A Security Architecture for Use in Mobile Medical and Electronic Health

Mostafa Akhavansaffar*, Ali Nakhaei, Mostafa Mokhtari Ardakan
Department of ICT Engineering, Payame Noor Universtiy(PNU), Tehran of Iran.

*Corresponding author. Tel.:(098)5632835300; email:akhavansaffar@pnu.ac.ir
Manuscript submitted September 2017; accepted November 2017.
doi: 10.17706/jcp.13.7.794-804

Abstract: E-health and providing health services is one of the areas of science and technology with an increasingly growth in health - care area in the world. In this system, all health services ranging from the patient's electronic file, telemedicine, evidence-based medicine, informing the citizens and informing the professionals and virtual medicine teams are provided. However, due to high importance of sending confidential data through communication lines in electronic systems, including telemedicine medical and probable irreparable damage in failure to address security issues and possible attacks, designing the security mechanisms before using such systems seems vital and necessary. Hence, in this paper, a secure and low-risk model for use in telemedicine systems is suggested using cryptography and safe functions. One of its features besides having high security includes using a lightweight asymmetrical cryptographic system rather than conventional methods and heavy encryption systems. To demonstrate the usefulness of the proposed protocol, we needed to design it in such a way to be used with available wireless technologies and Internet. Actually, the proposed protocol comparing with the current authentication systems, which use the public key encryption algorithms with heavy computing, increases the security of mobile health systems without having to do heavy computations meanwhile simplifying the process of mutual authentication. The system provides the security requirements for mobile medical systems by using the lightweight cryptographic functions such as symmetric encryption and hash functions. In this paper, a new protocol for bidirectional authentication and exchange of session keys for use in mobile medical systems was proposed. It has all services of a mobile medical system without increasing the size of calculations with minimal computational requirements and it providing high security.

Key words: Telemedicine, authentication, mobile health, security, X.509 certificate.

1. Introduction

Information and communication technology and its development have made many changes in every science and industry; the medical science has not been exempted from this rule. In addition to Internet effects on medical science progress, it has also a significant impact on development and improvement of providing health services. Following the creation and development of computer and subsequent emergence of advanced information systems such as computer networks and Internet globalization, everyone thought of using these systems for informing on their own profit. Meanwhile, the treatment sections also thought to provide better services to all people through the Internet, since this sector was responsible for one of the most tasks. Electronic health and providing health services is one of the areas of science and technology that has grown increasingly in health - care domain in the world. In fact, "Electronic Health" is a new word that we need to use a combination of information technology and electronic communications in the health and treatment sector to describe it. Electronic- health is a new approach in health care, diagnostic and

therapeutic procedures that is supported by electronic and communicative processes. In this system, all health services ranging from the patient's electronic file, telemedicine, evidence-based medicine, informing the citizens and informing the professionals and virtual medicine teams are provided. Telemedicine is a communicative bridge between medical and engineering sciences, in which the medical society uses engineering services to promote the community's health level. Telemedicine is a new term that is defined in using electronic information and communication technologies to provide services and protect the consumers when there is a distance between two groups of the clients and the service providers. The goals of telemedicine include improvement of patient care, improvement of access to medical care for rural and underserved areas, better access to doctors for counseling, making the facilities and equipments available for physicians to conduct automatic physical examinations, reducing medical care costs, development of health care services (in vast geographic and demographic levels), reducing the transfer of patients to the hospitals and treatment centers. Telemedicine includes distance counseling, electronic learning of remote monitoring, remote operation, remote treatment of skin diseases, remote ultrasound imaging, remote pathology, remote cognitive disorders therapy. Today, telemedicine has progressed up to a level to make distance surgeries possible. This means that a proficient surgeon in one country can perform a surgery in a surgery room of another country by applying robots with using very powerful Internet communications and accurate technical infrastructure. Security is considered as a serious issue and a major challenge in mobile medical systems due to the users' mobility, limited resources in wireless devices and the expensiveness of radio bandwidth. However, mobile medical systems provide a set of security requirements such as authentication, privacy, integrity, non-repudiation, protection of the private bounds, availability and reliability. Among the mentioned security services, authentication is considered a basic and important mechanism. The authentication is a process by which the system investigates and confirms the reliability of a user who intends to communicate; using this system, the users with and without access permissions to service can be differentiated. In the mobile medical field, comprising three pillars, namely the patient, physician and hospital should have resources and software by using which, they could make sure the accuracy and health of the established communication with the expected person. In addition, they need to establish a secret session key to perform private activities such as patients' test results and patients' online visits. In recent years, the problems related to providing authentication service in mobile environments have been studied and some methods have been also suggested for their improvement that suggested bilateral authentication protocols in normal conditions require heavy operational load, especially in the side of mobile phone in all of them [1]. Symmetric authentication protocols are used to reduce the heavy volume of the calculations in mobile devices. However, all of them need an authentication server to create a session key for two final users. Therefore, the server not only can help to the authentication process, but can also access to the subsequent confidential exchanges, which were encrypted by the session key. To solve the problem, the protocols are used that enable the two end-users to produce the session key without contribution of the authentication server [2], [3]. These methods are more secure than other proposed methods because the server has no access to the confidential exchanges after authentication. However, these methods are also insecure due to weaknesses against password-guessing attacks [1]. Although the proposed solutions had made this method safer and more convenient compared to other protocols, but one of its fundamental problems was the necessity of heavy calculations.

The main objective of this paper is to provide a safe and effective authentication protocol to use in mobile medical systems. This mutual authentication protocol is the session key establishment between the mobile patient and online medical center, and needs lower calculations in comparison with existing protocols in mobile medical systems. Hence, it is much more suitable for using in mobile medicine due to savings in cost, memory and power consumption of mobile devices. For this purpose, the authentication services have been

used in the proposed protocol to establish mutual authentication and reduce the calculations, which are supported by network operators [4].

In the next section, after a brief description about the requirements for authenticating in mobile medical systems, we will describe and analyze the details of the provided protocol.

2. Security Requirement

To create a session key and performing secure authentication between the mobile patient and the hospital or medical center through the Internet, the authentication protocols needs to provide the following security requirements [5], [6]:

- Hospital's authentication by the mobile patient

The authentication protocol should make it possible for the mobile patient to check the accuracy of the treatment service provider center, which is called hospital. This will prevent impersonation attacks. Using this protocol, the attacker cannot introduce himself as the treatment center and communicate to the mobile patient.

- Mobile patient's authentication by the treatment center

The authentication protocol should make it possible for the health center or hospital to check the accuracy and validity of the mobile patient for assurance.

- Creating an end-to-end session key

The protocol should make it possible so that the patient and the treatment center can use a shared secret session key to exchange confidential information.

- Verification of the session key

The protocol should make it possible for both the patient and the medical center to check the correctness of the session key that the front side is using it. This makes it impossible to use any other key as the session key for both parties in the session.

- Refreshing the session key

The protocol should guarantee the newness of the session key. This causes the inability of the attacker to access to the confidential communications by using the session keys that have already been used.

3. The Security Protocol

The public key encryption system and Hash functions are used in this design. Later in this section, after explaining the reasons for using hash functions and public-key encryption system in the protocol, we will describe the assumptions and the required network infrastructure to implement the authentication protocol.

3.1. The Reason to Use Hash Functions

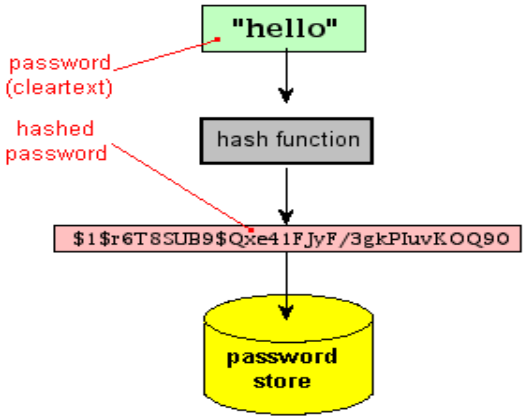

Fig. 1. The performance of hash functions.

Hash code can be considered as the digital fingerprint of a given data. By this method, a fixed-size string of a data can be acquired that is encrypted "one-sided" by mathematical method [7], [8]. Efficient discovering the major string of its Hash string (reverse operation) is almost impossible. Another considerable point is that each data creates a completely unique hashed string. These properties have made "Hashing" to an efficient and ideal method for storing passwords in different applications (Fig. 1).

3.2. Identifying the Users by Using Hash Functions

As mentioned, recovering the original password from the hash string is almost impossible. However, how to detect the passwords by our applications and whether the user has entered the password correctly or not, is so simple! By generating a hash string of the password entered by the user and comparing it with the hash string stored in the database record related to the user, it can be found whether two strings are equal or not. Fig. 2 illustrates this point [9], [10].

Fig. 2. User authentication using the hash function.

We also used the attributes of hash functions in this protocol for secure sending of values and passwords as between the patient, authentication server and mobile care center.

3.3. Public Key Encryption System

Distribution and exchange of encryption keys has been always one of the problems in cryptographic systems. Regardless of how an encryption system is powerful and robust, when a trouble-maker or a hacker could steal an encryption key, the entire system will be worthless [11]. The code breakers always and wholeheartedly welcome the methods in which the encryption and decryption keys are the same (or can be calculated by each other). In these methods, the keys should be finally distributed among the system users. An inherent and internal problem seems to be existed just here. On one hand, the keys should be protected against stealing, and on the other hand, they have to be distributed among the users. One of the available systems to confront such weaknesses, in which the encryption and decryption keys are different, is public key encryption system. In this system, the decryption keys cannot be actually decoded even having the encryption keys [12], [13]. Public-key encryption requires that each user has two keys: a public key that the whole world uses to send a message the user and a private key that the user needs to decode the messages. This system has the following features [14], [15]:

- P = D (E (P))
- Deduction of "d" (decryption key) from "e" (encryption key) is extremely difficult.
- It is not decoded through the mechanism of "attacking with selected and known texts".

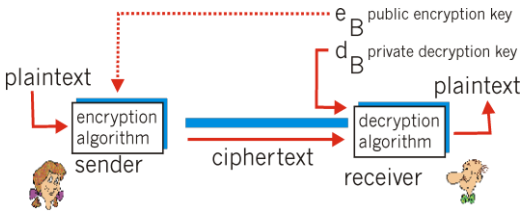

Fig. 3. Public key cryptography system.

4. Scheme Assumptions

The assumptions used in designing the protocol are as follows:

- (a, b): Joining the values of a and b
- h (m): A one-way hash function that should have at least the following characteristics (Bart, 1993):

1. Calculation of h (m) should be easy for each input such as "a".
2. Preview resistance: For any given m, calculating of "m", when h = hash (m), should be difficult.
3. Weak collision resistance: For any given m1 input, finding the m2 input when $hash(m_1) = hash(m_2)$ should be difficult.

Note that the first condition is stronger and actually contains the second condition.

4. Collision resistance (strong): Finding each pair of input, when $hash(m_1) = hash(m_2)$, should be difficult. Since there is the possibility to use the birthday paradox to find a collision, the length hash value in this case should be at least two times of the required resistance for the preview.

An example of hash functions associated with the generated string length is shown in Table 1.

Table 1. Examples of Hash Functions with Generated String-Length (Danilo 2008)

Length	Function Name	Length	Function Name
160 bits	HAS-160	160 bits	SHA-1
512 bits	Whirlpool	128 bits	MD5
160 to 512 bits	FSB	128 bits	MD4
512 bits	SHA-512	128 bits	MD2
256 bits	BLAKE-256	224 bits	SHA-224
512 bits	SWIFFT	256 bits	SHA-256
512 bits	BLAKE-512	256 bits	GOST

K_{A-B} : Joint session key between two communicating parties of A and B

$pubK_A$: "A" public key

$privK_A$: "A" special key

g=f(a): A function that converts a to the DH basis.

$\{m\}K$: The encrypted m value, which is encrypted by "K" key and using a public key encryption system such as RSA.

X.509:the certificate base X.509 standard.

CA: the abbreviation of Certificated Authority

AS: Authentication server in Network operator.

5. Hardware and Software Infrastructure of the Network

The protocol presented in this paper provides a useful and secure authentication service between the two communication parties in the mobile medical system. Its infrastructure consists of three main components:

- A mobile patient who uses a mobile device such as a mobile phone or a PDA (called P)
- An online treatment center (called H)
- A secure authentication server, which is called as "AS" within the network operator.
- A Certificate Authority Server, which is called "CA" .

"P" communicates with "H" to do a secure transaction in a mobile medical environment. "H" responds to performing the secure transaction with "P". The network operator provides the required

conditions for a wireless connection as well as the required bandwidth for communication between "H" and "P". The "AS" is also responsible for performing mutual authentication task between "H" and "P".

6. Increasing the Security Index of the Mobile Medicine System Protocols by Attachment of Digital Signature to the Encryption Algorithm

The signatories can be made to identify themselves to confirm the comprehensiveness of the document through signing the end of a document; it also makes the individuals to be committed to its contents. For the same reason, in addition to make the data confidential through encryption, using the X.509 protocol in public-key encryption algorithm to verify the digital signature made by the message sender, which is the same patient, will be suggested.

A digital signature is a number that is generated by the sender of the message and is attached to the message. It is performed in order to determine the identity of the sender and confirm the integrity of the message and prevent the tampering of the message while communicating by an attacker. In this transmitting system, the private key is used to generate a digital signature. The relevant public key, which exists in the X.509 digital certificate of the sender, is used to verify the signature. The digital signature is used so that the recipient becomes sure the received message is from the same valid sender, which is expected and no one else; also, as the message has been signed by the sender, its content has not changed along the way. The public key will be distributed among all to decrypt the message and verify the signature, while the private key is only available to its owner. The following Fig. 4 shows the digital signature process with the public key.

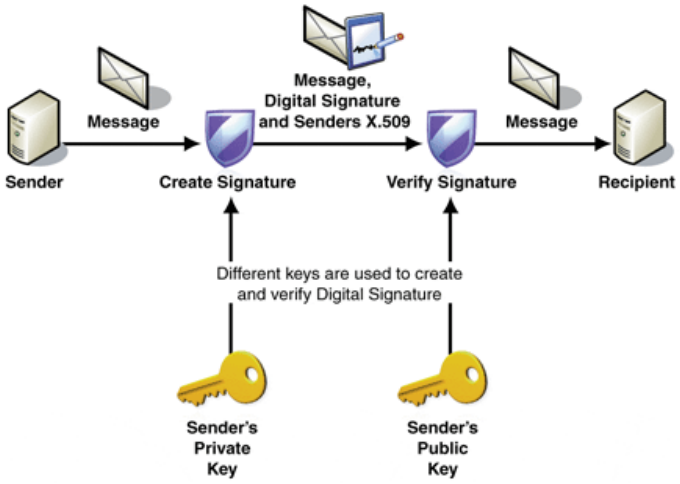

Fig. 4. Creating and verifying a digital signature.

6.1. X.509 Certifications

The predicted structure for fields of this certification is stored by ASN.1 format. ASN1 is a standard that is used to code and decode the data in the network level. The reason for using this type of encoding for X.509 certificate storage is independent from its machine format and can be easily coded and decoded by any other machine. The structure ofx.509 digital certificate includes the following parts: Certification copy, certification serial, encryption algorithm by which this certificate is signed by certificate issuance centre, the certificate issuer information, certificated authority start date, certificated authority end date, information of an individual or a centre that the certificate was issued to him, the algorithm that its public key has been registered in the certificate, like RSA or DSA, containing the public key certificate.

6.2. Certificated Authority

C.A. is the abbreviation of Certificated Authority and means that the certificate is valid. It is the organization responsible for issuance of the electronic certificates that is responsible for verifying the electronic transaction of the trader. For obtaining digital certificates without extra work, one of the CAs can be used in the structure of the mobile medicine. CA types will not be discussed here. The following Fig. 5 shows the request and issuance process of X.509 digital certification.

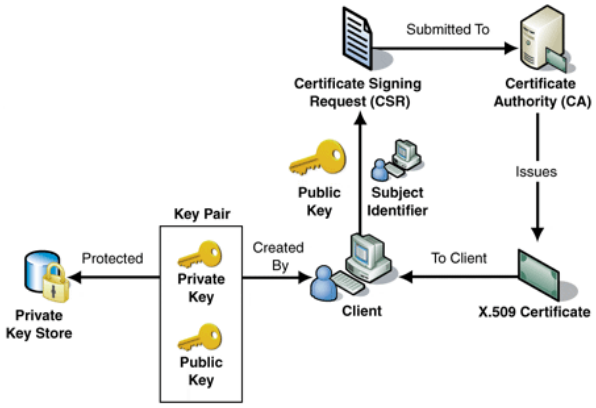

Fig. 5. Request and issuance process of X.509 digital certification.

7. Protocol Description

In this section, we explain different stages of the designed protocol work.

1. "*P*" generates g using a differ helman function ($g = f(a)$), with a secret random number as "*a*" and encrypts it with "*H*" public key. This message means the request for authentication. The public key algorithm makes the calculation of "*a*" so difficult for the attacker without knowing the private key of "*H*". Therefore, "*a*" is a secret value that is shared only between "*P*" and "*H*". Then, "*P*" generates a hash function that is formed from joining a random number encrypted by the public key, "*H*" index, "*P*" index number and the K_{P-AS} Key, which only the "*P*" and "*AS*" are aware of it and is used for communication between the "*P*" and the authentication server.

$$h(\{g = f(a)\}pubK_H, id_H, id_p, K_{P-AS}) \quad (1)$$

Then, "*P*" sends the random number encrypted with the public key, "*H*" index, "*P*" index and the generated hash function with to the authentication server.

2. Upon receiving information from the phase *I*, the authentication server generates a new value by using the information received and its available K_{P-AS} key and using the same hash function and compares it with the received Hash function value. If the two values of Hash function are not equal, the authentication server will ask the "*P*" to re-send the data from phase 1 or will terminate the connection. Otherwise, the authentication server becomes sure that the authentication of "*P*" has been properly done. Then, the server will generate a new value by applying Hash function on the parameters, including the random number encrypted by the "*H*" public key, server index, "*P*" index and the K_{H-AS} key and send it to "*H*".

$$h(\{g = f(a)\}pubK_H, id_P, id_{AS}, K_{H-AS}) \quad (2)$$

K_{H-AS} is the shared key between the "*H*" and the authentication server.

3. After receiving the phase II data, the "*H*" verifies the accuracy of received Hash value using the K_{H-AS} key. If its accuracy was confirmed, the "*H*" would ensure that the data have been sent from the server. Since

the "*AS*" is a trusted server, the "*H*" ensures that the server has authenticated the "*P*" before sending data in phase II. Therefore, the "*H*" will decrypt the random number, which the "*P*" had encrypted it in phase I with the "*H*" public key, by using the private key that it owns. Then, the "*H*" generates a random number as "*b*" and a session key to communicate with *P* (K_{P-H}). The K_{P-H} session key is obtained from applying the hash function on the two random parameters of "*a*" and "*b*"; meaning: $K_{P-H} = h(g, g')$. This key is used to perform secure exchanges between "*P*" and "*H*". In this phase, the "*H*" sends the values of y, id_p index, id_H and The Hash value($h(\{g' = f(b)\}, id_H, id_p, K_{P-H})$) to "*P*", so that it can verify the accuracy and the credibility of "*H*".

4. In this phase, can compute the K_{P-H} key by using the received "*y*" value and the "*x*" value that has generated in phase I like the other party of the communication and by use of the Hash function on (g, g') ,($K_{P-H} = h(g, g')$), and then using it, it will verify the accuracy of Hash value that had received in Phase III ($h(\{g' = f(b)\}, id_H, id_p, K_{P-H})$). If verification is successful, the "*P*" will ensure that the "*H*" has been authenticated, since only "*H*" can decrypt the authentication message by using the K_{H-AS} key and calculate the "a: value. Finally, the "*P*" calculates the value of $h(K_{P-H})$ and sends it to "*H*", so that the accuracy of key will be verified.

Finally, the "*H*" will calculate the value of $h(K_{P-H})$ using the method and with the K_{P-H}, which it owns. If the calculated value is equal to the received value, the conditions have been provided for sending and receiving data in a secure environment, and the data send-receive phase and will begin.

8. Security Protocol Analyse

As mentioned in Section 2, a suitable and secure protocol for authentication in the Internet environment and for mobile medicine needs to fulfill some security requirements. In this section, we show with the analysis of those requirements on the proposed protocol that theprotocol can cover all the mentioned security requirements.

- The hospital or medical center (*H*) authentication by the patient (*P*)

"*P*" authenticates the "*H*" through authentication message ($\{g = f(a)\}pubK_P$). In Phase III, the "*H*" calculates the value of "*a*" using the $prevK_H$ private keyand DF function, and then generates the K_{P-H} session key using the obtained "*a*". The process is completed, as mentioned in previous section, in phase IV by sending hash values and comparison of the two obtained values.

- The mobile patient authentication by the treatment center

The K_{P-AS} key in phase I indicates that the "*P*" is aware of the server authentication key, and therefore, the "*P*" is authenticated by the server. In addition, the "*H*" knows that the authentication server, as a trusted partner, has authenticated the "*P*". Thus, at the end of phase II, the "*H*" could authenticate the "*P*" successfully.

- Creating an end-to-end session key

Since the session key between the main two parties in the communication is only transmitted in phase III and phase IV and just through hash functions of $K_{P-H} = h(g, g')$, its calculation would not be possible by other users. As noted above, except for the two sides of the communication, the attacker would not be able to calculate "*a*" and "*b*" due to lack of information on public and private keys.

- Verifying the session key

In phase III, the K_{AB} session key is used to calculate the hash value by the "*H*". Then, the "*P*" will calculate the K_{AB} key in this phase upon receiving the message and by using the "*x*" and the "*y*", and compares the received hash value with the hash value that has generated itself. In case of equality, the session key is validated. This is also done in phase IV for its validation by the "*H*". Therefore, this feature will be also

realized in the new protocol.

- Refreshing the session key

The K_{AB} session key is generated using two random numbers of "x" and "y"; the "x" in phase I and the "b" in phase II are generated for each communication. Thus, the session key is refreshing for each connection.

- We suggested the X.509 digital signature to increase the security index as well as a more robust system against the attacks, which will be as following after being applied.

As can be seen in Figure, before starting the first stage, the patient initially sends the request to issue a digital signature to the Center for Digital Certification (CA). Following the issuance of the certification as the previous section, the following items will be sent for authentication server in the network operator:

$$h(\{g = f(a)\}pubK_H, id_P, id_H, K_{P-AS}) \tag{3}$$

$$\{g = f(a)\}pubK_H, id_P, id_H, K_{P-AS}\ , X.509 - certificate \tag{4}$$

Then, the authentication server while doing all security functions described in the previous section, will verifies the accuracy of the patient's digital signature by its owning public key. If confirmed, by repeating all the mechanisms mentioned in the previous section, the request for digital signature to CA is sent, and after receiving the digital signature certificate, will send it to the mobile medical center or the hospital. The same process is performed there to verify the signature, and thus, the last security concern, which is the denial of the sender – receiver, will disappear by verifying the accuracy of the digital signatures.

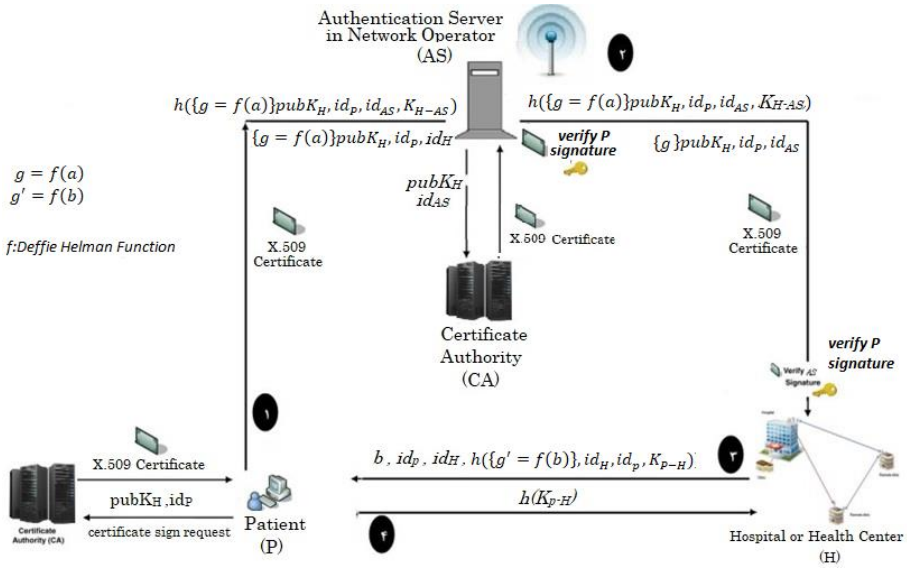

Fig. 6. Telemedicine security scheme.

9. Conclusions and Future Word

In this paper, a new protocol for bidirectional authentication and exchange of session keys for use in mobile medical systems was proposed. This protocol uses an authentication server that is placed in a network operator, which provides the authentication service between the mobile patient and the treatment center. The provided security analysis showed that the studied protocol will realize all the required security requirements in the mutual authentication in mobile systems. It is much more efficient regarding computations and saving in resources in comparison with other systems, because it performs the public key decryption for once (in P side) and does not use encryption exponential functions, while in all the previous examples, the number of encryption has been two times or more, and the encryption exponential functions

have used in them that needs a high volume of calculation. This protocol can be developed for use in wireless systems, especially the mobile communication environments that use of the Bluetooth protocol. Also, the station-to-station key exchange protocol and message authentication code (MAC) can be used to increase the confidence coefficient.

References

[1] Etsuo, K. (2002). Authentication services in mobile networks. *Wireless Personal Communications, 22(2),* 237-243.

[2] Cruzecosta, J., Ojala, T., & Korhonen, J. (2008). Mobile lecture interaction: Making technology and learning click. *Proceedings of International Conference Mobile Learning.*

[3] William, M. (1988). *Daley, Entity Authentication Using Public Key Cryptography.* Department of Computer, Secretary National institute of Standards and Technology.

[4] Minho, S., Justin, M., William, A., & Arbaugh, A. (2005). *Novel Protocol For Iidirect Authentication in Mobile Networks Based on Elliptic Curve Cryptography.* USA: Department of Computer Sciencen University of Maryland College Park.

[5] Wary, J. P., & Maknavicius, M. L. (2011). Secure communications between multi-capacity device with authentication support by network operators. *Charles Fourier*.

[6] Shakibafar, M. (2006). *Setup and Control of Auxiliary Devices by Computer.* NS Press.

[7] Ilya, M. (2005). Hash functions: Theory, attacks, and applications. *Microsoft Research, Silicon Valley Computers*.

[8] Kaavi, J. (2009). *Strong Authentication with Mobile Phones.* Helsinki University of Technology.

[9] Saffarzadeh, M., & Manouchehri, K. (2010). Education through mobile electronic devices. *Proceedings of the 2nd International Conference on Electronic.*

[10] Danilo, G. (2008). *Cryptographic Hash Function Blue Midnight Wish.* Norwegian University of Science and Technology, Trondheim, Norway.

[11] Bart, P. (1993). *Analysis and Design of Cryptographic Hash Functions.* Ph.D thesis, Kathoiliec University Leuven.

[12] Moustafa, H. (2002). Bourdon authentication and services access control in a cooperative ad hoc environment. *G. France Telecom R & D, Issy les Moulineaux*.

[13] Yohans, A., & Bokhman, B. (2004). *Introduction to Cryptography, Technical University of Darmstadt,* Germany: Isfahan Technical University Publications.

[14] Montazeri, G. M., & Mahmoodi, K. M. (2016). Optimized predictive energy management of plug-in hybrid electric vehicle based on traffic condition. *Journal of Cleaner Production, 139,* 935-948.

[15] Anoop, M. S. (2008). *Public Key Cryptography, Applications Algorithms and Mathematical Explanations.* India: Tata Elxsi Ltd Press.

Mostafa Akhavansaffar received B.Sc degree in computer engineering-hardware and received his M.Sc degree in information technology-secure communication from Iran University of Science and Technology. He has been working as a lecturer and a faculty member with the department of ICT, Payame Noor University. He has also published many papers on international conferences and journals. His research interests mobile security, information systems, social network and bigdata.

Ali Nakhaei received his B.Sc degree in computer software engineering from Payame Noor University (PNU), Iran in 2007, and the M.Sc degree in computer system architecture engineering

in Faculty of Electrical and Computer Engineering from Islamic Azad University, Dezful Branch, Iran In 2011. He is working as a faculty member in Department of Computer Engineering at Payame Noor University of Iran since 2014. His research interest includes e-learning, artificial intelligence and mobile app developing.

Mostafa Mokhtari Ardakan received his B.S and M.Sc degree in computer engineering from Iran.He is currently Ph.D student of computer engineering. He has been working as a lecturer and a faculty member with the department of computer engineering, Payame Noor University,meybod,Iran. He is leader of multiple research projects, translator two book in computer science, multiple journal and conference papers. His research interests include image processing, meta-heuristic algorithms and big data.