution scheme to maintain user anonymity in the distributed networks. Later, Wu and Hsu pointed out that the Lee and Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. identified a weakness in Wu-Hsu scheme and proposed for improvement. In 2006, Mangipudi and Katti pointed out that Yang et al. scheme suffers from Denial of Service (DoS) attack and presented new scheme. In 2011, Hsu and Chuang showed Yang et al. and Mangipudi – Katti scheme were insecure under identity disclosure and proposed an RSA based user identification scheme to overcome the drawbacks. Hence, Single Sign-On mechanism was introduced and presented so that user can remember single username and password for the distributed service providers. A similar concept, called the Public/Private key was proposed to provide user identification and key agreement to access all applications.
When user registers, then with all the details it gives IP address, which is accepted if not occupied by other users. Administrator will have all the details regarding the IP. Administrator will then allocate different IP to all users. And according to it users will be bonded in the network. Registered users will have their own specific IP address which will be accessed by themselves. When registered user will send some message to the service provider it will change into encrypted signature which will have public key and to prove the service provider's identity, the service provider will verify and decrypt through the private key which he has. While registration, users will use special type of password which will have specific pattern. That special pattern will have Zero knowledge identity (ZKI) . With the complex password and public/private key the system will have credential users and privacy. Soundness will obviously be satisfied by the user by entering valid pair of username and password that is registered and maintained by the server. Third party will not be able to login as they are illegal to the application. As, he/she is not registered to the application, so credential forgery and recovery attacks from outsiders, users, service providers and potential collusion of them will not be possible.

There are many works in the literature that deal with key based security, among them Lee et al in proposed a new authentication scheme with anonymity. This scheme provides an enhanced security, backward secrecy, mutual authentication and protection against forgery attack. This scheme is simple and efficient .Ku W.C and Chen S.M in made improvements in providing efficient password based on user authentication scheme using smart cards. This scheme solves the reflection attack and insider attack. This scheme faces difficulties in maintaining the random numbers in the user smart cards. Buouyoucef and Khorasani in focus on robust distributed congestion control strategy for differentiated services network. With this scheme, calculating the control algorithm for each node is very difficult. Sun D.Z et al in proposed a new protection mechanism using a password, authentication key agreement scheme for smart cards.
This scheme overcomes the weakness and also maintains the benefits .In this scheme, protection against unauthorized data such as deletion or insertion is provided. But performing this task was very difficult.Lee W.B and Chang C.C in proposed a user identification protocol that provides session key establishment and user anonymity for distributed computer networks. This paper solves all the possible attacks Rafael Tonicelli et al in proposed a framework for secure single sign on with the proxy signature schemes. It provides a framework that handles both session states across this multiple services and granular access control. This is the first approach and secures single sign-on security on public key cryptography. It is an open problem to obtain a session state and access control protocol that remains secure if the adversary is given control of the user's computer. Yanjiang Yang et al in proposed a new efficient user identification scheme and key distribution for providing security. This scheme overcomes the drawbacks .It has shown the efficiency in terms of communication and computation by performance analysis. Comparing with all the works present in the literature the work implemented in this project work is different in many ways. It uses a one-way hash function, new nonce and efficient encryption techniques. Hence it uses tokens for validation. To tackle this problem, single sign-on (SSO) mechanism has been introduced so that after obtaining a credential from a SCPC, each legal user can use this single credential to authenticate itself and then access multiple service providers. Instinctively, an SSO scheme should meet at least two basic security requirements, soundness and credential privacy. Soundness is an unregistered user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees that malicious service providers should not be able to fully recover a user's

credential and then impersonate the user to log in other service providers. Formal security definitions of Single Sign-On schemes. Chang and Lee made a careful study of Single Sign-On mechanism. Firstly, they claimed that Hsu-Chuanguser identification scheme, essentially an Single Sign-On scheme, has two weaknesses:
(a) An outsider can forge a valid credential by mounting a credential forging attack since Hsu- Chang scheme employed naive RSA signature without any hash function to issue a credential for any random identity selected by a user and (b) Hsu-Chuang scheme requires clock synchronization since timestamp is used in their scheme. Then, Chang and Lee proposed stimulating RSA based Single Sign-On scheme, which is highly efficient in computation and communication, and does not rely on clock synchronization by using nonce instead of timestamp. Finally, they proposed efficient security analysis to show that their SSO scheme supports secure mutual authentication, session key covenant,and user privacy.

III. PROPOSED WORK

The steps involved in this process are Creating and Deploying services, Token Formulation, Authentication and Validation, Attack avoidance, reprocessing data using slicing techniques, Encrypt data is hidden in to an image using image as a secret key, Decrypt a hidden data obtained from an image using same image as a secret key, Retrieval data using reshuffling techniques.

3.1 Creating and Deploying Service It creates at least three applications for the users with the authentication facility. The developed applications will be imported to the local server. From that server the users will access the desired application as their need. Applications are imported separately but stored in the same local server. For each application separate login for the user will be created and maintained in the database.

3.2 Token Formulation
The token will be generated by the RSA crypto system algorithm and it will be given to the user for the other login purpose. Other application will be accessed by the token itself. The token will be generated by the algorithm each token will be unique.
3.3 Authentication &Validation The token will be buffered in the server for the identification of the user the token will be checked by the BAN logic it will check the message freshness, trustworthiness the authenticated key approach protocol will be called for the validation.
3.4 Attack Avoidance The attacks like brute force attack will be avoided by the session period termination the token will be expired after the termination of the session period so that the attacks will be avoided wrong passwords entered by a person will be saved on the database.

3.5 .Pre-processing Data using Slicing Techniques The user data initially undergoes a process called slicing techniques. After slicing the data, where sliced data are shuffled. It has to be done by using shuffling procedure. Slicing partitions the data. It preserves the data utility than other existing schemes. Slicng can be used for preventing Information disclosure based on the privacy requirement of l-diversity. It can handle high dimensional data. After slicing the data, where sliced data are shuffled By partitioning user data in to array of characters, slicing reduces the dimensionality of the data. Each data can be viewed as a sub-data with a lower dimensionality. So it can able to handle high dimensional data. 1. Get the data from an authenticated user. 2. Initialize the variable b as a string. 3. Assign the variable b is equal to the user data. 4. Partitions the data in to array of characters and partitioned data is stored as an array. 5. Count the number of characters in the given data. 6. Assign the variable n is equal to number of characters present in an array.

3.7 Encrypt Data is Hidden in to an Image using Image as a Secret Key The shuffled data initially undergoes a process called encryption. After encryption process, where the encrypt text is splitted up and using LSB algorithm the data is hidden in to an image and this process is done by using image as a secret key, then the resultant image is stored in a different database.
3.8 Decrypt a Hidden Data obtained from an Image using same Image as a Secret Key

During the process of decryption, the stored data from a different database is accessed and integrated. Then the integrated data finally undergoes a process called decryption.
3.9 Encryption and Decryption-:

ElGamal Public key encryption algorithm is used for the encryption and decryption between user and the provider. The
ElGamal Algorithm provides an alternative to the RSA for public key encryption.
1. Security of the RSA depends on the difficulty of factoring large integers.
2. Security of the ElGamal algorithm based on the difficulty of computing discrete logs in a large prime modulus Data which is send from each provider to user is encrypted and send to user, then user decrypts it and the original data is regained. All these encryption and decryption are done using Elgamal Public key encryption algorithm. This implemented in Java using socket programming and it uses server programs and client programs. We can run the providers parallel byusing multithreading features of Java. Elgamal has the advantage that the same plaintext gives a different Cipher text each time it is encrypted. The ElGamal Algorithm provides an alternative to the RSA for public key encryption. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime

modulus. ElGamal has the disadvantage that the cipher text is twice as long as the plaintext. Elgamal is quite slow.

ElGamal:

To overcome the drawback in the Chang-Lee scheme , we propose an improvement by implementing ElGamal Public keyencryption algorithm.
Elgamal comprises two users. In Elgamal,

☐ Each user has a private key x

☐ Each user has three public keys: prime modulus p, generator g and public Y = gx mod p

☐ Secure key size > 1024 bits (today even 2048 bits)

☐ Elgamal is quite slow; it is used mainly for key authentication protocols

Say Alice and Bob is two user, Prime p and generator g are public keys of Bob, Alice chooses the random key k, Bob chooses random x, then bob calculate Y as Y = g x mod p and send it to Alice, Alice then calculate K as K = Y k mod p,From the k and K Alice calculate the two cipher c1 and c2,C1= g k mod p and C2=M K mod p. and two users, say Alice and Bob. The basic idea of VES is that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses a no interactive zero-knowledge (NZK) proof [35] to convince Bob that she has signed the message and the trusted party can recover the signature from the ciphertext.After validating the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice should send her signature in plaintext back to Bob after accepting Bob's signature. If she refuses to do so, however, Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

Credential privacy or credential irrecoverableness requires that there be a negligible probability of an attacker recovering a valid credential from the interactions with a user. Again this property can be deduced from the signature hiding property of RSA-VES, defined as the third property of Definition. Signature hiding means that an attacker cannot extract a signature from VES without help from the user who encrypted the signature or the trusted authority who can decrypt a VES. So, if this improved SSO scheme fails to meet credential privacy, it implies that Ateniese's RSA-VES fails to satisfy signature hiding, which is contrary to the analysis .In fact, soundness and signature hiding are the two core security properties to guarantee the fairness of digital signature exchange using VES. More rigorous security proofs are interesting topics for further study by considering formal definitions first.

IV. CONCLUSION

In this project work, a secure single sign-on mechanism for distributed computing security environment has been developed to overcome the possible attacks by using cryptographic one-way hash function and random nonces. We have used the AES algorithm for encryption and decryption and BAN logic analysis for validate the token for freshness .

In order to provide a high level of security a technique slicing has been introduced. After slicing the data, where sliced data are shuffled. It has to be done by using shuffling procedure. In addition to slicing the data, the encrypt data is hidden in to an image. This process is done by using image as a secret key and original data will obtain by using same image as a secret key. Further works in this direction can be proposed and implementation of key management schemes to provide effective security.

REFERENCES

[1] A. C. Weaver and M. W. Condtry, "Distributing internet services to the network's 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] 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, 2000.
[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. 2008.
[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. 2011.
[8] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," *IEEE Trans. Ind. Inf.*, vol. PP, no. 99,2012, DOI 10.1109/TII/2012.2198666.
[9] T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks,"*Comput. Security*, vol. 23, no. 2, pp. 120–125, 2004.
[10] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," *Comput. Security*, vol. 23, no. 8, pp. 697–704, 2004.
[11] K. V. 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, 2006.
[12] 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, 2009.
[13] B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 689–696, Aug.2012.