Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.396 – 405

RESEARCH ARTICLE

A Novel Authentication Scheme to Increase Security for Non-Repudiation of Users

Khalid Waleed Hussein[1], Dr. Nor Fazlida Mohd. Sani[2], Professor Dr. Ramlan Mahmod[3], Dr. Mohd. Taufik Abdullah[4]

[1-4] Faculty Computer Science & IT, University Putra Malaysia (UPM), Kuala Lumpur-Malaysia

[1] Khaled_it77@yahoo.com, [2] fazlida@fsktm.upm.edu.my,

[3] ramlan@fsktm.upm.edu.my, [4] mtaufik@fsktm.upm.edu.my

Abstract: Protection of sensitive information is a growing concern worldwide. Failure to protect sensitive information can lead to loss of clients in the banking sector or threaten national security. Access to sensitive information starts with e-authentication. Most authentication systems are designed for authenticated users only. However, the user is not the only party that needs to be authenticated to ensure the security of transactions on the Internet. Existing one- time password (OTP) mechanism cannot guarantee non-repudiation and fail to guarantee reuse of a stolen device, which is used in authentication.

A novel authentication scheme based on OTP is presented in this paper. This paper proposes a secure multi-factor electronic authentication mechanism. This mechanism is intended to authenticate both the user and the mobile device of the user to ensure non-repudiation and protect the integrity of the OTP against adversarial attacks. The proposed mechanism can detect whether the mobile device is in the hands of the rightful owner before the OTP is sent to the user. The system requires each user to have a unique phone number and a unique mobile device (unique International Mobile Equipment Identity (IMEI)), in addition to an ID card number. The proposed system can ensure that the user who misuses the system becomes liable for the act committed. Therefore, the proposed system can be used in e-banking, e-government, and ecommerce systems, among other areas requiring high-security guarantees.

Keyword- Security; non-repudiation; multi factor authentication; IMEI; authenticate mobile device; nested multi factor authentication

I. INTRODUCTION

Protection of sensitive data is a growing concern for organizations worldwide because of its financial implications[1]. Access to sensitive information starts with authentication. User names and passwords are commonly used by people during a log in process to validate user identity[2]. Passwords remain as the most common mechanism for user authentication in computer security systems. However, the use of passwords includes disadvantages, such as poor choice of passwords by users and vulnerability to capture [3-5]. Another major problem is that users tend to reuse passwords for different sites[6]. Several studies indicate that more than 70% of phishing activities are designed to steal user names and passwords. The Anti-Phishing Working Group reported[7] that the number of malicious Web pages designed to steal user credentials at the end of the second quarter in 2008 increased by 258% over the same period in 2007. Therefore, protecting user credentials from fraud attacks is extremely important. Many studies have proposed schemes to protect user credentials against theft [8-10].

Authentication is the process of confirming or denying the claimed identity of a user[11]. The service provider has to trust the authentication performed by the identity provider of the user. This process is critical in terms of security because authorization and access control of the service highly depend on the authentication results. Weak authentication jeopardizes the security of the dependent service by increasing the risk that a user can impersonate another person and improperly gain access[12]. One effective authentication method is a mathematical model that combines different authentication methods, similar to that used in multi-factor authentication, to build a high security trust system[13, 14].

Multi factor authentication (MFA) overcomes the vulnerability of passwords, which refers to the use of more than one factor in the authentication process [15-17]. One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information, such as the login IDs and passwords of legitimate users. Once captured, this information can be used at a later time to gain access to the system. One-time password (OTP) systems are designed to counter this type of attack, called a replay attack[18, 19]. An OTP is valid for only one login session or transaction. OTPs prevent a number of shortcomings associated with traditional authentication (such as usernames and passwords)[20].

Mobile authentication is one of the main methods of multi-factor authentication. This technique uses mobile devices (after software token is installed on the mobile device) for multi-factor authentication instead of other authentication methods, such as the use of hard tokens, smart tokens, or smart chip cards. Mobile authentication requires the installation of software on a mobile device to generate an OTP [21-23].

The use of a mobile device in user authentication presents difficulties[24]. These disadvantages include the following:

- The user enters a password periodically to initialize a mobile application. As a result, the user is compelled to either save the passwords on their devices or select weak passwords that can be easily inputted on devices[25].

- When a user's mobile device is lost or stolen, others could use it to access the user's information[26].

Most solutions employed to generate OTP on mobile devices require connecting the user’s mobile device to a PC by Bluetooth or Wi-Fi to install the software on the mobile phone[27, 28]. However, more than 370 mobile malwares are in circulation, most of which are spread through installed software (applications) from the Internet or by connecting mobile devices to infected PCs[29].

The International Mobile Equipment Identity (IMEI) number is utilized by a Global System for Mobile Communications network to identify valid devices and can therefore be employed to prevent unauthorized access to a stolen phone[30, 31].

Methods of certification are generally required to authenticate a user when the user requests for a service from the service provider. These methods, classified into four types according to the element that becomes the basis of certification, are as follows [16, 32, 33]:

- Type I: Something you know such as password, PIN.
- Type II: Something you have such as Mobile Phone, Token device, or ID card number.
- Type III: Something you are such as Iris scan, or Fingerprint.
- Type IV: Something you do such as voice.

An OTP mechanism creates a password only once along with additional features such as user certification and electronic transaction security to protect user information against leakage and simultaneously address the problem of a static password mechanism. However, for electronic authentication, face-to-face communication cannot be established. To confirm the identity of a person accessing the system, the existing OTP mechanism encounters problems such as failure to guarantee certification (the identity of authenticity) and non-repudiation [34-36].

This paper proposes a mechanism to reduce the problems related to existing OTP authentication and guarantee certification and non-repudiation of users. The proposed system requires that each user register personal information, such as ID card number, mobile number, IMEI, and PIN, into the system. The server generally provides this practical service. The server generates an OTP by combining the various personal information (as above) of the user and transmitting the created OTP to the user by encoding the OTP after executing the Advanced Encryption Standard (AES). The user registers personal information during the registration phase. The server also verifies the IMEI validity during this phrase by checking whether the IMEI number exists. The user then proceeds to the login phase for authentication by username and password.

When the user enters the correct username and password, the server allows the user to advance to the second authentication phase (a new layer), which is known as the confirmation phase. During this phase, the user is compelled to enter the original personal information that had previously been entered into the system. This layer combines two factors — something the user knows and something the user has — after the user confirms these two factors and submits them to the server. The server then generates an OTP and sends this OTP to the user by encrypted SMS. During this phase, the server verifies the IMEI validity and simultaneously provides a certification guarantee and non-repudiation because the OTP is not sent directly to the user. Meanwhile, the server checks whether the mobile device is in the hands of the same user.

The remainder of this paper is organized as follows: Chapter 2 presents existing studies on OTPs. Chapter 3 discusses secure authentication methods proposed in this research. Chapter 4 describes the experimental environment and comparisons with existing mechanisms. Finally, Chapter V concludes the paper and suggests possible directions for future research.

II. RELEVANT STUDIES

OTP authentication mechanisms are applied using various tools such as a hardware device (token device) or a software token (mobile phone) [37].

A. Hardware Device (Token Device)

A token device is used to prove the user's identity in electronic authentication. This method is conducted in some commercial transactions or e-government services, as practiced in New Zealand[38]. A token device is also used in addition to or as a substitute for a static login ID to prove user identity. The token acts as an electronic key to confirm the identity of a user accessing the system[39].

A hardware token is considered more secure than a user ID or a password. The use of hardware tokens enhances the reputation of an organization by securing user credentials more effectively. However, the hardware may cause problems, such as the need for users to constantly carry the token with them and the multiple-token requirement for multiple Web sites. The token device is not fully protected from man-in-the-middle attacks. The hardware also involves additional costs, such as the cost of the token and replacement fees in case of loss [23, 40, 41].

B. Software Token (Mobile Phone)

A software token is a form of multi-factor authentication. Software tokens are stored on hardware devices, such as mobile phones, which then become vulnerable to threats, including viruses and software attacks[41]. However, mobile phones are easily lost or stolen, allowing criminals to easily use personal data and access information without a great effort through services such as SMS[42].

Studies have been conducted to address the problems related to security of authentication either by using mobile phones as software tokens to generate an OTP, which is then sent to the server[22, 43], or using mobile phones as tools to receive an OTP from servers through SMS. In this case, the system requires that the users log into the system with a username and a password and correctly entering credentials. The OTP code is then sent to the mobile phone through SMS[44]. In both cases (the mobile phone as a soft token and the mobile phone for receiving SMS), the authentication systems cannot guarantee user certification and non-repudiation[35, 36].

III. PROPOSED SYSTEM

Using existing communication infrastructure, the proposed system requires no additional costs. The identity, authenticity, and non-repudiation of transactions are particularly important in any system that involves processing of electronic authentication[45]. In this paper, the problem of non-repudiation during authentication is resolved. The proposed system can contribute to the increased security of multi-factor authentication by sending OTPs only to trusted users.

A. Registration Phase

During the registration phase, users are compelled to use their personal information (username, password, a four- to six-digit PIN, email, ID card number, and mobile number) in addition to the IMEI. Some algorithms perform an IMEI validation check for the mobile phone of the user. If the IMEI is not valid, the user is prevented from registering in the system (system not safe wrong data). Thus, the user is compelled to enter a valid IMEI during registration. In addition, if the IMEI and the mobile number are repeated (that is, registered by another user), the user cannot complete the registration process. The use of this method ensures that every user has one mobile number and one IMEI number apart from the ID card number of that user. Most

authentication systems that use OTP authentication allow users to create many accounts with the same mobile number, which is not allowed in the proposed system. This limitation is set to control management of multiple accounts by the same user and reduce the occurrence of errors in user information on the database. After successful registrations, the user advanced to the login phase.

B. Traditional Login Phase

During the login phase, the user logs into the system with a username and a password. If the user enters the wrong credentials (that is, the username and the password), the user is denied access by the system. Thus, the user cannot proceed the second authentication phase (a new layer of authentication) until the correct credentials are entered.

C. New Layer (Confirmation Phase)

This layer prevents OTP generation by the server, as well as sending the OTP to the user, until the personal information (PIN, mobile number, IMEI) that was registered in the previous phase (registration phase) is confirmed by the user. This layer also ensures the authenticity of the identity and non-repudiation. In other authentication systems, the users can receive OTPs directly from the server by SMS after submitting their credentials (username and password) to the system. The proposed system does not generate OTPs and thus, sends nothing to the user until the system ensures that the mobile device is in the hands (that is, in the hands of the same user who requested the authentication). This approach ensures that any person who misuses the system becomes liable for such improper use. This layer combines two factors — something the user knows (PIN) and something the user has (mobile number and IMEI). The application of the new layer of authentication to confirm the identity of the user is considered a new idea, which is represented as a nested multi-factor process in Figure 1.

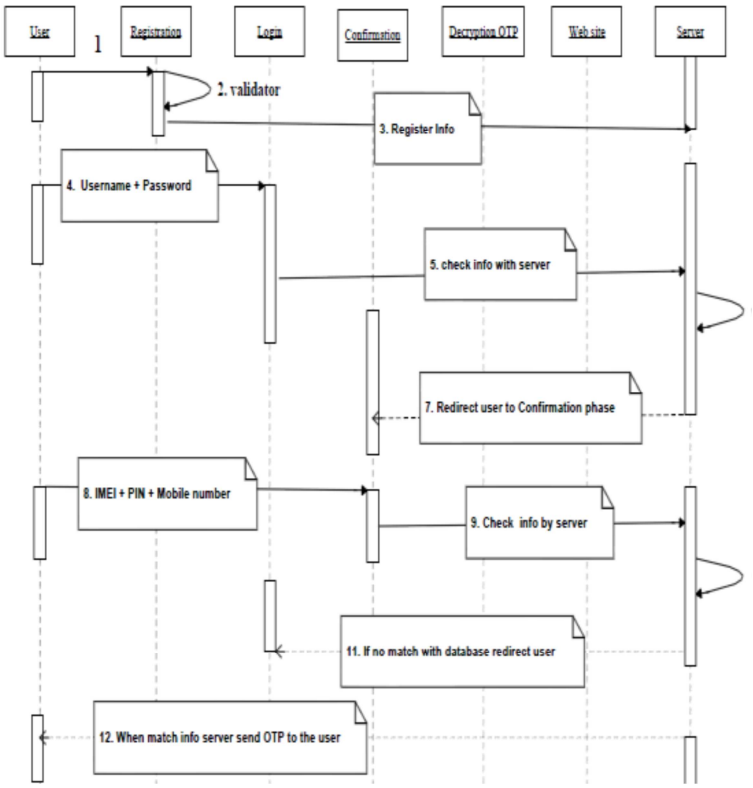

Figure1. Sequence diagram of the system

The user can then choose a method for receiving the OTP. If the user prefers not to receive the OTP by SMS, the user may receive it by e-mail. Thus, in this layer, the user can choose the method of receiving the OTP as preferred. Receipt of OTP by e-mail requires information on the e-mail, PIN, and ID card number. Regardless of how the user prefers to receive the OTP, an encrypted OTP is sent to the user by using Rijndael AES 256. The OTP is decrypted using the PIN, which is a symmetric key between the user and the server. If the user enters the wrong information during the confirmation phase, the server redirects the user to the first login (traditional login), and authentication begins again.

If another person impersonates a legal user, all pieces of information pertaining to the legal user would be required, such as the username and the password (to pass from the first login phase), stolen mobile phone (to pass from the confirmation phase and receive SMS), ID card number and the e-mail of the user (username and password to access email), and PIN (required during the confirmation phase and for decryption of SMS or e-mail.).

D. Generating and Sending an OTP

After the user passes through the confirmation phase, the server generates an OTP based on user information. An OTP may be generated in two ways. First, the user may opt to receive the OTP either by SMS or by e-mail. If the user opts for SMS, the elements required from the user during confirmation phase (mobile number, IMEI, and PIN) contributes to the generation of OTP. If the user chooses to receive the OTP by e-mail, the elements required from the user during confirmation phase (PIN and email) contributes to the generation of OTP. By this method, future OTPs cannot be predicted because the OTP varies completely from one user to another. Second, the OTP can be generated randomly based on the user information. Thus, the user is not likely to receive the same OTP in the proposed system. In this paper, the processes involved in the multifactor mechanism for secure authentication system are shown in Figure 2.

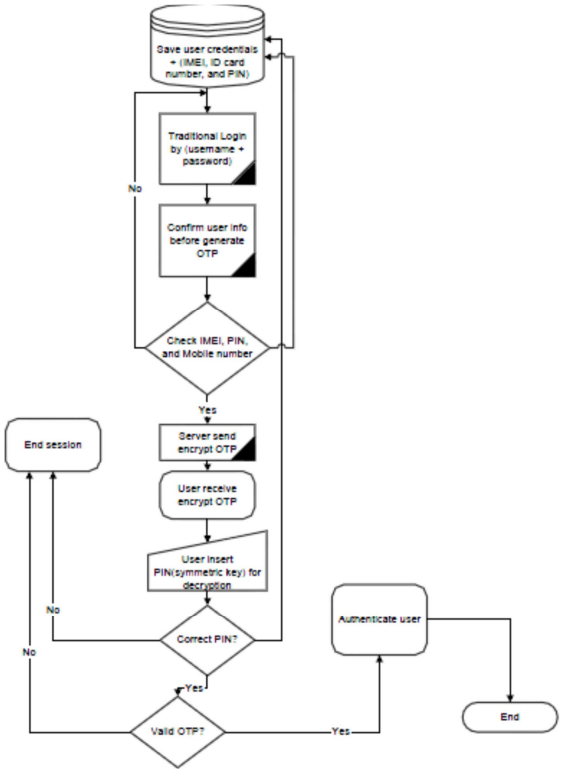

Figure2. Procedure involved in the proposed system

The server sends the encrypted OTP according to the method preferred by the user (SMS or email). After receipt of an encrypted message by OTP, the user enters information on another screen to prove the validity of the PIN and simultaneously decrypt the OTP (a symmetric key for encryption and decryption). If the PIN is incorrect, the session ends.

IV. COMPARISION ANALYSIS

A. Comparison and Analysis

Eight performance evaluation elements were compared to analyze the performance of the proposed mechanism and the existing mechanism. These elements include non-repudiation, long password, tracking of user, mobile device blocking, user and mobile phone authentication, user information reuse prevention, mobile phone reuse prevention, and certification type.

Non-repudiation: Because the proposed mechanism works to authenticate the user and his or her mobile phone (IMEI plus mobile number), so the proposed system has all important information about the user such as ID card number, mobile number, and IMEI, all of which are unique. Thus the proposed system can ensure the liability of the person that misuses the system.

Long password: A long password for authentication is generally considered safer than a short one. However, complex or meaningless passwords are difficult to remember[46]. During confirmation phase, the user is only required to rewrite long passwords (such as IMEI, the mobile number, or the ID card number), which they already possess. The user can also derive the password from the user ID card or mobile phone, other systems require users to remember these details.

Tracking of user: Most authentication systems that generate OTPs through the server and send the OTP to the user by SMS cannot track whether the user is tampering with the system because the authentication system only has the mobile number, in addition to the username and the password, of the user. The system may be tampered with by a person who receives an OTP through SMS and then changes or discards the SIM card. The proposed system can determine the liability of the person who misuses the system or is tampering with the system through the ID card number of the user, which is a unique number, in addition to the mobile number (every user has a unique mobile number and unique IMEI).

Mobile device blocking: The mobile device can be located using the IMEI. The device can also be made unusable in any network by blacklisting. The proposed system requires the IMEI to authenticate the device and as a necessary precaution against system tampering. An administrator of the proposed system who detects any attempt to tamper with the system can cancel the account of the user and prevent the user and the associated mobile device from registering in the system. If an OTP system cannot prevent the use of the same device, the illegal user can return and register (if the administrator discovers illegal attempts by the user) as a legal user and gain access to the system.

User and mobile phone authentication: Compared with other authentication systems that use mobile phone to generate OTPs or receive SMS, these systems authenticate the user and ignore other parties that are used in electronic authentication such as the mobile phone of the user. However, the user is not the only party that needs to be authenticated to ensure the security of transactions on the Internet[47]. The proposed system authenticates both the user and the mobile device, in addition to mutual authentication between the user and the server through Secure Socket Layer (SSL).

User information reuse prevention: The proposed system adopts an OTP approach. Every user has unique information, which requires no separation of data as in other systems. This system enhances privacy protection and minimizes the probability of data matching.

Mobile phone reuse prevention: The proposed system can prevent a mobile phone from being reused illegally by requiring that every user have a unique phone number and a mobile device (IMEI) while indicating that the mobile phone of the user is lost or stolen. The attacker is prevented from accessing the system until other elements such as the PIN or ID card number (used in the confirmation phase) of the user are obtained.

Certification type: Existing methods in which OTPs are generated or received using the mobile phone of the user rely on what the user knows. The proposed system depends on a combination of two factors — what the user knows and what the user owns (IMEI). In addition, this approach uses a new way to authenticate the use of a mobile phone. The proposed system also enhances security and operates as a multi-factor authentication mechanism (nested multi-factor authentication).

V. CONCLUSION

In this paper, a mechanism is proposed for OTP authentication. This mechanism can reinforce the security of authentication and the mechanism of guaranteeing non-repudiation by authenticating the user and the device necessary to receive encrypted OTPs. Although this mechanism cannot completely ensure the proper use of the system, it can ensure that the user who misuses the system becomes liable for such act. In contrast to existing methods in which users receive OTPs through their mobile phones, this mechanism requires the users to present more information to prove their identity as rightful owners. Therefore, the proposed method is suitable for areas in which security is crucial, such as providing authentication for Internet banking, authentication for electronic payment, electronic government authentication, and cloud computing authentication.

REFERENCES

[1] Tanveer A Faruquie, Sumit Negi, and L Venkata Subramaniam, *Protecting Sensitive Customer Information in Call Center Recordings*, in *International Conference on Services Computing*,2009, IEEE: Bangalore p. 81-88.

[2] Bander AlFayyadh, et al., *Improving Usability of Password Management with Standardized Password Policies*, 2011, Queensland University of Technology,: Australia,. p. 8.

[3] Abdulaziz S. Almazyad and Y. Ahmad, *A New Approach in T-FA Authentication with OTP Using Mobile Phone.* Springer 2009. **58**: p. 9-17.

[4] Jiří Sobotka and Radek Doležel, *Multifactor authentication systems.* elektro revue, December 2010. **1**(1213-1539): p. 1-7.

[5] John Brainard, et al., *Fourth-factor authentication: somebody you know.* ACM, 2006: p. 1-11.

[6] R.R.Karthiga and K.Aravindhan, *Enhancing Performance of User Authentication Protocol with Resist to Password Reuse Attacks.* International Journal Of Computational Engineering Research (IJCER), 2012. **2**(8): p. 106-115.

[7] Chun-Ying Huang, Shang-Pin Ma, and Kuan-TaChen, *Using one-time passwords to prevent password phishing attacks.* Science Direct, 2011.

[8] Chuan Yue and HAINING WANG, *BogusBiter: A Transparent Protection Against Phishing Attacks.* ACM, 2010. **10**(2): p. 31.

[9] Heng Yin, et al., *Panorama: capturing system-wide information flow for malware detection and analysis*, in *ACM conference on Computer and communications security*2007, ACM: USA. p. 116-127.

[10] Scott Garriss, et al., *Trustworthy and Personalized Computing on Public Kiosks*, in *6th international conference on Mobile systems, applications, and services*, 2008, ACM: USA. p. 199-210.

[11] Priti C. Golhar and Dr. D.S. Adane, *Graphical Knowledge Based Authentication Mechanism.* International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),, 2012. **2**(10): p. 48-54.

[12] Ivonne Thomas, Michael Menzel, and Christoph Meinel. *Using Quantified Trust Levels to Describe Authentication Requirements in Federated Identity Management*. in *ACM workshop on Secure web services (SWS)*. 13 Oct 2008. New York, USA: ACM.

[13] Akash K Singh, *Authentication Trust Level Network Architecture*. International Journal of P2P Network Trends and Technology, 2012. **2**(6): p. 99 - 129.

[14] Nicolae Constantinescu and Claudiu Ionut Popirlan, *Authentication model based on Multi-Agent System.* University of Craiova/ Department of Mathematics and Computer Science, 2011. **38**(2): p. 59-68.

[15] Do van Thanh, et al., *Strong authentication with mobile phone as security token.* IEEEXplore, 2009: p. 777-782.

[16] Jae-Jung Kim and Seng-Phil Hong, *A Method of Risk Assessment for Multi-Factor Authentication.* Journal of Information Processing Systems,, 2011. **7**: p. 187--198.

[17] Jing-Chiou Liou and S. Bhashyam, *A feasible and cost effective two-factor authentication for online transactions* in *International Conference on Software Engineering and Data Mining (SEDM), 2010 2nd* 2010, IEEEXplore: Chengdu, China. p. 47 - 51

[18] Jongpil Jeong, Min Young Chung, and Hyunseung Choo. *Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks*. in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*. 2008. Waikoloa, HI IEEE.

[19] N. Haller Bellcore and C. Metz *A One-Time Password System*. 1998. **2012**.

[20] K.Aravindhan and R.R.Karthiga, *One Time Password: A Survey.* International Journal of Emerging Trends in Engineering and Development, 2013. **1**(3): p. 613-623.

[21] Gianluigi Me, Daniele Pirro, and R. Sarrecchia, *A mobile based approach to strong authentication on Web*, in *International Multi-Conference on Computing in the Global Information Technology*2006, IEEE Xplore. p. 67

[22] Havard Raddum, Lars Hopland Nestas, and K.J. Hole', *Security Analysis of Mobile Phones Used as OTP Generators*, in *international conference on Information Security and Privacy of Pervasive Systems and Smart Devices*, , International Federation for Information Processing (IFIP), Editor 2010, ACM: Berlin. p. 324-331.

[23] Trupti Hemant Gurav and Manisha Dhage, *Remote Client Authentication using Mobile phone generated OTP*. International Journal of Scientific and Research Publications, 2012. **2**(5): p. 4.

[24] Hung-Min Sun, Yao-Hsin Chen, and Y.-H. Lin, *oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks.* IEEEXplore, 2012. **7**(2): p. 651- 663.

[25] Xing Fang and J. Zhan, *Online Banking Authentication Using Mobile Phones*, in *5th International Conference on Future Information Technology (FutureTech)*,2010, IEEEXplore: Busan p. 1-5.

[26] Mahendra Singh Bora and Amarjeet Singh, *Cyber Threats and Security for Wireless Devices.* Journal of Environmental Science, Computer Science and Engineering & Technology (JECET), 2013. **2**: p. 277-284.

[27] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj, *Two Factor Authentication Using Mobile Phones*, in *International Conference on Computer Systems and Applications*2009, IEEE: Rabat p. 641-644.

[28] Indu S., Sathya T.N., and Saravana Kumar, *A Stand-Alone and SMS-Based Approach for Authentication Using Mobile Phone*, in *International Conference on Information Communication and Embedded Systems (ICICES)*2013, IEEEXplore: Chennai p. 140 - 145

[29] Lei Liu, et al. *Exploitation and Threat Analysis of Open Mobile Devices*. in *5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems* 2009. ACM.

[30] GSM Association, *IMEI Allocation and Approval Guidelines*, Official Document TS.06 (DG06), Editor 2011. p. 33.

[31] Jörg Eberspächer, et al., *GSM Architecture, Protocols and Services* 2009, John Wiley & Sons: UK. p. 327.

[32] Jing-Chiou Liou and S. Bhashyam, *On Improving Feasibility and Security Measures of Online Authentication*. International Journal of Advancements in Computing Technology, 2010. **2**(4.1): p. 11.

[33] Kumar Abhishek, et al., *A Comprehensive Study on Multifactor Authentication Schemes.* 2013. **177**: p. 561-568.

[34] Chii-Ren Tsai, *Non-Repudiation In Practice*, 2002, Second International Workshop for Asian Public Key Infrastructure (IWAP'02),: Taipei,Taiwan. p. 5.

[35] Hyun-chul Kim, et al., *Design and Implementation of Multi Authentication Mechanism for Secure Electronic Commerce*, 2009, IEEEXplore: Seoul, South Korea, . p. 215-219.

[36] Miloš Milovanovic, et al., *Choosing Authentication Techniques in e-Procurement System in Serbia*, in *International Conference on Availability, Reliability and Security*2010, IEEE Xplore. p. 374- 379.

[37] Jing-Chiou Liou and Sujith Bhashyam, *A feasible and cost effective two-factor authentication for online transactions*, in *2nd International Conference of Software Engineering and Data Mining (SEDM)*2010, IEEEXplore: Chengdu, China p. 47 - 51

[38] Yu-Cheng Tu and C. Thomborson. *Preliminary Security Specification for New Zealand's igovt System*. in *Seventh Australasian Conference on Information Security (AISC)*. 2009. Darlinghurst, Australia: ACM.

[39] Nermin Hamza and Dr.Bahaa El-Din M.Hassan, *A Dynamic ID-based authentication scheme with smart token*, in *International Conference on Computer Engineering & Systems*2009, IEEEXplore: Cairo p. 294 - 299.

[40] Gauri Rao and Dr. S.H. Patil, *Three Dimensional Virtual Environment for Secured and Reliable Authentication* Journal of Engineering Research and Studies (JERS), 2011. **2**(2): p. 68-73.

[41] Manav Singhal and Shashikala Tapaswi, *Software Tokens Based Two Factor Authentication Scheme.* International Journal of Information and Electronics Engineering, 2012. **2**: p. 383-386.

[42] David Lisoněk and Martin Drahanský, *SMS Encryption for Mobile Communication.* IEEEXplore, 2008: p. 198-201.

[43] Fadi Aloul, Syed Zahidi, and Wasim El-Hajj, *Multi Factor Authentication Using Mobile Phones.* International Journal of Mathematics and Computer Science, 2009. **2**(1814-0424/ 2009): p. 1-16.

[44] D.Parameswari and L.Jose, *SET with SMS OTP using Two Factor Authentication.* Journal of Computer Applications (JCA), 2011. **4**(4): p. 4.

[45] Xian-ge Huang, Lei Shen, and Yan-hong Feng, *A User Authentication Scheme Based on Fingerprint and USIM Card*, in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*,2008, IEEEXplore: Harbin p. 1261 - 1264.

[46] Sonia Chiasson, et al. *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords*. in *16th ACM conference on Computer and communications security* 2009. ACM.

[47] Audun Jøsang, et al., *Service Provider Authentication Assurance*, in *Tenth Annual International Conference on Privacy, Security and Trust*2012, IEEE Xplore. p. 203- 210.

