Journal of Network and Innovative Computing
ISSN 2160-2174 Volume 6 (2018) pp. 034-040

An Ultra Lightweight and Secure Architecture for Mobile Commerce Using Cloud Based Mobile Agents

Mohammad Rasoul Momeni[1], Fatemeh Haghighat[2]

[1] Department of IT Engineering, Faculty of Electrical and Computer Engineering,
Golpayegan University of Technology, Iran
m.momeni@gut.ac.ir

[2] Department of Administrative Affairs
Golpayegan University of Technology, Iran
haghighat@gut.ac.ir

Abstract: Statista.com believes in 2021, 72.9 percent of all retail e-commerce is expected to be generated via mobile commerce, up from 58.9 percent in 2017. One of the obstacles to the expansion of mobile commerce is the restrictions of mobile devices include battery lifetime limitation, less processing power and storage capacity. Cloud computing technology makes mobile users stronger beyond the mobile computing capabilities. Security and privacy issues are another obstacle. In this paper we proposed an ultra lightweight and secure architecture for mobile commerce using cloud based mobile agents. Due to the significant advantages of mobile agents, we used them in the proposed architecture. Our proposed architecture has many advantages such as session key agreement, Support for user anonymity and so on. Also our proposed architecture is robust against related attacks such as parallel session, known plaintext and so on.

***Key Words*:** Mobile Commerce- Lightweight- Security- Cloud Computing- Mobile Agent

I. Introduction

Due to technological advances, a new type of e-commerce has emerged, namely mobile commerce (m-commerce). M-commerce can be defined as any type of e-commerce transaction carried out on mobile devices such as smartphones and tablets. As mentioned earlier, 72.9 percent of all retail e-commerce is expected to be generated via mobile commerce in 2021, up from 58.9 percent in 2017. Statistics show worldwide mobile commerce revenues amounted to 96.34 billion U.S. dollars in 2015 and are set to surpass 693 billion U.S. dollars in 2019. Also in second quarter of 2018, online orders which were placed from smartphone and tablets had an average value of 109 U.S dollars and 118 U.S dollars respectively. As we see m-commerce is changing economy and having a great influence on lifestyle of the people of the world. More precisely, m-commerce is more than just a simple evolution of e-commerce. It has also served as a trigger for new services or industries, or helped existing ones grow. The use of mobile devices has significant advantages such as availability, portability and mobility. More clearly, m-commerce enabling people to buy and sell goods or services from almost anywhere, simply using a smartphone or tablet device. But as we know mobile devices have some problems. Indeed, mobile devices face some restrictions that the most important of these is battery lifetime [1]. In order to overcome the limitations of mobile devices, we use technologies such as cloud computing and mobile agent.

The most comprehensive definition of cloud computing is provided by NIST. NIST defines Cloud computing as "a model for enabling ubiquitous, convenient on demand network access to a shared computing resources that can be delivered with minimal managerial effort" [2]. Cloud computing technology offers high processing power and unlimited storage space. In order to save energy on mobile devices, long time application execution on mobile devices is stopping. In fact, implementing heavy and energy-intensive applications is done on cloud servers. In order to have high speed and slight latency in the proposed architecture, we use mobile agent technology. Mobile agent paradigm has recognized as a promising trend of technology. The use of mobile agents in mobile commerce has many benefits such as support automation of decision making, tolerate poor network connections, reduce network traffic, improve trading efficiency and so on. Mobile agent technology is widely adopted in numerous areas like e-commerce [3], computer networks [4], database management systems [5] and medical data transmission [6]. The symbols used in our proposed architecture are given in the Table 1.

II. Related Works

In this section, we will analyze some of the methods proposed in this domain. Nilashi et al proposed a scheme and evaluated the role of security, design and content factors on customer trust in mobile commerce [7]. They used Analytic network process (ANP) from the multi-criteria decision making approaches and fuzzy logic from artificial Intelligence approaches. They developed an ANP-fuzzy logic based model to evaluate and select the most suitable mobile commerce website. The main reason for using ANP in choosing appropriate website was the consideration of interdependency

among sub-criteria that affects the priority of criteria. Fuzzy logic was used for measuring trust level, uncovering hidden relationship between websites' features and trust level, solving the uncertainty problem and handling human reasoning where the reasoning processes behind customers' trust in mobile commerce transactions were taken into account.

Shirazi and iqbal proposed a framework focusing on privacy topics in mobile commerce [8]. They established a link between community clouds and m-commerce. They tried to provide an understanding of the various shopping domains and their convergence through mobile devices. Two models called privacy by design (PbD) and privacy enhancing technology (PETs) have been used in this research. Leu et al proposed a secure m-commerce scheme called secure m-commerce system [9].

Table 1. Symbols

Symbols	***Description***
R	*A high entropy secret random number*
H()	*A collision free one way hash function*
IMSI	*International mobile subscriber identity*
TMSI	*Temporary mobile subscriber identity*
‖	*Concatenation operator*
LAS	*Local authentication server*
MAC_{LAS}	*MAC address of local authentication server*
P_{MU}	*Service permissions allocated to the mobile user*
$Cert_{MU}$	*An authentication certificate*
SK	*A session key*
r_1 *and* r_2	*Random numbers*
AK	*An authentication key*
E	*Symmetric Encryption Algorithm*

In this scheme users can create a safe credit-card transaction for Internet shopping. Their proposed scheme uses a Data Connection Core to link the card-issuing bank and consumers before their wireless communication starts so as to significantly improve the security level of m-commerce environment. The analysis of performance and security is based on three theories. Shoaib alam proposed a secure m-commerce framework using post quantum cryptography [10]. They used McEliece cryptosystem. McEliece cryptosystem is an asymmetric encryption method and it has some benefits over RSA. The encryption and decryption operations are very fast. McEliece cryptosystem is a type of public key cryptosystem based on error correcting codes called Goppa code. Goppa codes are linear, error correction code that can be used to encrypt and decrypt the information or messages. Already, McEliece cryptosystem is unbreakable. Prisha et al proposed and developed a Mobile Identity Verification Application (MIVA) [11]. MIVA consists of two-factor login verification, order verification and fingerprint scanning with risk analysis. MIVA requires first time users to register themselves with a unique user ID and password. Also a risk analysis feature was incorporated to categorize suspicious users to respective risk groups based on risk range and ratings from ‘Very Low’, ‘Low’, ‘Moderate’, ‘High’, ‘Very High’ to ‘Extreme’ during the fingerprint scanning process. Their main goal is to protect identity against identity theft attacks.

III. Proposed Architecture

In this section our ultra and secure architecture is presented. The time for remote authentication protocols is too long, especially in wireless mobile environments. Hence our architecture provides local authentication. In our architecture mobile user is authenticated in his/her mobile network and therefor this protocol provides very low latency and saves bandwidth. Low latency is a key feature in level of user satisfaction. In the end of mutual authentication and session key agreement mobile user receives a $Cert_{MU}$ from his/her mobile service provider then presents it to the cloud service provider. Note that mobile service provider and cloud service provider are fully trusted together. Proposed lightweight and secure architecture consists of four phases namely: registration phase, mutual authentication and session key agreement phase, authentication key change phase and finally user eviction phase. First, we describe the registration phase. General architecture of our proposed scheme is presented in Figure 1.

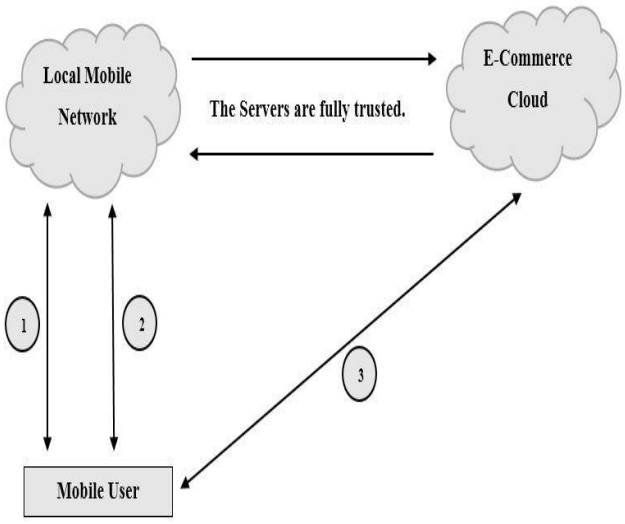

Figure 1. *General Architecture of the Proposed Architecture*

A. Registration Phase

In this phase mobile user performs registration phase via secure channel as follows. Note that registration phase is done only once when the mobile user wants to join the local mobile network.

1- The mobile user submits his/her *IMSI* as identity and some personal secret information to the local authentication server located in the local mobile network.

2- Now the server validates the *ID* and if it exists in the server database then rejects it immediately. Mobile user must prepare unique *ID*. According to the above procedure, identity management is provided. Now the server can compute authentication key $AK = H(IMSI \| R)$ which R is a high entropy secret random number and $H()$ is a collision-free one-way hash function.

3. The server returns AK and P_{MU} to the mobile user, which P_{MU} is permissions of mobile user allocated by local mobile network.
Details of registration phase is depicted in Figure 2.

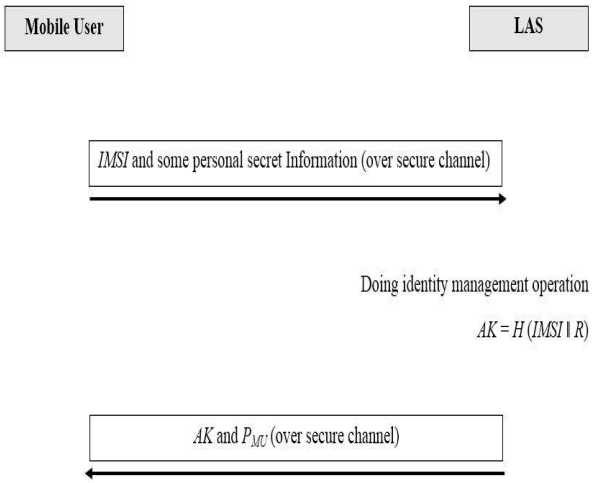

Figure 2. *Registration Phase*

B. Mutual Authentication and Session Key Agreement

After registration phase whenever mobile user wants to use mobile network services, he/she must be authenticated. Therefor he/she sends a login request message to the local authentication server and then local authentication server verifies the authenticity of the login request message as follows:

1- The mobile user generates a random number r_1 and message $N_1 = (P_{MU} \| r_1)$, then encrypts N_1 by the AK. He/she sends $M_1 = (TMSI, E_{AK}(N_1), MAC_{LAS}, H(TMSI, E_{AK}(N_1), MAC_{LAS}))$ to the LAS. To provide user anonymity and ensure user privacy instead of using *IMSI*, *TMSI* is used.

2- After receiving M_1, the local authentication server computes $H^*(TMSI, E_{AK}(N_1), MAC_{LAS})$, then checks $H = H^*$ for detecting modification attack. If H is not equal to H^* and *TMSI* is not valid then LAS aborts the current session. Hence denial of service attack can be eliminated. Then LAS decrypts the N_1 and obtains P_{MU} and r_1. Now LAS generates r_2, $Cert_{MU}$ and message $N_2 = (Cert_{MU} \| r_1 \| r_2)$. Also LAS generates $SK = H(TMSI \| r_1 \| r_2)$ and sends $M_2 = (E_{AK}(N_2), MAC_{LAS}, TMSI, H(E_{AK}(N_2), MAC_{LAS}, TMSI))$ to mobile user.

3- After receiving M_2, mobile user computes $H^*(E_{AK}(N_2), MAC_{LAS}, TMSI)$ then checks $H = H^*$ for detecting modification attack. If H is not equal to H^* then mobile user aborts the current session. Hence denial of service attack can be eliminated. Then mobile user decrypts the N_2 and obtains the $Cert_{MU}$, r_1 and r_2. Also he/she checks random number r_1 to avoid replay attacks. Mobile user generates $SK = H(TMSI \| r_1 \| r_2)$, hereafter both sides use SK for encrypting the messages instead of AK. Note that AK and SK are valid only in each session, namely they will be different for different sessions. Authentication and session key agreement is shown in Figure 3.

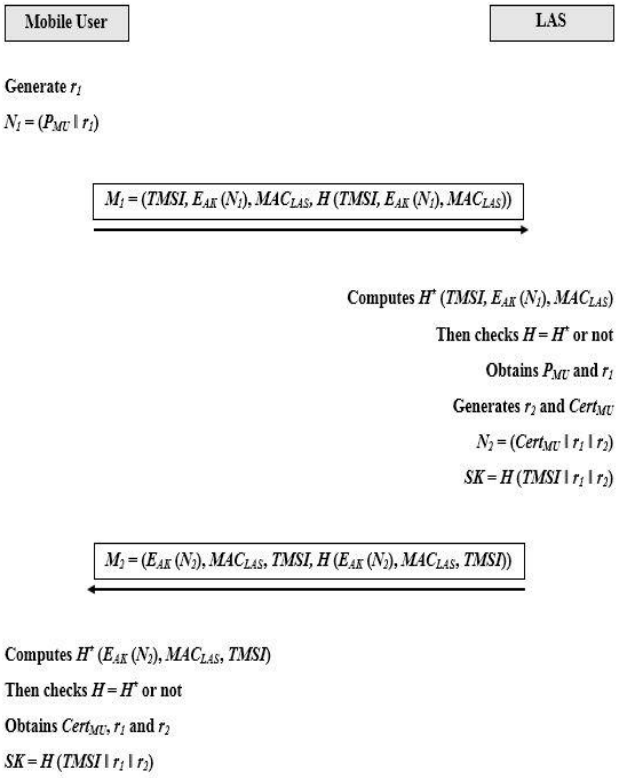

Figure 3. *Authentication and Session Key Agreement*

C. Connecting to E-Commerce Cloud

How can mobile user connect to e-commerce cloud? It is very simple. The mobile user submits his/her certificate ($Cert_{MU}$) to the e-commerce cloud. The certificate consists of issue date, expiration date, *IMSI*, *TMSI* and digital signature of local mobile network. E-commerce cloud validates the submitted certificate and will issue a permit if it is successful. We use mobile agent technology to exchange messages between the mobile user and the e-commerce cloud. Mobile agent technology prevents enormous workload which is resulted from enlargement of network. Mobile agent technology has several advantages such as dynamical adaptation, heterogeneity, high network latency resistance, asynchrony

and autonomy, network traffic reduction, natural low network loads, and fault tolerance [12, 13]. In this way, the low latency and high speed of the proposed architecture are maintained.

D. Authentication Key Change Phase

Whenever mobile user wants to change his/her authentication key (e.g. when an authentication key is leaked, he/she needs to get a new one.) he/she must submit his/her *IMSI* as identity, old authentication key and some personal secret information through secure channel to the LAS. Now LAS validates the mobile user and if it is successful, then selects a new random number R^* and generates the new authentication key $AK^* = H(IMSI \parallel R^*)$. Now LAS sends AK^* to the mobile user. Authentication key change phase is depicted in Figure 4.

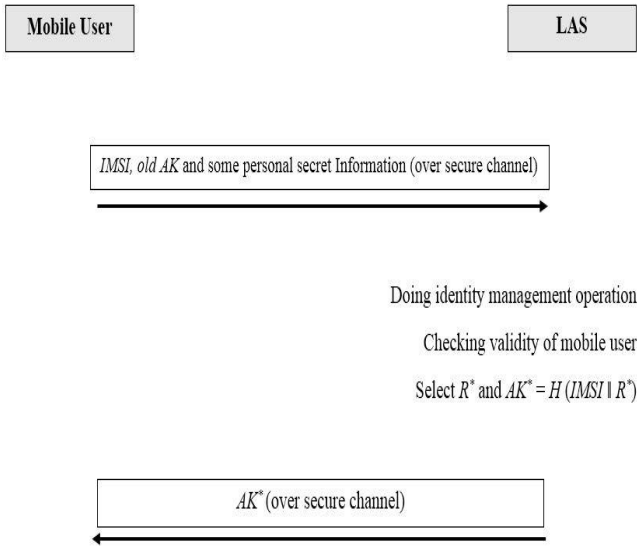

Figure 4. *Authentication Key Change Phase*

E. User Eviction Phase

Whenever local mobile network evicts a mobile user, his/her assigned certificate must also be revoked. The certificate revocation operation must be immediately notified to e-commerce cloud. Because the user may be revoked before the expiration of his/her certificate. In this case, the revoked mobile user cannot log in to e-commerce cloud. The user eviction operation consists of two steps: First delete the *IMSI* and then enter it in the blacklist. Consequently, at each step, identity management is performed and mobile user request to log in is denied.

IV. Security Analysis

In this section, security features of our proposed architecture is presented. We demonstrate our proposed architecture is robust against related security attacks.

A. Modification attack resistance

In order to avoid modification attack, we used a collision free one-way hash function. If an adversary sends a modified message, both local authentication server and mobile user can easily detect it by validating the hash values.

B. Parallel session attack resistance

Both local authentication server and mobile user exist in the hash functions of exchanged messages M_1 and M_2. This mechanism prevents parallel session attack and our proposed architecture is robust against parallel session attack.

C. Man in the middle attack resistance

Because of having mutual authentication in our proposed scheme, man in the middle attack does not enter to our scheme. In our proposed architecture, local authentication server authenticates the mobile user and also mobile user authenticates the local authentication server.

D. Replay attack resistance

Our proposed architecture uses random numbers to prevent replay attack. It is hard for adversaries to guess the values of random numbers. Random numbers change in each session and time of authentication. Thus our proposed architecture is robust against replay attack.

E. Server spoofing attack resistance

As mentioned above, our proposed architecture provides mutual authentication. This feature eliminates the possibility of server spoofing attack.

F. Password guessing attack resistance

Our proposed architecture is robust against password guessing attack, because it is not password based. Password based schemes are highly vulnerable and so we did not use password in our proposed architecture. Password based schemes must follow strict security policies to keep itself away from possible attacks.

G. Known plaintext attack resistance

Adversaries don't know the value of $AK = H(IMSI \parallel R)$. Because *IMSI* transmits through secure channel in the registration phase and in the authentication phase, *TMSI* transmits instead of *IMSI*. Also R is a high entropy secret random number and guessing the value of R is very difficult.

H. Stolen verifier attack resistance

Local authentication server does not keep any secret table or

any pre-shared secret key. There for adversaries cannot obtain any valuable information from launching this attack. As a result, our proposed architecture is robust against stolen verifier attack.

I. Known key attack resistance

Our proposed scheme is robust against known key attack, because random numbers are one-time and change in each session and time of authentication. Hence obtaining a session key does not mean getting other session keys.

J. Denial of service attack resistance

Every time a modification attack is discovered, the session is canceled immediately. Also, if three consecutive unsuccessful login operations are evaluated, the user's account is temporarily disabled. Hence our proposed architecture is robust against denial of service attack.

V. Performance Analysis

In this section, we evaluate the performance of our proposed architecture. Note that an appropriate scheme for mobile commerce should be lightweight and have low computation cost.

A. No clock synchronization problem

Many of proposed authentication protocols use timestamp mechanism to prevent replay attacks. Timestamp mechanism is difficult and expensive in wireless mobile communications [14] and distributed networks [15, 16, 17]. Our proposed architecture is nonce-based and does not have clock synchronization problem

B. Local authentication

Our proposed architecture presents local authentication. Saving bandwidth and low latency are two big advantages of local authentication [18].

C. Mutual authentication

Whenever it requires a high level of security in the communication between the server and the mobile user, mutual authentication is required. Our proposed architecture supports mutual authentication that eliminates the possibility of some attacks like server spoofing, impersonation and man in the middle [19].

D. Identity management

Our proposed architecture supports identity management as follows. In the registration phase, second step of mutual authentication and session key agreement and also in the authentication key change phase identity management is done.

E. Session key agreement

In our proposed architecture a session key is generated which uses random numbers. This session key provides secure communications over open channels by encrypting the exchanged messages. Session key agreement significantly increases security.

F. Scalable and fast

Using an independent center for authentication operations makes our scheme scalable [20]. In this case, it is possible to respond to requests from a large number of users simultaneously. Also, the use of symmetric encryption algorithm and local authentication have prompted a very high speed on our proposed architecture.

G. User Eviction

User eviction phase is an important feature of our proposed architecture. This phase guarantees the proposed scheme's security at a high level. Whenever an evicted user tries to login, he/she will fail, because identity management operation is done in our proposed architecture.

H. User anonymity

User anonymity means protecting real identity of user against public, no server [21]. Our proposed scheme satisfies user anonymity, because in the registration phase *IMSI* (real identity of user) transmits through secure channel. In the authentication phase and session key agreement instead of *IMSI*, *TMSI* transmits to the local authentication server.

I. Authentication key Change Phase

When an authentication key is leaked, mobile user needs to a new authentication key. Our proposed architecture supports Authentication key change phase. As mentioned, after evaluating the validity of mobile user, local authentication server generates a new authentication key and sends it to the mobile user.

J. Low latency and bandwidth

Because of having local authentication and using symmetric encryption algorithm, low latency and bandwidth features are realized.

VI. Conclusions

In this paper we proposed an ultra lightweight and secure architecture for mobile commerce using cloud based mobile agents. Our research has two important achievements. The first achievement is combination of technologies such as mobile commerce, cloud computing, security and mobile

agents. The second achievement is proposing local authentication. The time is long for remote authentication protocols, especially in wireless mobile communications. Extending the authentication time will cause the user to be dissatisfied. In our proposed architecture mobile user is authenticated in his/her mobile network, therefor this mechanism provides low latency and saves bandwidth. Also our proposed architecture satisfies mutual authentication, user anonymity, identity management and so on. In terms of resistance against related attacks, our proposed architecture is robust against server spoofing attack, modification attack, replay attack and so on. It is important to note that our proposed architecture is according to real communication scenarios. Our future research directions include developing a lightweight and secure electronic payment platform for our proposed architecture and considering multiple e-commerce clouds.

References

[1] M. R. Momeni. "A Survey of Mobile Cloud Computing: Advantages, Challenges and Approaches". International *Journal of Computer Science and Business Informatics*, Special Issue: Vol. 15, No. 4, pp. 14-28, 2015.

[2] P. Mell, T. Grance. the NIST definition of cloud computing (draft). 2011. http://csrc.nist.gov/publications/drafts/800–145/Draft-SP-800-145_cloud-definition.pdf.

[3] Y. F. Chung, Y. T. Chen, T. L. Chen, and T. S. Chen. "An agent based English auction protocol using elliptic curve cryptosystem for mobile commerce". *Expert Syst. Appl*. 38(8):9900–9907, 2011.

[4] N. Saxena, G. Tsudik, and J. H. Yi. "Threshold cryptography in P2P and MANETs: The case of access control". *Comput. Netw*. 51:3632–3649, 2007.

[5] J. Biskup, D. W. Embley, and J. H. Lochner, "Reducing inference control to access control for normalized database schemas". *Inf. Process. Lett*. 106:8–12, 2008.

[6] S. Wu, and K. Chen. "An efficient key-management scheme for hierarchical access control in e-medicine system". *J. Med. Syst., Springer*, DOI: 10.1007/s10916-011-9700-7, 2011.

[7] M. Nilashi, O. Ibrahim, Reza Mirabi V., L. Ebrahimi, M. Zare. "The role of Security, Design and Content factors on customer trust in mobile commerce". *Journal of Retailing and Consumer Services*, 26, pp. 57-69, 2015.

[8] F. Shirazi & A. Iqbal. "Community clouds within m-commerce: a privacy by design". *J Cloud Comp*, 6: 22, 2017. https://doi.org/10.1186/s13677-017-0093-0

[9] Leu F.-Y., Huang Y.-L., Wang S.-M. "A Secure M-Commerce System based on credit card transaction". *Electronic Commerce Research and Applications*, 14 (5), art. No. 607, pp. 351-360, 2015.

[10] Md Shoaib alam. "Secure M-commerce data using post quantum cryptography". *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. 2017. DOI: 10.1109/ICPCSI.2017.8391793.

[11] P. Prisha, HF. Neo, TS. Ong, CC. Teo. *IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2018. DOI: 10.1109/ISCAIE.2018.8405467

[12] M. Nikooghadam, and A. Zakerolhosseini. "Secure communication of medical information using mobile agents". *J. Med. Syst., Springer*. DOI: 10.1007/s10916-012-9857-8, 2012.

[13] Gian, P. P., *Mobile agents: An introduction*. Microprocess. Microsyst. 25:65–74, 2001.

[14] Giridhar, P. Kumar, "Distributed clock synchronization over wireless networks: algorithms and analysis", in: *Proceedings of the 45th IEEE Conference on Decision and Control, IEEE*, pp. 4915–4920, 2006.

[15] D. Mills, "Internet time synchronization: the network time protocol", *IEEE Transactions on Communications*, 39 (10) 1393–1482, 1991.

[16] R. Baldoni, A. Corsaro, L. Querzoni, S. Scipioni, S. Piergiovanni, "Coupling-based internal clock synchronization for large-scale dynamic distributed systems", *IEEE Transactions on Parallel and Distributed Systems*, 21 (5) 607–619, 2010.

[17] J. Han, D. Jeong, "a practical implementation of IEEE 1588–2008 transparent clock for distributed measurement and control systems", *IEEE Transactions on Instrumentation and Measurement* 59 (2) 433–439, 2010.

[18] M. R. Momeni. "A Lightweight Authentication Scheme for Mobile Cloud Computing". *International Journal of Computer Science and Business Informatics*, Vol. 14, No. 2, pp. 153-160, 2014.

[19] M. R. Momeni. "A Cloud-based Platform to Ensure Security and Privacy of Medical Data". *International Journal of Information and Communication Technology Research*. Vol. 6, No. 8, 2016.

[20] Momeni, M. R. "An Efficient Authentication Protocol for Mobile Cloud Environments using ECC". *International Journal of Computer Science and Business Informatics*, Special Issue: 15(4), 29-39, 2015.

[21] Z. Tan. "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems". *Journal of medical systems*, 38(3), 1-9, 2014.

Mohammad Rasoul Momeni received the BSc degree from Payame Noor, Iran, in 2011 and MSc from the Imam Reza International University, Iran, in 2014. Currently he is an IT security architect in department of IT at Golpayegan University of technology, Iran. His current research interests are Information security and privacy, lightweight cryptography and computer networks security (Especially security in the SDN and MANet).

Fatemeh Haghighat received the BSc and MSc degree from the Allameh Tabatabai University in 2012 and 2014, respectively. Currently she is a director of welfare affairs in department of administrative affairs at Golpayegan University of technology, Iran. Her current research interests are human resource management, strategic management and organizational learning.