Efficient and Secure Single Sign on Mechanism for Distributed Network

Madhavi A. Indalkar
ME II Year MMCOE
Computer Department
Pune University

Ram Joshi
Assistant Professor MMCOE
Computer Department
Pune University

ABSTRACT
Distributed network is act as core part to access the various services which are available in the network. But the security related to distributed network is main concern. In this paper single sign-on SSO mechanism is introduced which gives access to all services by allowing to sign on only once by users. In this mechanism once user logs in to the Trusted Authority Center TAC then application or services which are register to trusted center will automatically verifies the user's credentials details and these credentials like password or digital signature will be only one for all applications or services. Unlike all other previous mechanisms where in, if user wants to have access multiple services then for every service distinct user credentials (username, password) must be required. SSO act as single authentication window to user for admittance multiple service providers in networks. Previously introduced technique based SSO technology proved to be secure over well-designed SSO system, but fails to provide security during communication. So here emphasis is given on authentication as open problem and on to refining the already proposed SSO process. And to do this along with RSA algorithm which was used in previous SSO process, we will be using MAC algorithm, which is intended to provide secured pathway for communication over distributed network.TAC i.e. Trusted Authority Center is used for sending token integrated with private and shared public key to user.

General Terms

1. Plaintext (Clear-text)

The human readable message which will be converted into an human unreadable (meaningless) message.

2. Cipher-text

It is a message in encrypted form.

3. Encryption

It is the process which converts a plaintext message into a cipher text message.

4. Decryption

It is the process which converts a cipher text message into a plaintext message.

5. Key

An important factor (parameter) used in the encryption and decryption Process.

6. Cryptosystem

It is a system to encrypt and decrypt information.

7. Symmetric Cryptosystem

Symmetric cryptographic system uses the same key to encrypt and decrypt information.

8. Asymmetric Cryptosystem

Asymmetric cryptographic system uses one key to encrypt and a different key to decrypt.

9. Cryptography

The use of cryptographic systems is to maintain the confidentiality of information.

10. Crypto analysis

It is the study of breaking cryptographic systems.

Keywords
Authentication, Attacks, Distributed network services, Single Sign on mechanism, SSO

1. INTRODUCTION
User authentication [4][5] is an important task in distributed network services. As distributed network is a broadly spreading technology for accessing various types of services by users. So need to provide security with respect to user as well as provider. The aim of a single sign on mechanism is to provide centralized verification and access control management. In SSO the user is registered to any trusted authority center TAC and after verifying details of users TAC gives unique token by which user can able to access the services which also registered to TAC. The service provider verifies details of user by TAC only. However, in existing system, to access the multiple services user need to sign in again and again for each service using the same set of identification details i.e. user id & password, which are validated at the identity provider by each service. Also to prevent/secure from bogus servers, users need to validate service providers every time when want to access the services. After mutual authentication, a session key may be negotiated to keep the privacy of data exchanged between a user and a provider [5], [6],

[7]. in many scenarios, the confidentiality of legal users should be protected [5], [8], [7]. But this is big task to design well-organized and protected authentication protocol. This paper aims to ensure more security to the existing Chang Lee SSO scheme [5] and Hsu and Chuang's scheme [9]. The main purpose of this paper is to improvise security for single sign-on solutions and reduce the need for users to frequently prove their identities to different applications and hold different credentials for each application. Also it aims to add additional security during communication between user and provider and security during passing of secrete token.

2. LITERATURE SURVEY

In the literature survey we are going to discuss various existing methods which allow user to access the services from multiple service providers in distributed network. Below in literature we are discussing some of them.

1. Chang and Lee [5] proposed a new SSO scheme. But in that scheme two attacks are found as the first attack allows a malicious/bogus service provider to pick up the user's secrete credential details and then it act as a genuine service provider for user to access resources and services. In another attack, an unregistered user without any credential details able to access services offered by service provider. This leads to soundness attack.

2. L. Harn and J. Ren [10] proposed a similar concept like SSO known as generalized digital certificate (GDC), in this system authentication is done by digital certificate. It is used in wireless network system. In this system a user will get the digital signature GDC which is provided by a trusted authority center, then user can authenticate itself with the help of GCD signature only. Every user will get unique GCD Signature.

3. Hsu–Chuang user identification scheme [9] is also based on single sign on mechanism. There are two weaknesses found in scheme as 1) an outside user can able to create a valid authentication details without registered to any trusted authority and with that details also able to access the services. 2) Scheme requires clock synchronization as it is based on time stamp.

4. Han [12] proposed a generic SSO structure which is based on broadcast encryption in addition with zero Knowledge (ZK) proof [20]. In this scheme user knows the equivalent private key of a given public key. By this each user is assumed to have been issued a public key in a public key infrastructure (PKI). By making use of RSA cryptosystem ZK proof is very inefficient and unproductive due to the complexity of interactive communications between the a user and the verifier (a service provider).

5. A. C. Weaver and M. W. Condtry[2] propose an alternative- a client server architecture that can assign some multifaceted data processing and device interface tasks to a network edge device, the Net Edge. This device can support services thought to be useful to the industrial environment like language translation technique, image translating scheme, access device adaptation/revision system, virus scanning processor device, content assembly method, local content insertion method, and caching.

6. L. Lamport [4] propose password authentication with insecure communication scheme. This system is secure even if an intruder can read the system's data, and can tamper or corrupt with or snoop on the communication between the user and the system/server. The method uses a secure one-way encryption function and can be implemented with a microcomputer in the user's terminal.

In this paper we are promoting the formal study of the soundness of authentication as one open problem. By using an efficient encryption of MAC (Message Authentication Code) algorithm we provide high level of security. Instead of using only RSA signatures which is use in previous paper we propose MAC (Message Authentication Code) algorithm for better performance and improving the security of the system during communication. Also encryption and decryption technique is used for transfer the secrete token from Trusted Authority Center (TAC)

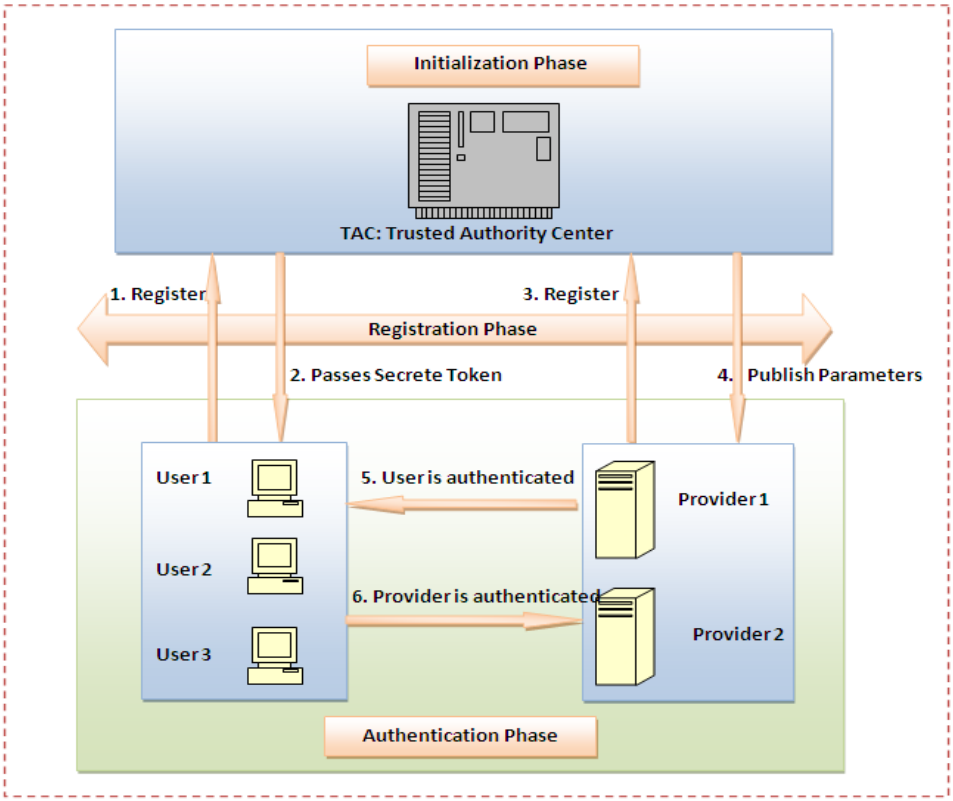

Fig 1: ESSO System Design

3. SYSTEM DESIGN

3.1 Problem Definition

To enhance the security, accuracy of current secure Single Sign on Mechanism to improve the key generation technique by providing dual authentication mechanism i.e.by the use of both MAC and RSA public key algorithm while providing the security to web based client server architecture.

3.2 ESSO System Design

In Efficient Single Sign on (ESSO) mechanism the trusted authority center send the secrete token to user by which user can able to access the services from authorized services providers which are already registered to TAC. The system is divided into three phases as TAC Initialization phase, User providers Registration phase and User providers' authentication phase.

3.3 System Architecture and Working of System

This paper proposes a web-based architecture of single sign on mechanism which use dual authentication mechanism. There are three secured services provided by trusted authority center TAC. The user want to access these different services are registered to TAC. Then TAC creates a secured token for that particular user after validating the credential details of user. With that same token user can able to access the various services which are registered to TAC. For the creation of secured token first MAC algorithm is used then the output is encrypted using RSA and then stored in database of service provider. When user want to access the services then after login code is generated as MACi and services provider also calculate the code for that user depending upon value stored in database as MACj. If MACi == MACj then provider gives access to user.

3.3.1 System Initialization Phase

Trusted Authority Center TAC initialization is done in the initialization phase. This phase is required for TAC to calculate secrete token value for user and parameters for providers. It is based on RSA cryptographic systems.

Steps:

1. Selects large two primes p, q and computes p*q.

2. Determines the key pair (e, d) such that e *d ≡ 1mod φ (N),

Where φ(N)=(p − 1)*(q − 1).

3. Chooses a generator g and ElGamal decryption key u and compute the value of y as y= $g^u \bmod N$

4. Chooses a cryptographic hash function h (.)

5. TAC publishes the value as (e, g, y, h (.), n, N) and protects the confidentiality of d and u.

3.3.2 Registration Phase

There are many users which want to access the services from TAC. All users are registered itself to TAC. Also there are various providers which also authenticated by TAC to provide the services.

a. TAC sends IDi, Si=h(KBi || mac_vc_genkey) to user

Where IDi = Unique identity of user

KBi = KeyBytes as KBi ← Ui AND Pj

b. TAC done RSA Sign Up Action for services provider

1. MACi ← h(KBi || mac_vc_genkey)

2. Epwi ← $MACi^e \bmod n$

Where e = public key generated by RSA cryptosystem

3. TAC sends IDi, EPWi and d(decrypt key) to service provider

In the proposed system dual authentication mechanism is used. For the token creation first it is created by the use of MAC then it is encrypted by RSA. And also TAC do not directly send the token created for user to services provider. It is first encrypted then store.

3.3.3 User Authentication Phase

Authentication is done between user and service provider. Before granted the access to user first user is authenticated by service provider. Then before accessing the services, user checks the provider's authentication details.

Steps:

a. User : m1(IDi, Si) ⟶ Provider

b. Provider : MACj ← Si=h(KBi || mac_vc_genkey)

c. Provider : EPWi ← database

d. Provider : MACi ← $EPWi^d \bmod n$

Where d = RSA decryption key

e. Provider : Compare (MACj == MACi)

If yes,

Then allowed to access the services to user

Else,

Assume user is not a valid and terminates the connection.

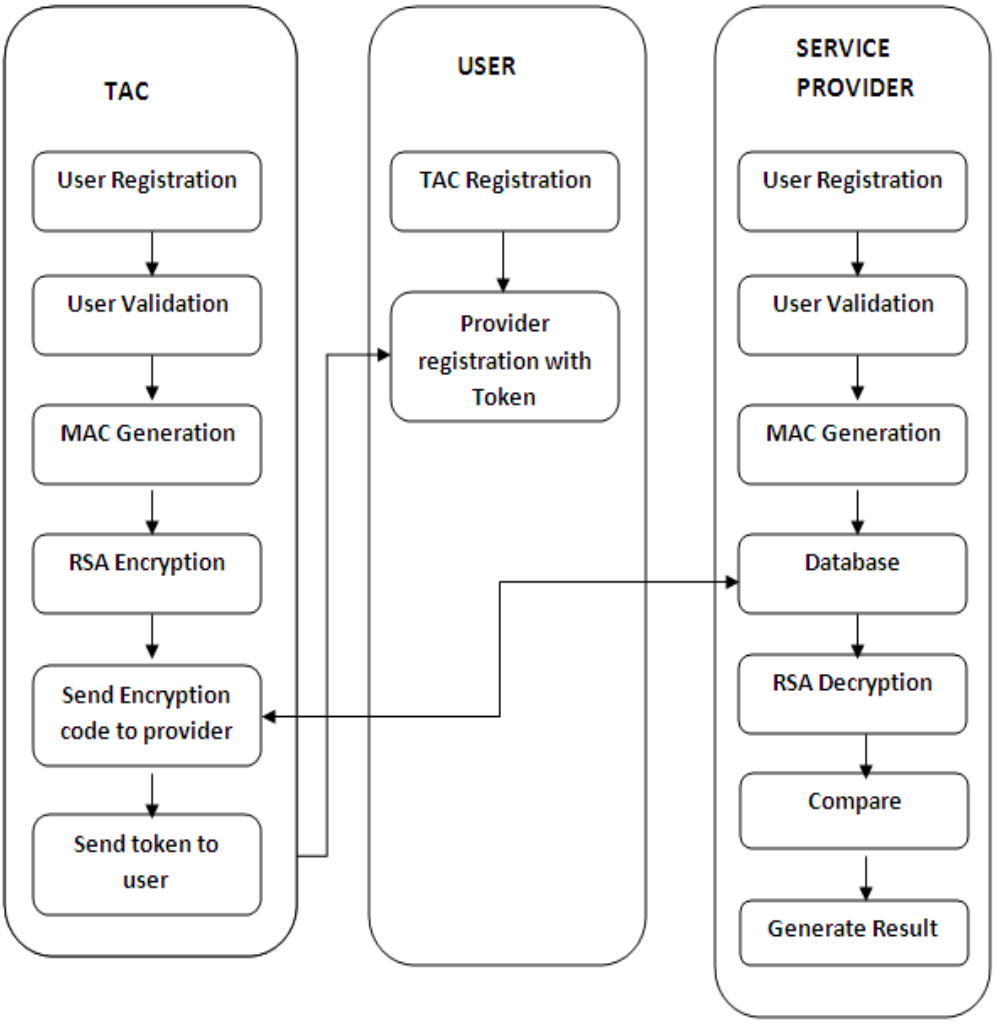

Fig 2: System Architecture

4. Hardware and Software Used

4.1 Hardware Configuration

- Processor - Pentium –IV 2.6 ghz
- Speed - 1.1 GHz
- RAM - 512 mb dd ram
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Monitor - 15" color

4.2 Software Configuration

- Operating System: Windows XP/7/8
- Front End: Java and J2EE
- DATABASE: MYSQL Server 2008
- Tools Used: Eclipse

5. RESULTS AND DISCUSSION

Implementation of proposed secured SSO System is done successfully. And also security is provided to the system in such a way that will protect to communication link between client & server as well as database. While sending the password from client to server, the code is generated which is providing more security and key generation technique for communication; which is faster. That comparative study is specified in table given below and graphical representation is also provided in figure given below.

Table 1: Comparative Results Generated by Different Algorithms

Algorithm → / **Key size ↓**	**RSA**	**Dual Authentication**
10 bits	0ms	0ms
64 bits	20 ms	10 ms
120 bits	100 ms	80ms
160 bits	150 ms	120 ms
200 bits	250 ms	150 ms
260 bits	350 ms	200 ms
350 bits	500 ms	350 ms
450 bits	700 ms	500 ms

5.1 Comparative Study

For comparative study between an improved key generation approach and the simple RSA approaches, the key generation rate & encryption strength parameters are used.

X axis-Encryption strength in bits

Y-axis key generation time in millisecond

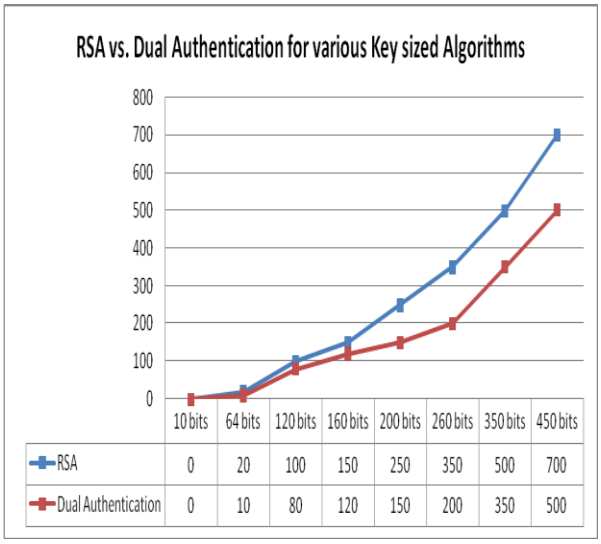

Fig 3: Graph showing key generation time verses encryption strength

By observing this graph, we can say that improved key generation algorithm is having the more encryption strength than simple RSA security algorithm based on different key sizes; also key generation time of is less than simple key generation RSA.

6. CONCLUSION AND FUTURE WORK

We have proved that improvement in authentication protocol against key generation can be achieved by using dual authentication process. The modified key generation technique is used to generate keys in MAC and RSA algorithm. This improved key generation approach for the web-based security is compared with the simple key generation RSA algorithm for protecting system as well as data present in the database for different performance parameters like

- Encryption Strength
- Time for key generation

The comparative study indicates improved Key Generation approach is better than the simple key generation technique RSA.

The projected system involves two bedded security and accuracy; this is main advantage of the system. Study cryptography schemes are used to offer more security. The system won't reveal concerning biometric details of the person to the database information. Within the same means consumer doesn't grasp what's happening within the server. The system is secure under a variety of attacks and it may be used in various biometric traits in future.

In future we can use some compression algorithms for high speed processing with security and also used in biometric traits in future.

7. REFERENCES

[1] Guilin Wang, Jiangshan Yu, and Qi Xie "Security Analysis of a Single Sign On Mechanism for Distributed Computer Networks", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL 9 NO 1 FEBRUARY 2013

[2] A. C. Weaver and M. W. Condtry, "Distributing internet services to the network edge" IEEE Transaction Ind. Electron, volume 50 no. 3pp. 402 to 413, June 2003.

[3] L. Barolli and F. Xhafa, "JXTA-OVERLAY A P2P platform for distributed, collaborative and ubiquitous computing system" IEEE Transaction Ind. Electron. Volume 58 no. 6 pp. 2160 to 2174 October 2010.

[4] L. Lamport, "Password authentication with insecure communication" Communication. ACM volume 24 no 11 pp 770 to 774, November 1981.

[5] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks" Computation System Science Engineering volume 15 no. 4, pp. 113 to 116, February 2000.

[6] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," IEEE Transaction Ind. Electron. Volume 15 no. 6 pp. 2553 to 2558, June 2008.

[7] 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 Transaction Ind. Electron. Volume 57 no. 2, pp. 793 to 800, February 2010.

[8] M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote field bus access" IEEE Transaction Ind. Inf. volume 7 no. 1 pp. 30 40, February 2011.

[9] C.L. Hsu and Y.H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," Inf. Science volume 179 no. 4 pp. 422 to 429, February 2009.

[10] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications" IEEE Transaction for Wireless Communication, volume 10, no. 7, pp. 2372 to 2379, July 2011.

[11] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity" J. Cryptography, volume 1, no. 2, pp. 77 to 94, 1988.

[12] J. Han, Y. Mu, W. Susilo, and J. Yan, "A generic construction of dynamic single sign on with strong security," in Proc. Secure Communication pp. 181 to198, Springer, 2010.