International Journal of Artificial Intelligence and Mechatronics
Volume 2, Issue 4, ISSN 2320 – 5121

Compare Authentication Algorithms for Mobile Systems in Order to Introduce the Successful Characteristics of these Algorithms against Attacks

Shahriar Mohammadi
Assistant Professor of Industrial Engineering Department,
KN Toosi University of Technology, Tehran, Iran
Email: mohammadi@kntu.ac.ir

Hakimeh Ameri
M.Sc. in E-Commerce, Department of Industrial Engineering,
KN Toosi University of Technology, Tehran, Iran
Email: hameri@mail.kntu.ac.ir

Abstract **– Nowadays use of Ecommerce with mobile devices through the special capabilities, such as mobility and widely used become more popular. The security of transactions in these devices is a great challenge due to limited computing power and relatively weak processors. Mutual authentication and session key agreement can be very influential in term of security. Algorithms introduced in the 1990s had major drawbacks. In the 2000s, a new algorithm based on hash functions were introduced, which had a small computational load, but not a high security and mutual authentication cannot fully support. Algorithms introduced from 2010 onwards due to a combination of hash functions Salt and Nonce are safer. This paper examines the success of the algorithms introduced in this field since 2004 deals.**

Keywords **– e-Commerce, Mobile Devices, Mutual Authentication, Security, Session Key Agreement.**

I. INTRODUCTION

E-commerce Describe the processes of business, including buying and selling goods and services over the internet. Since the 1990s, the Internet and a variety of telecommunications have been promoted in many aspects of daily life. According to Internet Telecommunications Union In 2011, there are nearly 7 billion internet users and 5.95 billion mobile phone users worldwide (2013). Mobile broadband subscribers have grown 45% a year in the last four years, and Today's mobile broadband subscribers are twice as fixed broadband subscribers [1].

Development of the Internet and related technologies has revealed new opportunities for business. This led to finding new ways to manage the business and communicate information through the development and expansion of e-commerce. Progress in the E-Commerce has created significant developments in relation to guidelines and strategies, requirements, and development of e-business applications. Consequently, new types of communication services using Internet have emerged through mobile devices. These developments led to the emergence of new opportunities and various services or digital content, called mobile commerce (M-commerce) [2]. Considering that Mobile devices only belong to a particular person, a mobile device allows users better and easier access to services than those use the wired Internet.

Mobile devices such as smart cards, mobile phones and PDA due to the limited memory and computing power, faced with the flaws and shortcomings [3]. Compared with online brokerage services and telephone-based trading services, brokerage mobile services have unique features, such as ubiquity and mobility. These characteristics have led to extremely rapid growth in mobile commerce transactions. Due to the limitations of mobile networks and mobile devices, the Mobile Services Commission has the simpler instruction, slower pace and a simpler interface because of less bandwidth. And Given that smaller devices, smaller screens are used and data entry is inappropriate [4]. As mobile applications become more developed and used in various forms of trade, criminals are more willing to enter this space.

II. PRELIMINARIES

A. Self-certified public key

Self-certified public key procedure includes initialization, public key certificates, and partial private keys, generate a private key and extraction the public key.

B. Collision resistant one-way hash function

One-way hash functions are the original Preparations for authentication. A family of hash functions called collision resistant if after applying a random function H, finding two different inputs x and y that H (x) = H (y) is not practical for an attacker. In other words, finding the input value x is not possible from the outputs of the function H [5].

C. Salted Hash

Adding a random string (0, 1) to the Salt before hashing the password can produce more random hash output and enhanced security. This leads to totally different hash output for the same password string. No need to hide the Salt content. Salt is needed to unlock the password. Salt is often stored associated with a hash or as part of the account [6].

D. Encryption based on nonce

The nonce is a value like a counter that can be used once per session. Using Nonce ensure that unauthorized users cannot access encrypted text without relating Nonce [6].

III. COMPARING ALGORITHMS FOR USER AUTHENTICATION IN MULTI-SERVER ENVIRONMENTS

With the advent of the Internet tow-way authentication lost its effectiveness. Generally remote systems, provide different services that create a variety of sources. Efficient multi-server authentication systems have features such as single registration, mutual authentication, session key

agreement, productivity and security. Single registration is a very important feature in multi-server environments because users need to register once to access all the servers. So do not have too many passwords to remember to communicate with each server. On the other hand Single registration raises Security because the possibility of disclosing passwords in various servers is further. Secure authentication of users in multi-server systems is very important. For greater security, single server registration in this type of networks is an important issue. Recently, remote user authentication protocols based on password and smart cards are highly regarded due to lower costs. Each multi user authentication algorithm based on smart card involves six basic steps: the lunch algorithm to adjust the parameters of the overall system that is done by the server, the key generation algorithm for distributed servers, registration algorithms for the users, Log in algorithm, authentication algorithm, and change passwords.

In this paper we try to review and compare the provided algorithms for mutual authentication in multi-server environments that are suitable for mobile devices. The features that have been improved algorithms are investigated.

One of the first proposed remote authentication algorithms was introduced by Lee and et al. In 2003 is based on the discrete logarithm problem in a multi-server environment. But Jung proved that this model is not efficient. That should be stored plenty of parameters for authentication in applications that are not suitable for smart cards and also did not support mutual authentication and session key agreement. In 2004, Jung improved Lee and et AL's authentication scheme. In This scheme user has one registration at the registration center but its drawback is that each server must hold the approved table that store several key shared between users [7]. In the same year, C. C. Chang and et al proved that Jung's model has not suitable functionality for registration and authentication, so a new model based on Jung's model provided that had little computational cost [8]. Wang and et al in 2007 introduced a secure algorithm with acceptable efficiency for mobile authentication systems to solve the security problems in the algorithm proposed by Yoon et al [9]. In 2008 J. H. Lee and D. H. Lee presented one of the first schemes based on secure and efficient authentication key agreement between a remote user and multi-server environment. The model designed for mutual authentication and session key agreement among users of mobile systems specifically the smart card and server applications. Due to The low-power mobile processors, XOR and Hash functions are used in this system and therefore very suitable for the mobile environment [10].C-C.Chang and T-F.Cheng in 2011 proved that Lee and Lee model is not stable against forgery attack and users had to re-registration in order to use different servers. To resolve these problems, a new method provided based on mutual authentication and session key agreement. BAN logic was used for mutual authentication and claiming their model can resist against forgery attack, Replay, Server Spoofing loss of smart card and could not [11]. C.T.Li and et alIn 2012 proved that Chang-Cheng model is not secured against the smart card loss attacks, guessing offline dictionary attacks and expose session key. Then proposed a model based on that model that would have fixed security bugs [12]. C.T.Li and et al. Demonstrated that Chang-Cheng model In addition to these bugs are not secure against internal attacks. Then presents a model and claim their model is secure against the smart card loss attacks, insider attacks, guessing offline Dictionary attack, forgery and Replay attack, and support mutual authentication, session key agreement and once registration. The computation cost is light because of Hash functions and XOR [13]. Y.P.Liao and S-Sh.Wang in 2009 presented a model based on dynamic ID for secure mutual authentication in a multi - server environment. To avoid the problem of time synchronization, used Nonce-based method to and argued their model is resistance against attacks such as Replay, Two-factor and Server spoofing [14].

H-C Hsiang and WK. Shih the same year demonstrated that the model proposed by La-Wang's is not secure against insider attack, Server spoofing, Replay, Two-factor and forgery attack and not easily modifiable. As a result the new model offers that can resolve better features for multi-server authentication system and eliminates security problems in previous model [15]. In 2008 Tseng and et al. offered a plan to authenticate users with respect to their limited computational power and Claimed their scheme for remote authentication of users in a multi - server environment works pretty well [16]. But Y.P.Liao and CM. Hsiao in 2013 proved that this scheme does not have mutual authentication and session key agreement and failed against insider attacks, guessing offline dictionary attacks and malicious server. The new design for remote user authentication based on the strong coupling provided and claimed the scheme is robust against all types of attacks [3]. In the same year P. Jiang and et al. stated Liao-Hsiao model fails against guessing offline dictionary attacks, Server Spoofing, forgery attack and in addition it does not support user anonymity. Jiang and et al. presented a new model for authentication in multi-server environments that does not require the pairing and supports user anonymity. They also claim that their model resists against a variety of attacks and has low computational cost [17]. In 2012 C. C. Lee and et.al proved that the model proposed by Lee et al in 2011 that is based on a dynamic ID to authenticate users in multi-server environment [18] is not secure from Replay attacks and loss of smart card and does not support user anonymity. Therefore a new model was introduced and claimed is safe against a variety of attacks; this model also supports user anonymity and meets the highest standards of efficiency [19]. In 2011 T. H. Chen demonstrated, the Wang et al model is vulnerable against forgery and parallel session's attacks. Therefore presents a model and claim meets all the security requirements of a session key agreement and authentication as well [20].

But S.Kumari and et al In 2012 demonstrated Chen model is vulnerable against legitimate user attacks, loss of smart card and know the key, has serious consequences to

password guessing attacks, Replay and forgery attack. Therefore a new model was presented and argued is safe against guessing offline dictionary attacks, insider attack, forgery attack and Replay and meets all the desirable features [21]. In 2008, Jung et al model was introduced for user authentication using smart cards that required features like low computational cost, freely chosen password, no synchronization problem, and the agreement of a session key but not secure against anonymity and guessing offline dictionary attacks [22]. To resolve this problem, China and et al (2012) have developed a model based on Jung model that would overcome this problem [23]. Yoon and et al in 2005, submitted a proposal for smart card authentication [24], which did not support mutual authentication, To resolve this problem, Li et al in 2010 provides a model based on two-factor authentication scheme for mutual authentication and session key agreement between the user and unsecured channels [25].In 2012 Qiuyan and et al proved the model proposed by Lee and et al is not secure against lost smart card attack and the Yoon et al. model does not prevent against Denial of Service attacks (DOS) and Fail [26].Zhu et al (2008) proved that Hwang and Yeh model that was a recovery for Peyravian-Zunic password authentication scheme is not secured against attacks. So, introduced a new model for enhanced security based on collision-resistant hash functions, and Salt techniques with time stamped and claim their model is robust against a variety of attacks [27]. But in 2011 Islam and Biswas expressed Zhu and et al. model due to the timestamp has synchronization problem and is not secure against forgery attack [28]. Xu and et al (2009) claimed the model proposed by Lee-Kim-Yoo and Lee-Chiu in 2005 that were designed to Improve remote authentication scheme with smart card [29] ifthe information stored on the smart card is disclosed by the adversary are not secure against Forgery attacks. The new model proposed and provides the security in the random oracle model under the assumption for computational Diffie-Hellman algorithm [30]. In 2010 Song proved that the model proposed by Xu et al. is vulnerable against internal attacks and forgery attacks. Presented a new model based on Xu model and claimed that the new protocol satisfies the security requirements and smart card authentication, are highly efficient [31].Hu et al (2007) introduced a new model based on Liu and et al and argued that is safe against forgery, parallel sessions, lost smart card, interior and Replay attack [32]. In Table I, the performance of algorithms from 2004 to 2013 in terms of the required calculations is compared.

Table I: Comparing the performance of the proposed algorithm from 2004 to 2013 in terms of computation required.

Row	Authors and year	Computations in registration phase	Computations in login phase	Computations in authentication phase	Amount of computation cost
1	Jang's algorithm(2004)[7]	n^* syn (n+1) Hash 1 XOR	1 syn 2 Hash 1 XOR	6 syn 3 Hash	n+7 syn n+6 Hash 2 XOR
2	C.C.Chang and Lee's algorithm(2004)[8]	2 Hash 1 XOR	1 syn 2 Hash 1 XOR	5 syn 6 Hash	6 syn 10 Hash 2 XOR
3	X-M.Wang et al.'s algorithm(2007)[9]	3 Hash 4 XOR	6 Hash 7 XOR	6 Hash 7 XOR	15 Hash 18 XOR
4	Hu,Niu and Yans's algorithm(2007)[32]	2 Hash 1 XOR	1 syn 2 Hash 1 XOR	1 syn 10 Hash 2 XOR	2 syn 14 Hash 4 XOR
5	Tseng et al's algorithm(2008)[16]	2 Hash 1 XOR	2 Hash 1 XOR	2 Hash	6 Hash 2 XOR
6	J.H.Lee and D.H.Lee's algorithm (2008)[10]	4 Hash 2 XOR	4 Hash 6 XOR	4 Hash 1 XOR	12 Hash 9 XOR
7	Zhu and et al.'s algorithm (2008)[28]	2 Hash 1 XOR	1 EXP 3 Hash 1 XOR	7 EXP 23 Hash 8 XOR	8 EXP 28 Hash 10 XOR
8	Y. P. Liao and S. S. Wang's algorithm (2009)[14]	5 Hash 2 XOR	6 Hash 3 XOR	10 Hash 3 XOR	21 Hash 8 XOR
9	Xu and et.al's algorithm (2009)[30]	2 Hash 1 XOR	3 Hash	6 Hash	11 Hash 1 XOR
10	Hsiang and Shih's algorithm (2009)[15]	6 Hash 5 XOR	7 Hash 6 XOR	16 Hash 13 XOR	29 Hash 24 XOR
11	Li,Lee and Wang's algorithm (2010)[26]	1 Hash 2 XOR	2 XOR	7 Hash 2 XOR	9 Hash 5 XOR
12	C.C.Chang and Cheng's algorithm (2011)[11]	2 Hash 1 XOR	3 Hash 4 XOR	14 Hash 17 XOR	19 Hash 22 XOR
13	Chen et al's algorithm (2011)[21]	5 Hash 5 XOR	6 Hash 6 XOR	5 Hash 5 XOR	16 Hash 16 XOR
14	S.Kumari and et al.'s algorithm (2012)[22]	4 Hash 2 XOR	5 Hash 4 XOR	7 Hash 2 XOR	16 Hash 8 XOR
15	Li and et al.'s algorithm (2012)[12]	6 Hash 1 XOR	7 Hash 4 XOR	21 Hash 20 XOR	34 Hash 25 XOR
16	C.Li and C.C.lee's algorithm (2012)[13]	3 Hash 1 XOR	4 Hash 5 XOR	15 Hash 18 XOR	32 Hash 24 XOR

17	C.C.Lee,Y-M.Lai,C-T.Li's algorithm (2012)[20]	5 Hash 3 XOR	4 Hash 5 XOR	15 Hash 4 XOR	24 Hash 12 XOR
18	Y-P Liao, C-M Hsiao's algorithm (2013)[17]	Server: 2 Hash User: 2 Hash 1 XOR	3 Hash 1 XOR	9 Hash	16 Hash 2 XOR
19	P.Jiang and et al.'s algorithm (2013)[18]	Server: 2 Hash User: 6 Hash 3 XOR	4 Hash 4 XOR	7 Hash 3 XOR	19 Hash 10 XOR

*here n refers to number of service providers

Considering that the XOR computational cost is minimal, the XOR operation is ignored in calculation the amount cost. Chart 1, compared the amount of computation required for this algorithm. In this chart algorithms that only use XOR and Hash functions are compered. According to the chart this is obvious that Computations in authentication phase are more than the other phases and play a great rule to providing security against attacks and critical features of these environments.

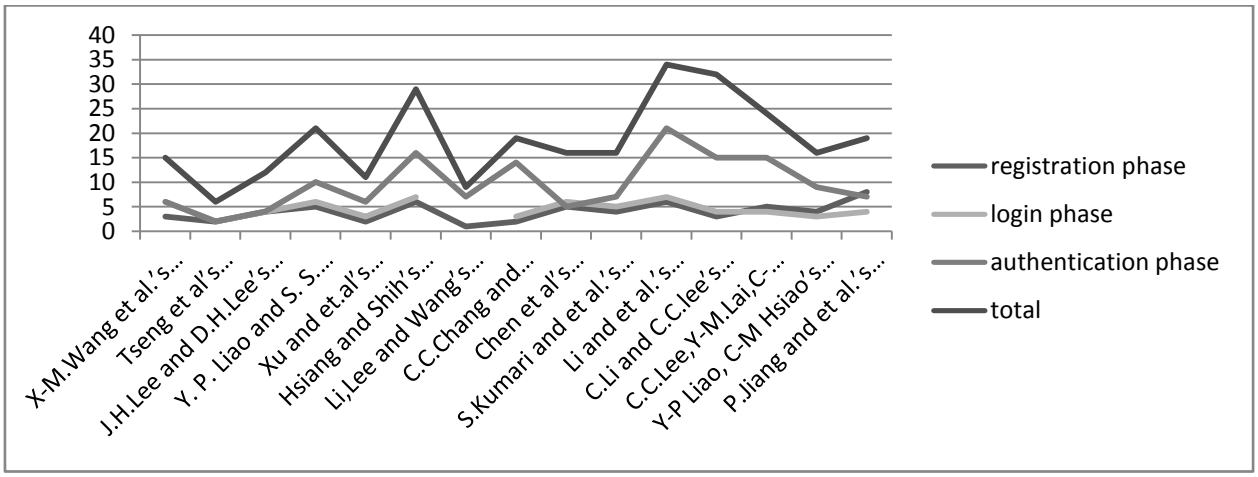

Chart 1: Comparison the computational cost for used algorithms

IV. Key Concepts for Securing Communication in Multi-Server Environments

Lee and et al. introduced necessary factors to create a secure communication in a multi - server environment. These features include the lack of verification table, passwords, user friendliness, mutual authentication and session key agreement, productivity, security and easy change and freely chosen password, individual registration and lightweight computational functions. For more details see [7].

Table II: Compares the performance of the proposed algorithms from 2004 to 2013.

Row	Authors and Year	Main functions	Compu-tation cost	Once registrat-ion	No need to syn-chronize	Session key agree-ment	Mutual authenti cation	Lack of verificati on Table	Easy to change the password	Freely chosen password
1	Jang's algorithm (2004)[7]	Symmetric Cryptography	High	☒	✓	✓	☒	☒	✓	✓
2	C.C.Chang and Lee's algorithm (2004)[8]	Symmetric Cryptography	High	undefine d	✓	✓	☒	✓	✓	✓
3	X-M.Wang et al.'s algorithm (2007)[9]	One way hash	Low	undefine d	✓	✓	✓	✓	✓	✓
4	Hu,Niu and Yans's algorithm(2007[32]	One way hash, Symmetric Cryptography	Middle	undefine d	✓	✓	✓	✓	✓	✓
5	Tseng et al's algorithm (2008)[16]	One way hash	Low	✓	☒	☒	☒	✓	✓	✓
6	J.H.Lee and D.H.Lee's algorithm (2008)[10]	One way hash	Low	☒	✓	✓	✓	✓	✓	✓
7	Zhu and et al.'s algorithm (2008)[28]	Discrete logarithm, One way hash	Middle	undefine d	☒	✓	✓	☒	undefined	✓
8	Y. P. Liao and S. S. Wang's algorithm (2009)[14]	One way hash	Low	✓	✓	✓	☒	✓	✓	✓

9	Xu and et.al's algorithm (2009)[30]	One way hash	Low	undefined	✓	✓	✓	undefined	undefined	✓
10	Hsiang and Shih's algorithm(2009)[15]	One way hash	Low	✓	☒	✓	☒	✓	☒	✓
11	Li,Lee and Wang's algorithm(2010)[26]	One way hash	Low	☒	✓	✓	✓	✓	✓	✓
12	C.C.Chang and Cheng's algorithm (2011)[11]	One way hash	Low	✓	✓	✓	✓	✓	✓	✓
13	Chen et al's algorithm(2011)[21]	One way hash	Low	undefined	✓	☒	✓	✓	✓	✓
14	S.Kumari and et al.'s algorithm (2012)[22]	One way hash	Low	undefined	✓	✓	✓	✓	✓	✓
15	Li and et al.'s algorithm (2012)[12]	One way hash	Low	✓	✓	✓	✓	✓	✓	✓
16	C.Li and C.C.lee's algorithm(2012)[13]	One way hash	Low	✓	✓	✓	✓	✓	✓	✓
17	C.C.Lee,Y-M.Lai,C-T.Li's algorithm (2012) [20]	One way hash	Low	☒	✓	✓	✓	✓	✓	✓
18	Y-P Liao, C-M Hsiao's algorithm (2013) [17]	One way hash, Asymmetric encryption	Very low	✓	✓	✓	✓	✓	✓	✓
19	P.Jiang and et al.'s algorithm (2013)[18]	One way hash	low	✓	✓	✓	✓	✓	✓	✓

V. ATTACKS

Creating a formal proved security with encryption and authentication protocols is very important. Introduction of a formal suitable technology, efficient, safe and simple to correct security protocol analysis is not yet possible.Security vulnerabilities in multi-server environments are divided into four categories: insecure channel attacks, vulnerabilities of client-related, vulnerabilities in register server and vulnerabilities in service provider. For more information see [14].

In general attacks related to authentication divided into two categories: the offline theft of confidential information and theft of internet channels. Steal confidential information related to the Users login attacks on a security system. The information collected is done withexceeding the user's personal systems that are unprotected like Shoulder surfing attacks or deceive to the user that voluntarily gives information to the attacker such as social engineering. InInternet channel attacks, attacker gathers data transferred between the client and the server by eavesdropping or replacement as one of the two parties. The following are some of the kinds of attacks we describe more detail. Comparison between Algorithms in terms of security attacks from 2004 to 2013 is presented in the table III.

Table III: Comparison of the performance of the proposed algorithms from 2004 to 2013 in terms of security

Row	Authors and Year	Offline password dictionary	Loss of smart card	Replay attack	Forgery attack	Server spoofing	Insider attack
1	Jang's algorithm(2004)[7]	☒	☒	✓	✓	✓	☒
2	C.C.Chang and Lee's algorithm(2004)[8]	Undefined	undefined	undefined	☒	☒	☒
3	X-M.Wang et al.'s algorithm(2007)[9]	✓	☒	✓	✓	✓	✓
4	Hu,Niu and Yans's algorithm(2007)[32]	Undefined	undefined	✓	✓	undefined	✓
5	Tseng et al's algorithm(2008)[16]	☒	☒	✓	✓	☒	☒
6	J.H.Lee and D.H.Lee's algorithm(2008)[10]	☒	☒	✓	☒	✓	☒
7	Zhu and et al.'s algorithm(2008)[28]	☒	undefined	✓	✓	undefined	✓
8	Y. P. Liao and S. S. Wang's algorithm(2009)[14]	✓	☒	☒	☒	☒	☒
9	Xu and et.al's algorithm(2009)[30]	Undefined	undefined	undefined	☒	✓	☒
10	Hsiang and Shih's algorithm(2009)[15]	Undefined	☒	☒	☒	☒	✓
11	Li,Lee and Wang's algorithm(2010)[26]	✓	☒	undefined	✓	✓	☒
12	C.C.Chang and Cheng's algorithm(2011)[11]	☒	☒	✓	☒	✓	☒
13*	Chen et al's algorithm(2011)[21]	Undefined	undefined	undefined	✓	undefined	☒
14	S.Kumari and et al.'s algorithm(2012)[22]	✓	✓	✓	✓	✓	✓
15*	Li and et al.'s algorithm(2012)[12]	✓	undefined	✓	✓	✓	✓
16*	C.Li and C.C.lee's algorithm(2012)[13]	✓	✓	✓	✓	✓	✓
17*	C.C.Lee,Y-M.Lai,C-T.Li's	✓	✓	✓	✓	✓	✓

	algorithm(2012)[20]						
18	Y-P Liao, C-M Hsiao's algorithm(2013)[17]	✓	✓	✓	☒	✓	✓
19*	P.Jiang and et al.'s algorithm(2013)[18]	✓	✓	✓	✓	✓	✓

*Repudiation of the claimed Accuracy and security of these algorithms not found yet in any article

The success rate of proposed algorithms against 6 review attacks is shown in chart 2.

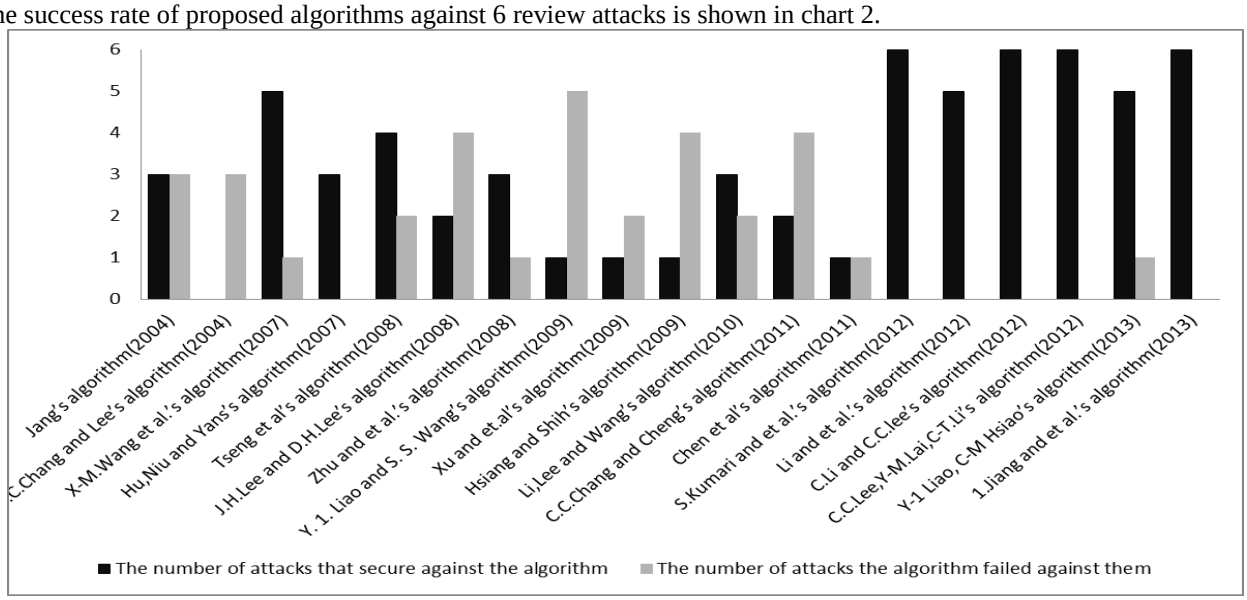

Chart 2: The success rate of analysis algorithms against six presented attacks

VI. Investigate the Reasons for the Success of Algorithms

Multi-user authentication algorithms are based onsmart cart consist of six main steps, including setup algorithm which is performed by the registration server to set the overall system parameters, registration phase for users, login algorithm, authentication algorithm and the changed password phase. In the following influencing factors on success and security of algorithms are reviewed.

A. Registration phase

Three types of attacks can occur based on registration algorithm mistakes.

1) Insider attack

This type of attack occurs when the information related to the user's login such as ID or password, is stored Plaintext on the server. In this case, if a malicious person has access to server information can easily take user passwords and use it illegally. An effective solution to this problem is using Hash algorithm on the user's side. This encrypted password is sent to the server.

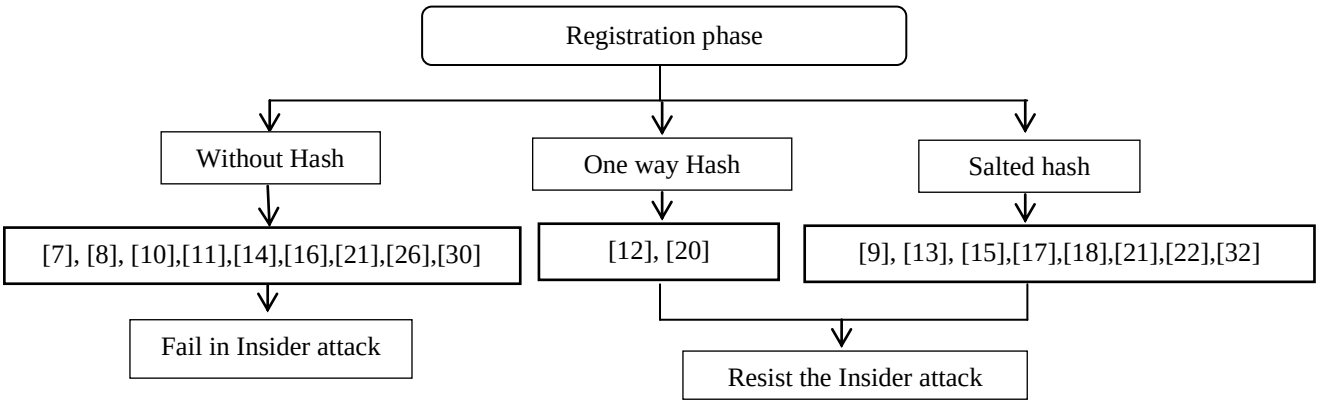

Fig.1. Evaluate the reasons for the success of the algorithm against internal attacks

*Number in figures denote the according reference

As shown in Fig. 1, According to the algorithms being studied, Algorithms thatused simple hash functions or salt to send the password to the server have been able to resist these attacksas well.

2) Loss of smart card

If the information stored on a smart card, have an important role in the Login process computing, and login parameters can be obtain from the stored information in the smart card, in the case of an illegal access to smart card information, transaction security is endangered.

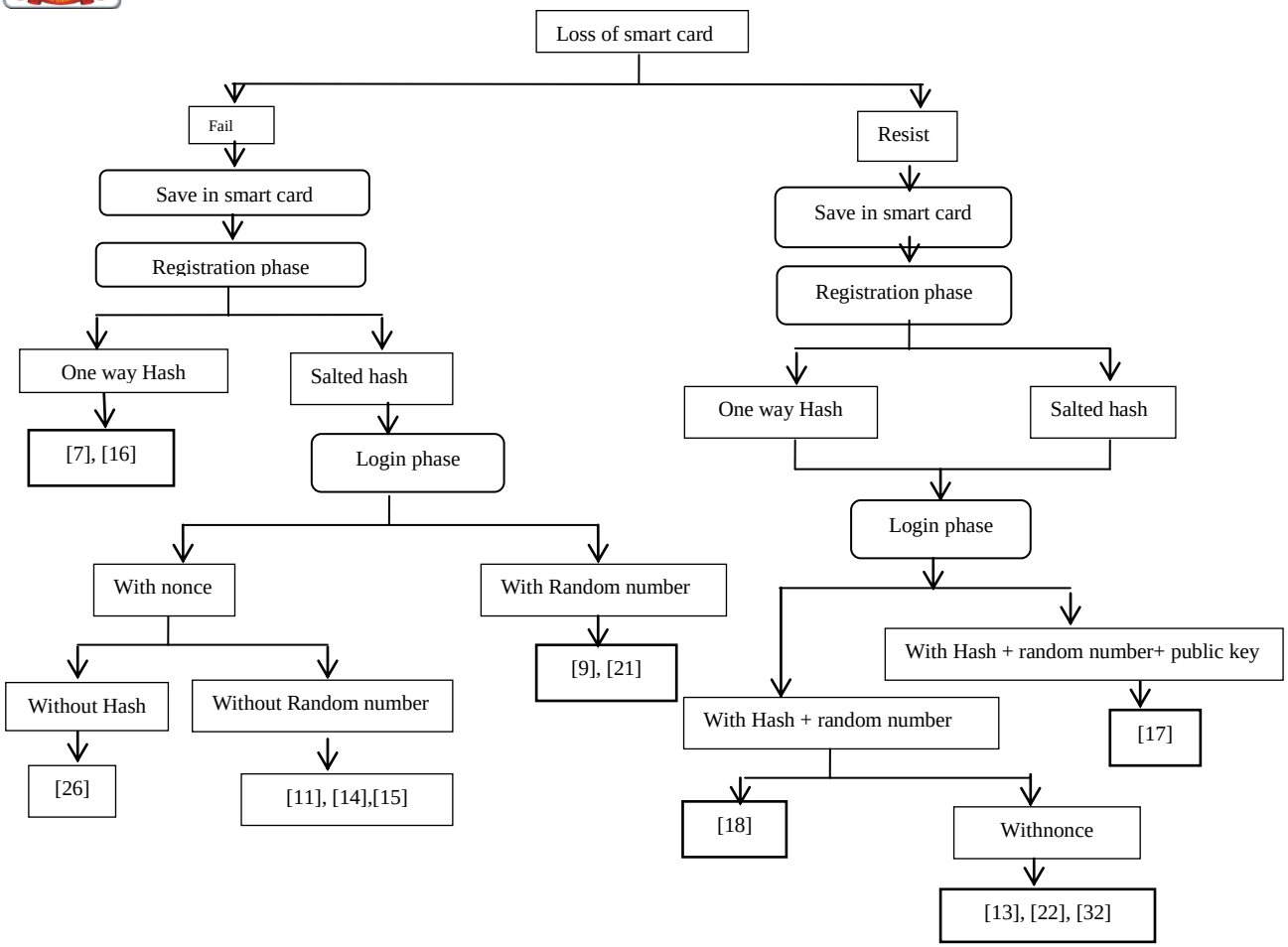

Fig.2. Assess reasons for the success of the algorithm against the smart card loss attacks

As shown in Fig. 2, the algorithms used simple hash and Salt functions in registration process, and the use of hashing, random number, Nonce and public keys in Login phase are secure againstthe missing cards attack and not used any of them in the Login process cause failure in these algorithms.

3) Offline password dictionary attack

This attack accrued once illegal user can access the password files that are stored on the server side and use the same way server generate password verification data,like hash functions, to calculate its own dictionary.

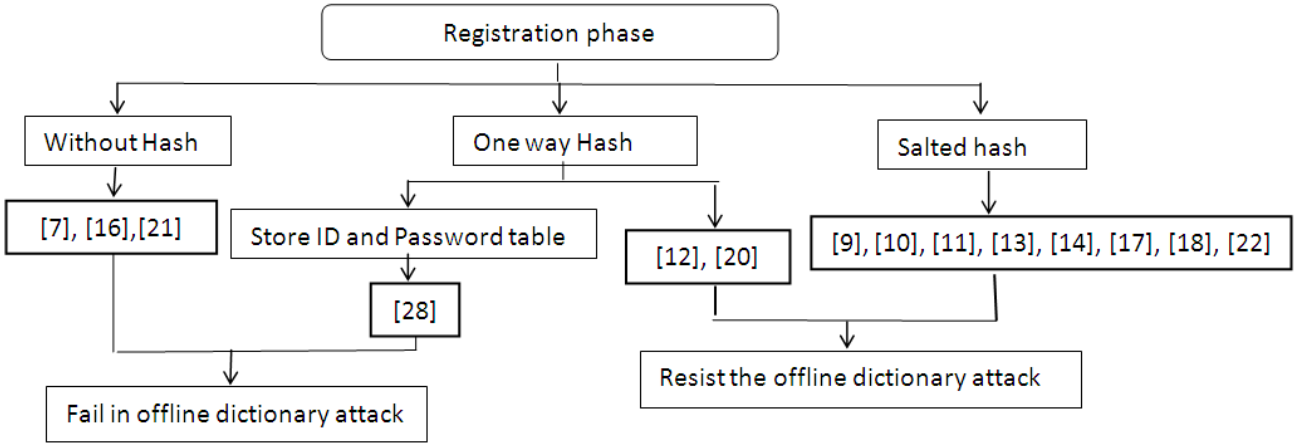

Fig.3. Evaluate the reasons for the success of the algorithm against Offline password dictionary attack

According to fig. 3 algorithms which use hash function or salt without store any ID or password table are secure against this attack. Not using hash or use the storing table causes algorithms to fail in the face of these attacks.

B. Login phase

Forgery attack and replay attackcan be mentioned as malicious attacks that occur due to bugs of login algorithms.

1) Forgery attack

By revealing the password or user data associated with login process, despite a gap in the program or find a way to authentication process this type of attack may occur.

As it is apparent from Fig. 4, the use of a simple hashfunction with a random number and public keyOr Salt with Nonce and random number and also salt without nonce and with random number in login phase can secure algorithms against forgery attack.

2) Reply attack

This is also known as Man in the Middle Attack. Attacker by eavesdropping the communication between user and server, steal user login information and by sending this information to server repeatedly Convince the server that is the legal user and start their malicious actions.

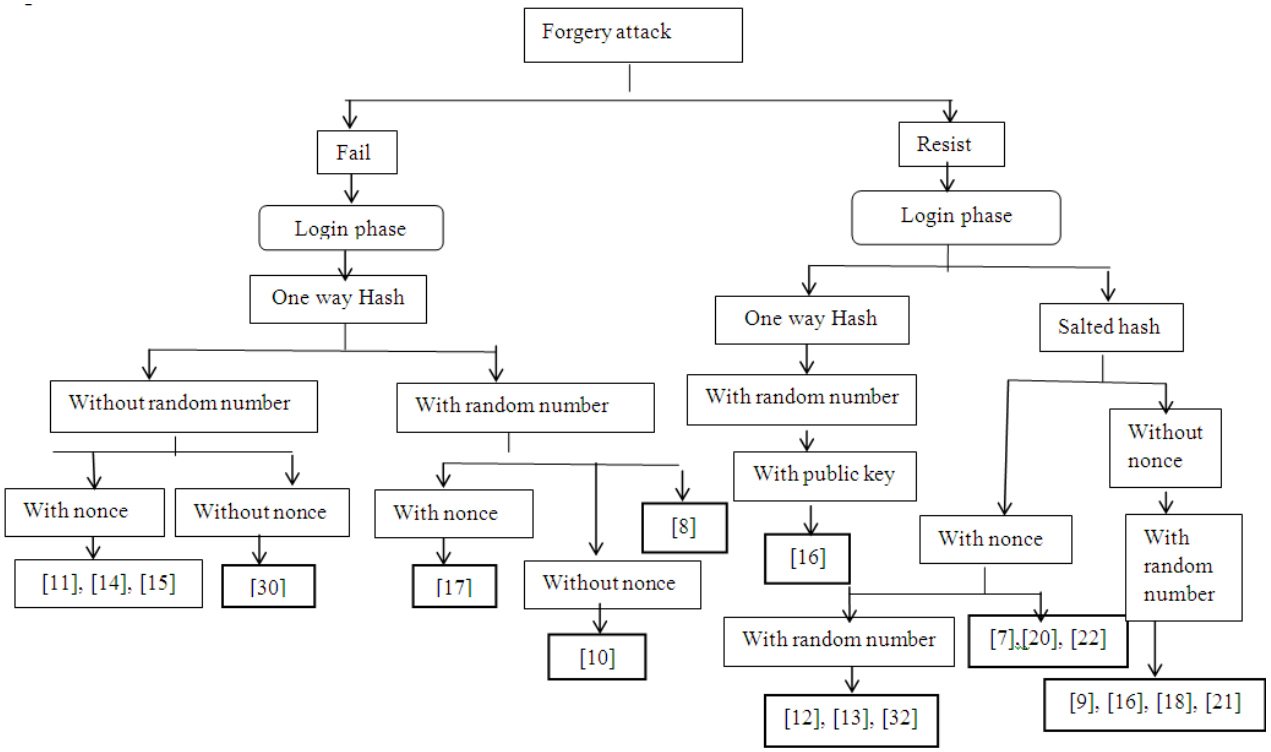

Fig.4. Evaluate the reasons for the success of the algorithm against forgery attack

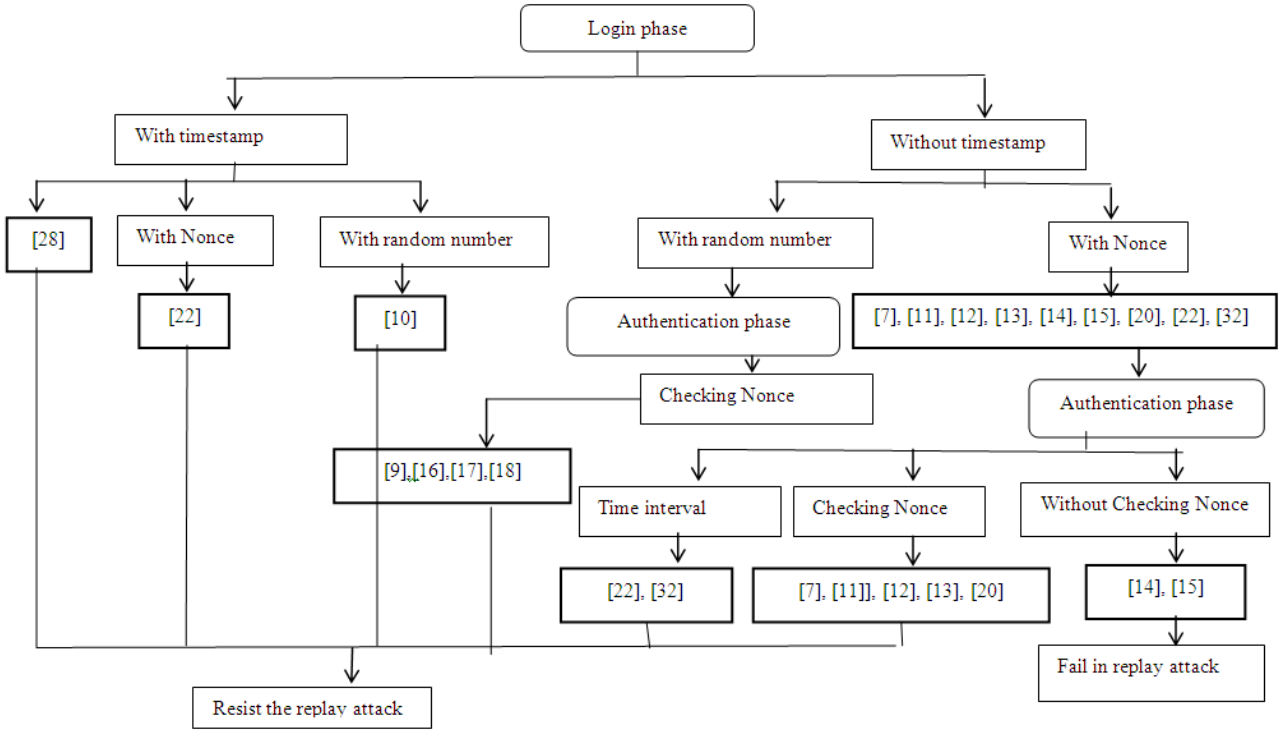

Fig.5. Evaluate the reasons for the success of the algorithm against Reply attack

International Journal of Artificial Intelligence and Mechatronics
Volume 2, Issue 4, ISSN 2320 – 5121

According to fig. 5, use of timestamp with nonce or random number in login phase can secure the algorithms against reply attack. If algorithms does not use time stamp, the use of random number in login phase along with checking nonce in authentication phase or use nonce in login phase along with checking nonce or use of time interval in authentication phase can also secure the algorithms against replay attack.

C. Authentication phase

Server spoofing is one of the highly destructive attacks that would happen due to security bugs in authentication algorithms.

1) Server spoofing attack

In this type of attack, an attacker server S', plays the role of the user U and tries to access to the primary server S that the user U has account. After communicating, S ' has received the random number stored in S and then cut off the connection. The next step, S convinces the user by phishing to enter his system and thereby acquires the password associated with that number. In the final stage S ' as the user U enters into the server S by achieved Password and can access the user account and perform their malicious actions.

To prevent this attack, how the algorithms worked in authentication phaseis very important. In addition, mutual authentication between the client and server and agreement on a common session key for security against this type of attack is vital.

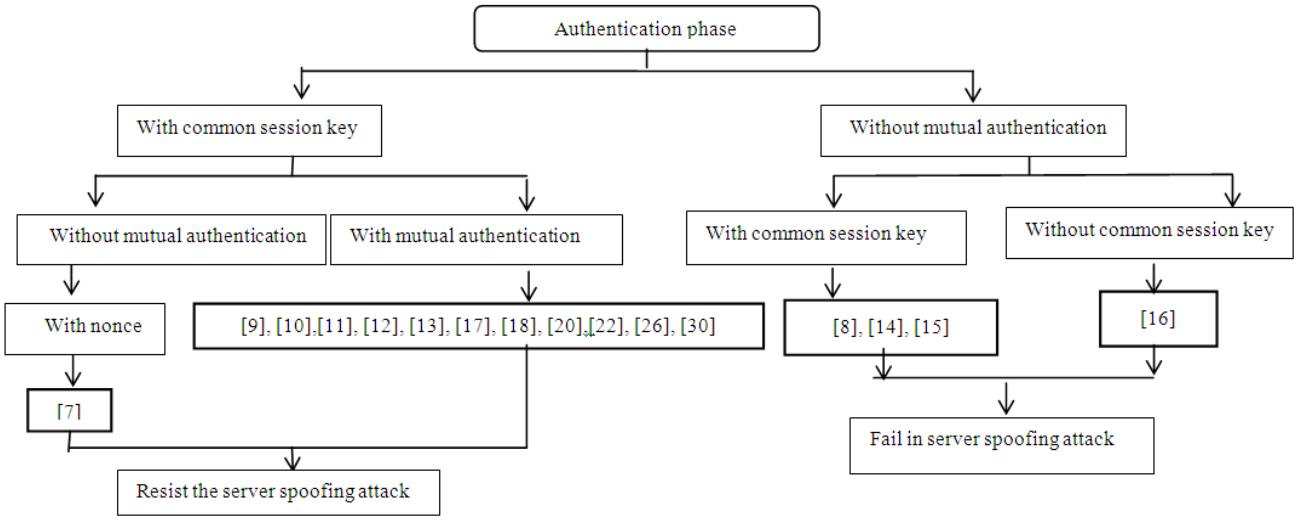

Fig.6. Evaluate the reasons for the success of the algorithm againstserver spoofing attack

According to fig. 6, use of nonce in authentication phase without mutual authentication or mutual authentication along with common session key agreement can secure algorithms against server spoofing attack. The lack of mutual authentication and nonce make failure against the attack.

VII. CONCLUSION

This paper discussed multi-user authentication algorithm in mobile systems. Considering the mobile devices with limited energy resources and computing capability, the design of the secure authentication scheme suitable for mobile systems is a big challenge. Hash functions are used to overcome the problem of poor computational power. To have a secure business communication in mobile systems, features and properties have been introduced, such as mutual authentication, session key which algorithms should be able to provide them. In this paper, these characteristics are fully explained and successes of the proposed algorithms from 2004 to 2013 to meet these needs are compared.

By comparing these algorithms and evaluate their success or failure reasonssome results are obtained as follows:

- To prevent insider attacks, passwords should be sent in encrypted form to the server.
- To prevent smart card attacks using hashing, random number with the public key or Nonce in login phase has an impact.
- To prevent offline dictionary attack use of the one-way hash functions without storing passwords table or using a hash function in the registration phase is useful.
- To prevent forgery attack in login phase, one -way hash functionsor random number and public key or use of Salt function with Nonce and random number or random number without Nonceis used.
- In login phase, use of time stamp, random number and nonce, or use of random number and nonce without time stamp in authentication phase used to prevent from reply attack.
- To prevent server spoofing attack use of random number and public key in authentication phase and mutual authentication, the algorithm can reach the desired security level.

According to these results and applying them, can improve secure authentication algorithms in mobile systems.

REFERENCES

[1] http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx#, available

[2] Choi, J., Seol, H., Lee, S., Cho, H., & Park, Y. "Customer satisfaction factors of mobile commerce in Korea."*Internet research, 18 (3), 2008, pp.313-335.*

[3] Liao, Y. P., & Hsiao, C. M. "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients."*Future Generation Computer Systems, 29 (3), 2013, pp. 886-900.*

[4] Lin, J., Lu, Y., Wang, B., & Wei, K. K. "The role of inter-channel trust transfer in establishing mobile commerce trust. "*Electronic Commerce Research and Applications, 10 (6)2011, pp., 615-625.*

[5] Li, X., Hess, T. J., & Valacich, J. S."Why do we trust new technology? A study of initial trust formation with organizational information systems."*The Journal of Strategic Information Systems, 17 (1), 2008, pp. 39-71.*

[6] Kim, K. K., Park, S. H., Ryoo, S. Y., & Park, S. K. "Inter-organizational cooperation in buyer–supplier relationships: Both perspectives."*Journal of Business Research, 63 (8), 2010, pp.863-869.*

[7] Juang, W. S. "Efficient multi-server password authenticated key agreement using smart cards."*Consumer Electronics, IEEE Transactions on, 50 (1),2004, pp. 251-255.*

[8] C. C. Chang and J. S. Lee." An efficient and secure multi-server password authentication scheme using Smart card."*Proc. Of the 3rd International Conference on Cyberworlds, Tokyo, Japan,2004, pp. 417-422.*

[9] Wang, X. M., Zhang, W. F., Zhang, J. S., & Khan, M. K. "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. "*Computer Standards & Interfaces, 29 (5), 2007, pp.507-512.*

[10] Lee, J. H., & Lee, D. H. "Efficient and secure remote authenticated key agreement scheme for multi-server using mobile equipment."*In Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers. International Conference on, January, 2008, pp. 1-2.*

[11] Chang, C. C., & Cheng, T. F."A robust and efficient smart card based remote login mechanism for multi-server architecture. " *International Journal of Innovative Computing, Information and Control, 7 (8),2011, pp. 4589-4602.*

[12] Li, C. T., Weng, C. Y., & Fan, C. I. "Two-factor user authentication in multi-server networks." International Journal of Security and Its Applications, 6 (2), 2012, pp.261-267.

[13] Li, C. T., Lee, C. C., Mei, H., & Yang, C. H." A Password and Smart Card Based User Authentication Mechanism for Multi-Server Environments."International Journal of Future Generation Communication and Networking Vol. 5, No. 4, 2012, pp.153-164.

[14] Liao, Y. P., & Wang, S. S. "A secure dynamic ID based remote user authentication scheme for multi-server environment. "*Computer Standards & Interfaces, 31 (1), 2009, pp. 24-29.*

[15] Hsiang, H. C., & Shih, W. K."Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. "*Computer Standards & Interfaces, 31 (6),2009, pp. 1118-1123.*

[16] Tseng, Y. M., Wu, T. Y., & Wu, J. D." A pairing-based user authentication scheme for wireless clients with smart cards. "*Informatica, 19 (2), 2008, pp. 285-302.*

[17] Jiang, P., Wen, Q., Li, W., Jin, Z., & Zhang, H."An Anonymous User Authentication with Key Agreement Scheme without Pairings for Multi server Architecture Using SCPKs."*The Scientific World Journal, 2013.*

[18] Lee, C. C., Lin, T. H., & Chang, R. X."A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. "*Expert Systems with Applications, 38 (11), 2011, pp. 13863-13870.*

[19] Lee, C. C., Lai, Y. M., & Li, C. T." An improved secure dynamic ID based remote user authentication scheme for multi-server environment."*International Journal of Security and Its Applications, 6 (2), 2012, pp. 203-209.*

[20] Chen, T. H., Hsiang, H. C., & Shih, W. K." Security enhancement on an improvement on two remote user authentication schemes using smart cards."*Future Generation Computer Systems, 27 (4), 2011, pp. 377-380.*

[21] Kumari, S., Gupta, M. K., & Kumar, M. "Cryptanalysis and security enhancement of Chen et al.'s remote user authentication scheme using smart card."*Central European Journal of Computer Science, 2 (1), 2012, pp.60-75.*

[22] Juang, W. S., Chen, S. T., &Liaw, H. T. "Robust and efficient password-authenticated key agreement using smart cards. "Industrial *Electronics, IEEE Transactions on, 55 (6), 2008, pp. 2551-2556.*

[23] Chain, K., Kuo, W. C., Hsiang, C. P., Cheng, J. C., & Yang, J. F. . "Improved Password-Authenticated Key Agreement Using Smart Cards."*ISA 2012.*

[24] Yoon, E.J,Ryn,E.K,Yoo,K.Y."An improvement of H-Wang-Lee-Tang's simple remote user authentication scheme.", *Cmputer& security, 24 (1),2005, pp. 50-56.*

[25] Li,C-T,Lee,C.C,Wang.L-J. "A two-factor user authentication scheme providing mutual authentication and key agreement over insecure channels."*Journal of information assurance and security 5, 2010, pp.201-208.*

[26] Qiuyan, J., Lee, K., & Won, D. " Cryptanalysis of a two-factor user authentication scheme over insecure channels."*ISA 2012.*

[27] Zhu, L., Yu, S., & Zhang, X." Improvement upon mutual password authentication scheme. "*In Business and Information Management, 2008. ISBIM'08. International Seminar on IEEE,Vol. 1, December 2008, pp. 400-403.*

[28] Hafizul Islam, S. K., & Biswas, G. P. "Design of improved password authentication and update scheme based on elliptic curve cryptography. "*Mathematical and Computer Modelling,2011.*

[29] Lee, N. Y., & Chiu, Y. C." Improved remote authentication scheme with smart card. "*Computer Standards & Interfaces, 27 (2), 2005, pp. 177-180.*

[30] Xu, J., Zhu, W. T., &Feng, D. G. "An improved smart card based password authentication scheme with provable security. " *Computer Standards & Interfaces, 31 (4), 2009, pp. 723-728.*

[31] Song, R. "Advanced smart card based password authentication protocol."*Computer Standards & Interfaces, 32 (5), 2010, pp.321-325.*

[32] Hu, L. L., Niu, X. X., & Yang, Y. X. "Weaknesses and improvements of a remote user authentication scheme using smart cards."*The Journal of China Universities of Posts and Telecommunications, 14 (3), 2007, pp.91-94.*

AUTHOR'S PROFILE

Dr. S. Mohammadi

is a former senior lecturer at the University of Derby, UK. He also used to be a Network consultant inthe UK for more than fifteen years. He is currently a lecturer in the Industrial Eng. Department of the University of K.N.Toosi, of Iran. His main research interests and lectures are in the fields of Networking, Data Security, Network Security, e-commerce and e-commerce Security. He has published more than one hundred papers in various ISI, international, and internal ElmiPajoheshi journals as well as conferences. In addition, he has published four books and two book chapters in his field so far while he is expecting to publish three further books by the Winter 1390 (2012). Email: Mohammadi@kntu.ac.ir or smohammadi40@yahoo.com

Hakimeh Ameri

is graduated in M.S at K.N Toosi University of technology in information technology. Her main research interests are in Security, Network Security, and Data mining. Email: hameri@mail.kntu.ac.ir or ha.amery@gmail.com