ENHANCING EFFICIENCY OF EAP-TTLS PROTOCOL THROUGH THE SIMULTANEOUS USE OF ENCRYPTION AND DIGITAL SIGNATURE ALGORITHMS

Seyed Milad Dejamfar[1], Sara Najafzadeh[2]

[1]Computer Department, Engineering School, Malard Branch, Islamic Azad University, Tehran, Iran

[2]Computer Department, Yadgar-e Imam Khomeini Branch, Islamic Azad University, Shahr-e Rey, Tehran, Iran

ABSTRACT

Security and its subcategory authentication are among the important subjects of cloud computing. In this system, user authentication mechanisms are carried out before providing access to resources. It is noteworthy that this input gate is actually the pathway of many attacks. Therefore, designing a secure user authentication mechanism significantly contributes to the overall security of the system. This process blocks attacks where the objective is to authenticate a user and when the user requests for cloud computing services. As a result, this article aimed to introduce a new security solution for cloud computing environments through employing the EAP-TTLS protocol, replacing the common Data Encryption Algorithm (DEA) with a new one, and adding a digital signature to the authentication process. After implementation of the proposed method in matlab, its performance was evaluated with RSA and ECDSA algorithms. The results of simulation showed the improvement of performance in terms of memory usage, authentication time, and verification delay. The proposed method [digital signature], along with username and password, is used to improve security in user authentication process.

KEYWORDS

Cloud Computing, Security, Authentication, Encryption, EAP-TTLS

1. INTRODUCTION

Given the intrinsic communicational challenges, such as insecurity, as well as heterogeneity issues, the inclusion of security mechanisms into a cloud computing technology is a complex and difficult task. In addition, due to energy density limitations in mobile devices, they need lightweight security mechanisms. User authentication is among the most important and initial security mechanisms. It is the most important factor in protecting the cloud from cyber-attacks. This is because it verifies the identities of clients that want to connect to a cloud before giving them access to the system. The proper function of this factor maintains the system performance through satisfying cloud security to a great extent and preventing system overloading by next levels of security mechanisms. In particular, authentication mechanisms should be lightweight and carry minimal computational and communicational costs.

2. COMMON AUTHENTICATION PROTOCOLS

- Password Authentication Protocol (PAP): It is a simple authentication method to establish a connection. In this protocol, a word is shared between the user and the workstation in the form of a simple text, and when it is used with RADIU server for authentication, the message is exchanged between the server and the workstation to establish a point-to-point connection.

DOI: 10.5121/ijnsa.2017.9404

- Challenge-Handshake Authentication Protocol (CHAP): It is a stronger authentication method to establish a connection between a workstation and a server. In this method, the access request is sent to the server after the initial information is exchanged between the workstation and network access server (NAS) and the authenticity is verified.
- Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP): This CHAP-based protocol was developed by Microsoft to establish secure connections between its remote workstations. In general, MSCHAP is similar to CHAP. Differences between these two protocols can be summarized in two regards. MS-CHAP works based on hashing function used in Windows networking. In addition, the initial response created by MS-CHAP for authentication is in complete compliance with Microsoft's Windows operating systems.
- Extensible Authentication Protocol (EAP): It is a very secure authentication method with a greater flexibility, capable of working with different algorithms, such as MD5. This protocol can be encapsulated in other protocols' frames. Therefore, it had more extensive applications than CHAP and PAP. This protocol transmits authentication messages between the supplicant and the authentication server [1].
- Extensible Authentication Protocol (EAP) over LAN: Each EAP-based protocol defines a way to encapsulate EAP messages. In 802.11 standard, this encapsulation method is called EAP over LAN (EAPOL).

3. AUTHENTICATION PROCESS IN EAP

Devices make use of EAP packets for the port authentication process. Until authentication is successful, the supplicant can only access the authenticator to perform authentication message exchanges. Initial 802.11 control begins with an unauthenticated supplicant and an authenticator. A port under 802.11 control, acting as an authenticator, is in an unauthorized state until authentication is successful.

3.1. Common Extensible Authentication Protocols

The point-to-point EAP is a mechanism that defines a standard message exchange between devices over the authentication protocol. EAP is a basic technology that allows wired and wireless services to authenticate networking equipment. EAP does not require IP connectivity, instead it uses a data link layer. EAP is suitable for networks that use DHCP for providing network devices with IP addresses. This is because, until a client is not authenticated, it cannot receive an IP address from an HHCP server.

EAP alone cannot be used as an authentication protocol, as it is merely a standard exchange message that provides mutual authentication between a supplicant and a network. EAP supports a number of identity authentication protocols that ensure security during the authentication process. Different security and encryption characteristics of these protocols allow companies to use the one that satisfies the needs of their applications under 802.11 standard [28]. There are several EAPs to support identity authentication systems and security policies of their networks. Following protocols are the more common EAPs:

- EAP-MD5 is an EAP algorithm that provides base-level EAP support. This algorithm uses a 128-bit message (the hashed value of a server challenge and the user’s password) to verify the authenticity of the supplicant. EAP-MD5 is a very secure method for a local-area network [2].
- EAP-OTP: It is very similar to EAP-MD5, except that it uses the One-Time Password (OTP) as the response. The request contains a displayable message. The OTP method is used in VPN and PPP networks.

- Lightweight EAP (LEAP): LEAP supports mutual authentication and employs dynamically generated WEP keys to encrypt transmitted data. Mutual authentication reduces the risk of access point masquerading. LEAP is suitable for organizations that want to modestly raise their security bar.
- EAP with Transport Layer Security (EAP-TLS): EAP-TLS, which is based on Secure Sockets Layer (SSL), is now the most common EAP implementation method for wireless local area networks (WLAN). Today, SSL is used for authentication of the majority of secure web transactions. In EAP-TLS, users require certificate-based and mutual authentication of the client and the network. Both the station and the RADIUS server have to prove their identities via public key cryptography in the form of digital certificates of their smart cards. If used in wireless stations, WEP keys that are dynamically generated can be used to establish a secure connection between the WLAN service provider and the access point.

3.2. EAP with Tunneled TLS (EAP-TTLS)

In this protocol, similar to other EAP methods, a client cannot connect to an access point until its authenticity is verified by the main server. In this operation, the access point mediates the exchange of messages.

4. REVIEW OF AUTHENTICATION METHODS

4.1. Secure Access and Storage in Cloud Computing with Cryptography [3]

Elliptic curve cryptography is used to protect data files and achieve secure storage and access on outsource data in the cloud. This scheme has two sections in the cloud storage server, namely private data section and shared data section. These two sections allow for easy data access and storage. The private data section is used for personal data storage to which only a specific user is given access; whereas, the public data section is used for storage of data, which is shared by a group of trusted users. Elliptic curve cryptography is used for data encryption in both private and public data sections. Data stored in the private data section is encrypted with ECC private key; whereas, data stored in the public data section is encrypted with ECC public key. The public data section is used for storing data that should be shared by trusted users.

4.2. Cloud Computing Model Based on Data Classification [4]

The author offers a framework that enables users to encrypt data using a key that is not accessible to the service provider. Databases are encrypted by the degree of confidentiality. The proposed secure cloud storage model encrypts data at three cryptographic levels based on the degree of confidentiality of data: basic, confidential, and highly confidential. The solution is based on manual classification and the user should determine the level of data confidentiality. Data with high confidentiality level is stored on faster devices; whereas, data with low confidentiality is stored on slower devices. Different cryptographic algorithms, such as secure hash algorithm (SHA), advanced encryption standard (AES) transport layer security (TLS), are used based on the security level of data.

4.3. Key Generation Mechanism [5]

It addresses some security concerns about cloud technology, as well as some solutions to limit and overcome such issues in cloud layers, using mobile technologies. In this scheme, the user is allowed to make data accessible to the public, to secure it, or give limited access to it. The private data is accessible only through an authorized key. When the user presents the key to the service provider, the service provider verifies that this credential is assigned to an authorized network of the requested service. This verification process is called *digital authentication*. If the authentication succeeds, the user can see download [link] and change it; otherwise, the user is unauthorized and does not receive requested information.

4.4. Authentication Mechanism [6]

They introduced a method for user registration and authentication. Both methods use secure and simple authentication algorithms for cloud systems. This method employs a mobile device for one-time password generation in cloud services. To apply advanced encryption standard (AES), both the client and the server are configured and connected. Their proposed scheme was fairly secure and user-friendly.

4.5. Authentication with Cellphone in Hybrid loud [7]

They proposed two systems including user authentication and mobile device authentication with a hybrid cloud service. Based on their studies, they proposed a system comprised of device certification, user authorization and service authentication certificate for users. This method used two-factor authentication and RADIUM schemes. In fact, they proposed a secure authentication system for hybrid cloud services, which was capable of providing security, compliance, accessibility, and resistance to a man-in-the-middle attack (MITM). The user certificate-based authentication device and the authentication service are supported by the proposed scheme. RADIUS does not provide supplemental security services.

4.6. Authentication and Certification [8]

They addressed authentication and certification system in a cloud space. In this article, the author proposed a cloud security system and contributed to the area of identity authentication and certification. The author proposed an architecture that included portable and central security servers. Advantages of this architecture included flexibility, security, reliability, efficiency, and management simplicity. There is no private section in this process. All security documents are stored in the central security system. In this way, activities of the end user are tracked by the provider of the cloud authentication service.

4.7. Mobile Signature for Authentication and Secure Connection [9]

It is an identity authentication mechanism that uses different technologies, such as mobile signature, SFTP, SOA, SSL, and their combination to develop a comprehensive solution for a mobile cloud space. The security of user identity is ensured through mobile signature. This is a simple solution for tracking the actual client in each operation. The security of the communicational tunnel is ensured by using SSL in the middle. Session key and serial number make impossible the replacement or repetition of the network message by MITM.

4.8. Rijndael Encryption along with EAP-CHAP Encryption [10]

They discussed authentication in a cloud security space. In this regard, they used Rijndael, along with EAP-CHAP for identity authentication. The EAP-CHAP algorithm is used to address identity authentication and certification issues in cloud computing. Rijndael is the most secure algorithm. They mainly focused on the client-side security. Both the encryption and decryption processes are carried out by the user, that no intruder can decrypt data.

4.9. Data Encryption, Diffie–Hellman Key Exchange, and Elliptic Curve Cryptography [11]

They designed a cloud structure that provided client-side and server-side security. They used elliptic curve cryptography and Diffie–Hellman key exchange mechanisms for data encryption and communication establishment, respectively. However, the complexity of cryptography directly affects the access establishment speed. They employed elliptic curve cryptography as computation cost and [thus] the speed of algorithm was lower. This model has subexponential time complexity which makes it difficult to crack.

5. PROPOSED METHOD

Simultaneous use of new encryption algorithm and digital signature In this method, a strong cryptography is used for sending data and identity information. Abbreviations used in this multi-signature algorithm are as follows:

C: User
S: Server
n_s, n_c: New random number
Specification $_C$: Cryptography specifications of C
Specification S: Cryptography specifications of S
S_{CS}: a pre-master secret used for public key generation
E_{PS} [S_{CS}]: cryptography of S_{CS} with the entity public key S (Ps) using identity-based encryption (IBE) algorithm
M: All messages coming after ClientHello message
S_{igSC} ([M]): Signature of message M with private key of an entity C (Sc) using the identity-based signature
Ver $_{pc}$ (S_{igSc} ([M])): verification of S_{igsc} ([M]) by means of P_C, using IBS
Ds_s (E_{ps} [S_{cs}]): encryption of E_{ps} [S_{cs}] by means of the private key of entity S (SS), using IBE.

According to the figure, in the first step, the user C sends the ClientHello to the server S. This message includes a new random number (n_c), session ID (S_{ID}), and cryptography specifications (specifications $_c$). The specification $_c$ uses improved TTLS. IBS and IBE have been used as providers of communication security. MD5 is a typical hash function. AES is a symmetrical encryption algorithm. ClientHelloDone signals the end of the first step. In the second step, the server S responds with ServerHello, which includes the new random number (n_s), a session ID (S_{ID}), and secret Specification *s*. Specification *s* is a cryptography set supported by the server S. ServerHelloDone signals the end of the Second step. In the third step, the user C adopts a pre-master S_{cs} first and encrypts it with the public key (Ps) of server S, as well as IBE algorithm. The secret text is sent to the server S with ClientKeyExchange. Then, the user C creates a signature $S_{ig\ SC}$ ([M]) and sends it as an IdentityVerify message to the server S. Finally, ClientFinished signals the end of the third step. In the fourth step, the server S uses IDc to obtain the public key (Pc) of the user C and then employs Pc in the IBS to verify $S_{ig\ SC}$ ([M]). The authenticity of the user C is verified only if the owner of IDc is valid. This process completes the verification of C through S. Then, the server S decrypts Ss with its private key Eps [Scs]. Since SSC is new, accurate decryption indicated that the S is valid owner of IDs. This step verifies the authenticity of the S. ServerFinished signals the end of the Fourth step. Finally, a secret public key is calculated between S and C by K_{CS} = PRF (S_{CS}, n_C , n_S).

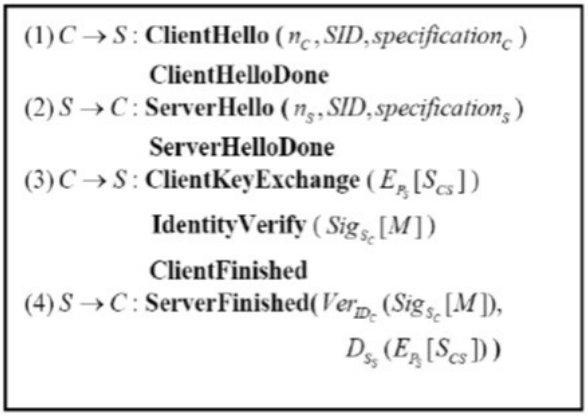

Figure 1 Cryptography and Digital Signature operations

6. SIMULATION SPECIFICATIONS

Simulation specifications are as follows:

- Network architecture: EAP-TTLS
- Carrier protocol: RADIUS
- Tracking protocol: RIP
- Number of servers: 1
- Number of APs: 5-200
- Number of clients: 5-50
- Number of simulations: 10 timers per stage

7. PRODUCTIVITY ANALYSIS

Since we aimed to use this architecture in cloud computing environments that serve different users (in terms of access speed and network device), runtime, authentication time, authentication delay, and memory usage are specifically important factors. Given that ECDSA and RSA have been used for communication encryption under EAP-TTLS, our proposed method was compared to these two algorithms.

7.1. Runtime

Using this new cryptography architecture with EAP-TTLS improved the runtime and productivity. The runtime of EAP-TTLS with the proposed cryptography method was compared to that with ECDSA and RSA in two different modes (router number change and client number change).

7.1.1. Runtime and Router Number Change

First, a fixed number of connected users was considered, while the number of routers between AP and the main server increased in each stage. Runtime of the proposed cryptography was compared to RSA and ECDSA under EAP-TTLS architecture in similar conditions. Results are presented in following Figure.

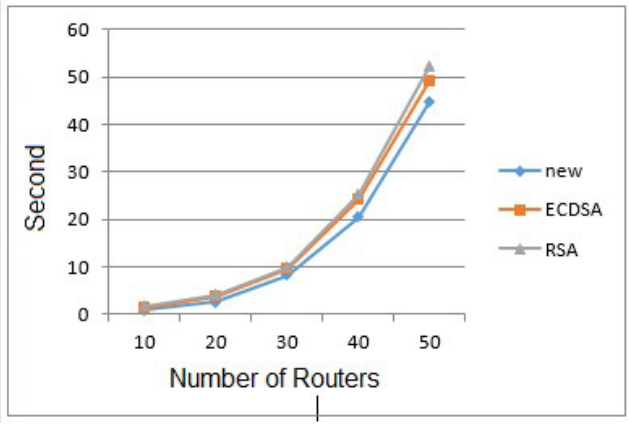

Figure 2 Comparison of runtime between the proposed method with ECDSA and RSA with increasing number of routers

This figure shows that the use of new cryptography algorithm improved authentication time, as compared to two other algorithms.

7.1.2. Runtime and Client Number Change

In this scenario, fixed number of routers was considered, but the number of simultaneously connected users was increased. Results are as follows:

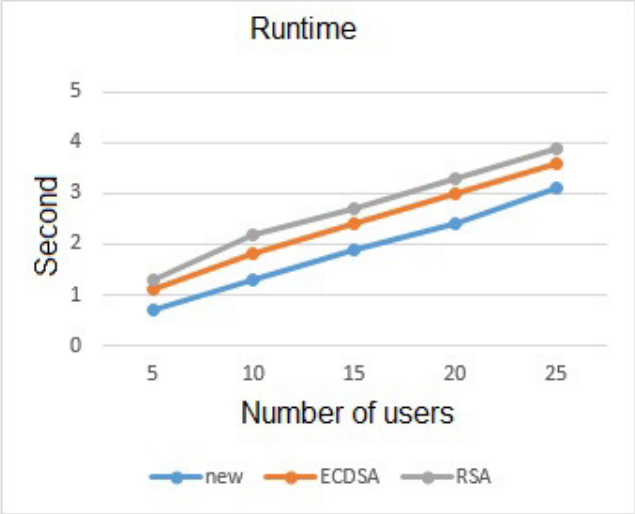

Figure 3 Comparison of runtime between the proposed algorithm with ECDSA and RSA with increasing the number of users

According to this figure, authentication time reduced by the proposed method, which can be attributed to its encryption/decryption type.

7.2. Memory Usage

To compare the memory usage, the proposed authentication method was compared to two aforementioned ones under two different scenarios.

7.2.1. Memory Usage and Router Number Change

In this scenario, fixed number of users and varied number of routers were considered. Results are presented in the following figure.

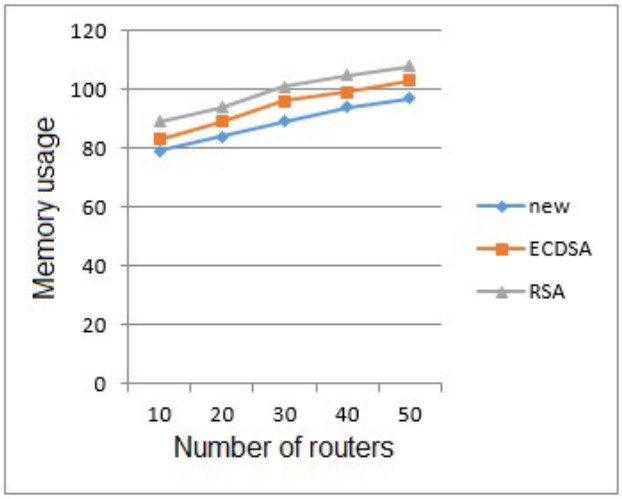

Figure 4 Comparison of memory usage between the proposed algorithm with ECDSA and RSA with increasing the number of routers

According to this diagram, memory usage was reduced in the new identity authentication architecture, which can be attributed to less message exchange in EAP-TTLS.

7.3. Authentication Time

In this scenario, authentication time was compared. Comparison results are presented in the following figure.

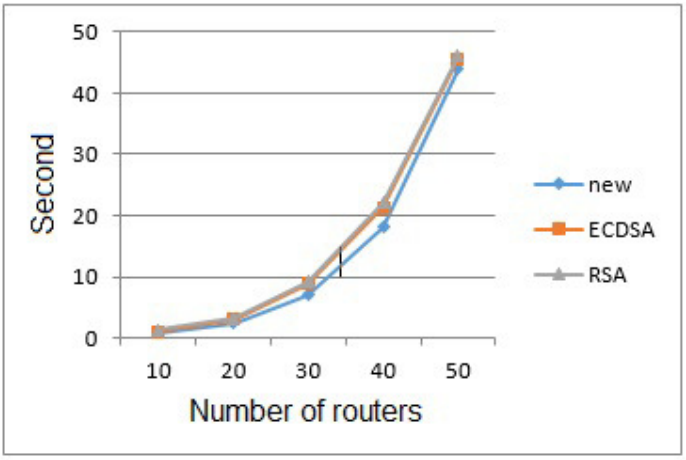

Figure 5 Comparison of authentication time between the proposed algorithm with ECDSA and RSA

Simulation result indicates that the proposed method was faster than two other algorithms.

7.4. DELAY

Delay refers to the length of time between user authentication and user connection to the network. The following figure presents the authentication delay results.

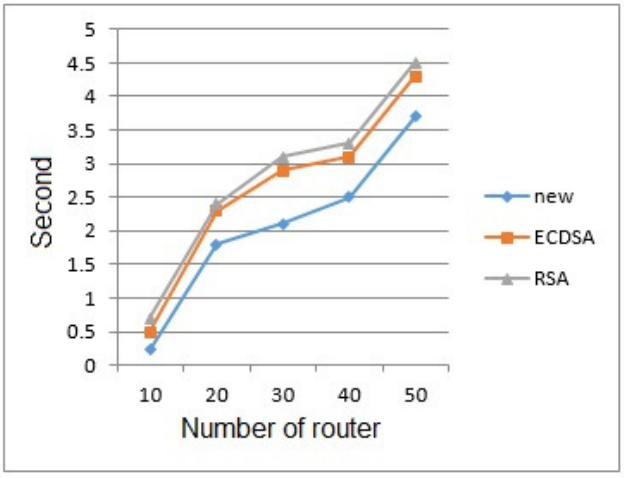

Figure 7 Comparison of delay between the proposed algorithm with ECDSA and RSA

According to the simulation results, authentication delay was reduced in the proposed algorithm as compared to two other algorithms.

7.5. Extent of Authentication Time Improvement

The extent of authentication time improvement is presented in the following figure.

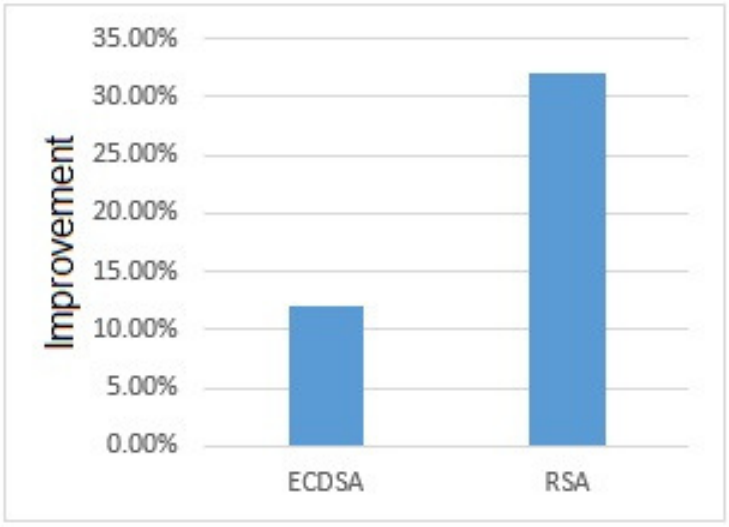

Figure 6 Extent of authentication time improvement

7.6. Extent of Runtime Improvement

The extent of run time improvement is shown in the following figure.

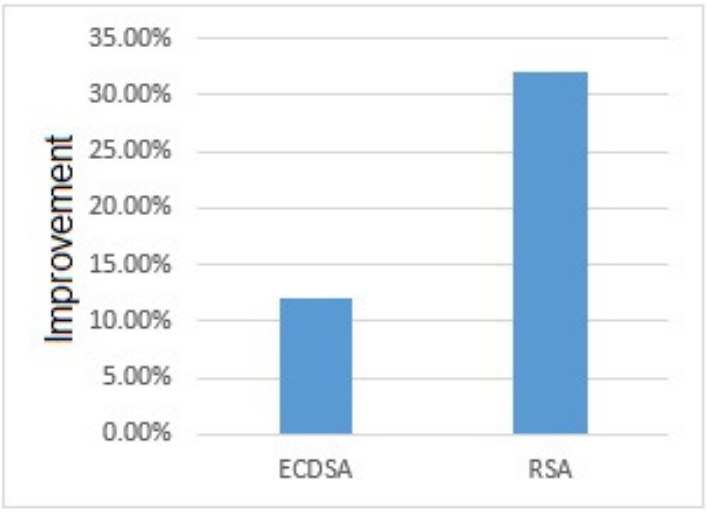

Figure 7 Extent of runtime improvement

7.7. EXTENT of Delay Reduction

The extent of delay reduction is presented in the following figure.

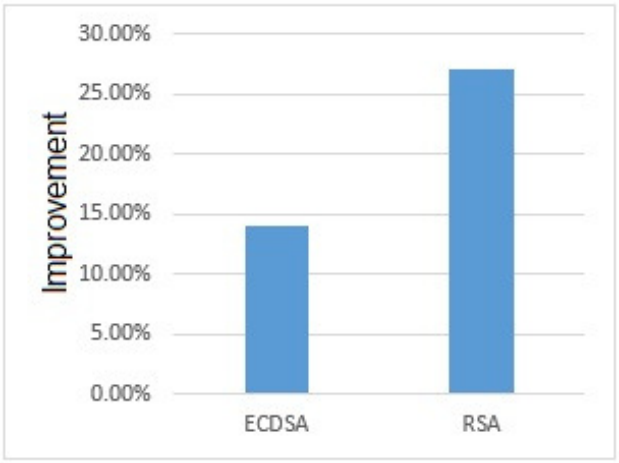

Figure 8 Extent of delay reduction

8 . CONCLUSION AND FUTURE WORK

This study addressed the improvement of EAP-TTLS authentication protocol by simultaneous use of cryptography and digital signature. It also evaluated the proposed method in terms of time and memory usage. Simulation results demonstrate an improvement in this regard. Given that the security of computer systems is among current challenges, assessing the performance of the proposed method against known attacks such as replay attacks, Denial of Service attack , man in the middle, masquerade attack, guessing password attack and security of session key can be a subject of future studies.

9. REFERENCES

[1] Jagyasi, T.,& Pimple, 2014, "JSecurity Enhancement in Cloud Computing Using Triple DES Encryption Algorithm", Conference on Industrial utomation And Computing, pp.200-231.

[2] Masayuki Okuhara,Tetsuo Shiozaki,Takuya Suzuki, Security Architectures for Cloud Computing, Fujitsu Sci. Tech.J., Vol.46,No.4,October 2010

[3] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", IEEE on ICTC, 2012.

[4] Lo'aiTawalbeh,Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari, "A Secure Cloud Computing Model based on Data Classification", ELSEVIER 2015.

[5] Vineet Guha, Manish shrivastava, "Review of Information Authentication in Mobile Cloud Server SaaS & PaaS Layers", International Journal of Advanced Computer Research, Vol. 3, No. 1, Issue 9, March 2013, ISSN: 2249-7277, pp. 31-35

[6] Indrajit Das, Riya Das, "Mobile Security (OTP) by Cloud Computing", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2, Issue 4, August 2013,

[7] Jin mookkim, Jeong-Kyung moon, "Secure Authentication System for Hybrid Cloud service in Mobile Communication Environments", International Journal of Distributed Sensor Networks, Vol. 2, July 2014, pp. 62-66.

[8] Davit Hakobyan, "Authentication and Authorization Systems in Cloud Environments, International Journal of Information and Communication Technology, Vol. 4, Issue 5, October 2012, pp. 165-169.

[9] R. Gokaj, M. Ali Aydin, R, Selami Z bey, "Mobile Cloud Authentication and Secure Communication", In Proc. of International Conference on Information Security and Cryptology, September 2013, pp. 42-45.

[10] Sanjoli single, Jasmeet Singh, "Cloud Data Security Using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET),Vol. 2, Issue 7, July 2013, ISSN: 2278-1323, pp. 81-85.

[11] Neha Tirthani, Ganesan R., "Data Security in Cloud Architecture Based on Diffie-Hellman and Elliptical Curve Cryptography", Vol. 4, Issue 7, July 2013, pp. 82-86