ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Novel Approach to Multifactor Authentication for Mobile Devices using Jumbled Image Set

Sunny Dagar

Assistant Professor, Dept. of CST, Manav Rachna University, Haryana, India

ABSTRACT: In this ever changing world of global data communications, high-speed internet connections, and rapid software development, security has emerged as a challenging issue. Security has become the basic need of any efficient computing system and more focus is required in this field. Attackers may obtain unauthorized access to the system for their personal or social gain, which is commonly known as "crackers". They can use the gained knowledge to impersonate the actual user and steal information, or even deny the access to computer systems or other resources. It is a fact that no computer system is completely secure. There are some loopholes in every system. Therefore, all we can do is to make the system more difficult for the intruder to compromise. Therefore, if anyone wants to use the system, he/she/it has to prove his/her/its identity first. The process of determining and proving the identity of the user is known as authentication. User authentication is one of the most crucial areas in information security which can be implemented in various ways. The most common method for accessing the computer system is through alphanumeric passwords. But in today's challenging world, only one factor of authentication does not provide much security. Therefore, a new and advanced scheme is required in which user has to qualify two or more levels of authentication in order to gain the access of computer system. This is called multifactor authentication. In this paper, a new hybrid scheme which is the combination of authentication based on hand's movement) and graphical password based authentication is proposed. The user first has to pass the first level of authentication then only the user will authenticate itself using a graphical password. The effectiveness of the scheme is measured by its level of usability and security. This scheme is proposed for smart mobile devices which are more convenient to carry than the traditional desktop computer systems.

KEYWORDS: Multifactor Authentication; Mobile device Authentication; Jumbled image

I. INTRODUCTION

Authentication is the process of proving one's identity and assuring that only allowed or authorized user is able access the system. Authentication is basically performed by using one or more of the following ways:

- What you know e.g. passwords
- What you have e.g. smart cards
- What you are e.g. biometrics

Computer applications today uses user authentication as its fundamental security component. User authentication is one of the most essential areas in information security which can be implemented in various ways. User authentication involves issues of both usability and security. Too often, one or the other is ignored even though both are important and necessary. It provides the basis for access control and user accountability [1]. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by intruder or attacker [2]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [3]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. Human factors are quite often considered as the weakest link in a computer system related with security. Patrick, et al. [4] pointed out

DOI: 10.15680/IJIRCCE.2017. 0503051

three major areas where human-computer interaction is important: authentication, developing secure systems and security operations. Here we focus our attention to the authentication problem.

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication
  - ➢ Text based authentication
  - ➢ Picture based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: **recognition-based** and **recall-based graphical techniques**. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

The most common computer authentication method for a user is to submit a username and a text password. The vulnerabilities of the alphanumeric method of authentication have been well known. One of the major problems is the difficulty in remembering passwords. Studies have also shown that many users tend to pick passwords that are easy to remember or a very short password [5]. Unfortunately, such passwords can easily be guessed or broken. According to a news article on Computerworld, a network password cracker was run by a security team at a large company and within 30 seconds, they were able to identify about 80% of the passwords [6]. In the contrary, passwords that are hard to break or guess are often very hard to remember unless one writes down in a piece of paper or somewhere. Studies showed that since user can only remember a limited amount of different passwords, they tend to use the same passwords for different accounts or write them down [7]. To counter the inherent problems with traditional username/password authentication, various alternative authentication methods, such as biometrics, have been used.

In this paper, however, the main focus is on multifactor user authentication which is nothing but utilizing two or more factors of authentication as one factor of authentication does not provide much security. It is true that only one factor of authentication may offer usability benefits but not the security benefits. A new hybrid scheme which is the combination of authentication based on hand's movement and graphical password based authentication is proposed. The user first has to pass the first authentication method then only the user will authenticate itself using graphical password. The effectiveness of the scheme is measured by its level of usability and security. Multi-factor authentication provides both stable and secure system. It is motivated partially by the fact that humans are capable of remembering pictures or images better than texts; even psychological studies supports such assumption [8]. Pictures or images are generally much easier to be remembered or recognized than that of textual objects. In addition to memorability, if the number of possible pictures or images is significantly large, then the possible password space of a graphical password scheme may exceed that of text based schemes.

II. RELATED WORK

Yoon et al. proposed a mutual authentication scheme based on generalized EIGamal signature scheme using smart cards. The Yoon-Ryu-Yoo's scheme can be divided into three phase: registration, login and authentication. In addition, user can change their passwords freely and securely without the help of remote system. The drawback of their authentication is that the intruder is able to reveal previous session keys by means of the disclosed secret parameters. Then in 2005, Bin Wang and Zheng-Quan Li [10] proposed a new scheme which offers forward secrecy. Text-based username and password is vulnerable to guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering.

Li Yang, Jian-Feng Ma, Qi Jiang [11] proposed a mutual authentication scheme based on smart cards and password under trusted computing, in which hash functions are used to authenticate identities, and remote attestation is used to verify the platform. Analysis showed this scheme can resist most of the possible attacks. Is secure and efficient and fulfils the designed security goals, such as secure session key agreement, user identity anonymity, password free changing, platform certification updating.

Smart card scheme still suffers from the smart card loss problem and fails to provide user traceability and also vulnerable to desynchronization attack. Qi Jiang, Jianfeng Ma, Guangsong Li, Li Yang [12] proposed a robust two-factor authentication and key agreement scheme with user privacy preservation achieving all the goals of security.

AyuTiwari, SudipSanyal, Ajith Abraham, Svein Johan Knapskog, SugataSanyal [13] proposed the secure and stable protocol using multifactor authentication. They used a unique approach based on TIC (Transaction Identification Code) and SMS (Short Message Service) to provide extra security level with traditional Login/Password based system. Al-Qayedi et al. have proposed the use of SMS but have not used TIC's in their protocol TIC's are user specific unique transaction identification codes which are issued by banks or financial institutions to the user. This code is similar to One Time Password (OTP) and code is used only once. They suggested using TIC's as secret codes on cell phones. The user if authenticated only when he enters the TIC's code which he receives. Therefore, this scheme is more secure and stable than other schemes.

AlirezaPirayeshSabzevar,AngelosStavrou [14] proposed a series of methods to authenticate the user with a graphical password. To that end, they employ the user's personal handheld device as the password decoder and the second factor of authentication. In their methods, a service provider challenges the user with an image password. To determine the appropriate click points and their orders, the user needs some hint information only to its handheld device. They have proposed the system that leverages both graphical passwords and multifactor authentication. They have employed graphical password combined with a handheld device to form a novel method of multifactor authentication.

J.K. Lee, S.R. Ryu and K.Y. Yoo proposed fingerprint-based remote user authentication scheme [15]. They proposed that the fingerprint verification method is based on minutia extraction and matching. Whenever a fingerprint is input, a different map of minutia is made and matched. This scheme requires a system to authenticate each user by each user's knowledge, possession and biometrics and this makes the authentication mechanism more reliable.

The biometrics uses physiological or behavioural characteristics like fingerprint or facial scans and iris or voice recognition to identify users. The biometrics includes the following: - voice recognition, fingerprints, face recognition, iris scan, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics.

GAIT authentication has gained a lot of interest in recent years. It is basically developed for mobile phones for quick, easier and secure authentication. Gait recognition systems can be categorized into three classes: machine vision based (MV-based), Floorsensor based (FS-based) and Wearable sensor based (WSbased) [16]. Gait recognition is based on person's movements like walking, moving hands.

In May, 2014 Shrirang Mare, Andr´es Molina-Markham, Cory Cornelius, Ronald Peterson, and David Kotz described and evaluated Zero-Effort Bilateral Recurring Authentication called ZEBRA [17]. ZEBRA is a token-based authentication scheme that authenticates users based on their interactions with the device. Unlike keystroke-based biometrics that authenticates users based how they type, ZEBRA authenticates users based on what interactions (e.g., typing, scrolling) they perform on the device and when. In ZEBRA users wear a wrist-bracelet (token) that has built-in accelerometer and gyroscope sensors and a short range wireless radio to communicate with the device. ZEBRA authenticates users by monitoring their hand movements, using the sensors in the wrist-bracelet, when they are interacting with the device, and comparing the hand movements with the inputs received by the device during the interaction. In ZEBRA the bracelet contains the identification information for its associated user, which it shares with the device to authenticate the user. The user can associate the bracelet with her. when she wears the bracelet, say by entering a PIN on the bracelet or through a secure channel to the bracelet. The bracelet clasp can detect when it is being taken off and it de-associates with the user when it is taken off

III. PROPOSED ALGORITHM

The proposed scheme is as follows:

- The scheme includes combination of authentication based on hand's movement and graphical password based authentication. The user first has to pass the authentication that is integrated through an android application which takes the hand's movement left and right as the password.
- Then only the user will authenticate itself using graphical password. For this user implicitly provided with the set of images and click on images in any preferred order. Psychologically, graphical passwords are much easier to remember than the text-based passwords.

A. User Registration:

Step1: The home screen of the designed tool

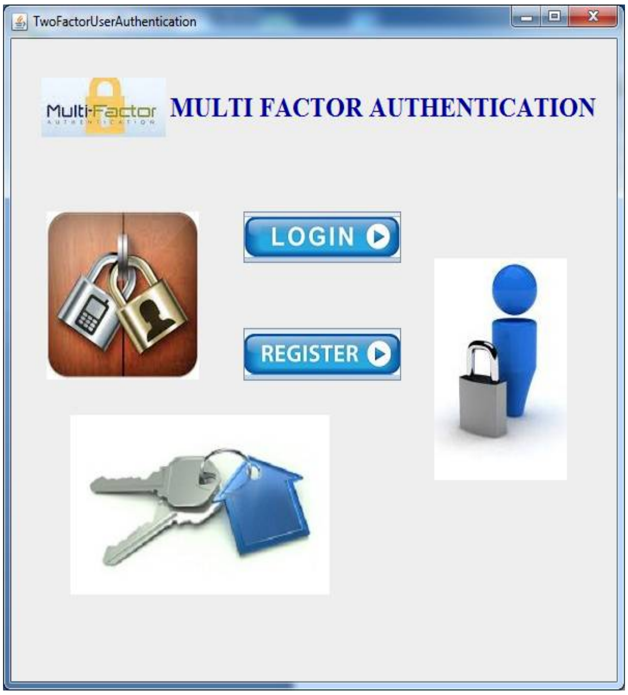
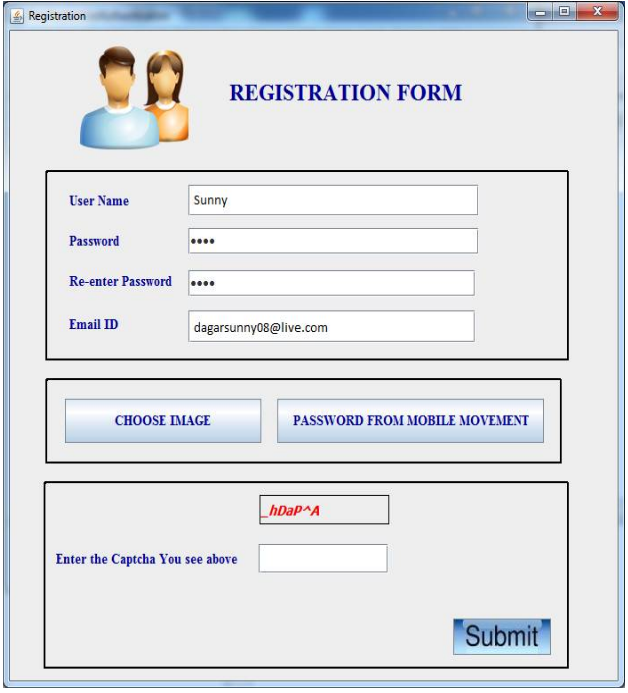


Fig 1: Home screen of designed tool

Step 2: The user registration screen appears as the user click on Register button and enter their details

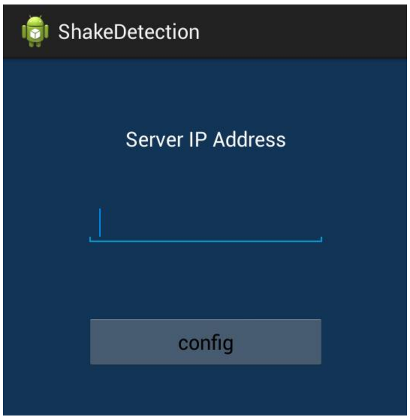


User Name Sunny
Password ••••
Re-enter Password ••••
Email ID dagarsunny08@live.com

_hDaP^A
Enter the Captcha You see above

Fig 2: New user registration page

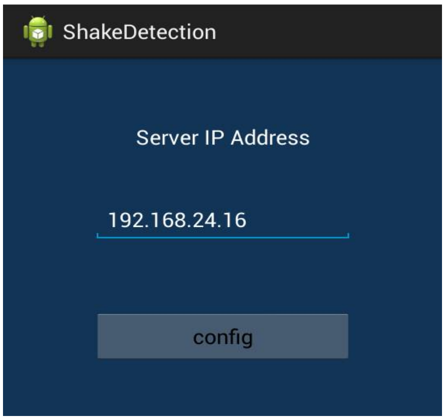
Step 3: Firstly, the user has to provide the password from the mobile movement. For doing so, the user has to connect the android phone with the system by providing the IP Address of the system to the Shake Detection Application (which is an android application integrated with the designed and implemented tool). The phone is then moved left and right as the user wants and that movement of (LLRR, LRLR, LLLR) is then saved to file and passes as the mobile movement password


ShakeDetection

Server IP Address

config

Fig 3: Shake detection screen

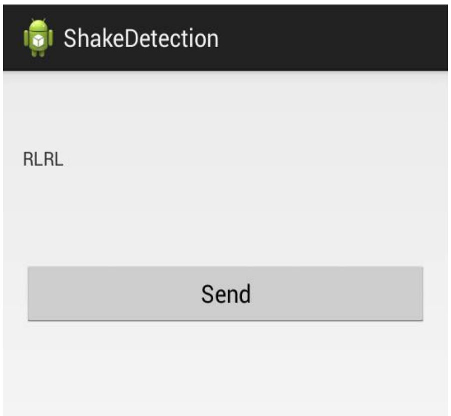

ShakeDetection

Server IP Address

192.168.24.16

config

Fig 4: Retrieved IP address after shake

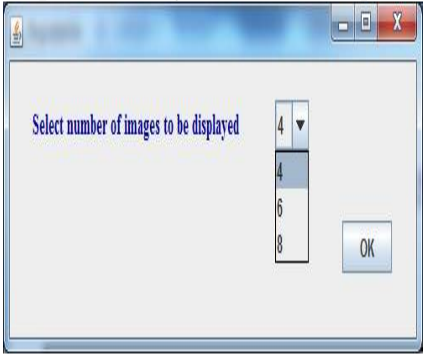

ShakeDetection

RLRL

Send

Fig 5: Phone movement recorded

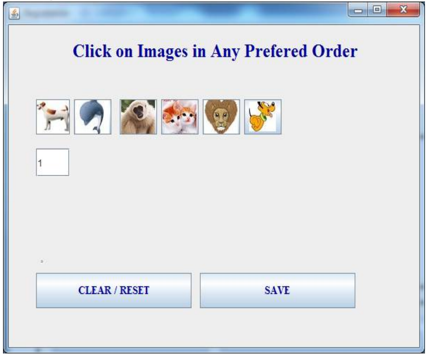
Step 4: Secondly, the user has to provide the graphical password. User can also reset the password.


Select number of images to be displayed

4 ▾ (4, 6, 8)

OK

Fig 6: selecting no. of images

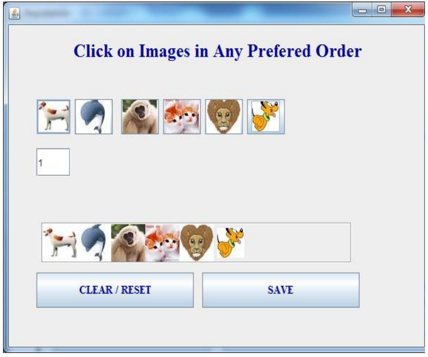

Click on Images in Any Prefered Order

1

CLEAR / RESET

SAVE

Fig 7: Predefined images for selection


Click on Images in Any Prefered Order

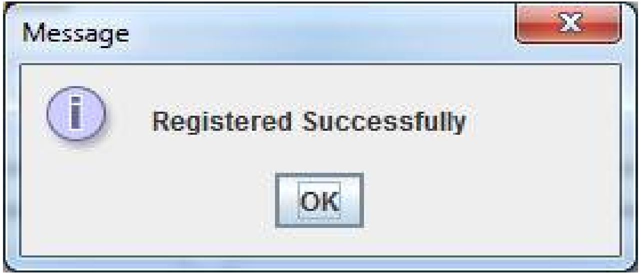
1

CLEAR / RESET

SAVE

Fig 8: Image and order selected

Step 5: Then, after passing the correct Captcha, the successful registration message is displayed.


Message

Registered Successfully

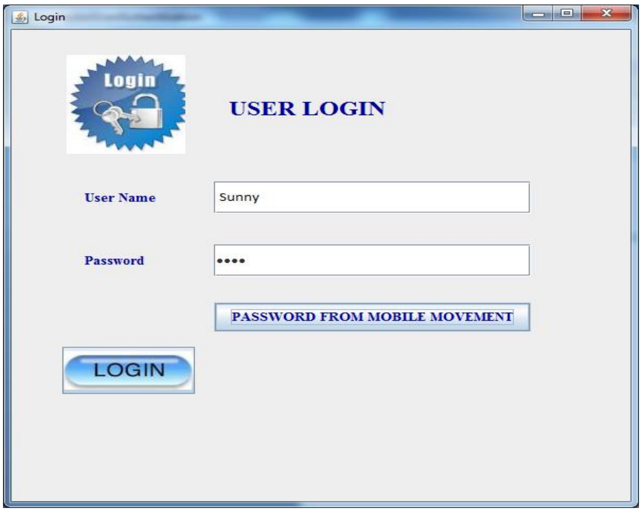
OK

Fig 9: Registration Success Message

B. User Login:

Step 1: The user can LOGIN to access his/her account. Initially, user has to validate his/her identity by the password from mobile movement. If this is validated and verified then only the second factor will be visible otherwise, login will be failed.

Step 2: If the user passes the first level, then he/she has to enter the graphical password that was selected at the time of registration.



User Name: Sunny

Password: ••••

Fig 10: User login page

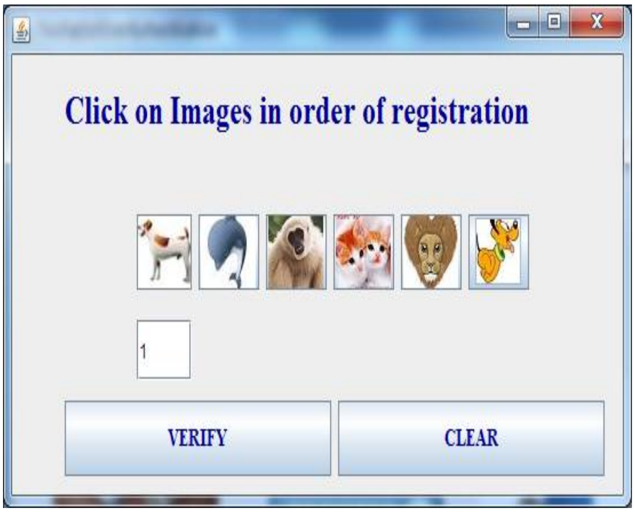
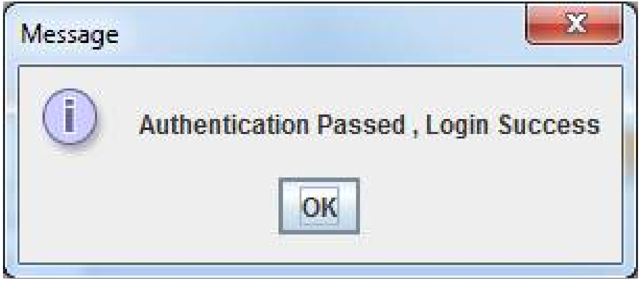


Fig 11: Image selection page

Step 3: After selecting the images in the correct order, user can access his/her account.



Authentication Passed , Login Success

Fig 12: Authentication success message

IV. Pseudo Code

```
Step 1: Open the home screen.
Step 2: If user is already registered then go to step 4, otherwise go to step 3.
Step 3: User registration page:
        3.1 User has to enter his/her details.
        3.2 User has to provide the password from the mobile movement.
        3.3 User selects the no. of images for graphical password
        3.4 User selects images from predefined set of images in an order
        3.5 User clicks on save button to store the credentials.
        3.6 Registered successfully
Step 4: User login page:
        4.1 User enter his/her details
        4.2 First stage password will be extracted from mobile movement
            If (Password is correct)
                Go to step 4.3
            Else
                Go to step 4.2
        4.3 For second stage password, User selects images in the same order as selected at the time of
        registration.
            If (selected images and order is correct)
                Go to step 4.4
```

DOI: 10.15680/IJIRCCE.2017. 0503051

```
            Else
                Go to Step 4.3
        4.4 Login successfully
Step 5: End.
```

V. SIMULATION RESULTS

The simulation involves the study and usage of this newly developed authentication mechanism. Shake detection plays a trivial role in this authentication mechanism. This eliminates the chances of eavesdropping. Only after clearing the first phase, user can access the second phase of authentication page. For this, user must choose the images in the same order as he chooses at the time of registration. Figure 1-9 describes the registration process and fig 10-12. Remembering pictures is easy and secure as compare to passwords.So this approach is simple, robust and secure.

VI. CONCLUSION AND FUTURE WORK

The secure system considers security, reliability, usability, and human factors. The process of determining the identity of the user is called authentication. It is required as a prerequisite to allow accessing the computer system and its resources. As per the evaluation, it is determined that single factor of authentication does not provide as much security. Therefore a new technique is developed with combines two factors security and usability is ensured. Moreover, it is true that graphically passwords are easier to member than the alphanumeric passwords. The first factor of authentication is very easy to deploy and access and second factor is very easy to remember. Therefore, the proposed scheme offers both usability and security benefits which is important for the authentication process.

REFERENCES

1. William Stallings and Lawrie Brown, "Computer Security: Principle and Practices." Pearson Education, 2008.
2. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and NasirMemon, "Passpoints: Design and Longitudinal Evaluation of a Graphical Password System." International Journal of Human-Computer Studies, 63:102127, July 2005.
3. Daniel V. Klein, "Foiling the Cracker: A Survey of and Improvements to, Password Security." In Proceedings of the 2nd USENIX UNIX Security Workshop, 1990.
4. A.S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.
5. A.Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
6. K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.
7. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
8. R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
9. M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest link - a human/computer interaction approach to usable and effective security," BT Technology Journal, 19(3): PP.122-131, July 2001.
10. Bin Wang and Zheng-Quan Li, "A Forward-Secure User Authentication Scheme With smart Cards", International Journal of Network Security, Vol.3, No.2, PP.116–119, Sept. 2006.
11. Li Yang, Jian-Feng Ma, Qi Jiang, "Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing". International Journal of Network Security - Volume 14 Issue 3 Pages 156-163, 2012.
12. Qi Jiang, Jianfeng Ma, Guangsong Li, Li Yang, "Robust Two-Factor Authentication and Key Agreement Preserving User Privacy", IJNS,2014,pp 321-332.
13. AyuTiwari, SudipSanyal, Ajith Abraham, Svein Johan Knapskog, SugataSanyal, "A Multi-Factor Security Protocol For Wireless Payment- Secure Web Authentication Using Mobile Devices". Proceedings of the IADIS International Conference on Applied Computing, Salamanca, Spain, 18-20 February 2007.
14. AlirezaPirayeshSabzevar, AngelosStavrou, "Universal Multi-Factor Authentication Using Graphical Passwords". SITIS, 2008, 2013 International Conference on Signal-Image Technology & Internet-Based Systems, 2013 International Conference on Signal-Image Technology & Internet-Based Systems 2008, pp. 625-632, doi:10.1109/SITIS.2008.92.
15. J.K. Lee, S.R. Ryu and K.Y. Yoo, "Fingerprint-Based Remote User Authentication Scheme Using Smart Card", Electronics Letter, 6th June 2002, Vol 38 No. 12.
16. LI Yuexiang, WANG Xiaobo and QIAO Feng, "Gait Authentication Based on Accelerating Signals of Ankle", Chinese Journal of Electronics Vol.20, No.3, July 2011.
17. Shrirang Mare, Andr´es Molina-Markham, Cory Cornelius2, Ronald Peterson, and David Kotz. "ZEBRA: Zero-Effort Bilateral Recurring Authentication (Companion Report)", Proceedings of the IEEE Symposium on Security and Privacy, May 2014.
18. SurbhiChugh, Sunny Dagar, "Comparative Analysis of Various Factors of Authentication", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 5, Issue 3, Mar 2015, pp. 416-420.

BIOGRAPHY

Sunny Dagaris an Assistant Professor in the Department of Computer Science and Technology, ManavRachnaUniversity, Faridabad, Haryana, India. He received Master of Technology (M.Tech.) degree in 2013 from IPU, Delhi, India. His research interest includes Steganography, Authenticationand Algorithms.

DOI: 10.15680/IJIRCCE.2017. 0503051