SINGLE SIGN-ON MECHANISM FOR DISTRIBUTED COMPUTING SECURITY ENVIRONMENT

K.karthika[1], M. Daya kanimozhi Rani[2]

[1]K.karthika, Assistant professor, Department of IT, Adhiyamaan College of Engineering, Hosur
[2]M. Daya kanimozhi Rani , Associate professor ,Department of IT, Adhiyamaan College of Engineering, Hosur

Abstract

The rapid development of the distributed networks, made the work of sharing the information with large number of people easily. Nowadays distributed networks provide lots of computational resources, reliability, scalability and price to performance. It is useful for so many applications such as telecommunication networks, distributed database etc. Especially it plays a vital role in network file system. In distributed networks the different service providers provide the resources in a very efficient and convenient manner. But the user must register with each service providers, for accessing the resources they have different identity/password for accessing each service provider. Recently some user identification schemes have been proposed but it has some drawbacks. The user will have so many secret information, the security problems can occur and it also increases the overhead of the network. The proposed scheme overcome these challenges by providing a user friendly environment and also enables the security policy by using secure single sign-on mechanism. It is done by using cryptographic hash function and random nonce's. This proposed scheme is unable to protect the information disclosure during encryption and decryption of data. In order to provide a high level of security a technique slicing has been introduced. 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.

Key Words: *Distributed networks, Security, Slicing, Random nonce's, Cryptographic hash function etc..*

----------***----------

1. INTRODUCTION

The aim of this project is to develop a secure single sign-on mechanism for distributed networks. To make the existing distributed system performs in an efficient, convenient manner and too overcome several possible attacks. In any client/server relationship, sign-on is an authentication process that permits multiple applications. But in the existing user identification schemes, it fails to protect the user from several possible attacks and also required time synchronized mechanism. We have proposed a secure single sign-on access control mechanism for client/server networks to enable the users to login quickly and securely to multiple applications such as websites with just a single identity. In this mechanism, the user can login once for every domain and it also provides only one password which makes it very secured and easy to access the resources from different service providers. It also provides integrity, availability authentication and access control. It could be done by using one way hash function with random nonces.

We have proposed a secure single sign-on access control mechanism for client/server networks to enable the user to login quickly and securely to multiple applications such as websites, mainframe session with just a single identity. In this mechanism the user can login once for every domain and it also provides only one password which makes it very secured and easy to access the resources from different Service providers. It also provides integrity, availability authentication and access control.

2. RELATED WORKS

There are many works in the literature that deal with key based security [1][2][3], among them Lee et al in [1] 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 [2] 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 [3] 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 [4] 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 [5] proposed a user identification protocol that provides session key establishment and user anonymity for distributed computer networks.This paper solves all the possible attacks

but it does not have formal security. Wu T.and Hsu C.L in [6] proposed another scheme that overcome the drawbacks of the scheme in [5].This scheme solves the masquerading attacks but it could not protect the users token against a malicious service. Yang et al in [7] proposed an enhancement to prevent the previous attacks types and to prevent the denial of service attacks. Lee in [8] proposed a user identification scheme that generates a secret token to solve the issues of the schemes proposed in the literature but solve the issues of the schemes proposed in the literature but katti R.S in [9] proposed an enhancement that prevents denial of service attacks but it is vulnerable to identity disclosure service attacks.Hsu C.L and Chuang in [10] proposed a novel user identification scheme with key distribution preserving user anonymity for distributed computer networks. scheme overcomes the drawbacks of [7] and [9].It prevents the identity disclosure attacks, but it does not provide all of the security problems. Phillip Rogaway et al in [11] proposed an entity authentication and associated problems key distribution. It solves problems of entity authentication and key distribution in distributed computing environment. Rafael Tonicelli et al in [12] 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 [13] proposed a new efficient user identification scheme and key distribution for providing security. This scheme overcomes the drawbacks [6].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.

3. 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.

3.6 Shuffling

After slicing, where sliced data undergoes a process called shuffling. It has to be done by using loop.
1. Initialise the variable i as an integer value
2. Initialise the variable z,w,x,y,z as a string.
3. Assign the variable n is equal to the number of characters.
for i in 1:n loop
//Check Condition using if loop if i% 3 == 0 then
z :z +b[i-1];then i :=i+1
end if

//check condition using if loop
if i % 3 == 1 then
y : y + b[i-1]; then i : = i +1; end if
if i % 3 == 2 then
x : x +b[i-1];then i : = i + 1;
end if end for
end shuffling.

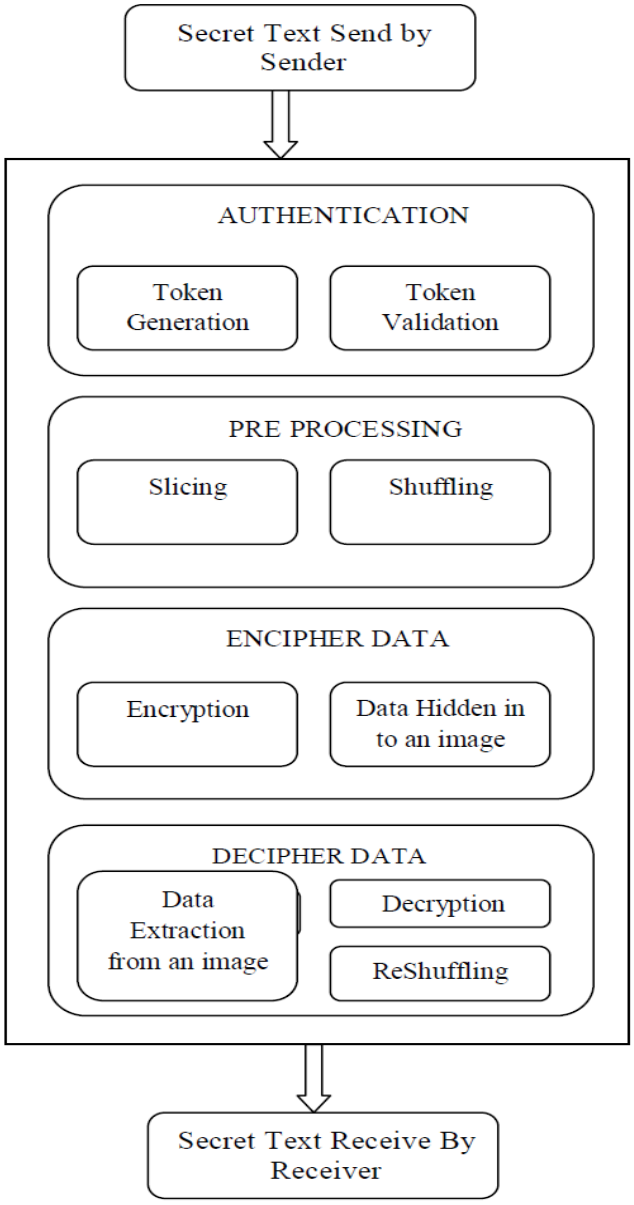

Fig -1: Overall Architecture

The user input data initially undergoes a process called slicing ,where the sliced data are shuffled followed by encryption .After encryption ,encrypted data is hidden in to an image using image as a secret key, then the data is splitted up and stored in a different database. For retrieving data, the data is accessed from a different database and the data is to be integrated. After integrating the data, hidden data is obtained from an image using same image as a secret key. It has to be done by using LSB algorithm. Hidden data undergoes a process called decryption, where the decrypted data are reshuffled and finally the data is collected and formulated.

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 Retrieval of Original Data

Decryption is followed by reshuffling and finally the original data is collected and formulated.Reshuffling has to be done by using reshuffling procedure.

Initialise the variable p is equal to the append of x, y, z values as string.

Initialize the variable n is equal to the number of characters in a string variable p.

Initialise the value g, t, o, l as integer g=n%3;
t=n/3;
o=t*3;
for i in 1 : t loop
l : l +w[i] + r[i] + q[i];
i : i+1;
end for end
//Check condition using ifloop if g == 1
l : l + w[t];
end if
if g == 2
l : l + w[t];
l : l + r[t]; end

4. EVALUATION PARAMETERS

In our proposed scheme, we will compare the communication cost and computation cost of our proposed scheme with four other related schemes.

4.1 Computation Cost

The evaluation parameter of computation cost is time complexity. Based on the evaluation we conclude that our proposed scheme is more efficient has lower energy consumption than the other schemes.

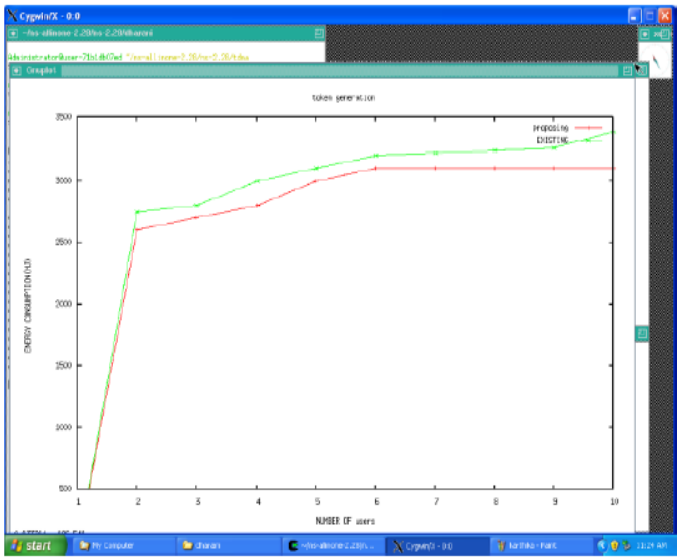

Fig -2: Computation Cost

From the Figure 2 it has been observed that the computation is reduced in the proposed scheme when it is compared with the existing scheme. This is due to the fact that the number of calculations required is reduced in this proposed scheme.

4.2 Communication Cost

We consider some assumption to compare the communication of our proposed scheme with four other related schemes.

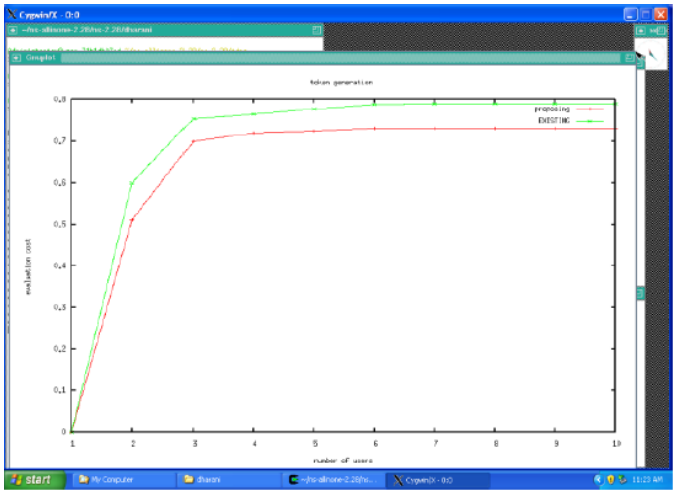

Fig -3: Computation Cost

From the Figure 3 it has been observed that the communication is reduced in the proposed scheme when it is compared with the existing scheme. This is due to the fact that the number of validation required is reduced in this proposed scheme.

5. CONCLUSIONS

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]. C.C.Lee,M.Hwang and I.E.Liao,"Security Enhancement on a new Authentication Scheme with anonymity for wireless environments,"IEEE Transaction on Industrial Electronics, vol.53, no.5, pp.1683-1687, October.2006.

[2]. W.C.Ku and S.M.Chen,"Weakness and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transaction on Industrial Electronics, vol.50, no.1, pp.204-207, February.2004

[3]. K.Bouyoucef and K.Khorasani,"A Robust distributed congestion-control strategy for differentiated services network,"IEEE Transaction on Industrial Electronics, vol.56, no.3, pp.608-617, March .2009.

[4]. Z.Y.Feng,"Improvements of Juang's password-authenticated key agreement scheme using smart cards," IEEE Transaction on Industrial Electronics, vol.56, no.6, pp.2284-2291, June .2009.\

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

[6]. T.S.Wu and C.L.Hsu,"Efficient user identification scheme with key preserving anonymity for distributed computerNetworks,"ComputerSecurity,vol.23,no.2,pp.120-125,March.2004.

[7]. Y.Yang,S.Wang,F.Bao, J.Wangand R.H.Deng,"New efficient user identification and key distribution scheme providing enhanced security," Computer Security,vol.23,no.8,pp.697-704,December.2004

[8]. C.C.Lee,"Two attacks on the Wu-Hsu user identification scheme, "International Journal on Network Security, vol.1, no.3, pp.147-148, November.2005

[9]. K.Mangipudi and R.S.Katti,"A Secure identification and key agreement protocol with user anonymity(SIKA),"ComputerSecurity,vol.25,no.6,pp.420-425,September.2006.
[10]. 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, February.2009
[11]. Minir Bellare,Phillip Rogaway,"Entity Authentication and key distribution advances in cryptology, Lecture Notes in Computer Science.,vol.773,pp.232-249,1994.
[12]. Singh R K,"A Framework or secure single sign-on, "In the proceedings international conference on advances in recent trend in communication and computing, pp.430-432, 2009
[13]. 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,February.2009.
[14]. Tiancheng Li,Ninghui Li,Senior Member, and lan Molloy,"Slicing: A new approach for privacy preserving, data publishing,"IEEE Transaction on knowledge and data engineering,vol.24,no.23 March.2012