Asian Journal of Engineering and Applied Technology
ISSN 2249-068X Vol. 7 No. 2, 2018, pp. 86-90
© The Research Publication, www.trp.org.in

A Two-Fold Authentication Mechanism for Network Security

D. Selvamani[1] and V Selvi[2]
[1]Assistant Professor, Department of Computer Science, SIVET College, Gowrivakkam, Chennai, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India
E-Mail: selvamani.bhaskar@gmail.com, selvigiri.s@gmail.com

***Abstract* - Security is very important90 for any kind of networks. As a main communication mode, the security mechanism for multicast is not only the measure to ensure secured communications, but also the precondition for other security services. Attacks are one of the biggest concerns for security professionals. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies. This paper presents a double way authentication mechanism which uses the functionality of Elliptical Curve Cryptography, Kerberos System and RSA algorithm. ECC algorithm utilized to encrypt the user information whereas RSA used to encrypt the secret key itself to ensure the more security in the networks.**

***Keywords:* Network security, Authentication, Elliptical Curve Cryptography, RSA, Kerberos system, Bit Level, Secret key, Encryption, and Decryption**

I. INTRODUCTION

Computer industry has created an array of identification and authentication technologies like userID/Passwords, One Time Password, Biometrics, Smartcards, Secure Socket Layer, and Lightweight Directory Access Protocol, Security Assertion Markup language (SAML), OpenID and CardSpace address varying business and security requirements[1]. Each organization adopts one or more of these technologies to secure information against misuse and un-authorized access. In a networked environment, users are granted access to the network only when they provide their access information (e.g. User name & password) securely to check and validate their identity. If a person can prove that he is, also knows something that only he could know, it is reasonable to think that a person is he who claims to be. The purpose of personal authentication is to ensure that the rendered services are being accessed only by a legitimate user. All Network users aim to access information and transfer data safely. To make certain secure transmission of information between the parties; a group of challenges must.

II. RELATED WORKS

Jiliang Zhou[2] proposed an efficient and secures routing protocol based on encryption and authentication for WSNs. BEARP especially mitigates the loads of sensor nodes by transferring routing related tasks to BS, which not only maintains network wide energy equivalence and prolongs network lifetime but also improves the security mechanism performed uniquely by the secure BS.

Pawani Porambage[3] proposed a pervasive lightweight authentication and keying mechanism for WSNs in distributed IoT applications, in which the sensor nodes can establish secured links with peer sensor nodes and end-users.

Imran Memon[4] proposed the prevent user private information and secure communication by asymmetric cryptography scheme. The authors solved the wireless communication problem in A3 algorithm such as eavesdropping and this problem solved by asymmetric cryptography scheme because of its robustness against this type of attack by providing mutual authentication make the system more secure

Khalid Mahmood[5] proposed a hybrid Diffie–Hellman based lightweight authentication scheme using AES and RSA for session key generation. To ensure message integrity, the advantages of hash based message authentication code are exploiteds.

Kakelli Anil Kumar[6] proposed a new secure multipath routing protocol (NSRP) for military heterogeneous wireless sensor network (MHTWSN) for secure data transmission. NSRP uses elliptic curve cryptography (ECC) to discover trusted neighbor nodes and establish the secure multiple routes for reliable data delivery in MHTWSN.

Sravani Challa[7] proposed scheme supports functionality features, such as dynamic sensor node addition, password as well as biometrics update, smart card revocation along with other usual features required for user authentication in wireless sensor networks.

III. IMPORTANCE OF AUTHENTICATION

Using of authentication mechanism lead to address the following problems. The definition problems are given below:

1. *Authentication:* Authentication means enabling the network to only admit the authorized users to have access to its resources. It provides the way where the claimed identifier is verified by the access control mechanisms through some means.
2. *Access Control:* The discipline in which mechanisms and policies are established that restrict access to the computer resources only to correct users.
3. *Identification:* It is a way where a resource claims (or is identified through other means) a specific and unique identifier.

4. *Authorization:* Which determines the privileges associated with authenticated identity.
5. *Security:* The ability of a system to protect data, services and resources against misuse by unauthorized users.
6. *Privacy:* The ability of a system to protect then identity and location of its users from un-authorized disclosure.

IV. PROPOSED TWO-FOLD AUTHENTICATION MECHANISM

The Kerberos protocol uses a central KDC (key distribution center) which acts as a trusted third party. In Kerberos, the KDC and the other entities use a “secure” clock for the purpose of detecting replay attacks and checking token validity. Kerberos uses timestamp as an authenticator. The clocks are assumed to be synced with a small amount of known clock drift.The nodes in the networks are connected to each other, and there is also an authentication server, which provides authentication service to each other. Given a distributed set of services, we believe Kerberos is an appropriate architecture for enabling inter-service and user to service authentication. In this proposed work, the primary thought is that the information is encrypted utilizing any AES symmetric encryption algorithm [8]. The encrypted data is then stored. The symmetric key used to encrypt the information is then encrypted utilizing the RSA public key [9]. Consequently, the best way to decrypt the symmetric key is by utilizing the ECC private key [10].

The data is first encrypted with a symmetric key and that symmetric key is then encrypted using the RSA public key of the data owner. That is,

$$E_k(d) = C$$
$$G_{pub}(k) = K$$

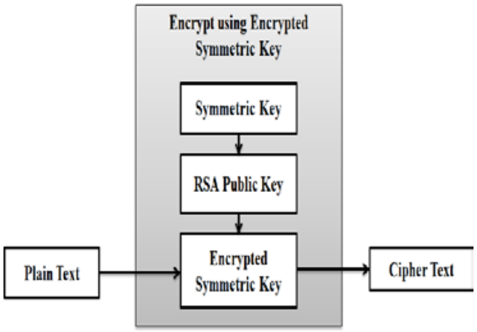

Fig. 1 Encryption of user Data and Key for encrypting the data

Where k is the symmetric key, E is the symmetric encryption operation, C is the ciphertext, G is the RSA encryption operation, pub is the RSA public key of the information owner and K is the encrypted symmetric key.

Since the ECC algorithm speaks to its private keys and public keys as huge numbers, this makes key partitioning possible and subsequently, fractional decryption is additionally conceivable. In this way, if we somehow happened to partition the ECC private key C into two sections A and B with the end goal that A + B = C, the symmetric key could be somewhat decrypted utilizing A and the in part decrypted key can then be completely decrypted utilizing B.

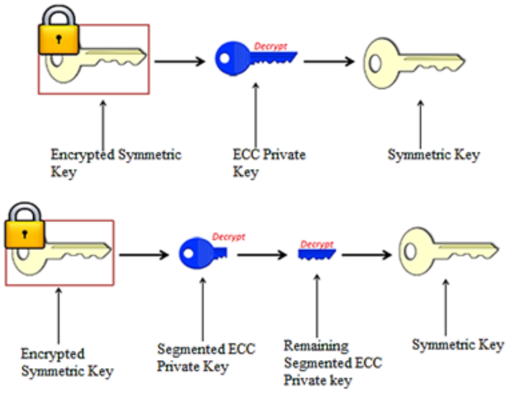

Fig. 2 Decryption process of the encrypted symmetric key

In Kerberos [11], the KDC is considered as a certificate authority. The KDC has every one of the certificates and public key of each element, and every one of the substances have the certificate of KDC, with the goal that they can confirm the signature of KDC. And likewise, KDC has a secret key. Just KDC thinks about this key, and no other substance has the learning of it. In this proposed two-fold authentication mechanism the secret key (Symmetric key) is encrypted with RSA public key and it is decrypted with segmented ECC private key.

TABLE I LIST OF ABBREVIATIONS AND EXPLANATIONS USED IN THE PROPOSED MECHANISM

Abbreviation	Explanation
TGT	Ticket Granting Ticket
KDC	Key Distribution Center
sk	Session Key
SK	Symmetric Key
ESK	Encrypted Symmetric Key
K_X	Key for Client X generated by KDC
SK_U	Session key for user and server
DKDB	The database that stores encryption keys which are they encrypted.
DO	The owner decides who can access the data and give permission to the data.
DC	Any user who has permission to access data given by the DO

A. Step by Step Procedure of Two-fold Authentication Mechanism

1. Registration Phase

Step 1: The DO selects his/her ID and password.
Step 2: The DO request the server for sharing the data or resources.
Step 3: DO chooses the random number as the symmetric key (SK).
Step 4: KDC generates a private and public key by RSA Encryption algorithm.

Step 5: The SK is then encrypted itself by KDC using RSA public key.
Step 6: Then the ESK is used to encrypt the user information and it is stored in KDC.

2. Login Phase

Step 1: The user sends a request by using ID and Password to TGT.
Step 2: KDC generates a ticket and a session key (sk).
Step 3: User selects the secret key from the keypool using Elliptical Curve Cryptography (ECC). Then the secret key is partitioned into two pieces for the decryption process.
Step 4: The user computes the values using secret key and the cipher key. Generates the signature and sends a message to the KDC.
Step 5: When the KDC receives the messages from the user and restores its cipher text.
Step 6: It extracts the secret key from the value. The decryption process is carried out.
Step 7: The cipher key is decrypted with the partitioned secret key and cipher text is decrypted with the symmetric key using KDC and it verifies the signature with the secret key.
Step 8: Finally, the KDC verifies the signature of the user and gets client certificate, gives the ticket and session key for the transmission.

V. RESULT AND DISCUSSION

In this paper, Kerberos system, Elliptical Curve Cryptography, RSA, Symmetric Key Encryption algorithms provides two essential services for securing the networks.

1. Securing the Information: It has provided by using encryption and decryption.
2. Authenticating the Information: Kerberos and Digital Signature has used for providing the authentication.

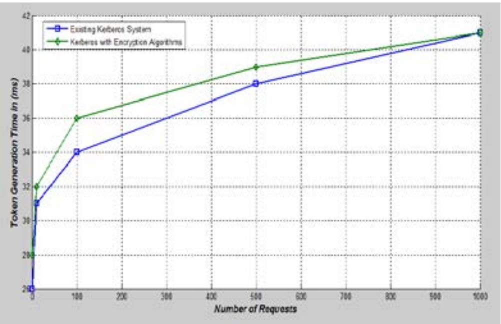

Fig. 3 Graphical representation of the performance analysis of proposed Kerberos with encryption algorithms and existing Kerberos system

The above table represents the token generation time in milliseconds (ms). The current Kerberos system utilizes the digital signature for metadata, so the time taken for token generation is minimal, whereas the proposed two-fold authentication uses the encryption by one algorithm and decryption by other algorithm increases the time taken for token generation.

TABLE II RECOMMENDED SECURITY BIT LEVEL BY NIST

Security Bit Level	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Table II gives the National Institute of Standards and Technology recommended security bit levels for existing RSA encryption and ECC method. The size of the key increases with the security bit level for RSA method. ECC utilizes only small number of key when comparing with RSA.

TABLE III TIME TAKEN FOR ENCRYPTION BY RSA, ECC AND PROPOSED TWO-FOLD AUTHENTICATION MECHANISM AT THE SECURITY BIT LEVEL OF 80

Number of bits in Encryption	Time taken for Encryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8bits	0.0406	0.4776	0.0581
64 bits	0.2455	2.2776	0.3568
256 bits	0.6687	7.8331	0.8976

Table III depicts the Time taken for encryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 80.

TABLE IV TIME TAKEN FOR DECRYPTION BY RSA, ECC AND PROPOSED TWO-FOLD AUTHENTICATION MECHANISM AT THE SECURITY BIT LEVEL OF 80

Number of bits in Decryption	Time taken for Decryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	0.8634	1.4376	1.3487
64 bits	5.6281	5.8188	5.7269
256 bits	18.4266	21.9371	21.8763

Table IV depicts the Time taken for decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 80.

TABLE V TIME TAKEN FOR ENCRYPTION BY RSA, ECC AND PROPOSED TWO-FOLD AUTHENTICATION MECHANISM AT THE SECURITY BIT LEVEL OF 112

Number of bits in Encryption	Time taken for Encryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	0.0288	2.2121	0.0318
64 bits	0.1746	9.8877	0.1863
256 bits	0.4926	21.9228	0.4966

Table V depicts the Time taken for encryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 112.

Table VI Time taken for Decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 112

Number of bits in Decryption	Time taken for Decryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	2.8186	1.6774	1.6898
64 bits	20.3217	6.8444	6.9543
256 bits	103.1446	25.4442	25.6421

Table VI depicts the Time taken for decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 112.

Table VII Time taken for encryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 128

Number of bits in Encryption	Time taken for Encryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	0.0416	3.7874	0.0527
64 bits	0.2763	15.1771	0.3854
256 bits	0.6522	36.5567	0.7123

Table VII depicts the Time taken for encryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 128.

Table VIII Time taken for Decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 128

Number of bits in Decryption	Time taken for Decryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	6.8518	1.8781	2.0110
64 bits	45.5691	7.4493	7.8832
256 bits	208.7175	26.5171	26.8761

Table VIII depicts the Time taken for decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 128.

Table IX depicts the Time taken for encryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 192.

Table X depicts the Time taken for decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 192.

Table IX Time taken for encryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 192 bits

Number of bits in Encryption	Time taken for Encryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	0.04971	4.6377	0.5878
64 bits	0.2496	20.1419	0.3187
256 bits	0.6829	76.6145	0.7538

Table X Time taken for Decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 192 bits

Number of bits in Decryption	Time taken for Decryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
8 bits	12.5563	2.113	2.3244
64 bits	76.6553	7.5896	7.8785
256 bits	258.7175	31.2633	31.5745

A. Performance analysis

Table XI depicts the Time taken for 8 bits encryption and decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the various security bit level. Figure 8a gives the graphical representation for Time taken for 8 bits encryption and decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the various security bit level.

Table XI Total Time taken for 8 bits encryption and decryption by RSA, ECC and proposed Two-fold Authentication Mechanism

Security Bit Level	Total Time taken for 8 bits Encryption and decryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
80 bits	0.904	0.9152	1.4068
112 bits	2.8474	3.8895	1.7211
128 bits	6.8934	5.6655	2.0637
192 bits	12.606	6.7510	2.9122

Table XII depicts the Time taken for 64 bits encryption and decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the various security bit level.

Table XII Total Time taken for 64 bits encryption and decryption by RSA, ECC and proposed Two-fold Authentication Mechanism

Security Bit Level	Total Time taken for 64 bits Encryption and decryption in seconds		
	RSA	ECC	Proposed Authentication Mechanism
80 bits	5.8736	8.0964	6.0837
112 bits	20.4963	16.7321	7.1406
128 bits	45.8454	22.6264	8.2686
192 bits	76.8059	27.7315	8.1972

Table XIII depicts the Time taken for 256 bits encryption and decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the various security bit level.

TABLE XIII TOTAL TIME TAKEN FOR 256 BITS ENCRYPTION AND DECRYPTION BY RSA, ECC AND PROPOSED TWO-FOLD AUTHENTICATION MECHANISM

Security Bit Level	**Total Time taken for 256 bits Encryption and decryption in seconds**		
	RSA	**ECC**	**Proposed Authentication Mechanism**
80 bits	19.0953	29.8202	22.7739
112 bits	103.6372	47.367	26.1387
128 bits	209.3697	63.0738	27.5884
192 bits	259.4004	107.8778	32.3283

VI. CONCLUSION

In this paper, a two-fold authentication mechanism with Kerberos system has proposed in the context of the network security. The proposed Two-Fold authentication scheme composed of two phases: i) Registration phase and ii) Login and an Authentication phase. Proposed Two-Fold authentication mechanism takes less time for decryption than RSA and ECC in the higher security level. Proposed Two-Fold authentication mechanism performs in less total time for Encryption and decryption of details among the user, Kerberos system and the server. When it has compared with the various security bit levels, the proposed Two-Fold authentication mechanism with Kerberos system it performs better than the ECC and RSA.

REFERENCES

[1] Xuanxia Yao, *et al.*, “A lightweight multicast authentication mechanism for small scale IoT applications,” *IEEE Sensors Journal,* Vol.13, No. 10, pp. 3693-3701, 2013.

[2] Jiliang Zhou, “Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks,” *International Journal of Distributed Sensor Networks,* Vol. 9, No. 4, pp.108968, 2013.

[3] Pawani Porambage, *et al.*, “Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications,” *International Journal of Distributed Sensor Networks,* Vol.10, No.7, pp.357430, 2014.

[4] Imran Memon, *et al.*, “Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme,” *Wireless Personal Communications,* Vol.84, No.2, pp.1487-1508. 2015.

[5] Mahmood, Khalid, *et al.*, “A lightweight message authentication scheme for Smart Grid communications in power sector,” *Computers & Electrical Engineering,* Vol.52, pp.114-124, 2016.

[6] Kakelli Anil Kumar, Addepalli VN Krishna and K. Shahu Chatrapati, “New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks,” *Journal of Information and Optimization Sciences,* Vol.38, No. 2, pp.341-365. 2017.

[7] Sravani Challa, *et al.*, “An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks,” *Computers & Electrical Engineering,* Vol.69, pp.534-554, 2018.

[8] Chi Cheng, et al., “Securing the Internet of Things in a quantum world,” *IEEE Communications Magazine,* Vol.55, No. 2, pp.116-120. 2017.

[9] Marcos A. SimplicioJr, *et al.*, “Lightweight and escrow-less authenticated key agreement for the internet of things,” *Computer Communications,* Vol. 98, pp. 43-51, 2017.

[10] Han Shen, *et al.*, “Efficient RFID authentication using elliptic curve cryptography for the internet of things,” *Wireless Personal Communications,* Vol. 96, No. 4, pp.5253-5266, 2017.

[11] Hui Li, *et al.*, “Securing Offline Delivery Services by Using Kerberos Authentication,” *IEEE Access,* Vol. 6, pp. 40735-40746, 2018.