1-1-2019

Online authentication methods used in banks and attacks against these methods

Anoud Bani-Hani
Zayed University

Munir Majdalweieh
Zayed University

Aisha AlShamsi
Zayed University, alanood.alshamsi@zu.ac.ae

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 151 (2019) 1052–1059

Procedia Computer Science

www.elsevier.com/locate/procedia

The 6th International Workshop on Machine Learning and Data Mining for Sensor Networks (MLDM-SN)

Online Authentication Methods Used in Banks and Attacks Against These Methods

Anoud Bani-Hani[a*], Munir Majdalweieh[a], Aisha AlShamsi[a],

[a] *College of Technological Innovation, Zayed University, Dubai 19282, UAE*

Abstract

Growing threats and attacks to online banking security (e.g. phishing, identity theft) motivates most banks to look for and use stronger authentication methods instead of using a normal username and password authentication. The main objective of the research is to identify the most common online authentication methods used widely in international banks and compare it with the methods used in six banks operating in UAE. In addition, this research will cover the current authentication threats and attacks against these methods. Two well-defined comparison matrices [15], one based on characteristics and second one on attack vectors, will be used to examine and assess the authentication methods of those six banks. This paper is different than other studies and works since it will help to identify the common authentication methods used in banks operating in UAE. Moreover, the comparison matrices will help to examine those authentication methods, define their weaknesses, and evaluate them.

Keywords: Authentication, banks, comparison matrix, characteristics, attack vectors, methodology, UAE, password.

* Corresponding author. Tel.: +971-0-44021735;
E-mail address: Anoud.Bani-Hani@zu.ac.ae

1877-0509
10.1016/j.procs.2019.04.149

1. Introduction

Online Banking or E-banking is the practice of initiating banking transactions through the internet [5]. Major Banks currently offer different online banking services to their customers. For example, it reduces physical visits to the bank, it enables serving more customers at a fraction of the cost and solves the issue of customer's convenience [17]. As Bhatt [5] posted too, online banking can help the customers to check his/her balance, make deposits, withdrawals, transactions, and even pay the bills from anywhere [17].

This research is focus on online authentication methods, so our main concern is on the first two factors what the user knows and what he/she has. The authentication methods related to biometric characters, something the user is, will not be discussed in this paper. Authentication through the use of a username & password (i.e., something the user knows) only considers a single-factor authentication. While, depending on something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN, password) considers two-factor authentication or multifactor authentication. Authentication methods that depend on more than one factor (multifactor authentication) are stronger, more reliable and more difficult to compromise than single-factor methods [7]. *"As online transactions require new authentication methods, banks are trying to introduce new approaches in order to prevent attacks being successful and to increase security*" [6].

2. Background

By strengthening the security and protocols of online banking, it would prevent unrestricted access to private information and further strengthen the relationship with customers. A key step in protecting the information is authentication. Username and password are the most common type of authentication [3].

However, authentication through single factor authentication like username and password is considered weak. Similarly, partial password is form of password authentication. Unlike the regular password, the system would request random characters from the password [25]. Furthermore, A newer form of authentication that has been integrated in many authentication systems. Secret image or identifiable picture uses an image in place of a password [11].

Password and PIN are vulnerable to a variety of insidious threats such as dictionary attack, brute force attack and password guessing attack. The goal of the attacks is to find the username and password to gain unauthorized access. In addition to that, keyloggers are another threat that can capture all the keystrokes done on the keyboard by the user [10]. It is noteworthy to mention that keyloggers can have an advanced feature that enables the attacker to capture the screen of the victim [24]. However, not all form of attacks would require advanced skills. Some attacks such as social engineering and phishing depends more on the manipulation skills of the attacker to trick victims into revealing information [26]. Similarly, with shoulder suffering and hardware (observation) attack, it would require the attacker to have better more observational skills.

3. Methodology

The aim of this research is to examine common existing online authentication methods. In addition, this study examines the current authentication threats and attacks against these methods. Then, discuss and analyze the methods used in six banks operating in UAE, which for will be referred to as Bank A, Bank B, Bank C, Bank D, Bank E, and Bank F. Discussion and analysis section are based on the data captured through observation while navigating through the internet banking services of the targeted banks and from the user's aspect who has the privilege (credentials) to access the online services of the banks. Jong [15] evaluated the authentication methods in his paper based on three primary subjects, which are characteristics, attack vectors and user acceptance. We are interested mostly in characteristics and attack vectors, and we are going to use the two matrices belong to these two subjects only to evaluate the authentication methods. Based on the Comparison Matrix Characteristics of Authentication Methods used in Jong's paper [15], the characteristics of authentication methods used in these six banks, for example, requirement of additional Hardware and Software, Complexity, Scalability, Portability and System requirements will be compared and evaluated. Comparison Matrix Attack Vectors of Authentication Methods will be used also to represent the

probability to succeed the attack for each authentication method discussed earlier, for example, shoulder Surfing, Keylogger, Screen Capturing, Brute force attack, Guess attack, Dictionary attack, Hardware Observation attack, Social engineering, Phishing attack, MITM attack, MITB attack, Network Sniffing and Short Access [15].

3.1. Online Banking Authentication Methods

The objective of this section is to review the common different online authentication methods used in banks around the world. The Comparison Matrix Characteristics of Authentication Methods done by Jong shows the authentication methods and their characteristics based on a scale from 1 to 5, where higher is better. Using this matrix, we can evaluate the specified authentication methods and point out their strengths and weaknesses. We did a small modification in the matrix by adding new suitable authentication methods that need to be evaluated, which are (PIN, Secret Image, Smart card, USB token and Security questions) * and deleting some that are not relevant. At the end, we got a matrix with 13 authentication methods. In addition, some characteristics have been deleted from the characteristics' row in the matrix, which are Login time, Acquisition cost, Deployment cost and Operating cost. The reason behind removing them is because it's difficult to estimate acceptable values for these specific characteristics. A short explanation for the new authentication methods is found in Table 1 and a short explanation for each characteristic is found in Table 2.

Table 1. Comparison Matrix Characteristics of Authentication Methods [15].

Authentication Method	Explanation
Username & password	Authenticating the user by what he knows which the username and password [3].
PIN*	Is a personal identification number. It is commonly assigned to bank customers to use for transactions of ATM [19].
Virtual Keyboard	It's a keyboard shown on the screen. The user needs to enter his password by clicking on the proper characters [18].
Partial Password	Authenticating by requesting some random characters from the user's password instead of the full password [25].
Secret Image*	The user would have to select one memorable image from a group of random images to verify his identity [11].
Smart Card*	It has an inbuilt memory with the user's credentials and only requires a password to gain access [27].
USB token*	It is similar to a smart card. USB token is a secure way to provide authentication by providing credentials [16].
OTP manual, automatic, synchronous, a-synchronous OTP automatic OTP synchronous OTP a-synchronous	The problem with password is that users tend to use short and common combinations to avoid memorizing [3]. Using one-time passwords that are valid for one time use only could solve this problem and reduce the risk. One-time password is valid for one time use and a new password is generated for the next authentication process [24].
Security Questions*	Security questions are used to authenticate users when they forgot or lost their passwords [1].
Bookmark authentication	Bookmark authentication depends on a bookmark the user creates during the registration process. It's often sent to the new customer via emails, so he/she can add it easily [15].

* new authentication methods

Table 2. Explanation of Characteristics.

Characteristics	Explanation
Additional Hardware	Does the solution require additional hardware? (1= card + reader), (2 = hardware token), (3 = cell phone), (4 = paper or card), (5 = none)
Additional Software	Does the solution require additional software? (1= application), (2 = cookie), (3 = n/a yet), (4 = Flash/Java enabled), (5 = none)
Complexity	How complex is to implement the solution? (1 = very difficult), (2 = difficult), (3 = medium), (4 = easy), (5 = very easy)
Scalability	Can the solution grow? (1 = very difficult), (2 = difficult), (3 = medium), (4 = easy), (5 = very easy)
Portability	Is the solution portable? (In your pocket or to another computers/smart phone) (1 = very difficult), (2 = difficult), (3 = medium), (4 = easy), (5 = very easy)
System Requirements	(1= card + reader), (2 = compatible cell phone), (3 = normal cell phone), (4 = Flash/Java enabled), (5 = normal computer)

3.2. Current Authentication Threats and Attacks

The objective of this section is to review the common threats and attacks that the previous authentication methods are vulnerable to. The Comparison Matrix Attack vectors of Authentication Methods done by Jong shows the attack vectors on online authentication methods used by hackers based on a scale from 1 to 5 (see table 3), where higher is a better resistance against the attack. Using this matrix, we can measure and determine whether the authentication method is more vulnerable to a specific attack or represent higher probability to succeed this attack than other methods or not. The attack vectors are similar to the ones mentioned in Jong's study, no addition or elimination was necessary since the author covers the most common authentication threats and attacks as shown in (Table 4).

Table 3 Likely to succeed the attack [15].

Likely to succeed the attack	Values of Scale
Very likely	1
likely	2
possible	3
Not likely	4
negligible	5

Based on Jong's study, online banking authentication systems are vulnerable to several different threats and attacks:

Table 4 shows the description of the Attack vectors.

Attack Vector	Description
Shoulder Surfing	Is an observation technique that can be done by looking at someone while they enter their password or PIN [16]
Keylogger	Is a hardware or a software that runs in the background and records all the keystrokes done by the user [10].
Screen Capturing	Is used by attackers to get both the user's keystrokes and screenshots of the victim's computer screen [24].
Brute force attack	Is a method to crack passwords by generating all the possible passwords and tries them [10].
Guess Attack	Is when attacker knows a little about the target's social life and try to guess the victim's password [10].
Dictionary Attack	A technique that uses words from the dictionary to find the password combination [10]
Hardware Observation	This attack involves trying to look inside the hardware and its risk determined on the cost and the profit [15].
Social Engineering	Is the art of convincing people to reveal confidential information like passwords for malicious use [26].
Phishing	It works by imitating a trusted well-known website and tricking users into entering their credentials [4].
MITM Attack	When an attacker insert himself between the victim and a legitimate connection [21].
MITB Attack	It uses a malware to create a realistic browsing environment for the victim to gather personal information [9].
Network Sniffing	It is used by attackers to sniff confidential information such as usernames and passwords [13].
Short access	It describes the possibilities of an attacker to get short access to the computer like an unlocked computer [15].

4. Discussion and Analysis

As mentioned earlier, discussion and analysis section are based on the data captured through observation while navigating through the internet banking services of the targeted banks and from the user's aspect who has the privilege (credentials) to access the online services of these banks. In Table 5, we will discuss about the authentication methodology for each bank:

Note: The inserted score/value for each authentication method is based on scale 1-5, where higher is better as explained in Table 2 (Explanation of Characteristics [15]).

Table 5 Discussion about the authentication methodology for each bank.

Bank	Login	Characteristics	Attack vectors
Bank A	1. Enter his/her username or ATM number only to proceed 2. Bank A website displays the secret image and comment below it. User needs to verify that the image and the comment shown is the one he/she chose/wrote while registration with the bank online service before entering his password. 3. user must enter his/her correct password. 4. In case user forgot his/her login password, he/she will need to use Al-Barq 4-digits Telephone Banking PIN (TPIN). 5. if the user wants to make a transaction, for example, online payment or transfer money to a new account, he/she needs to answer the security question successfully to be able to do so.	Bank A use only 4 authentication methods out of 13 methods available in the matrix, which are 1. Username and password, 2. Virtual Keyboard, 3. Secret Image and 4. Security Questions. Unfortunately, the methods that we added to the matrix (Secret Image and Security Questions) * are not mentioned in Jong's study [15] as authentication methods. This means we need to give reasonable values for these new methods by comparing them with other similar methods mentioned in Jong's study.	Refer to Appendix A - Comparison Matrices
Bank B	1. Enter his/her username to proceed. 2. After, user will be asked to either answer the security question correctly (one out of 5 questions randomly displayed) or selecting the correct security image. Selection depends on the method the user chose during registration with the bank online service. 3. Any transaction, like transferring money from your bank's account to another account or making online payments, requires the user to enter the One Time Password that sent to his/her cell phone via a Short Message Service (SMS). That One Time Password is a temporary password and valid for a short time (timer).	Bank B use 5 authentication methods out of 13 methods available in the matrix, which are 1. Username and password. 2. Virtual Keyboard (optional), 3. Secret Image, 4. OTP automatic (SMS) and 5. Security Questions.	
Bank C	1. Enter his/her username to proceed. 2. After, user will be asked to answer the correct security image chosen during registration with the bank online service along with mandatory fields for entering both the password and Token password (RSA). 3. Similar to UserID, user can use the physical keyboard or the virtual keyboard (optional) to enter his/her password. To enter the token password (RSA), user should have the hardware token (RSA Secure ID) that generates that password. 4. Bank C uses RSA SecureID 700, a small durable device that can be connected easily to any key ring and is very convenient for the user. Every 60 seconds, a new code generated by the RSA SecureID AES algorithm is displayed ("Technische Daten," n.d.	Bank C use 5 authentication methods out of 13 methods available in the matrix, which are 1. Username and password, 2. Virtual Keyboard (optional), 3. Secret Image, 4. OTP Synchronous (RSA hardware token) and 5. Security Questions.	
Bank D	1. Enter his/her username to proceed. 2. After, user will be asked to answer the security question correctly and enter the partial password correctly to be able to log in. The security question never changes or selected randomly among different questions, the same question is asked by the bank each time	Bank D use 3 authentication methods out of 13 methods available in the matrix, which are 1. Username and password, 2. Partial Password and Security Questions.	Refer to Appendix A - Comparison Matrices
Bank E	1. User enters the User ID that he/she created during the registration and press login button (If the user has the recent version of JAVA application installed on his/her PC or laptop, then he/she will be able to successfully log in after entering the correct password) "In case the user PC/laptop is not updated with latest version of JAVA, then he/she will receive a SMS in his/her mobile phone from the bank". This SMS notifies the user to install JAVA and includes a temporary access password valid for 5 minutes. 2. User can enter this password and log in to Bank E internet banking service. Bank E depends mainly on One Time Password (OTP) for authentication and protection of the user.	Bank E uses 4 authentication methods out of 13 methods available in the matrix, which are 1. Username and password, 2. PIN, 3. OTP Automatic (SMS) and 4. Security Questions.	
Bank F	1. Enter his/her username to proceed Bank F depends on Short Messages Service (SMS) to notify the user with any action or update happened in the account.	Bank F uses 2 authentication methods out of 13 methods available in the matrix, which are 1. Username/password and 2. Virtual keyboard (optional).	

5. Findings

The evaluation shows that virtual keyboard is the default keyboard to enter the password in Bank A Internet banking, while other banks make the virtual keyboard optional. Bank B depends on One Time Password (OTP automatic) that sends to the user's cell phone via a Short Message Service (SMS) when making transactions, while other banks depend on security questions for that purpose. Bank C is the only bank among our sample that depends on Token password (RSA) to authenticate the users by distributing hardware token (RSA Secure ID) to them. In addition, partial password is a good authentication method used by Bank D. User will be asked to enter random characters of the password each time he/she tries to log in. On the other hand, Bank E depends mainly on One Time Password (OTP automatic) for authentication and protection of the user. The bank sends SMS with a temporary password to the user's mobile phone to allow him/her to make most transactions. Although, Bank F doesn't use unique authentication method like other banks and depends mainly on username and password, the bank keeps notify the user with any update occurs in the account via SMS. Through navigation and observation, the shared authentication method used by most of the targeted bank is username/password and virtual keyboard (optional).

6. Implications for practice and future research

As per the results mentioned earlier, banks could use different kinds of security methods to strengthen their online authentication systems. Depending on one authentication method only, for example username/password combination, considers weak and not sufficient like before. Implementing a defense-in-depth strategy by adding different protection layers/challenges for the user makes the job of an intruder or attacker more difficult.

Our sample consists of only six banks because of the time restriction. Soon, we are thinking about adding international banks and including online services of UAE government agencies. As we all know, Dubai has started working on eGovernment Strategy to make all government services available online. We are going to use both matrices (characteristics and attack vectors) to evaluate the authentication methods of these agencies. Our methodology depends on the observation only; in future we can conduct survey (questionnaire) to know customers' opinions and to evaluate the authentication methods based on that as Jong [15] did also using the third Matrix (User Acceptance).

7. Limitation

In this research, we didn't cover all the authentication methods that involve using cell phones. Today, many banks offer good telephone services and allow users to make transactions on their cell phones for example, Al-Barq cell phone services of Bank A.

8. Conclusion

Today, authentication of the user is required in all online services. Day by day, governmental agencies and companies emerge their services to the internet for the public. And since the findings from matrices are not restricted to evaluate online banking, these governmental agencies can use the matrices to find the best authentication methods that suit their needs. Banks were our first choice to be evaluated because the main concern for banks is to protect the confidentiality and integrity of the information. If the authentication methods used are advanced, then they can reduce the threat of unauthorized access. If the authentication method is very good and less vulnerable to attack, then they can ensure that only authorized people can access the secret information and they are the only ones who can make modification. The guidance of Federal Financial Institutions Examination Council [7] emphasized on the point that Financial Institutions which adopt online banking systems should have effective and reliable methods to authenticate their customers before granting them access to particular services. An effective authentication System is necessary to avoid financial loss and reputation damage through fraud, identity theft, disclosure of customer information, corruption of data, or unenforceable agreements.

9. Comparison Matrices

Below are two examples of the comparison matrices for Bank A and Bank D.

Table 6 Bank A.

	Attack vectors													
Authentication Methods	Shoulder Surfing	Keylogger	Screen Capturing	Brute force attack	Guess Attack	Dictionary Attack	Hardware Observation Attack	Social Eng.	Phishing	MITM attack	MITB attack	Network Sniffing	Short access	Total Score
Username & password	3	1	4	2	2	1	5	3	1	1	2	1	3	**29**
Virtual Keyboard (optional)	1	5	1	2	2	1	5	3	3	1	3	3	3	**33**
Secret Image*	3	5	1	2	2	5	5	3	1	1	2	1	3	**34**
OTP automatic	4	4	4	5	5	5	5	5	4	4	4	4	3	**56**
Security Questions*	3	1	4	1	1	1	5	1	1	1	2	1	3	**25**

Table 7 Bank D.

	Attack vectors													
Authentication Methods	Shoulder Surfing	Keylogger	Screen Capturing	Brute force attack	Guess Attack	Dictionary Attack	Hardware Observation Attack	Social Eng.	Phishing	MITM attack	MITB attack	Network Sniffing	Short access	Total Score
Username & password	3	1	4	2	2	1	5	3	1	1	2	1	3	**29**
PIN*	1	1	4	1	1	1	5	1	1	1	2	1	3	**23**
OTP automatic	4	4	4	5	5	5	5	5	4	4	4	4	3	**56**
Security Questions*	3	1	4	1	1	1	5	1	1	1	2	1	3	**25**

References

[1] Armin Anvari, Lei Pan & Xi Zheng (2017): Generating security questions for better protection of user privacy, *International Journal of Computers and Applications*, DOI: 10.1080/1206212X.2017.1395132

[2] Authentication. (2007). SearchSecurity Retrieved 21-05-2012, from http://searchsecurity.techtarget.com/definition/authentication

[3] Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics, 35*(5), 1491-1511. doi:10.1016/j.tele.2018.03.018

[4] Bhadane, A., & Mane, S. B. (2018). State of research on phishing and recent trends of attacks. *I-Manager's Journal on Computer Science, 5*(4), 14-35. doi:http://dx.doi.org/10.26634/jcom.5.4.14608

[5] Bhatt, B. (2011). Online Banking. Retrieved from http://www.blognbuzz.com/online-banking.html

[6] CEPIS.(2008). Authentication approaches for online-banking. Marko Hölbl, CEPIS LSI Secretary, 1-5. LSI SIN (07)02 25 July 2008 Page 5 of 5

[7] Council, F. F. I. E. (2001). Authentication in an Internet Banking Environment. Arlington: Federal Financial Institutions Examination Council Retrieved from http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[8] Defense in depth. (2009). OWASP. Retrieved 31-05-2012, from https://www.owasp.org/index.php/Defense_in_depth

[9] Grau, D., & Kennedy, C. (2014). TIM lecture series - the business of cybersecurity. Technology Innovation Management Review, 4(4), 53-57. Retrieved from https://search.proquest.com/docview/1614470784?accountid=15192

[10] Harmandeep, S. B., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, 2018, 11. doi:http://dx.doi.org/10.1155/2018/1798659

[11] Hilger, S. (2014). U.S. Patent No. US 8,881.251 B1. Washington, DC: U.S. Patent and Trademark Office.

[12] Hiltgen, A., Kramp, T., & Weigold, T. (2005). Secure Internet Banking Authentication. IEEE SECURITY & PRIVACY, 1540-7993/05/$20.00 © 2005 IEEE, 24-32. Retrieved from http://www.zurich.ibm.com/pdf/csc/SecureInternetBankingAuthentication.pdf

[13] Diyeb, I. A., Saif, A., & Al-Shaibany, N. A. (2018). Ethical Network Surveillance using Packet Sniffing Tools: A Comparative Study. *International Journal of Computer Network and Information Security, 10*(7), 12-22. doi:10.5815/ijcnis.2018.07.02

[14] Jani, R. (2013). Multiple packet system: A security approach for wireless networks. *International Journal of Advanced Research in Computer Science, 4*(3) Retrieved from https://search.proquest.com/docview/1443745365?accountid=15192

[15] Jong, C. d. (2008). Online authentication methods. Universiteit van Amsterdam, Spui 211012WX Amsterdam. Retrieved from http://staff.science.uva.nl/~delaat/rp/2007-2008/p30/report.pdf

[16] L. Jiang, X. Li, L. L. Cheng and D. Guo, "Identity authentication scheme of cloud storage for user anonymity via USB token," 2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID), Shanghai, 2013, pp. 1-6. doi: 10.1109/ICASID.2013.6825270

[17] Mannan, M., & Oorschot, P. C. v. (2008). Security and Usability: The Gap in Real-World Online Banking. Carleton University, Ottawa, Ontario, Canada.

[18] Nayak, C., Parhi, M., & Ghosal, S. (2014). Robust Virtual Keyboard for Online Banking. *International Journal of Computer Applications, 107*(21), 36-38. doi:10.5120/19142-0530

[19] Onyesolu, M. O., & Okpala, A. C. (2017). Improving security using a three-tier authentication for automated teller machine (ATM). *International Journal of Computer Network and Information Security, 9*(10), 50. doi:http://dx.doi.org/10.5815/ijcnis.2017.10.06

[20] Peng, Y., Chen, W., Chang, J. M., & Guan, Y. (2010). Secure Online Banking on Untrusted Computers. Iowa State University, Ames, Iowa 50011. pin or PIN. (2005). SearchCIO-Midmarket. Retrieved 11-05-2012, from http://searchcio-midmarket.techtarget.com/definition/pin-or-PIN

[21] Rahim, R. (2017). Man-In-The-Middle-Attack Prevention Using Interlock Protocol Method. doi:10.31227/osf.io/8txn7

[22] Rajarajan, S., Maheswari, M., Hemapriya, R., & Sriharilakshmi, S. (2014). Shoulder Surfing Resistant Virtual Keyboard for Internet Banking. *World Applied Sciences Journal*, 1297-1304. doi:10.5829/idosi.wasj.2014.31.07.378

[23] Reuters. (2012). UAE Central Bank thwarts hacking attempt on its website, from http://www.emirates247.com/business/economy-finance/uae-central-bank-thwarts-hacking-attempt-on-its-website-2012-01-22-1.438907

[24] Reyes, A. R. L., Festijo, E. D., & Medina, R. P. (2018). Securing one time password (OTP) for multi-factor out-of-band authentication through a 128-bit blowfish algorithm. *International Journal of Communication Networks and Information Security, 10*(1), 242-247. Retrieved from https://search.proquest.com/docview/2047344505?accountid=15192

[25] Sama, V. (2014). U.S. Patent No. US 8,667.280 B2. Washington, DC: U.S. Patent and Trademark Office.

[26] Sharma, A., & Lenka, S. K. (2015). Analysis of QKD multifactor authentication in online banking systems. Polska Akademia Nauk.Bulletin of the Polish Academy of Sciences, 63(2), 545-548. doi:http://dx.doi.org/10.1515/bpasts-2015-0062

[27] Sharma, G., & Kalra, S. (2018). A lightweight multi-factor secure cuser authentication scheme for cloud-IoT applications. *Journal of Information Security and Applications*, 42, 95-106. doi:10.1016/j.jisa.2018.08.003

[28] Technische Daten. RSA Retrieved 13-05-2012, from http://germany.rsa.com/node.aspx?id=1311

[29] TRA Website. Retrieved 30-12-2018, from https://www.tra.gov.ae/aecert/en/resource-center/statistics.aspx