IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

A Systemic Review of Various Multifactor Authentication Schemes

Charanjeet Singh[1*], Tripat Deep Singh[2],

[1]I K Gujral Punjab Technical University, Jalandhar, Punjab, India
[2]Dept. of Computer Applications, Guru Nanak Institute of Management and Technology, Model Town, Ludhiana, Punjab, India

[*]*Corresponding Author: charanjeetss@gmail.com, Tel.: +91-98157-22115*

DOI: https://doi.org/10.26438/ijcse/v7i2.503510 | Available online at: www.ijcseonline.org

Accepted: 19/Feb/2019, Published: 28/Feb/2019

***Abstract*—** With the advancement in information technology, use of cloud has gained rapid acceptance. The usage of such public infrastructures not only increase the risk of data theft but also raise concerns for providing better security to data and resources. One aspect of security deals with authentication method that is used to gain access to the resources over these shared platforms. Strong authentication technique lays foundation for data protection. Simple username-password schemes (single factor) have been proved to be insecure and insufficient in providing secured access thereby urging the need for multifactor authentication (MFA) schemes. Multifactor authentication schemes not only provide an extra layer of security but are also robust against various types of network attacks. The objective of this paper is to review the various multifactor authentication schemes and models that are used to verify the identity of users. This paper highlights the technique, multi-layer cybersecurity strategy, strengths and weaknesses of various schemes with the view to enhance security.

***Keywords*—** Authentication, Multifactor, Security, Passwords, Attack

I. INTRODUCTION

Authentication refers to the process of verifying user's identity and is considered as one of the first wall of protection from unauthorised access. It differentiates legitimate user from unauthorized user[1].It is not only used to establish the user's identity on personal devices but also on various internet platforms such as e-mail, social networks and cloud. The authentication schemes are classified into various types [2]:

1. **Knowledge based**: Something that user knows e.g. alphanumeric password, Personal Identification Number (PIN), a pattern, pass phrase, secret question etc.
2. **Ownership base**: Something that user has e.g. smart card, cell phone with software or hardware token etc.
3. **Inherence based**: Something that user is or does e.g. biometric factor such as fingerprint, retina, voice, DNA, handwriting or signature etc.

Depending upon the number of factors used for authentication, it is divided into single factor and multifactor authentication [3].

1. Single factor: when only one factor is used e.g. username-password.
2. Multifactor (MFA): When two or more factor are used e.g. username-password with One Time Password (OTP).

Section I of this paper provides basic introduction to authentication. Section II explains the concept multifactor authentication. Section III reviews the various multifactor authentication techniques based on image passwords. Section IV briefs the multifactor authentication based on tokens. Section V contains the review of various techniques based on CAPTCHA. Section VI provides the review of multifactor authentication schemes based on biometrics .Section VII reviews the authentication techniques based on cryptography, OTP and other methods. Section VIII presents multifactor authentication methods based on smart card and section IX concludes the paper.

II. MULTIFACTOR AUTHENTICATION

It is a strong method of authentication that makes use of two or more factors to determine a person's identity. Multi-factor authentication adds an extra layer of protection on the top of username and password. It is based on the premise that if one factor is compromised an attacker still has to cross few more levels of authentication before he/she gets an access to a resource. Thus, multifactor authentication model creates a layered security in such a way that it becomes difficult for an unauthorized person to gain access to a database or a network. Multifactor authentication can be two factor (2FA) or three factors (3FA). When a username and password is used in conjunction with smart cards (tokens) or a graphical passwords or one-time passwords it forms two factor authentication (2FA). With addition of third factor (i.e. biometrics) it results in 3FA.

III. MULTIFACTOR AUTHENTICATION TECHNIQUES BASED ON IMAGE

Sabzevar et al [4] proposed a graphical password based multifactor authentication that uses cell phone as a second factor. The proposed technique is neither completely recognition nor recall-based. An image is provided to the user where he has to click certain points in specific order to get access to a resource. The user is provided a hint about the click point and their order by sending the same image in encrypted form to user's cell phone or any other handheld device.

Joshi et al in [5] proposes a combined approach of graphical, knowledge based and biometric authentication that is secure. Here, server generates a unique verification code for each user inside a certificate that is sent on user's mail id or on mobile phone. In case user fails to provide the certificate, he/she is authenticated on the basis of image. Another Image Based Password MFA scheme proposed by Parmar et al [6] uses recognition based graphical password and Hash - MAC based One Time Password using SHA-1 algorithm that is used for online transactions.

In [7] Varghese et al presented a 3-level password authentication scheme that includes image ordering, color pixels and the one time password. The scheme uses different hash functions such as SHA-1, MD5 for OTP generation. A 3-level security implemented by Vemuri et al in [8] uses text based authentication, image based authentication and OTP to email as its three levels. The benefit of this scheme is that any hacker who is able to cross first two security levels, will definitely not be able to cross the third security level, unless he has access to the original user's email id.

Yassin et al [9] presented a two factor authentication scheme that used digital image as second factor. The scheme used Cany's edge detection to encrypt/decrypt image. The technique supports mutual authentication, session key agreement and identity management. The scheme has lower transmission cost and has a capability to counter malicious attacks like insider attack, impersonate attack, dictionary, forgery, replay attack and reflection attack.

Abdellaoui et al [10] proposes a two factor authentication scheme based on out-of-band channel and an image-based one-time password (OTP). The user registers with user name, password, IMEI and his phone number in the cloud server. Depending on number of factors used for authentication, access is provided to two different types of data: public and sensitive. Access to public data is provided by the verification of textual user name and password however the access to sensitive data is provided using the image OTP. This image is supplied by the cloud server using the phone number and the IMEI that were provided to the server during the registration phase. The client then receives image based OTP in his smartphone from the cloud provider using the mobile network (OOB).The received image is watermarked using a secret number generated by truncating IMEI number. The user after verifying the image sends it back to the server by connecting his mobile to PC. The cloud server then checks the authenticity of the received image in order to provide access to sensitive data thereby providing mutual authentication.

Abdellaoui et al presented a novel strong password scheme based on a one-time password and two-factor authentication for the cloud environment in [11].It uses PassGenerator to overcome the security flaws of login/password scheme. The PassGenerator can be implemented in various devices like smartphone and PDA. In this scheme each user has a specific secret image. The user creates the OTP by means of a challenge, a secret image and a PassGen Apps. The PassGen extract a portion of the secret image and compute its hash value in order to create the OTP. The cloud server authenticates the user based on OTP sent by the user. The proposed scheme is immune to a common type of Attacks such as brute force, dictionary attacks, MIM, replay, guessing in a cloud environment. However this scheme does not implement data integrity.

A multistage authentication system proposed by Aldwairi et al [12] uses two different authentication methods: something the user has-devices' serial number and something the user knows-username and combination of patterns and consists of three different stages. First stage uses username and password and the system checks the device serial number to authenticate the user .In second stage user highlights at least *m* right squares from a grid of *n* independent squares. . In the final stage, the he has to select *s* images in a specific order .
Meena et al designed a unique 3 Level Authentication and Authorization system in [13] that is a combination of recognition and recall based techniques. In first level user has to provide user name and textual password, which he has created during registration. In second level, a grid of 16 images (4 x 4 matrix) is shown to the user. In this, user has to correctly identify the image that he had set his click points on during registration phase. On successful completion of first two level, the user will receive the OTP on his registered number in third level that he has to enter in order to complete verification process.

IV. MULTIFACTOR AUTHENTICATION TECHNIQUES BASED ON TOKEN

In [14], 2FA method using mobile phones suggested by Aloul et al uses mobile-based software tokens. OTP is generated using IMEI number, IMSI number, username, PIN, hour, minute, day and year/month/date. After concatenating these factors, the result is hashed using SHA-256 which returns a 256 bit message. The message is then XOR-ed with the PIN replicated to 256 characters. The result is then

Base64 encoded which yields a 28 character message. This message is then shrunk to an administrator-specified length by breaking it into two halves and XOR-ing the two halves repeatedly. This process results in a password that is unique for a ten minute interval for a specific user.

In a two factor authentication technique called SofToken Liou et al [15] used basic username-password as first factor and a random number is generated by software on client-side as a second factor. A pseudo-random number called codeword is generated by the software on client computer that is entered by the user and verified by the server. In [16] Nayak et al proposed a mutual authentication scheme that uses double authentication. In first phase user gets authenticated by username-password and in second phase a token is generated by an application that is delivered to the registered mail-id of user. In order to complete the authentication process the user has to enter the token in a stipulated time. The security of system is enhanced using mutual authentication, session key agreement between the users and the cloud server. The flexibility of changing password is also provided to the user. The proposed protocol resists many attacks such as replay attack and password stolen attack.

Abdul et al [17] presented a strong authentication scheme by using Dual Factor Authentication Protocol (DFAP) along with mobile token to disallow malware. First password verifies the profile of a user and second password allows access to cloud resources. These passwords are sent securely by server using shared secret key and are provided by the user through his mobile phone using mobile token (UMT). This technique addresses various issues such as MIM attacks, insider attack and impersonating attacks.

V. MULTIFACTOR AUTHENTICATION TECHNIQUES BASED ON CAPTCHA

Multifactor authentication model proposed by Banyal et al [18] uses multiple factors such as arithmetic captcha, Secret key, One Time Password and IMEI number. The model has various security features such as identity and credential management, mutual dynamic authentication, session access token agreement. The innovative factor used by framework for user authentication is secret-splitting and encrypted value of arithmetic captcha.

Althamary et al [19] proposes a multifactor authentication where passkey is generated by combining the user password with the modified characters of CAPTCHA. The scheme is effective against phishing, dictionary, password guessing, key logger and social engineering attacks.

VI. MULTIFACTOR AUTHENTICATION TECHNIQUES BASED ON BIOMETRICS

Kim et al in [20] presented a User Authentication Level System (UALS) with five levels that uses public key Infrastructure (PKI) with biometric in level 5. The scheme can be used for high-risk financial transactions or applications where a very high confidence is required in verifying the identity.

In [3] Fujii et al proposed a two factor authentication(SV-2FA) based on SMS and voiceprint challenge response. This scheme uses a one time phone number that is sent by SMS and oath & voiceprint authentication that is sent through voice calls. The user is authenticated by matching the voice print of the oath read by the user after calling on the given onetime phone number. The text of oath changes every time, which includes factors such as date.

Mohammed et al integrated multi factor authentication with multi-layer authentication techniques in [21]. The model consists of 5 different level where each level contain one or combination of authentication factors such as knowledge based, possession-based or biometric-based factors. The proposed system consists of two layers with three sub-systems. Layer 1 authenticates using two subsystems: username-password with face recognition system. Layer 2 use out of band authentication in form of SMS.

Khan et al [22] presents a two factor authentication scheme that combines human biometrics and knowledge factor. The handwritten signatures as a biometric factor are matched using dynamic time warping (DTW) technique. Although the cost and resource requirements of the proposed system are low and does not depend on user end platform, it has been tested for small group of people only.

Han et al [23] proposes a novel multifactor two-server authentication scheme under mobile computing called MTSAS. In this scheme, server does not store fingerprint information and the user's biometric characteristics cannot leave the user device. As a result, authentication is done by user's device and not by the server.

VII. MULTIFACTOR AUTHENTICATION TECHNIQUES BASED ON CRYPTOGRAPHY, OTP AND OTHER

Pietro et al [24] presented a two-factor authentication scheme. A user possessing bluetooth-enabled handheld device is authenticated based on username/password. The scheme uses two-party authentication protocol EKAP that is based on a shared string (including the case of low entropy human memorable passwords) and on well-known cryptographic primitives. The usage of Bluetooth enabled devices improves convenience and usability. This work focuses on financial institutions, in particular Home Banking Systems. The various benefits of scheme include simplified deployment, better scalability, reduced administration costs, and security against fraud and other cyber crimes

Lee et al [25] proposed a two-factor authentication framework for cloud services' authentication process using

Public Key Infrastructure (PKI) authentication and mobile out-of-band (OOB) authentication. A random one-time authentication code based on NLM-128 generator is used. The PKI authentication process uses public and private keys, digital certificate, digital signature and trusted third party CA security elements. Only registered users with valid certificates are authorized.

An OTP base two factor scheme by Eldefrawy et al in [26] uses algorithm with two nested hash functions to provide forward and infinite OTP generation. Multiple OTPs are generated in parallel from initial seed. The seed is created using unique parameters of the host and user such as International Mobile Equipment Identity (IMEI),International Mobile Subscriber Identity (IMSI), and registration date.

In a multitier authentication scheme by Singh et al [27], a user has to perform predetermined series of steps on a fake screen at second tier to get authenticated. First tier uses username-password scheme. The steps in second tier may include sequence of menu clicks, mouse events, and text field activity that are registered by the user during registration phase. The security is enhanced as the probability of breaking second tier security is nearly zero.
A two factor authentication scheme by Emam in [28] used a registered e-mail id to receive a dynamic link of a service that user wants to access on cloud. User has to use the link received from the server in a threshold time in order to use that service.

Hussein et al [29] proposed a mechanism in which server generates an OTP by combining the user's various forms of personal information such as PIN , mobile number and IMEI and transmits encoded OTP (using AES) to the user.

A two factor authentication scheme using TOTP developed by Kaur et al [30] involve seed exchange, software based token via TLS tunnel that generates OTP. Authentication takes place by verifying OTP generated on server and client side from the seed value.

VIII. MULTIFACTOR AUTHENTICATION TECHNIQUES BASED ON SMART CARD

Choudhury et al [31] proposed a strong user authentication framework based on smartcard where username password is verified by local system upon entering smart card. The cloud server then sends one time key to user's mobile through SMS using mobile network upon receiving the login request from local system. The user replies back with message based on smartcard, username and onetime key back to the server to get authenticated.

A Smart card based two factor protocol that authenticates users to a remote server was given by Candan et al in [32] that uses elliptic curve, a symmetric cipher algorithm and a secure hash function. During registration phase a secret random number is generated with username, password and smart card. The scheme produces a secret key on server and client side after user is successfully verified using username-password and smart card. This secret key can be utilized for further secure communication and the protocol ends after the derivation of the symmetric key.

IX. CONCLUSION

In this paper, we presented a comprehensive study of various multifactor authentication techniques that are used to overcome the limitation of simple username and password scheme in order to enhance the security of a resource on a public platform. In our paper, we categorised various multifactor authentication schemes as cryptography based, image based, CAPTCHA based, biometric based, OTP based and smart card based. The paper summarises number and type of factors involved in each scheme, along with their strengths, weaknesses and future directions. Each scheme offers different level of protection against various forms of attacks and incurs different costs. An organisation can opt any of these schemes considering the need, cost factor and level of security required.

Table 1. Comparison of various Multifactor Authentication Techniques

Author	Technique/ method	No. of factors	Type of factors	Strength	Weakness	Future Direction
Yassin et al 2015 [9]	Fast partial image encryption scheme using Canny's edge detection	2	OTP Image encryption	Lower transmission cost, capability to counter malicious attacks like insider attack, impersonate attack, dictionary, forgery, replay and reflection attack.		NA
Choudhury et al 2011 [31]	Strong Authentication Framework	2	Smartcard OTP	Identity management, mutual authentication, session key establishment	Cost of hardware and software	NA
Sabzevar et al 2008 [4]	Universal multi-factor authentication using graphical	2	Image , OTP	Resistant to screen recording attacks, shoulder surfing, key loggers, brute force attacks	Loss of mobile device makes scheme inoperable.	NA

	passwords					
Abdellaoui et al 2015 [10]	Out-of-band Authentication Using Image-Based One Time Password	2	OOB Image based OTP	Withstands common types of attacks :MITM,phishing,brute force, dictionary ,password guessing. Also includes OOB and mutual authentication	does not address confidentiality and integrity	To improve security by addressing confidentiality and integrity
Meena et al 2018 [13]	3 Level Authentication and Authorization system	3	Username-password Inage OTP	Protection against brute-Force attack and tempest attack Strong resistance against shoulder surfing and Spyware attack.	Inflexible as Password change option is not available	Forget password and password reset option needs to be implemented
Abdellaoui et al 2016 [11]	OTP and secret image using PassGenerator	2	Image OTP	Immune to a common type of attacks such as brute force, dictionary attacks, MIM, replay, guessing	Does not implement data integrity.	Security issues particularly –data integrity
Abdul et al 2016 [17]	Dual Factor Authentication Protocol (DFAP)	2	Username-password Mobile Tokens	Addresses various issues such as MIM attacks, insider and impersonating attacks.		NA
Aloul et al 2009 [14]	2FA using mobile phones	2	Mobile phone Software tokens	Saves the cost of purchasing and maintaining the hardware tokens.	GUI is not user friendly, not implemented for various mobile phones	More user friendly GUI and extending the algorithm to work on Blackberry, Palm, and Windows-based mobile phones.
Pietro et al 2005 [24]	Two-Factor Mobile Authentication Scheme	2	Username-password cryptography	Simplified deployment, better scalability, reduced administration costs, and security against fraud and other cybercrimes.	Working prototype not developed	Security issues need to be addressed
Fujii et al 2013 [3]	SV-2FA	2	SMS Biometric: voice pattern	Prevents man-in-the-middle attack and legitimate user's denial	Incurs cost in terms of SMS , voice calla and voice recorders	Need improvements
Liou et al 2010 [15]	SoftToken	2	Username-password Software based token	Eases the deployment process and greatly reduces the cost		NA
Candan 2017 [32]	Two factor Smart card Authentication	2	Username-password Smartcard	Simple Lightweight Withstands offline dictionary and replay attacks	Cost of smartcard processing equipment	NA
Mohammed et al 2013 [21]	Multi- layer of multifactors	3	Username-password Biometric: Face recognition SMS(OOB)	Secure Suitable for financial transactions	cost	NA
Joshi et al 2012 [5]	Multifactor Secure Authentication Scheme based on graphical authentication	2	SSL certificate Image	Usage on military operation, large data base server, nuclear plant and missile operation	cost	NA
Aldwairi et al 2016 [12]	Multi stage authentication system	2	Username-password Image pattern	Defence against brute force and dictionary attacks		NA
Eldefrawy et al 2011 [26]	OTP based 2FA	2	user name - password OTP	Cuts the SMS cost and delay in sending OTPs		NA
Parmar et al 2012 [6]	Secure one-time Password based on image authentication	2	Image HMAC based OTP	Simple,secure,less memory requirement		Recovery of lost password using secret question
Kaur et al 2016 [30]	Authentication using TOTP through secure tunnel	2	Username-password OTP	Security enhanced using multiple factors	Mobile phone theft can make entire security system to collapse, implemented only for android phones	Need to overcome flaws to enhance security

Khan et al 2015 [22]	MFA	2	Username-password Biometric: Handwriting	Scalable, low cost, low resource requirement	Implementation tested on small group of people	Need evaluation on a larger scale with more clients and users
Lee et al 2010 [25]	Two factor Authentication	2	PKI Mobile OOB	Protection against phishing and replay attacks	SMS incurs cost	
Varghese et al 2014 [7]	3-level password authentication system	3	Image ordering Colour pixels OTP	Tries to overcome limitations of each authentication scheme by combined effect	Prone to shoulder surfing attack	Security of system needs to be tested
Vemuri et al 2014 [8]	Secure Authentication System by Using Three Level security	3	Text based parole Image OTP	3-levels enhanced security		OTP to be sent to mobile number
Banyal et al 2013 [18]	Multi-factor Authentication Framework	4	Arithmetic captcha, Secret key, One Time Password and IMEI number	User friendly, Counter various attacks, Dynamic authentication		NA
Singh M. et al 2012 [27]	Multi-tier Authentication Scheme	2	Username-password, actions on fake screen	No additional hardware and software	Password change facility not implemented	Password change at first tier and second tier Multitier way of recovering the password
Kim et al 2011 [20]	User Authentication Level System (UALS) with five levels	Multiple	OTP PKI Two channel Biometrics :Fingerprints	Enhanced security for high-risk financial transactions	Biometric hardware incurs cost	NA
Emam 2013 [28]	Additional Authentication and Authorization using Registered Email-ID	2	Username-password Dynamic link via e-mail	Ensure that only the registered user with exact email ID is authorized to access the requested service	If mail id is hacked the security system collapses	NA
Hussein et al 2013 [29]	Multi Factor Mechanism for Secure Authentication System	3	username - Password OTP based on IMEI no. & PIN	Provides non-repudiation		NA
Althamary et al 2017 [19]	CAPTCHA-Based Authentication	2	CAPTCHA Encryption using public key	Effective against phishing, dictionary, password guessing, keylogger and social engineering attacks.		NA
Han et al 2017 [23]	multifactor two-server authentication scheme under mobile computing (MTSAS)	2	username - Password Biometric: Fingerprint	Lower the security risk of sever attack, Biometric characteristics are not stored on server	User re-registration due to the loss of the user device, leads to the problem of data redundancy in the cloud	Need to overcome this redundancy of user's data due to re-registration
Nayak et al 2012 [16]	Mutual Authentication Framework	2	Username-password Software token	Resist many popular attacks such as replay attack, password stolen attack, Supports mutual authentication, session key agreement, flexibility in password change	Formal security proof yet to be provided	Providing formal security proof to the proposed framework, preserving the privacy of the user's information provided to the server.

REFERENCES

[1] S. M.Sujatha. ,Y. U. Devi, "*Design and implementation of IoT testbed with three factor Authentication*", In the Proceedings of the 2016 International Conference on Communication and Electronics Systems (ICCES),IEEE,2016.

[2] M. Sunita, R. Syal, " *Authentication Scheme in Cloud Computing : A Review*", In the Proceedings of the 2017 Second International Conference on Electrical, Computer and Communication Technologies(ICECCT),2017

[3] H. Fujii, Y. Tsuruoka , "*SV-2FA: Two-Factor User Authentication with SMS and Voiceprint Challenge Response*", In the Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST -2013),IEEE pp-283-287, 2013.

[4] A. P. Sabzeva, A. Stavrou, "*Universal Multi-Factor Authentication Using Graphical Passwords*", In the Proceedings of the IEEE International Conference on Signal Image Technology and Internet Based Systems, SITIS'08, pp. 625-632 ,2008.

[5] A.Joshi, S. Kumar, R.H. Goudar, "*A More Multifactor Secure Authentication Scheme Based On Graphical Authentication*", In the Proceedings of the International Conference on Advances in Computing and Communications (ICACC),IEEE, pp.186-189,2012.

[6] H. Parmar, N. Nainan, S.Thaseen ,"*Generation Of Secure One-Time Password Based On Image Authentication*". Journal of Computer Science and Information Technology, No.7, pp.195-206,2012.

[7] L. Varghese, N. Mathew, S. Saju, V. K. Prasad, "*3-Level Password Authentication System*", International Journal of Recent Development in Engineering and Technology, ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014.

[8] V. K. Vemuri, S. D. V. Prasad, "*A Secure Authentication System by Using Three Level security",* International Journal of Engineering Science and Computing, ISSN-2321-3361, pp.344-348, 2014.

[9] A. A. Yassin, A. A.Hussain, K. A.-A. Mutlaq, "*Cloud Authentication Based on Encryption of Digital Image Using Edge Detection",* International Symposium on Artificial Intelligence and signal Processing (AISP), 2015

[10] A. Abdellaoui, Y. I. Khamlichi, H. Chaoui, "*Out-of-band Authentication Using Image-Based One Time Password in the Cloud Environment*", International Journal of Security and Its Applications Vol.9, No.12 , pp.35-46 ,2015.

[11] A. Abdellaoui, Y. I. Khamlichi, H.Chaoui, " *A Novel Strong Password Generator for Improving Cloud Authentication*", In the Proceedings of the International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science 85) pp.293 – 300 ,2016

[12] M. Aldwairi ,R. Masri, H. Hassan, M. E. Barachi , "*A Novel Multi-Stage Authentication System for Mobile Applications*", International Journal of Computer Science and Information Security, Vol 14, Issue 7, 2016.

[13] M. Meena, H. S. Lamba , D. Taterwal , M. Shaikh , "*System For 3 Level Security Verification Using Image Based Authentication & OTP*", IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250-3021, ISSN 2278-8719,Volume 13, pp. 46-52, 2018.

[14] F. Aloul, S. Zahidi, W. EI-Hajj, "*Two factor authentication using mobile phones*", In the proceedings of the International Conference on Computer Systems and Applications 2009. AICCSA 2009. IEEE/ACS, pp. 641-644, 10-13 May 2009.

[15] J. C. Liou and S. Bhashyam, "*A Feasible and Cost Effective Two-Factor Authentication for Online Transactions*", In the Proceedings of the 2nd International Conference on Software Engineering and Data Mining, IEEE, pp.47-51, June 2010.

[16] S. K. Nayak, S. Mohapatra, B. Majhi, "*An Improved Mutual Authentication Framework for Cloud Computing*" International Journal of Computer Applications, Volume 52, issue. 5, August 2012.

[17] A. M. Abdul, S. Jena, M. Balraju, "*Dual Factor Authentication To Procure Cloud Services*", In the Proceedings of the 2016 Fourth International Conference on Parallel,Distributed and Grid Computing(PDGC),IEEE,2016

[18] R. K. Banyal , P.Jain, V. K. Jain , "*Multifactor Authentication Framework for Cloud Computing*", In the Proceedings of the Fifth International Conference on Computational Intelligence, Modeling and Simulation, IEEE, 2013.

[19] I. A. Althamary, E. M. El-Alfy, "*A More Secure Scheme For CAPTCHA-Based Authentication In Cloud Environment*", In the Proceedings of the 8th International Conference on Information Technology (ICIT), Jordan, May 2017.

[20] J.- J. Kim, S.-P. Hong , "*A Method of Risk Assessment for Multi-Factor Authentication.*" Journal of Information Processing Systems, pp. 187-198,2011.

[21] M. M. Mohammed, M. Elsadig, "*A multi-layer of multi factors authentication model for online banking services*", In the Proceedings of the 2013 International Conference on Computing Electrical and Electronics Engineering (ICCEEE), pp. 220-224, 26–28 August, 2013.

[22] S. H. Khan, M. A. Akbar, "*Multi-Factor Authentication on Cloud*", In the Proceedings of the International Conference on Digital Image Computing: Techniques and Applications, pp. 1-7, 2015.

[23] Z. Han, L. Yang, Q. Liu, "*A Novel Multifactor Two-Server Authentication Scheme under the Mobile Cloud Computing*", In the Proceedings of the 2017 International Conference Networking and Network Applications (NaNA), pp. 341-346, 2017.

[24] R. D. Pietro, M. Gianluigi, M. A. Strangio, " *A Two-Factor Mobile Authentication Scheme for Secure Financial Transactions*", In the Proceedings of the International Conference on Mobile Business (ICMB'05), 2005.

[25] S. Lee, I. Ong, H. T. Lim, H. J. Lee, "*Two factor authentication for cloud computing*", International Journal of KIMICS, vol 8, pp. 427-432,2010

[26] M .H. Eldefrawy, M. K. Khan, K. Alghathbar, "*OTP-Based Two-Factor Authentication Using Mobile Phones*", In the Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, pp. 327-331,2011.

[27] M. Singh, S. Singh, "*Design and Implementation of Multi-tier Authentication Scheme in Cloud*", International Journal of Computer Science Issues(IJCSI), ISSN (Online):1694-0814, Vol. 9, Issue 5, No 2, pp. 181-187,September 2012.

[28] A. H. M. Emam, "*Additional Authentication and Authorisation using Registered Email-ID for Cloud Computing*", International Journal of Soft Computing and Engineering (IJSCE), ISSN : 2231-2307, Vol 3, Issue 2, May 2013.

[29] K. W. Hussein, Dr. N. F. M. Sani, Dr. R. Mahmod, Dr. M. T. Abdullah, " *Design and Implementation of Multi Factor Mechanism for Secure Authentication System*", International Journal of Computer Science and Information Security,Vol. 11, No. 7,pp.31-37, July 2013.

[30] N. Kaur, M. Devgan, S. Bhushan, "*Robust Login Authentication Using Time-Based OTP Through Secure Tunnel*", In the Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 3222-3226, 2016.

[31] A. J. Choudhury ,M. Sain, H. Jae-Lee, , H. Lim, P. Kumar, "*A Strong User Authentication Framework for Cloud Computing*" , In the Proceedings of the 2011 IEEE Asia -Pacific Services Computing Conference(APSCC), Jeju, Jeju Island Korea (South), pp. 110-115,2011.

[32] O. M. Candan, A. Levi, "*Robust Two-factor Smart Card Authentication*", In the Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom),IEEE,2017.

Authors Profile

Mr Charanjeet Singh pursed Bachelor of Computer Applications from Punjab Technical University, Jalandhar, Punjab in 2003 and Master of Computer Applications from Punjab Technical University, Jalandhar, Punjab in 2006. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Applications in Gujranwala Guru Nanak Institute of Management & Technology since 2006.. He has published more than 20 books on subjects like computer networks,computer graphics,operating system and system programming. His main research work focuses on Network Security, Cloud Security and Privacy, He has 12 years of teaching experience and 4 years of Research Experience.

Dr. Tripat Deep Singh pursed Master of Computer Applications from Punjab Technical University,Jalndhar, Punjab in year 2004. He did his Ph.D. in the field of digital image processing from Punjab Technical University, Jalandhar, Punjab in 2012. He has published more than 10 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. He has 14 years of teaching experience and 6 years of Research Experience.

