

Out-of-band Authentication Using Image-Based One Time Password in the Cloud Environment

Abderrahim Abdellaoui¹, Younes Idrissi Khamlichi², Habiba Chaoui¹

¹*Systems Engineering Laboratory, ADSI Team, ENSA Kénitra,
Ibn Tofail University, Morocco*

²*IR2M laboratory, UHI University,*

National School of Applied Sciences, khouribga, Morocco

¹*abderrahim90@gmail.com, ²ykhamlichi@gmail.com, ¹mejhed90@gmail.com*

Abstract

Authentication can be considered as the first wall of protection from unauthorized access of any system and most notably cloud environment. Its aim is to verify user's identity and thus the user's legitimacy of access to services. Nowadays, The most used method for policing user access is text password. However, Several studies have shown the inadequacy of this method due to the growth of network threats. In order to mitigate the deficiency of text password scheme, we propose an image-based one-time password scheme for the cloud environment called (imOTPC). The scheme uses an image as one-time password and mobile network, which makes the system more robust and, therefore, can withstand common types of attacks. The security of the proposed scheme is based on the one-way hash function, secret extraction and the IMEI.

Keywords: *Cloud computing, Security, One-time password, Multi-factor Authentication, Steganography*

1. Introduction

Nowadays cloud computing is used in various fields in the industry. Features like the pay per use, combined with elastic demand and the use of alternative local infrastructure to third-party data centers with internet access and managed by the cloud provider, are changing the way that information is processed in the business process model [17]. However, despite its advantages, the transition to this computing paradigm raises many security issues, which are the subject of several studies. In addition to problems derived from underlying technologies such as web and virtualization, the cloud introduces new issues that should be resolved in order to promote its deployment. Authentication in the cloud computing is one of these issues. It is a method for ensuring that only authorized users have access to cloud resources using their identity. We can distinguish three authentication types (simple, strong, single sign-on). we note that the most widespread authentication method is the simple authentication.

The users must provide a single "factor" for authentication. Whereas, Strong authentication uses at least two factors to access to resources. Finally, the Single Sign-on allows a user to access to multiple applications or services by means of only one authentication.

Overall, Authentication is based on three types:

- a. Something the User knows (password),
- b. Something the User has (smartphone)
- c. Something the User is (biometric identifier...).

The authentication issue in the cloud environment has grown in importance since simple text password is the most commonly used authentication mechanism in this environment. However, it was recently shown that text password scheme is insufficient to guarantee a secure access. In this regard, this paper proposes a novel way of authentication based on an out-of-band channel and an image-based one-time password. This paper is organized as follows: section 2 reviews the related works in the cloud environment access control, the proposed scheme is presented in section 3. The security and performance analysis is presented in section 4 and 5. We conclude with future works in section 6.

2. Related Works

Numerous works have addressed the authentication problem. Indeed, Chun-Ta Li and al [2] proposed an authentication scheme using a combination of techniques such as hash function and biometric verification. This scheme performs mutual authentication between client and server, password change and uses random numbers rather than timestamps. Whereas Guo and al [3] proposed a password-authenticated key agreement protocol using chaotic maps. This protocol avoids modular exponential computing and scalar multiplication used in traditional schemes using smart cards and withstands insider attack, replay attacks, and others. These works illustrate the use of smart card to enhance user authentication, however, they require extra devices such as smart card readers to ensure remote user authentication between client and server. Other examples of approaches include the multi-factor authentication, which is the case of Siddiqui and al [4]. The authors presented an authentication framework using multi-factor authentication in cloud computing using a smartphone as a unique identity required to access to the Telecare Medical Information System (TMIS) remotely. Hamdy and al [5] suggested 2FA scheme in which they produce multiple one-time passwords utilizing hash chains. The scheme resists to some attacks such as pre-play attack, non-repudiation attack, forgery attack and insider attack. In addition to those approaches, there exist the graphical-based schemes. In fact, it is an approach in which users use icons instead of text-based passwords for user authentication. By way of illustration, Gao and al [6] presented a scheme in which they combine graphical password and CAPTCHA. The users first select their pass-images and positions then, distinguish their pass-images from a set of images and finally enter certain parts of the CAPCHAs string. The scheme provides better protection and withstands spyware and dictionary attacks. However, it Cannot resist to strong shoulder-surfing attack. On the other hand, Wu and al [7] proposed an enhanced scheme compared to Wiedenbeck and al [8]. This scheme uses the convex-hull algorithm instead of clicking and choosing the password images. The scheme withstands strong shoulder attacks. Moghaddam and al [9] suggested a user authentication model in the cloud environment using two prime tools. They introduce firstly a mobile agent which validates the identity of a user from client-side. The second mobile agent is called cryptography agent, which enables to encrypt resources before storing them on the cloud servers. Then a software-as-a-service has been presented to confirm the process of authentication from the cloud-side. Liu and al [10] suggested a multi-factor authentication scheme applied to the cloud environment called MACA using the features of big data. In this scheme, the first factor is a password while the profile of user behavior plays the role of the second factor. MACA introduces techniques such as fuzzy hashing and fully homomorphic encryption (FHE) in order to protect user profiles and big data features in the authentication process. Yassin and al [11] presented a scheme where they use two-factor authentication: the first factor is based on cryptography hash password while the second used a new scheme that depends on possession of a credential file. This scheme is applied to the cloud environment.

So far we have focused on a variety of works related to user authentication in traditional and cloud environment and their limitations. In the following section, we will discuss our proposal in term of enhancing username password scheme.

3. Proposed Work

Image based one-time password in the cloud is an authentication scheme that has two major features:

- ✓ First, the scheme adopts two-factor authentication in the cloud environment and uses in addition to the password, an out of band factor, which strengthen the process of authentication, therefore, it enables us to provide additional security.
- ✓ Secondly, the scheme withstands common types of attacks, particularly: Man-In-The-Middle (MITM), Phishing attack, Dictionary and brute-force attacks and strong shoulder-surfing attack.

ImOTPC consists on the following phases: Registration phase, login phase, and image password change phase. The detailed steps of login and authentication phases are illustrated in Figure 3. Also, the notations used in this paper are defined in Table 1.

Table 1. Notation

NOTATION	DESCRIPTION
U	IDENTITY USER
Un_i	USERNAME
Ps_i	USER'S PASSWORD
S	CLOUD SERVER
$U \triangleright S[M]$	MESSAGE M IS SENT FROM U TO S
$U \triangleleft S[M]$	MESSAGE M IS SENT FROM S TO U
$\psi(.)$	HASH FUNCTION,
Γ	IMAGE
w	SECRET WATERMARK / RANDOM NUMBER
Γ_w	WATERMARKED IMAGE
C_r	CREDENTIALS
φ	FIRST FACTOR
ϕ	SECOND FACTOR
IMEI	INTERNATIONAL MOBILE EQUIPMENT IDENTITY
OTP	ONE-TIME PASSWORD
PN	PHONE NUMBER
α	POSITION WHERE THE TRUNCATION STARTS
\oplus	THE EXCLUSIVE-OR (XOR) OPERATION
\perp	DECONCATENATION OPERATION
$ $	CONCATENATION OPERATION

3.1. Preliminaries

We briefly introduce some important concepts used to construct imOTPC such as IMEI, one-time password, secret watermark and truncated output function.

3.1.1. One-way hash function: A function $\psi : \{0,1\}^* \rightarrow \{0,1\}^n$ is called secure one-way hash function if ψ operates on an input message x of arbitrary length and outputs a fixed-length value $\psi(x)$. Therefore, It is easy to compute $\psi(x)$, but practically impossible to invert it. Also, Given $x \in A$, find $x \neq x_1$ such that $\psi(x) = \psi(x_1)$ is computationally impossible.

The imOTPC is based on a special secure hash function called SHA-1 (secure hash algorithm).

3.1.2. International Mobile Equipment Identity: The International Mobile Equipment Identity (IMEI) is a unique number composed of 15-digits and assigned to mobile devices. It is often used conventionally to identify a mobile station as either a valid or not valid customer during call set-up. In our scheme, we use IMEI to construct the pass-phrase w which is an important parameter for user authentication in imOTPC. [12,14]

3.1.3. Image One-Time Password (imOTP): ImOTP is a strong authentication method. It is a concept that enables to use a password in only one session. The password is automatically generated by the cloud server using a pre-computed method. In the imOTPC scheme, a novel kind of one-time password is introduced using an image Γ and a pass-phrase w .

3.1.4. Secret Watermarking: A technic that enables to hide information in a digital document secretly. In our system, we use watermarking to incorporate w in the image Γ to construct a password based image Γ_w . The watermarking technic is a space of objects M and a finite set of watermarks N .

$\zeta : M \times N \rightarrow M$ is the encoding function and $\tau : M \rightarrow N$ is the decoding function such that $\tau(\zeta(m,n)) = n$ where $m \in M$ and $n \in N$. To incorporate an information w in Γ , we use the embedding function $\zeta(\Gamma, w) = \Gamma_w$. To extract the secret watermark, we use the extraction function $\tau(\zeta(\Gamma, w)) = w$ [13].

3.1.5. $Trunc_\alpha$ Function: The aim of $Trunc_\alpha$ in the imOTPC scheme is to truncate parts of IMEI number in order to generate a pass-phrase w that will be embedded in the image Γ in order to constitute the image based one-time password Γ_w . α denotes the position from where the truncation begins.

Example: If $\alpha = 3$ and $N = 351557010202731$ Then $Trunc_\alpha(N) = 1557$, $Trunc_\alpha(.)$ returns a 32-bit string.

3.1.6. The Data in the Cloud: We distinguish two types of data: simple data and sensitive data (Figure 1). The first level of authentication is the simple text password. In this level, the user is authorized only to access to his simple data. On the other hand, if the user would like to access to his sensitive data, he must provide the image OTP (imOTP) provided by the cloud service by means of his mobile device.

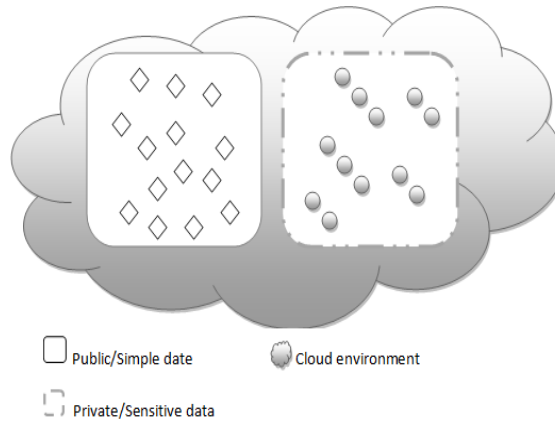


Figure 1. Data in the Cloud

3.2. Registration and Authentication Phases

3.2.1. Registration Step: The user registers his username Un_i , password Ps_i , IMEI and his phone number P_n in the cloud server S. The server saves (login, password, IMEI, phone number) as credentials $C_r : \{Un_i, Ps_i, IMEI, P_n\}$.

In this phase clients and service providers are supposed to be honest (Figure 2).

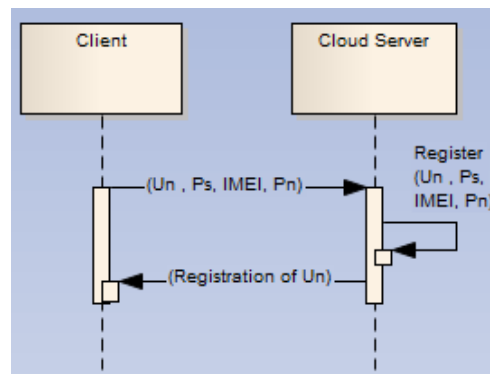


Figure 2. Registration Phase

3.2.2. Authentication step (Figure 3): Phase 1: In order to gain access to the cloud service, a user $Un_{i \in [1, \dots, n]}$ must be authenticated. So he must provide $\varphi_1 : \{Un_i, Ps_i\}$ for public data access. The user sends username and password to cloud provider $U \triangleright S[Un_i, Ps_i]$ and then, it checks the authenticity of the user ($\varphi = ? \varphi_1$). If the user is authorized ($\varphi = \varphi_1$), the cloud server will provide a restricted access to the client information (Only the public data).

Phase 2: When the client wants to access to his sensitive data, he must provide the image OTP Γ_w . This image will be provided by the cloud server (once $\varphi = \varphi_1$ is verified) using the phone number and the IMEI International Mobile Equipment Identity that were provided by the cloud server during the registration phase. In this regard, the client receives imOTP in his smartphone from the cloud provider using the mobile network (OOB).

Phase 3: Once the imOTP is received, the client connects his smartphone with the PC, transfer the imOTP (Γ_w) to cloud server $U \triangleright S[\Gamma_w]$. In this phase the user checks the authenticity of the image by extracting w from Γ_w .

Phase 4: The user sends the imOTP (Γ_w) to the cloud server $U \triangleright S[\Gamma_{\zeta^k(\alpha)}]$ then, the cloud server checks the authenticity of the imOTP. If $\Gamma_w = \Gamma_w^1$, once the user is authorized, the cloud server will provide a full user data access (public and sensitive data Figure.1)

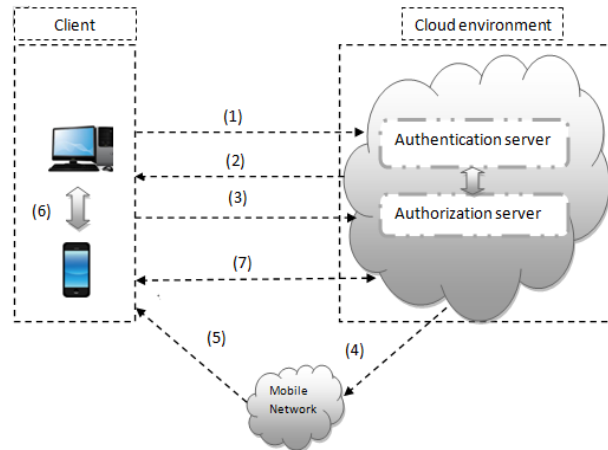


Figure 3. Authentication Phase

3.2.3. Password Update Step: A User Un_i can freely change his image-password Γ^1 to a new password Γ^2 following those steps:

Step1: The user inserts and sends $U \triangleright S[Un_i, Ps_i]$ to the cloud server. If $\varphi = \varphi_1$ then validates the first-factor verification.

Step2: The user Un_i requests to change his pass-image Γ^1 .

Step3: The provider requests Γ_w to validate the second factor. If $\Gamma_w = \Gamma_w^1$ then he selects the new image password Γ^2 .

3.2.4. Password Image Creation : We can describe the imOTP Generating operations in 3 steps:

Step 1: Extraction of a 4-byte string (Truncation) from the combination (IMEI,K, α)

Let $w = (Trunc_\alpha (SHA-1(IMEI) \oplus K \parallel \alpha)) //$

$|Trunc_\alpha (SHA-1(IMEI))|=4$ and $\alpha \in [1,9] \subset \square$ and $K = Trunc_\alpha (IMEI)$, W returns a 31-bit string.

Step 2: Retrieve Image from database and embed w in the image LSB plane. ImOTP is the OTP image using the following algorithm.

Pass-image Creation Algorithm

1 Input: $\Gamma, w;$

2 Output: $\Gamma_w;$

3 **Begin:**

4 **Step1-** Retrieve Image Γ_i and IMEI related to Un_i from the database;

5 **Step2-** Apply the $Trunc_{\alpha}$ Function over IMEI $Trunc_{\alpha}(IMEI)$ α denotes the position
6 from where the truncation begins.
7 **Step3-** Compute SHA-1(IMEI) and apply $Trunc_{\alpha}$ over SHA-1(IMEI):
8 $Trunc_{\alpha}(SHA-1(IMEI))?$
9 **Step4-** Apply the XOR operation over $Trunc_{\alpha}(SHA-1(IMEI))?$ and $Trunc_{\alpha}(IMEI)$ in
10 order to generate: $w = \alpha || Trunc_{\alpha}(SHA-1(IMEI)) \oplus Trunc_{\alpha}(IMEI)$
11 **Step5-** Embed w in the LSB plan of Γ creation of Γ_w
12 **End**

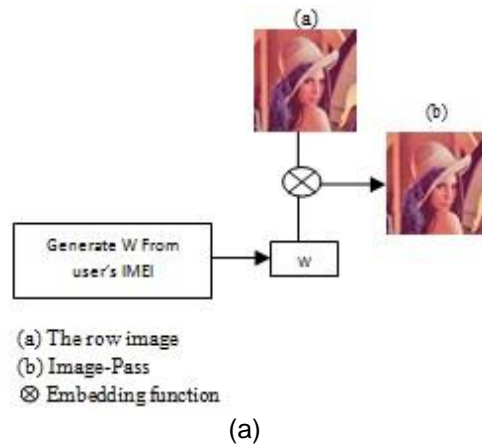


Figure 4. Embedding of w in the Image

Step 3: Send the image-pass Γ_w to the mobile device using the mobile network. And upon receiving the image-pass Γ_w , the cloud provider retrieves the concealed passphrase from the image-pass Γ_w , using the following algorithm.

Extracting Algorithm

1 **Input:** Γ_w
2 **Output:** $Trunc_{\alpha}(IMEI)$.
3 **Begin:**
4 **Step1-** Receive the pass-Image from Un_i $U \triangleright S[\Gamma_w]$
5 **Step2 -** Retrieve the concealed passphrase w from the LSB plan of Γ_w
6 **Step3 -** Separate α from W to produce $\beta // \beta = W \perp \alpha$
7 **Step4-** Retrieve IMEI related to Un_i from database and compute $\beta \oplus Trunc_{\alpha}(SHA-1(IMEI))$;
8 **Step5 -** if $\beta \oplus (Trunc_{\alpha}(SHA-1(IMEI))) = Trunc_{\alpha}(IMEI)$
9 **Step6 -** Un_i is authenticated
10 **End**

3.2.4. Mutual Authentication: Once the first authentication is done, the cloud provider sends the imOTPC to the user via his phone. So the user checks the authenticity of the image by extracting the secret α from the image:

1- Retrieve w from the LSB plane of the image.

2- Separate α from $W //$

$$W \perp \alpha = (\text{Trunc}_\alpha(\text{SHA-1}(\text{IMEI})) \oplus K' \parallel \alpha) \perp \alpha = \text{Trunc}_\alpha(\text{SHA-1}(\text{IMEI})) \oplus K'$$

3- Extract the IMEI from the Smartphone and apply SHA-1(IMEI).

4- α is the position from where the truncation begins $(W \perp \alpha) \oplus \text{Trunc}_\alpha(\text{SHA-1}(\text{IMEI})) = K'$

6- If $K=K'$ the image is authentic in other words the server is authentic.

7- When the user submits the imOTP to the server, it can confirm that the user's identity is valid and the corresponding import is correct.

4. Security Analysis

In this section, we conduct a security analysis of the proposed scheme and we demonstrate that our scheme can resist to various kinds of known attacks.

- ✓ **Withstand Man-In-The-Middle (MITM):** The scheme uses two-factor authentication $C_r : \{\varphi, \phi\}$ and an out of band channel for authentication. The imOTP is sent to the user's phone securely. In other words, the scheme withstands this attack.
- ✓ **Withstand Phishing attack:** Mutual authentication between the user and the server is performed in the scheme. Only the genuine server can send user's identification data, which will be verified by the user. Hence, the scheme is also strong against phishing attack.
- ✓ **Withstand dictionary and brute force attacks:** ImOTPC is not based only on alphanumeric strings, the user must own the authentication image Γ_ω in order to be authenticated. In other words, our proposed method withstands dictionary and brute force attack.
- ✓ **Withstand Password guessing attack:** An attacker may perform this attack by guessing the user's password. However, this attack is infeasible in our scheme. The adversary must provide an image pass ImOTP provided by the cloud server $U \triangleleft S[M]$. Therefore, he has to guess two values Un_i and Ps_i simultaneously to achieve the first factor, and ϕ which is infeasible without a user's smartphone and IMEI. Hence, the scheme withstands online password guessing attack.
- ✓ **Password registration table:** In our scheme, the cloud server has to maintain a secret image Γ , without registration of the password tables. An attack may try to construct Γ a fake Image password in order to be authenticated to the remote server. However, it is infeasible to construct Γ_ω without knowing Γ and the random information w from IMEI. In addition, during the login phase, the adversary can't intercept Γ_ω since an out of band channel is used.
- ✓ **Strong shoulder surfing attack:** An attacker can exploit the login process of a legitimate user in order to get some sensitive information such as username and password by means of the observation technic (surfing attacks) or some alternative technics using camera recording (strong surfing attacks) imOTPC uses two-factor authentication, the user must own the authentication image Γ_ω .

5. Performance Analysis

In this section, we evaluate the performance of our scheme compared to other related schemes.

Table 3 lists the performance and security properties comparisons between abdellaoui and all's scheme [1], the LI and al [2] scheme, Mishra and al[16], Lou and al [15] and the proposed scheme where:

- ✓ DA represents the dictionary attacks.
- ✓ BFA is the brute force attacks.
- ✓ MITM denotes the man in the middle attacks and KL the key logging attacks.
- ✓ SSA is the shoulder surfing attacks.
- ✓ CBA is a cloud-based authentication, PCh denotes password change.

CC is the time of execution from the client side and CS time of execution from the cloud parts. T_H , T_E , T_{ex} , T_{em} and T_{cr} are, respectively, the time of hash function, the exponential operation, embedding, extraction and encryption/decryption operation.

Table 2. Creation of the Image-Pass






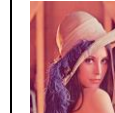


Users	User 1	User 2	User 3	User 4	User 5	User 6	User 7
IMEI	35155701 0202731	35812456 0202722	35342136 1924254	35756415 0204215	35155245 7419503	35325648 7865214	35242971 9254731
Original Image							
α	3	9	4	2	7	6	8
$w \perp \alpha$	ŽLŠN	2ù 2ù	È+Ħ*	ŸO`Jšq	iôjðPĚ	Â k ĩh	f×€Û
Image-pass (a)							
SHA-1(a)	50 5D 87 13 6A A2 2B 0D D0 11 16 91 46 A1 31 E6 42 62 41 5E	44 E1 73 7A 5D 61 7B 8E 2E 30 04 B2 7A F6 DC FF 79 58 D3 9D	00 01 03 CF E3 9A 55 94 AF 52 42 E5 8C 99 9E 3C 45 A6 32 B5	3C 90 E7 62 5746 AE 04 AE 0B A0 CC 44 1C 98 FD 87 C3 A4 ED	CE 51 03 91 76 D5 46 F2 79 9B 10 FB 0E A9 B1 78 36 DC 33 DB	05 F9 2C 3E 94 57 D5 BB 21 4B 88 B8 F5 30 DF 04 F3 40 22 82	36 73 9E EA D0 41 D2 8A DC 38 49 5E 6A 05 DE F8 4E 0C AD F0

Table 3. Comparing imOTPC with Previous Works

	ImOTPC	[1]	[2]	[16]	[15]
DA	✓	✓	x	x	x
BFA	✓	✓	x	x	x
MITM	✓	✓	✓	✓	✓
KL	✓	✓	x	x	-
SSA	✓	✓	✓	✓	✓
CBA	✓	✓	x	x	x
PCh	✓	✓	✓	✓	✓
CC	-	-	$3T_H$	$3T_H + 2T_e$	$9T_H + 3T_C$
CS	$2T_H + T_{ex} + T_{em}$	$2T_H + 2T_{cr}$	$4T_H$	$6T_H + 4T_e$	$6T_H + 3T_C$
Total	$2T_H + T_{ex} + T_{em}$	$2T_H + 2T_{cr}$	$7T_H$	$9T_H + 8T_e$	$15T_H + 6T_C$

As a result of the comparison study, we can obviously see that our proposed scheme has many advantages compared to the other schemes both in performance and security. It resists to common types of attacks with less computation cost.

6. Conclusion and Future Work

This paper presented a significant authentication scheme for the cloud environment. The scheme introduced many security features such as mutual authentication between users and the cloud server and the password change option which several schemes fail to satisfy. The proposed scheme presents a new way of authentication using a secret image with a password. Out-of-band authentication provides human interaction which strengthens the process of authentication. There are still several areas not addressed in this paper, particularly, confidentiality and integrity. These areas will be subject of further works. With this way, we will improve the overall security of our scheme.

References

- [1] A. Abdellaoui , Y. Khamlichi., H. Chaoui . , “An Efficient Framework for Enhancing User Authentication in Cloud Storage Using Digital Watermark”, (2015) *International Review on Computers and Software (IRECOS)*, 10, 2015, pp. 130-136. Doi: 10.15866/irecos.v10i2.5236
- [2] L., Chun-Ta et HWANG, M-Shiang. « An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*”, 2010, vol. 33, no 1, p. 1-5.
- [3] G., Cheng et CHANG, C-Chen. Chaotic maps-based password-authenticated key agreement using smart cards. *Communications in Nonlinear Science and Numerical Simulation*, 2013, vol. 18, no 6, p. 1433-1440. Doi: 10.1016/j.cnsns.2012.09.032
- [4] SiddiquiI, Zeeshan, Abdulla, A. Hanan, KHAN, M. Khurram, *et al.* “ Smart environment as a service: Three factor cloud based user authentication for telecare medical information system”. *Journal of medical systems*, 2014, vol. 38, no 1, p. 1-14. Doi: 10.1007/s10916-013-9997-5
- [5] Eldefrawy, M.Hamdy, Khan, M. Khurram, Alghathbar, Khaled, *et al.* “ Mobile one time passwords: two factor authentication using mobile phones”, *Security and Communication Networks*, 2012, vol. 5, no 5, p. 508-516. Doi: 10.1109/ITNG.2011.64
- [6] G., Haichang, L., Xiyang, W., Sidong, *et al.* “A new graphical password scheme against spyware by using CAPTCHA”. In : SOUPS. 2009.
- [7] W, T-Sun, L, M-Lun, LIN, H-Yu, *et al.* Shoulder-surfing-proof graphical password authentication scheme. *International journal of information security*, 2014, vol. 13, no 3, p. 245-254. Doi: 10.1007/s10207-013-0216-7
- [8] W, Susan, J. Waters, ,J-Camille Birget, , *et al.* “PassPoints: Design and longitudinal evaluation of a graphical password system”. *International Journal of Human-Computer Studies*, 2005, vol. 63, no 1, p. 102-127. Doi:10.1016/j.ijhcs.2005.04.010
- [9] M., Faraz Fatemi, M., S. Gerayeli, R., Sohrab, *et al.* “A scalable and efficient user authentication scheme for cloud computing environments. In : Region 10 Symposium”, 2014 IEEE. IEEE, 2014. p. 508-513. Doi:10.1109/TENCONSpring.2014.6863086
- [10] L, Wenyi, A. Uluagac, Selcuk, et B, Raheem. “MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data. In :Computer Communications Workshops (INFOCOM WKSHPS)”, 2014 IEEE Conference on. IEEE, 2014. p. 518-523. Doi: 10.1109/INFCOMW.2014.6849285
- [11] Y, Ali A., J, Hai, I, Ayad, *et al.* "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing". In Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International. IEEE, 2012. p. 1210-1217. Doi:10.1109/IPDPSW.2012.148
- [12] S. Robert. "Server request including code for customizing service to requesting cellular mobile station." U.S. Patent No. 6,275,692. 14 Aug. 2001.
- [13] Z., Qian et B., Nigel. ‘ QUANTIZATION INDEX MODULATION USING E~ 8 LATTICE. In : Proceedings of the Annual Allerton Conference on Communication Control and Computing”. The University; 1998, 2003. p. 488-489.
- [14] C. Anne SY. “Location privacy: The challenges of mobile service devices. *Computer Law & Security Review*”, 2014, vol. 30, no 1, p. 41-54. Doi: DOI: 10.1016/j.clsr.2013.11.005
- [15] D. C.Lou, , T. F Lee., & T. H Lin., (2015). Efficient biometric authenticated key agreements based on extended chaotic maps for telecare medicine information systems. *Journal of medical systems*, 39(5), 1-10.

- [16] R .Mishra,, A. K & Barnwal., **(2015)**. “A Privacy Preserving Secure and Efficient Authentication Scheme for Telecare Medical Information Systems. *Journal of medical systems*”, vol. 39, no.(5), pp.1-10.
- [17] D.A Fernandes, L. F Soares, , J. V., GomesFreire, M. M., & Inácio, P. R. **(2014)**, Security issues in cloud environments: a survey. *International Journal of Information Security*, vol. 13, no. 2, pp 113-170.

