

PAPER • OPEN ACCESS

A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number

To cite this article: Waleed A. Hammood *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **769** 012061

View the [article online](#) for updates and enhancements.

A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number

Waleed A. Hammood¹, Ruzaini Abdullah¹, Omar A. Hammood¹, Salwana Mohamad @ asmara¹, Mohammed A. Al-Sharafi¹, Ali Muttaleb Hasan¹

¹Faculty of Computing (FKOM)
College of Computing and Applied Sciences
Universiti Malaysia Pahang 26300
Kuantan, Pahang, Malaysia

engwaleed54@yahoo.com, ruzaini@ump.edu.my, omer_almajeed@yahoo.com,
salwanamohamad@ump.edu.my, ma_shrafi@yahoo.com, alimatlab65@yahoo.com

corresponding author: engwaleed54@yahoo.com

Abstract. The traditional banking system, such as transactions over the counter using bank book is enhanced by adding the elements of electronic banking, where nowadays all transaction can be done over the network, because of globalization and the advancement of information and communication technology. However, significant threats to this technology also come in parallel, such as from banking frauds. This is why building trust among banking users by providing security mechanisms is very important. In the electronic banking, security mechanisms mainly focus on proving a secure environment for the online transaction, especially user authentication. Many researchers have been proposed various models for the online user access authentication for the banking industry. Most of the researches are based on traditional the form of username and password, but with the varying mechanism of password forms. For example, password in arbitrary value, password in arbitrary value through secured channel, as well as biometric like fingerprint recognition, voice recognition, or retina recognition. In this paper we reviewed the current existing user access for online banking based on mobile phone, the functions of the SIM card, the characteristics mobile of the SIM card are described. Cloning, a threat to the SIM card is also described. Findings show that all the security model for online user access contains password in the form of value, biometric, or PIN. Thus, none of the existing user access proposed the idea of the user access based on International Mobile Equipment Identity (IMEI) number to strength the security of the user access. The IMEI is a 15- or 17-digit code that uniquely identifies mobile phone sets.

1. Introduction

Online security is more complicated than computer security, the hackers always try to hack social network account, personal bank account, and e-mail account [1]. According to Nattakant [2] has discussed the phishing that includes sending of e-mails pretending in the form of legal financial institutions to the receiver and request private information such as username and password. it may potentially to collect cash from e-account by hacking. These hackers till now chopped many bank's web site and collect hugs amount of money through their technological efficiency, the e-transaction is fully dependent by online banking. So, the mainly depends on e-banking security is the protection of software, called software security. In this modern world, the traditional banking transaction is changing from using bank book over the counter to the transaction over the internet [3], as a result of technological advancement. So, clients' of the banks can perform transaction online by using the



computer as well as mobile phone, which eases the transaction because clients' can make their banking regardless of time and place. That is why providing security to online banking transaction is the main concern in the modern banking system [4]. There are many security incidents reported in the news. In August of 1995, it was reported that there was a security incident, which involved attackers breaking into their system [5, 6] which estimate a \$10 million lost. It was the primary successful penetration by a hacker into the arrangement of the \$10 million dollars illicitly moved, \$400,000 was as yet not found. In August 2000, British police have captured three men regarding an endeavour of deceitful in Egg banking system [5]. As per the report, the bank was the target of an effort to get cash through deceitful records however no cash was stolen, then the Egg authority strongly said that none of their computer systems had been breached.

In April 2010, a fire alarm company in Arkansas lost more than \$110,000 because of a hacking incident [7]. Hackers hack into the system of the company and stole its online banking credentials and drained its payroll account. It was seen that through the span of the past couple of days, somebody had affirmed two bunches of finance instalments one for \$45,000 and another for \$67,000. A couple of days after the fact, Melanie Eakel, CEO of JE Frameworks Inc., was educated by the bank about the Web Address that was utilized to process the payments, the username and password of the online banking [8]. Different security policies or frameworks have been deployed to banking systems to secure financial transaction for their online users. For example, there are banks that provide their own application to their clients to make the transaction. There are also banks that provide two-way verification method by sending a code to the clients' mobile phone, called SMS-based authentication [9] while the transaction is made.

The banking frauds reported, it is clear that we need to strengthen the online banking system. Experts and researchers have published many types of research on banking security, especially in a user authentication scheme. Most of the papers describe new security policy or framework for the banking transaction. For example, digital watermarking scheme Alam et al [10], digital identity Chowdhury & Noll [11], and PKI-SIM Card scheme Xue et al [12]. In this paper, we studied authentication methods used in various banking operations of user authentication for online banking system.

2. Literature review

As a result of technological advancement, the current traditional banking system and financial services are being transformed to the electronic banking system [13, 14], which is called online banking system. Using this system, users can now perform transactions, pay the bill, and shop online without any hassle, which makes lives easier. While online banking system provides hassle-free banking to the users, security to banking transaction for users is the main concern. Many technologists are trying to enhance the security of the bank [15]. The concern is to make user authentication system more secure [16]. Authentication is the process by which the end user application is identified and authorized so that, the user can have access to the system or application [17, 18]. The authentication aim is to verify that the certain information provided is a request from a given individual to be authentic. [19]. Generally, some of the information security management (ISM) systems follow the guidelines of the International Electro-Technical Commission (IEC) 27001 standard and International Organization for Standardization (ISO). [20]. At the particular level of Internet banking security, there seems to be no common standard that can be followed by all Web banking services, but there are certain set of guidelines for specific contexts. Two of these are the Data Security Standard (DSS) for Payment Card Industry (PCI), and the VISA requirements for payment security [20]. According to Poetta et al [21], the existing user authentication can be summarized as follows:

- Password, which can be any arbitrary secret value.
- Password through secured channel.
- SMS Code – one-time password sent by SMS.
- PIN – limited confidential value.
- Grid Card – the client inserts these codes sequentially into the process with a paper card with payment.

- PKI – Public key cryptography-based encryption scheme.
- Token - Trustworthy tool for authentication.

From the above existing user authentication mechanisms, they have been classed in three groups of categories, based on the factors that are [22]:

2.1. Single Factor Authentication Mechanisms

This is the traditional security method that requires user ID and password [22] to logging into the web, mobile phone application, or system. It is also called Single Factor Authentication (SFA) [22]. The security in SFA is totally depended on end-user's creativeness of providing the password, because the password should be trickier making it harder to guess. We have classified SFA in two categories. They are:

- Password – arbitrary secret value

This is the traditional security method that requires user ID and password [22] for logging into the web, mobile phone application, or any system. Hence, the users should take more precautions [22, 23] to choose the password. They should create a strong password, which contains alphabet, numerical value, and special characters.

- Password through secured channel (for example SSL)

Like any other web application, Web banking systems use The Hypertext Transfer Protocol (HTTP) for data transfer [20]. Regarding data transfer through HTTP, all communications must be secured. That is why the Secured Socket Layer (SSL) or Transport Layer Security (TLS) protocol (i.e. HTTP Secure over SSL or HTTP over TLS (HTTPS)) must be used with POST method for sending data as POST method is more secured than GET method of HTTPS.

Clients can access to a website in a both secured or insecure manner. When clients have the opportunity to access to the website in a secure manner, the clients at that point be confirmed in certain designs. At the point when the client goes from an public page through a secure part, the web server begins SSL and secures this sort of communication. The difference between SSL and Non-SSL connection between user and bank website is shown in Fig 1.

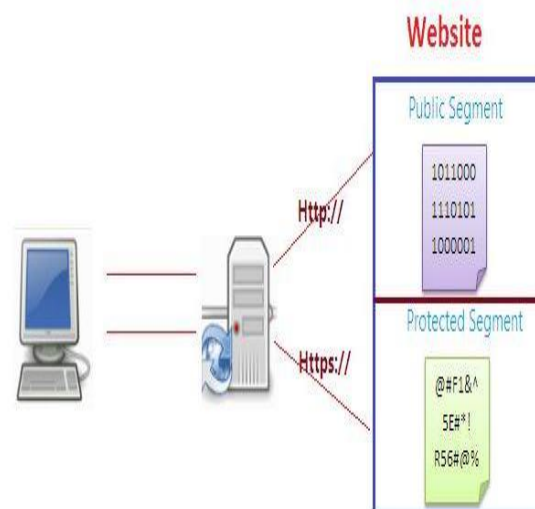


Fig. 1. Difference between SSL and Non-SSL connection adapted from [24].

In figure 1, it is shown that user is visiting a website. In Http://, the connection between user and server is a public segment, which means data is transmitted through the channel only on binary format. On the other hand, in Https://, the connection between the server and the user is protected segment or secured channel. Data is transmitted in a encrypted format through this secured channel.

The following Fig 2. is showing the overall process of mutual authentication for both client and server to each other in an SSL.

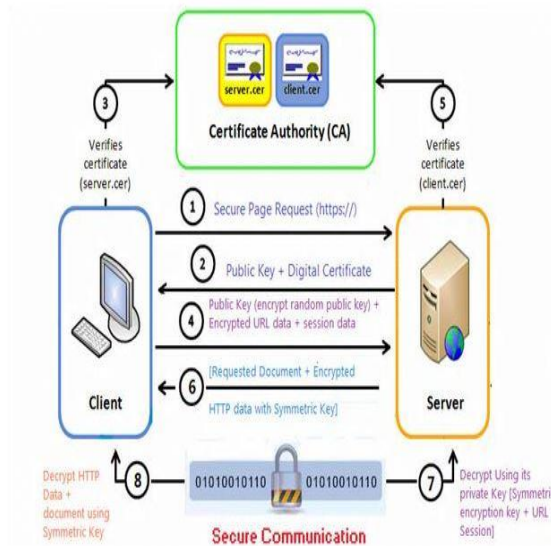


Fig. 2. Steps of SSL connection between user and bank server.

Asymmetric encryption is SSL's basic building block where the public key is freely shared to encrypt the message that the private key can only decrypt. SSL hires a third-party agency, a Certificate Authority (CA) to classify one or both ends of the transactions. The previous diagram shows how it works..

- A browser must send a request to interface with the server and requests a protected page (more often than not a report).
- The server of the web sends the public key with the user's labeling certificate.
- The browser tests if the certificate issued by the CA it trusts. The customer contrasts the data in the certificate and the data got from the site and checks every one of the subtleties. Assuming this is the case, the browser demonstrates the virtue of the server certificate by demonstrating a green lock and the customer continues.
- The browser creates a symmetric random encryption key and then encodes it to the server's open key. At last, it sends it to the server alongside the encoded URL and other encoded HTTP information.
- The web server decodes the approaching packet utilizing its private key and uses the symmetric key to decode the HTTP and URL information that was produced randomly at the user side.
- The requested file from the server is then sent back to the user together with other information encrypted with the symmetric key.
- Eventually, using the symmetric key, the browser decrypts the packet and safe handshaking is created.

Figure 3 shows a typical SFA log in procedure that normally has user name and password fields for users to enter their confidential information.

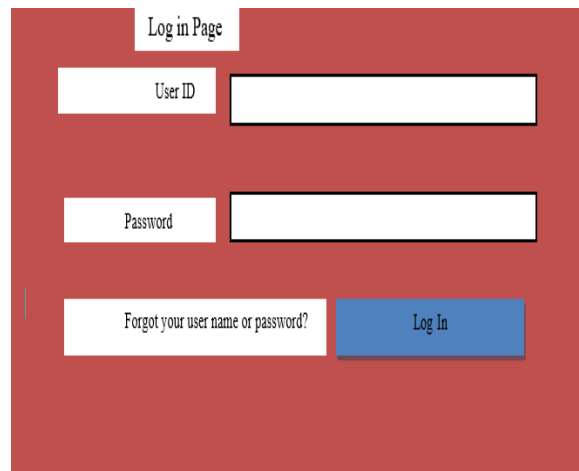
The image shows a login form on a red background. At the top, there is a white box with the text "Log in Page". Below this, there are three rows of input fields. The first row has a white box labeled "User ID" followed by a white input field. The second row has a white box labeled "Password" followed by a white input field. The third row has a white box labeled "Forgot your user name or password?" followed by a blue button labeled "Log In".

Fig. 3. A typical SFA login procedure.

2.2. Two-Factor Authentication Mechanisms (TFA)

Two-Factor Authentication is an end-user protection system having to go through following two factors. In this mechanism, user supplies or provides two types of identification, the one of which is normally a physical token, like a unique key generator or a smartphone, and the other of which is regularly something memorized by the user, for example, a security code or PIN or a token or a password. In this unique circumstance, the two elements included that you have and something you know. TFA methods are described below:

- SMS Code - One Time Password (OTP) Send by SMS

To fall in the TFA class, the user should have a device like Grid Card or Smart Card or “what you have” and user should know something (PIN or password) or “what you know”. In this method, user has something (e.g. Mobile phone) to receive a PIN or a Code and User knows something (PIN or Code) after receiving them in their mobile phone. For this, user needs to register his or her phone number on their accounts [25, 26].

OTP is a disposable password, which is impossible to find out because of its dynamic feature. That is why this password can not be used again once it is used next time [27]. Thus, it is valid only for a short time, which lasts for one session or transaction [22]. This method is a combination of time-synchronous method and the event-synchronous method [27]. This method is widely used nowadays. A new code is generated in every specific time interval and it changes the code by increasing the counter value for reattempt in each time interval.

An OTP log in process is shown in Fig 4. In this method, the user will visit the bank’s log-in page and will be asked to enter phone number to receive OTP after entering his or her user ID. The number will be verified in the server. Then, the user will receive a short code in their given mobile phone number. Thus, user will enter this given code in the password box in the user log-in page.

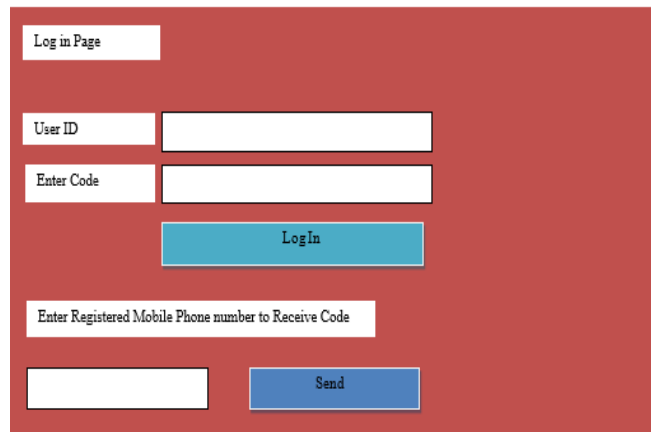


Fig. 4. OTP Log in process.

- Grid Card – paper card with transaction codes, user enters these codes in sequence into the system

This is a combination of paper card or device and something, such as Personal Identification Number (PIN) number or password or secret phase that the user knows [22, 28]. The use of Grid Card in our daily life is withdrawing money from Automate Teller Machine (ATM) system. The user needs to insert his or her debit card or credit into the ATM machine and then type their PIN. This process can be classified in two steps: Grid Card - user has something and PIN - user knows something. This authentication method can also be brought to the online or Internet world, especially for online banking transactions. In modern Grid Card, there is a smart chip, which contains user information stored in the bank server, has been pasted. The flowchart of Grid Card using PIN method is shown in Fig 5. below. In this flowchart, we have assumed that all banks share each other's users' information if it is their debit card.

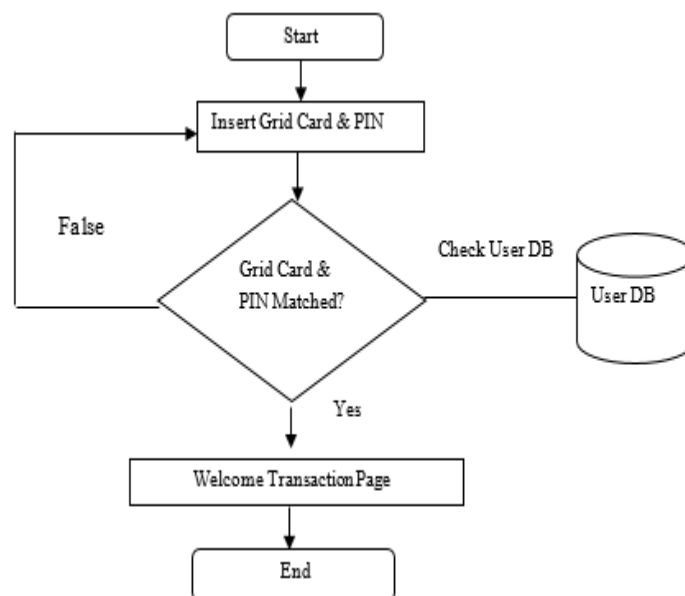


Fig. 5. Flowchart of Grid Card & PIN method.

- Token - trustworthy authentication device

Token is a small pocket-size device for authentication, which display passcode on Liquid Cristal Display (LCD) [22, 29]. It generates password based on an algorithm [25] and is increasingly used in banking industry for user authentication. If users try to log into the bank's internet banking system, a username and password created by the token will be requested from the protected web page. The token also has a PIN which must be inserted in token whenever a code is needed.

It can also provide an electronic signature code based on the key issued by the internet banking application's protected website. Consequently, it has two functions: Provide a login password (option 1 from the main menu) and a signature token if requested as part of a web page transaction (option 2 from the token main menu).

The token will have a registration number and is connected to the account of the user. For other accounts, it cannot be used to create passwords. Last, authentication system based the Public Key Cryptography (PKI) password through secured channel, in this mechanism, password is sent through secured channel using Public Key Cryptography.

2.3. Multifactor Authentication

Multi-Factor Authentication (MFA) or strong authentication mechanism [22, 30] authenticates users for transaction such as make a payment, fund transfer, or log into the system by providing multi-level security mechanism [31]. In addition to two factor authentication mechanism, where user provides two level of identification; for example, physical token like smart card or debit card and a security code or PIN or password, in MFA, an additional authentication method is used to verify users. The additional authentication method can be biometric verification process such as iris recognition, finger print scanning, facial recognition, or voice ID. MFA method is shown in Figure 6 below:

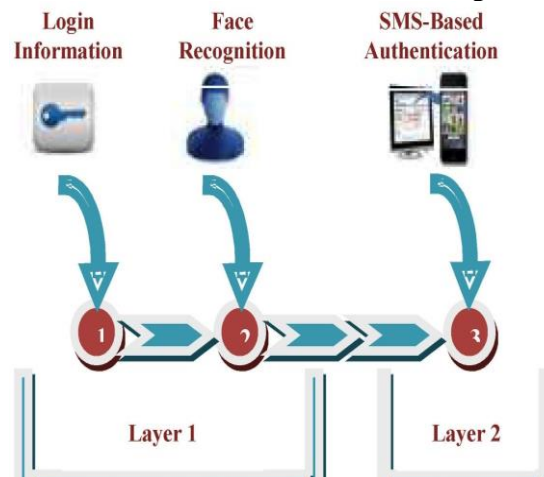


Fig. 6. MFA using face recognition process adapted from [32].

In the figure above, there are two layers for MFA. In step one of first layer, users will enter their typical user name and password. After they enter those credentials and values, the system will recognize users' face in step two. And lastly, in step 3 in layer two, users will enter the PIN number that is received in their mobile phone after completing Layer 1.

3. Security in Online Banking System

This section reviews the existing work in online banking, particularly the security procedures on user authentication, using mobile phones. Alam et al and McCarthy et al [10, 24] described mobile banking process - opening bank account using mobile phone, checking account balance, and making transaction through mobile phone. And later, they proposed a two-level security scheme for transaction by using: biometric verification, and digital watermarking.

In their proposed scheme, they divided the transaction method in two steps. The first step covers the security between Client and Mobile Server by sending SMS from their registered mobile number saved in the bank and then user will be prompted to record their own voice, which will be forwarded to and stored in the banking server. So, when the user wants to make any transactions later on, their given voice will be verified with the stored voice in the server, and if the voice is matched, they will be able

to make transaction. In the second step, they cover the security between Mobile Station and Bank Server by securing the stored data in the server using digital water making technique. To do so, they used two data hiding techniques namely the standard Least Significance Bit (LSB) method and Bit Least Significance Bit (BLSB) method. In this method all processes of user verification or authentication is performed using the registered mobile number of clients. However, this method is susceptible to mobile Subscriber Identity Module (SIM) card cloning. Another work proposed by Xue et al [12] is an authentication scheme called Public Key Infrastructure - Subscriber Identity Module (PKI - SIM), which generates authentication key independently both in mobile phone and in the authentication server. This is a good authentication scheme for online transaction, but still has some weaknesses, especially SIM card cloning. The summary of literature review is shown in the table 1:

Table 1. The existing security scheme and framework for the clients' authentication for online transaction.

Authors	Description
[10]	Propose two way security scheme for user verification and authentication using mobile SIM card.
[12]	Proposed PKI-SIM card based authentication method.
[9]	Online banking services: user authentication and data origin authentication. SMS based authentication by sending an OTP.
[11]	Described a model "My Digital Identity" using mobile SIM card.

4. Conclusion and Future Work

The traditional banking transaction is changing from using bank book over the counter to the transaction over the internet, as a result of technological advancement. This paper reviewed the existing framework for online user access for the bank. It was also shown the classification of the existing framework based on factors. As mobile phone is the main character of this research. It also gives primary idea about cloning SIM card, analysed the previous research works related to online user access authentication system for bank, building a trust among banking users by providing security mechanisms is very important. The previous work found that all the security model for online user access contains password in the form of value, biometric, or PIN. But it is time to get out of this current trend. Experts and researchers have published many researches on banking security, especially in user authentication scheme. Most of the papers describe new security policy or framework for the banking transaction. For example, digital watermarking scheme [10, 33], digital identity [34], and PKI-SIM Card scheme [35]. However, to best of our knowledge, none of the literature reviews have been performed that focuses on Subscriber Identification Module (SIM) card cloning attack for the online clients' authentication for the banking industry. So, future research should be focused on user authentication system or model without any password based on mobile IMEI number.

References

- [1] Sadekin, M.S. and A. Shaikh, *Security of E-Banking in Bangladesh*. Journal of Finance and Accounting, 2016.
- [2] Utakrit, N., *Security awareness by online banking users in Western Australian of phishing attacks*. 2012.
- [3] Adrian, T. and A.B. Ashcraft, *Shadow banking: a review of the literature*, in *Banking Crises*. 2016, Springer. p. 282-315.
- [4] Al-Otaibi, S., et al., *The satisfaction of Saudi customers toward mobile banking in Saudi Arabia and the United Kingdom*. Journal of Global Information Management (JGIM), 2018. 26(1): p. 85-103.
- [5] Lee, A.J.Y., et al., *Customers' Satisfaction Towards Online Banking In Malaysia: A Primary Data Analysis*. 2017, UTAR.
- [6] Yang, Y.-J. *The security of electronic banking*. in *Proc. Nat. I International Systems Security Conference*. 1997.
- [7] Gunson, N., et al., *User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking*. Computers & Security, 2011. 30(4): p. 208-220.
- [8] Hiltgen, A., T. Kramp, and T. Weigold, *Secure internet banking authentication*. IEEE Security & Privacy, 2006. 4(2): p. 21-29.
- [9] Panja, B., et al. *Cybersecurity in banking and financial sector: Security analysis of a mobile banking application*. in *2013 International Conference on Collaboration Technologies and Systems (CTS)*. 2013. IEEE.
- [10] Alam, S.B., et al. *A secured electronic transaction scheme for mobile banking in Bangladesh incorporating digital watermarking*. in *2010 IEEE International Conference on Information Theory and Information Security*. 2010. IEEE.
- [11] Chowdhury, M.M. and J. Noll. *Distributed identity for secure service interaction*. in *2007 Third International Conference on Wireless and Mobile Communications (ICWMC'07)*. 2007. IEEE.
- [12] Yin, X., et al. *An improved dynamic identity authentication scheme based on PKI-SIM card*. in *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*. 2009. IEEE.
- [13] Priya, R., V. Tamilselvi, and G. Rameshkumar. *A Novel algorithm for Secure Internet Banking with finger print recognition*. in *2014 International Conference on Embedded Systems (ICES)*. 2014. IEEE.
- [14] Al-khatib, A.A. and W.A. Hammood, *Mobile malware and defending systems: Comparison study*. International Journal of Electronics and Information Engineering, 2017. 6(2): p. 116-123.
- [15] de Oliveira Malaquias, F.F. and Y. Hwang, *An empirical investigation on disclosure about mobile banking on bank websites*. Online Information Review, 2018. 42(5): p. 615-629.
- [16] Rosener, D.K., W.O. Brown, and E.L. Reuss, *User authentication system and method*. 2016, Google Patents.
- [17] Basavala, S.R., N. Kumar, and A. Agarrwal. *Authentication: An overview, its types and integration with web and mobile applications*. in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*. 2012. IEEE.
- [18] Omar A. Hammood, M.N.M.K., Muamer N. Mohammed and Waleed A. Hammood *Issues and Challenges of Video Dissemination in VANET and Routing Protocol: Review*. Journal of Engineering and Applied Sciences, 2017. 12(11): p. 9266-9277.
- [19] Conklin, A., G. Dietrich, and D. Walz. *Password-based authentication: a system perspective*. in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. 2004. IEEE.
- [20] Martino, A.S. and X. Perramon. *A model for securing E-banking authentication process: antiphishing approach*. in *Services-Part I, 2008. IEEE Congress on*. 2008. IEEE.
- [21] Peotta, L., et al., *A formal classification of internet banking attacks and vulnerabilities*. International Journal of Computer Science & Information Technology, 2011. 3(1): p. 186-197.
- [22] Basavala, S.R., N. Kumar, and A. Agarrwal. *Authentication: An overview, its types and integration with web and mobile applications*. in *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*. 2012. IEEE.
- [23] Alghathbar, K. and H. Mahmoud. *Noisy password security technique*. in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*. 2009. IEEE.
- [24] McCarthy, C. and A.N. Zincir-Heywood. *An investigation on identifying SSL traffic*. in *2011 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*. 2011. IEEE.
- [25] Lupu, C., V.-G. Gaitan, and V. Lupu. *Security enhancement of internet banking applications by using multimodal biometrics*. in *Applied Machine Intelligence and Informatics (SAMi), 2015 IEEE 13th International Symposium on*. 2015. IEEE.

- [26] Arshah, R.A., W.A. Hammood, and A. Kamaludin, *An Integrated Flood Warning and Response Model for Effective Flood Disaster Mitigation Management*. *Advanced Science Letters*, 2018. 24(10): p. 7819-7823.
- [27] You, H.-N., et al., *A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment*. *The Journal of Korean Institute of Communications and Information Sciences*, 2011. 36(8B): p. 939-946.
- [28] Hammood, O.A., et al., *RESP: Relay Suitability-based Routing Protocol for Video Streaming in Vehicular Ad Hoc Networks*. *International Journal of Computers, Communications & Control*, 2019. 14(1).
- [29] Hammood, O.A., et al., *The VANET-Solution Approach for Data Packet Forwarding Improvement*. *Advanced Science Letters*, 2018. 24(10): p. 7423-7427.
- [30] Hammood, O.A., M.N.M. Kahar, and M.N. Mohammed. *Enhancement the video quality forwarding Using Receiver-Based Approach (URBA) in Vehicular Ad-Hoc Network*. in *2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*. 2017. IEEE.
- [31] Hashim, E.W.A., M.O.A. Hammood, and M.T.I. Al-azraqe, *A Cloud Computing System based Laborites' Learning universities: Case study of Bayan university's Laborites-Erbil*. *BOOK OF PROCEEDING*, 2016: p. 538.
- [32] Mohammed, M.M. and M. Elsadig. *A multi-layer of multi factors authentication model for online banking services*. in *Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on*. 2013. IEEE.
- [33] Alam, S.B., et al. *A secured electronic transaction scheme for mobile banking in Bangladesh incorporating digital watermarking*. in *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*. 2010. IEEE.
- [34] Chowdhury, M.M. and J. Noll. *Distributed identity for secure service interaction*. in *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on*. 2007. IEEE.
- [35] Xue, Y., et al. *An improved dynamic identity authentication scheme based on PKI-SIM card*. in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*. 2009. IEEE.

Acknowledgment

UMP Postgraduate Research Grants Scheme, PGRS190386, funds this research.