International Journal of Engineering & Technology, 7 (4) (2018) 4905-4910

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.23148
Research paper

Rehashing system security solutions in e-banking

Burhan Ul Islam Khan*, Rashidah F. Olanrewaju, Farhat Anwar

Department of ECE, Kulliyyah of Engineering, IIUM Malaysia
**Corresponding author E-mail: burhan.iium@gmail.com*

Abstract

Applications meant for exchanging cash, or individual data are becoming progressively common in mobile communications and on the Internet. The expansion of electronic banking services by utilizing various electronic channels provide added value to the users. As such, client authentication is required in these applications for affirming the legitimacy of the clients. The most widely recognized service of accreditations utilized today is the static passwords. Weak passwords prove to be an awful choice because it exposes online banking services to various security dangers. Different arrangements have been put forward to eradicate the clients' need for the creation and management of passwords. In this regard, a typical method developed is the one-time password (OTP), i.e., passwords which remain valid for a single exchange or session. Sadly, the vast majority of these password arrangements doesn't fulfil the requirement of usability and scalability and hence can be considered to be unreliable. In this paper, the usability and security facets of the present-day strategies for validation schemes centred on non-OTP and OTP structures are contemplated. At last, the loopholes, as well as the open challenges, are discussed, highlighting their prominence in the related field of study.

Keywords: *Authentication; Access Control; OTP Generation; Out of Band Authentication.*

1. Introduction

Presently, the Internet has turned out to be one of the popular mediums for service delivery equally in corporate and retail areas of banking [1]. The banking sector has been reformed and revolutionized by the introduction of electronic banking (E-Banking) [2]. Banking may be characterized as "the technology which allows customers to access the banking services electronically as payment of bills, transfer funds, and view the accounts details and advices" [3]. Electronic banking directly conveys the regular and new services or products related to banking to clients using electronic and intuitive channels of communication. Banking includes the frameworks that encourage clients of various monetary establishments and general people to avail their account information, execute their business exchanges, or access the data related to budgetary items/benefits by utilizing a public or private framework. Banking incorporates internet-based banking, mobile banking, telephone banking and so on. Besides, the evolution of banking by various methods of electronic channels of communication, for example, internet, phone, cell phone and so on, has displayed convenient and achievable method for banking services [4].

The rise of E-banking money isn't merely pressured by the need that the banks ought to minimize operational costs. It is also a manifestation of the clients' demand to have online access to their banking services whenever and wherever they want [1].

Various reasons make the significance of electronic banking quite apparent. As a matter of first importance, the clients of E-banking enjoy supreme ease as they are authorized to have 24×7 access to a large assortment of banking facilities. Also, it displays a cost-proficient proxy option to phone and branch banking because of the low capital and maintenance cost, alongside its capacity to entirely offer mechanized handling of exchanges [1], [5].

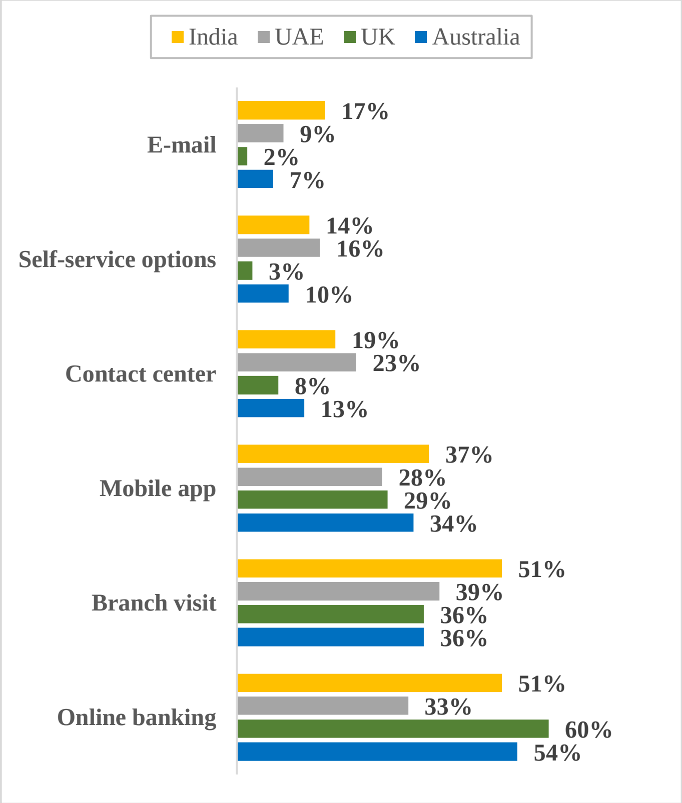

Fig. 1: Preferred Methods in Banking (Adopted From [6]).

Investigations have revealed that a significant portion of the clients likes to utilize internet banking. Fig. 1 represents the utilization of internet banking providing a substantial proof of acceptance of net-banking [6].

Banking institutions have made unmatched accomplishments in conveying its services which vary from PC based applications of banking to telephone banking advancing to Automated Teller Machine (ATM) and Internet Banking. Groundbreaking advancements have been achieved in technologies of mobile communication with WAP, SMS, 3G innovation, SMS, and so forth being introduced which has prompted an extensive development of telecommunication technology. The most recent advancements in the invention in combination with the expanded rate of the popularity of cell phones have influenced the business undertakings to build upon an assortment of services employing cell phones [7]. On similar lines, the banking industry set out to develop applications related to banking on cell phones with a specific end goal to give versatility, a particular highlight of mobile technology offered to their customers which was missing in most of the common strategies of banking [8]. A subsection of Electronic banking, mobile banking, has the advantages of dissemination, personalization, adaptability and omnipresence which guarantees unmatched efficiency, productivity and market potential to organizations.

Additionally, the clients find that managing their bank accounts on their cell phones is much convenient because of security and adoptability when contrasted with the generally utilized methodologies [9]. As an example, in India, the Governor of Reserve Bank of India (RBI) strongly favours the utilization of cell phones as gadgets for completing exchanges with banks [10]. Given the fact that there is a great fall in duties related with cell phones combined with the perfect availability of fixed and mobile line connections, mobile banking has rightly emerged as an economic methodology of banking [3].

The paper is organised in six sections. The necessity for authentication in online banking is highlighted in Section 2 followed by the elaboration on SMS-based authentication in Section 3. Section 4 altogether gives a short review of various present-day authentication strategies followed by the research gaps in Section 5. Finally, in Section 6 concluding remarks have been divulged.

2. Need of authentication in e-banking

Regardless of the various conveniences put forward by the banking based on the web, it isn't without its weaknesses. The current framework on which internet banking is based has been observed to remain available to the risks of hacking and scope of additional different assaults [1]. Even though the different assault techniques are varied, the primary aim of the hackers is to procure the secret data of clients, e.g., passcodes, usernames, social security and credit card numbers etc. All these do not change and are hence called static credentials. However, such credentials are helpless against an assortment of assaults, for example, dictionary assaults. In the current framework, neither the public nor the private system is entirely safe. In the past, there have been various occasions where trustworthy organizations, for example, Walmart, eBay, World Bank, ICICI bank, and so on were hacked bringing enormous losses in terms of both property and private data [11], [12]. Along these lines, there is an inclination to develop a key and long-lasting method which can cater the much-wanted security to the clients [1].

With the fast extension in computerization of small and expansive organizations, authentication is of paramount importance to give security against the developing attacks. Authentication guarantees that the online exchanges are secure and encourages improvement of trust among the exchanging accomplices [1]. An entity can claim property to another entity using authentication. Authorization determines if the entity that has been authenticated has permission to access a particular resource [13]. As a rule, authorization can be alluded to as the consent to access and the assurance of benefits that an element has on a framework and what that element is permitted to do with the assets [14]. The four ways of accomplishing authentication are [15], [16]:

i) Something that is known to the client only, e.g., a secret key or a password, a private key, a Personal Identification Number (PIN).
ii) Something controlled by the client or a physical thing just the client has, e.g. a credit card, a driver's permit, a travel permit, an identification mark or a smart card.
iii) Something the client is, e.g. fingerprints or retinal pattern, facial qualities.
iv) Something the client produces, e.g. customary signature, voice design, and handwriting characteristics.

The applications dealing with online banking require thorough authentication of the clients. Regularly, authentication of the client is accomplished by utilizing the technique of two-factor authentication (2FA), which is security approach working on two levels - in view of something the client just knows, e.g. a static password, and preferably something that is in possession of the client, e.g. a One Time Password (OTP) [17]. For purposes of validation and authentication, biometrics are not utilized in banking because of factors like reliability, cost, complexity and privacy. It has been discovered that the most regularly employed verification method depends on the use of passwords as they are not difficult to execute, advantageous, reasonable and exceptionally embraced by the majority of people yet they can be broken or stolen quite easily [1], [14]. Therefore, a dependable and robust method of authentication is required which can be given by the framework of One-Time-Password [18]. One-time-passwords are dynamic and hence can additionally be alluded to as passwords of single usage, i.e. upon each utilization, they are changed. OTPs are thought to be the most grounded variation of passwords and give a compelling answer to security concerns [13]. One-time passwords assume a conspicuous part in online banking to provide validation upgrading the security [19]. OTPs act as an additional security layer over the regular static passwords that constitute a defenceless solution against replay assaults. OTP is offering resistance against attacks resulting from replaying since the password once created will never be rehashed again indicating that regardless of whether the assaulter gets the OTP it will not be of any use [20]. OTPs are utilized in association with static passwords in banks which present a solid barrier against various online assaults [1]. Notwithstanding this win-win proposition, the delivery of OTPs to the involved client is a noteworthy concern.

3. SMS-based authentication in banking

Short Message Service (SMS) is a highly recognized approach utilized by the common frameworks to circulate the OTPs to the clients for performing on the exchanges over the internet [14]. As an example, in India, the technique of 2FA which is centred on SMS is the commonly utilized technique, especially in banks due to reasons like no charges for logistics and end-device liability [21]. Be that as it may, there are different confinements related to 2FA based on SMS which are talked about as under:

3.1. Delay in SMS delivery

Even if the SMS transmission, typically, happens in the blink of an eye, in case of congestion in the network there might be a transmission delay of SMS. Moreover, the queueing of the SMS while transmission causes the delay in its delivery. This postponement may prompt session time-out which may keep going for a couple of minutes, hence, obstruct the authentication/exchange to take place [14], [22].

3.2. Low security

Regarding the SMS based OTP, there are different conceivable issues related to security. In the beginning, between the provider of service and the client, various cell phone network administrators are required to be components of the trust chain and hence must be trusted. A noteworthy security break is conceivable when a gateway is assaulted in the case of roaming. Also, the encryption used for SMS can be effectively decoded with ease by an attacker. SIM swap assault is another rising risk for the SMS-based OTPs [14].

3.3. Coverage areas/service unreachability

The SMS-based OTPs using a 2FA eventually turn out to be a hassle for the clients because of problems faced while receiving the SMS when the clients are not in the area under the network coverage [22].

3.4. Roaming restrictions

Restrictions on roaming facilities form a significant drawback of the frameworks based on SMS that a client voyaging outside the country might have to face certain network restrictions and might be denied the SMS service. Regardless of whether the service is accessible, clients need to pay high expenses for roaming which result in limitations on SMS service. At the point where customers do not avail activation of roaming facilities, the banks will not succeed in distributing SMS-OTP, thus halting the clients to proceed with any further online procedures [23].

3.5. Government regulatory regulations

In severe crisis and critical conditions, the government needs to take after the specific arrangement of standard principles which includes blocking the service of mass SMS influencing SMS-based mechanisms of authentication [20], [24].

Although the use of OTP guarantees security in client validation yet the process of OTP generation from a server that is based on GSM in the present-day mobile based confirmation framework is liable to the danger of being compromised [25]. Accordingly, a proper financially savvy convention and a safe system of authentication which provides the much-needed ease to clients from an area of crisis without bargaining on security is required. To defeat all the shortcomings, a two-way method of authentication based on details of the device should be produced, advanced changes should be accomplished by taking into account SHA3, truncated SHA1 and RIPEMD-128 instead of SHA1 and MD5 and beating human simplicity of short entries of data compared to substantial length data [11].

4. Existing authentication solutions

Numerous specialists have analyzed the different critical issues related to authentication and security of private and profoundly classified data. Research work organized beneath in the table features various procedures that have been taken up in the past to alleviate different sorts of assaults on the system of authentication of the client and takes care of issues related to securing entities. During the time spent investigating different methods taken up in the past and even in the present-day framework, it was discovered that the use of OTP appears to ensure enhanced security in the field of access management in private as well as the public system [12]. OTP is legal for just a single try of access while attempting to make a unit of exchanges. One of the certain focal points of utilizing OTP is its profound security towards replay assault [26] which implies that unique passcode once generated will indeed not be rehashed for the second time, and henceforth if the secret key is in control of the attacker, it won't be of any utilization. In this manner, usage of OTP has been examined to consider a superior likelihood of making further upgrades in the authentication of the clients [27], [28].

Numerous authentication schemes have been put forward by researchers, but those based on OTPs have been found to be the strongest among all. Different OTP innovations like [29] are additionally observed to be patented, yet standardization of the OTP procedure is still considered to be a testing venture because of its various forms of utilization and architecture proposed by numerous past scientists and protocol producers. The correlation outline for earlier work planned in OTP as well as in non-OTP is displayed in Table 1.

Table 1: Review of Various OTP and Non-OTP Based Schemes

Author	Contribution	Findings	Limitations
(Davaanaym et al., 2009) [30]	Put forward a protected in addition to the market-good online/mobile mechanism of authentication that creates OTP utilizing Ping-Pong128 stream cipher.	➢ Time-memory trade-offs are overcome. ➢ Usage and implementation are easy and can be accomplished on present-day expenses brought about by servers from clients.	➢ For encryption of the OTP generated, AES has been utilized. ➢ The dual communication channel, i.e., GSM and TCP/IP used in this authentication scheme makes it burdensome.
(Moon et al., 2012) [31]	Three solutions are proposed for fuzzy fingerprint vault, enhancing the biometric information security.	➢ Biometric information cannot be changed, lost, speculated or duplicated. ➢ Use with unordered sets makes it suitable for crypto-biometric schemes. ➢ Resistant to correlation assault. ➢ Enhanced GAR execution brought about without any effect on FAR.	➢ Fuzzy vault cannot be disclaimed if compromised. ➢ Biometric data can be compromised by specific modern attacks. ➢ Apt for restricted applications because it is not scalable.
(Avhad and Satyanarayana, 2014) [32]	Proposed an authentication scheme based on a single, single biometric, OTP and password/user ID.	➢ Enhanced assurance information at lesser cost. ➢ Customer privacy in distributed environments is being preserved. ➢ Easy-to-implement configuration.	➢ Reliance on GSM network for transmission of OTP. ➢ Susceptible to MITM and imitation attacks.
(Oruh, 2014) [33]	Designed a security solution for ATMs by combining biometric, smart card and user PIN.	➢ Considerably more reliable, accurate, and secure client authentication strategy for ATMs.	➢ Non-matches and false matches in the biometric trait employed, i.e. fingerprint, are not entirely excluded.
(Alzomai and Josang, 2010) [34]	Exhibited cell phone as a versatile OTP gadget on the basis of trusted computing.	➢ A solution for accomplishing usability and scalability was provided. ➢ Man-in-the-middle (MITM) attacks were minimized.	➢ The OTP generator that has been utilized is SHA-1 on which assaults, in theory, have been accounted for.

			➢ The client is restricted to produce legitimate OTPs when an aggressor disguises as a masquerader of the service provider. ➢ The ease of use is restricted as mobile phones are separated from the client terminals of the users. ➢ Broad specialized versatility of the proposed framework isn't subsidized.
(Srivastava et al., 2011) [35]	An algorithm was put forward that actualizes a port knocking sequence utilizing AES fit for holding up sniffing and spoofing attacks.	➢ The uncovering of information is counteracted by the implementation of a multi-packet mechanism for authentication. ➢ The out-of-order distribution of packets is eliminated. ➢ Various attacks viz. Denial of Service (DoS) attack, Man-In-The-Middle attack (MITM), etc. are averted.	➢ The generated OTP is delivered through a GSM network.
(Hsieh and Leu, 2011) [36]	Given the location of the cell phone and the time, an authentication mechanism is proposed.	➢ Exhibits high resistance against various attacks, for example, replay, eavesdropping, user impersonation and brute force attacks. ➢ The process of client authentication is transparent.	➢ Cell phones empowered by GPS are needed. ➢ There is a need for clock synchronization between the mobile device and the server.
(Ren and Wu, 2012) [37]	Used two parameters time and location of the cell phone to propose a system of authentication.	➢ The high overhead connected with producing an OTP and the efforts of the user are minimized. ➢ Immune to stolen-verifier, Perfect-Man-in-the-Middle (MITM), fundamental phishing as well as replay assaults.	➢ Vulnerable, complex attacks such as phishing attacks which are also on the rise.
(Borowski and Lesniewicz, 2012) [38]	New use of old one-time pads or keys is exhibited by presenting 100 Mbits/sec binary generator.	➢ By utilizing a 100 Mbits/sec equipment random binary generator, supreme security is provided. ➢ An unlimited source of one-time keys is provided.	➢ Secure physical circulation of keys involves high cost; hence adoptability is hampered.
(Ma et al., 2013) [20]	Presented an authentication solution centred on identity by employing speech features.	➢ Better client ergonomics is provided.	➢ Can be of no use if a legitimate user's prerecorded voice gets compromised.
(Castiglione et al., 2014) [39]	Designed an effective end-to-end OTP validation strategy involving the keyed HMAC and AKE convention.	➢ Can work independently because of its simplicity and reduced computational overhead. ➢ Efficient as well as transparent. ➢ Resistant to a vast number of attacks, viz. eavesdropping, offline dictionary, replay, password guessing, Denial of Service (DoS), stolen verifier and brute force.	➢ Cannot be used when the number of iterations surpasses the length of the Master Key. ➢ Security of this mechanism wholly relies on the secure handling and storage of the Master Key.
(Boonkrong, 2017) [40]	Developed and designed a multi-factor authentication procedure, including a registration system producing the authentication factors, and a concrete authentication scheme.	➢ Needs just three messages between client and server of the bank for completing the authentication. ➢ Uses factors like username, password, public key, number of iterations, symmetric key, private key, IP address and the digital signature for authentication, all of which are unique to a user.	➢ Exposed to password reuse threat because of the failure to change password at every user login. ➢ Employment of MD5 and SHA1 that have been reported to be susceptible.
Akinyede and Esese, 2017) [41]	Presented a model that employs Salted SHA 512 for hashing, OTP for authentication and AES for encryption/decryption.	➢ More comfortable and valuable model for conquering online banking issues. ➢ Dependability and validity of the system were warranted with the help of a password recovery tool.	➢ SHA-2 was used exposing the system to length extension attacks. ➢ Utilization of AES for decryption/encryption.

5. Research gaps

Some limitations have been found in the existing security solutions for access management by researchers that range from computational complexity to adoptability to the usage of different media. The review carried out in this section concludes with the deduction of open issues which have been given as:

i) Additional hardware required for some authentication schemes [34], [36], [42] like smartcards cause inconvenience to the user and prove costly to the service provider. As a result, such authentication schemes are not technically adoptable. Therefore, the technical adoptability of those systems is being hampered because they lack user-friendliness.

ii) In several authentication schemes, GSM or authorized persons are used for distributing authentication messages and OTP which is a serious security concern in itself [30], [32], [35], [38].
iii) The contemporary authentication mechanisms [31], [38], [39] have been found to have several issues such as increased processing time, computational cost, reduced system speed and massive storage due to the employment of fuzzy vault schemes, public key operations, and self-updating hash chains.
iv) Only a few systems such as [34] offer the user the privilege to use the same token for different service providers. Maintenance of a separate token for every service provider in most of the authentication mechanisms again puts the user to inconvenience.
v) Due to the inability of some authentication systems [31] to provide extensive service pool scalability, they can be used only for limited applications.
vi) Employment of weak password generation techniques viz., AES, SHA-1, etc. in most of the authentication systems [30], [34], [40], [41] makes them vulnerable besides failing to support in due course of time owing to technological advancements.
vii) Multi-channel communication [30], [34] in some authenticating systems incurs service charges to the user thereby aggravating their burden.
viii) The authentication schemes so far developed rely on a single biometric trait as the third authenticating factor or in some cases take into consideration only biometrics ignoring the first two authentication factors which may be vulnerable to impersonation attacks. As a result, there are security breaches in those authentication schemes and cannot be used in applications demanding high security such as banking sector, airport information systems, etc. [20], [32], [33].
ix) Popularly used biometrics like voice, iris scan and facial features encounter several issues when used for authentication. The framework based on speech recognition can be rendered useless as the attacker can record the voice of the actual client and utilize this recorded voice to get through speech recognition framework on which the proposed authentication mechanism is based. Further, iris scanners need proper lighting else they can lead to false results [20].

6. Conclusion

The development in technology has altogether transformed the industry of banking. Security is perceived to be one of the main issues by the customers in banking transactions. Authentication and authorization assume a crucial part in guaranteeing security over any framework of communication, particularly for the GSM Network. The investigation demonstrates that it is required to propose and form a traditional one-time password utilizing the Android platform which should bolster the execution and also be in line with the existing system. The earlier research work talked about different plans using OTP which are not proficient enough in the arrangement of mobile communication. Moreover, the audit of the previous works shows that the current security frameworks over GSM aren't sufficient for guaranteeing productive security regarding authentication and authorization. Furthermore, a system should be developed that integrates the OTP as well as non-OTP mechanisms for authentication purposes. This can be done by including the biometric factor in the authentication process besides the conventional OTP generation.

Acknowledgement

This work was partially supported by the Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under Research Initiative Grant Scheme (RIGS) number P-RIGS19-020-0020.

References

[1] Two-Factor Authentication for Banking Building the Business Case. Denmark: Cryptomathic. https://cdn2.hubspot.net/hubfs/531679/Documents/White_Papers/Cryptomathic_White_Paper_-_2fa_For_Banking.pdf. 2012. Accessed November 2, 2018.
[2] Khan BUI, Olanrewaju RF, Anwar F & Yaacob M, Offline OTP Based Solution for Secure Internet Banking Access, In IEEE Conference on e-Learning, e-Management and e-Services (IC3e 2018), Langkawi, Malaysia, in press.
[3] Vashishta P & Kapoor S (2012), E-Banking: perspective for survival in current market. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 1(1), 42-46. http://ijettcs.org/Volume1Issue1/IJETTCS2012-05-22-022.pdf.
[4] Jatana R & Uppal RK (2007). E-banking in India: Challenges and Opportunities. New Century Publications.
[5] Pampori BR, Mehraj T, Khan BUI, Baba AM & Najar ZA (2018), Securely eradicating cellular dependency for e-banking applications. International Journal of Advanced Computer Science and Applications 9(2), 385-398. https://doi.org/10.14569/IJACSA.2018.090253.
[6] Das B. UAE customers prefer digital-first approach to banking services. Gulf News. https://gulfnews.com/business/sectors/banking/uae-customers-prefer-digital-first-approach-to-banking-services-1.2067786. 2017. Accessed October 8, 2018.
[7] Masihuddin M, Khan BUI, Mattoo MMUI & Olanrewaju RF (2017), A survey on e-payment systems: elements, adoption, architecture, challenges and security concepts. Indian Journal of Science and Technology 10(20), 1-19. https://doi.org/10.17485/ijst/2017/v10i20/113930.
[8] Khan BUI, Olanrewaju RF, Baba AM, Langoo AA & Assad S (2017), A compendious study of online payment systems: Past developments, present impact, and future considerations. International Journal of Advanced Computer Science and Applications 8(5), 256-271. https://doi.org/10.14569/IJACSA.2017.080532.
[9] Laukkanen T & Lauronen J (2005), Consumer value creation in mobile banking services. International Journal of Mobile Communications 3(4), 325-338. https://doi.org/10.1504/IJMC.2005.007021.
[10] Khan BUI, Olanrewaju RF, Anwar F, Mir RN & Yaacob M, Scrutinizing Internet Banking Security Solutions. International Journal of Information and Computer Security, in press.
[11] Dar H, Al-Khateeb WF & Hadi M (2013), Secure scheme for user authentication and authorization in Android environment. International Journal of Engineering Research and Applications 3(5), 1874-1882.
[12] Mehraj T, Rasool B, Khan BUI, Baba A & Lone AG (2015), Contemplation of effective security measures in access management from adoptability perspective. International Journal of Advanced Computer Science and Applications 6(8), 188-200. https://doi.org/10.14569/IJACSA.2015.060826.
[13] Stewart JM, Tittel E & Chapple M (2005), CISSP: Certified information systems security professional study guide, Sybex.
[14] Kizza JM (2005), Computer network security. Springer Science & Business Media.
[15] Behrouz AF (2010), Cryptography and network security. Tata McGraw-Hill.
[16] Salomon D (2010), Elements of Computer Security. Springer Science & Business Media. https://doi.org/10.1007/978-0-85729-006-9.
[17] Chen YP, Liu DL & Guo R (2010), Security and precaution on computer network. In Future Information Technology and Management Engineering (FITME), 2010 International Conference on, vol. 1, 5-7, IEEE. https://doi.org/10.1109/FITME.2010.5656536.
[18] Smith RE & Vázquez EG (1997). Internet cryptography. Reading, MA: Addison-Wesley.
[19] Olanrewaju RF, Khan BUI, Mattoo MM, Anwar F, Nordin AN & Mir RN (2017), Securing electronic transactions via payment gateways–a systematic review. International Journal of Internet Technology and Secured Transactions 7(3), 245-269. https://doi.org/10.1504/IJITST.2017.089781.

[20] Ma H, Yan S, Bai X & Zhu Y (2013), The research and design of identity authentication based on speech feature. In Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on, 166-169, IEEE. https://doi.org/10.1109/SNS-PCS.2013.6553858.

[21] Limitations of two factor authentication (2FA) technology. ComputerWeekly.com. http://www.computerweekly.com/tip/Limitations-of-two-factor-authentication-2FA-technology. Accessed October 8, 2018.

[22] Gohil B. How Secure Is the SMS Channel for OTP? Panamax. https://www.panamaxil.com/blog/how-secure-is-the-sms-channel-for-otp. 2016. Accessed October 8, 2018.

[23] Eldefrawy MH, Alghathbar K & Khan MK (2011), OTP-based two-factor authentication using mobile phones. In Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, 327-331, IEEE. https://doi.org/10.1109/ITNG.2011.64.

[24] Stallings W (2011). Cryptography and Network Security, 5/E. Pearson Education India.

[25] Hussain S, Khan BUI, Anwar F & Olanrewaju RF (2018), Secure annihilation of out-of-band authorization for online transactions. Indian Journal of Science and Technology 11(5), 1-9. https://doi.org/10.17485/ijst/2018/v11i5/121107.

[26] Mobile operating system. En.wikipedia.org. http://en.wikipedia.org/wiki/Mobile_operating_system. Accessed October 8, 2018.

[27] Duan X & Niu B (2016), A change password attack resistant scheme for remote user authentication using smart card. In Online Analysis and Computing Science (ICOACS), IEEE International Conference of, 269-272, IEEE. https://doi.org/10.1109/ICOACS.2016.7563094.

[28] Deore UD & Waghmare V (2016), Cyber security automation for controlling distributed data. In Information Communication and Embedded Systems (ICICES), 2016 International Conference on, 1-4, IEEE. https://doi.org/10.1109/ICICES.2016.7518881.

[29] Davaanaym B, Lee YS, Lee H, Lee S & Lim H (2009), A ping pong based one-time-passwords authentication system. In 2009 Fifth International Joint Conference on INC, IMS and IDC, 574-579, IEEE. https://doi.org/10.1109/NCM.2009.247.

[30] Moon KY, Moon D, Yoo JH & Cho HS (2012), Biometrics information protection using fuzzy vault scheme. In Signal Image Technology and Internet Based Systems (SITIS), 2012 Eighth International Conference on, 124-128, IEEE. https://doi.org/10.1109/SITIS.2012.28.

[31] Avhad PR & Satyanarayana R (2014), A three-factor authentication scheme in ATM. International Journal of Science and Research (IJSR) 3(4), 656-659.

[32] Oruh JN (2014), Three-factor authentication for automated teller machine system. IRACST-International Journal of Computer Science and Information Technology and Security (IJCSITS) 4(6), 160-166.

[33] Shivraj VL, Rajan MA, Singh M & Balamuralidhar P (2015), One-time password authentication scheme based on elliptic curves for Internet of Things (IoT). In Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, 1-6, IEEE. https://doi.org/10.1109/NSITNSW.2015.7176384.

[34] Alzomai M & Jøsang A (2010), The mobile phone as a multi OTP device using Trusted Computing. In 2010 Fourth International Conference on Network and System Security, 75-82, IEEE.

[35] Srivastava V, Keshri AK, Roy AD, Chaurasiya VK & Gupta R (2011), Advanced port knocking authentication scheme with QRC using AES. In Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on, 159-163, IEEE. https://doi.org/10.1109/ETNCC.2011.5958506.

[36] Hsieh WB & Leu JS (2011), Design of a time and location based One-Time Password authentication scheme. In Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, 201-206, IEEE. https://doi.org/10.1109/IWCMC.2011.5982418.

[37] Ren X & Wu XW (2012), A novel dynamic user authentication scheme. In Communications and Information Technologies (ISCIT), 2012 International Symposium on, 713-717, IEEE. https://doi.org/10.1109/ISCIT.2012.6380995.

[38] Borowski M & Leśniewicz M (2012), Modern usage of "old" one-time pad. In Communications and Information Systems Conference (MCC), 2012 Military, 1-5, IEEE.

[39] Castiglione A, De Santis A, Castiglione A & Palmieri F (2014), An efficient and transparent one-time authentication protocol with non-interactive key scheduling and update. In Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on, 351-358, IEEE. https://doi.org/10.1109/AINA.2014.45.

[40] Aboud SJ (2014), Secure password authentication system using smart card. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3(1), 75-79.

[41] Boonkrong S (2017), Internet banking login with multi-factor authentication. KSII Transactions on Internet & Information Systems 11(1), 511-535.

[42] Akinyede RO & Esese OA (2017), Development of a secure mobile e-banking system. International Journal of Computer (IJC) 26(1), 23-42.