International Journal of Engineering & Technology, 7 (3.34) (2018) 944-949

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Modelling of Multi Factor Authentication System

[1]P.L.P.Ramyasri, [2]D.Malathi

[1, 2]SRM Institute of Science and Technology, Chennai, Kattankulathur, India
**Corresponding Author E-mail: [1]plpramyasree@gmail.com, [2]malathi.d@ktr.srmuniv.ac.in*

Abstract

Authentication is a fundamental safeguard to access any information. A different type of authentication methods like single factor authentication method, two factor authentication method has been developed to improve user's security. Because of recent security attacks these methods are not reliable to provide better security. In this paper a multi-factor authentication framework is proposed that includes non-biometric authentication modalities like OTP, CAPTCHA, Graphical password, Textual Login. In this proposed framework users can randomly choose these authentication modalities. During login user interface time, failure verification count for each and every authentication modality is captured. A Feedback is collected from 20 user's and based on this time constraints, comparison of performance is done with respect to number of authentication modalities versus users interest. This proposed multi-factor authentication framework can be deployed in different levels of internet computing like email or social applications where user can randomly select authentication modalities based on time constraints.

Keywords: *Multi-factor authentication, Single factor authentication, Authentication modalities, Graphical password, OTP, CAPTCHA*

1. Introduction

Authentication with different features is an ongoing trend that provides security to user for accessing information. These different classifications of authentication methods are used to verify user's credentials. The common example for single factor authentication is textual password but the ultimate drawback is need of security and password memorability. To make the authentication more difficult and secure, a Multi factor authentication was introduced which is the combination of two or more credentials such as password and verification. Most common example is swiping an ATM card and entering PIN but the ultimate drawback is it doesn't provide continuous security. Another authentication method is Dynamic, risk-based authentication which is also known as continuous authentication that examines attributes like touch dynamics, keystroke dynamics and gait recognition that change and continually looks to validate the authentication. In this paper a Multi factor authentication framework is proposed that includes modalities like OTP (One time Password), CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), Graphical Password, and Textual Login that provides alternative options to user where user can select the modality based on the time constraints.

2. Related Works

A. Adams (1999) in [1] mentioned about an article published in the Computerworld news article where a company ran a password cracker. Within 30 seconds it was able to hack around 80 percent user passwords. Study has concluded, users can remember only a few number of passwords and they used the same passwords for various accounts. This paper deals with this alternative approach and the use of pictures as passwords. It takes too much of time for the password registration and login process. Required much more space then text password and shoulder surfing.A.Bianchi (2011) in [2] discussed on the performance and the implementation of the PIN entry system on the Audio and the haptic cues. A haptic cue is a sensory cue that is extracted from sensory input. An ANOVA (Analysis of variance) is a statistical technique that is imp Results show that the interaction between the two variables i.e. Pin length is significant. Future works can be proposed on combining PIN length and stimuli set size. Abramson(2013) in [3] performed an analysis on behaviour of web browsing by collecting large number of users. A random subspace method is proposed which dramatically improved the security for individual features of web browsing behaviour. Future work can be focused more on additional features such as one class learners or can extend this method in group profiles.

Antonella De Angeli (2003) in [4] proposed the Visual Identification Protocol which is considered as an innovative solution for the authentication process. It is based on visual memory and pictures. The proposed system was compared with three other authentication systems in a longitudinal evaluation (N=61). The observation was helpful to finalize on the attitudes and behaviour of the authentication systems. Among all the authentication systems, VIP was the most preferred method by the users. At the same time it was easily destructible there is a possibility of malicious person stealing the user's smartcard or the portable computing device. Complete error analysis is also provided in this paper to understand the cause of the destruct and point out the limitations of this system.Bianchi (2010) in [5] defines, that passwords are being encoded as sequence

of randomized vibration pattern that is impossible for the observer to copy or identify the selected items. Experimental results of this system outperform the previous interfaces that was used to tactile feedback to obfuscate passwords. The limitation of using randomized vibration pattern is that login and password does not provide an adequate security. A Loss or damage may happen to smart card or portable device in the biometric cryptographic systems. Existence of the single physical location focus to the attack.Bours (2009) in [6] proposed a dynamic authentication to verify the current user was same who performed the initial static authentication by monitoring the typing behaviour. A brief description was given on differences between static and continuous authentication using keystroke dynamics. A concept of penalty and reward function is proposed to measure the difference that user was not changed during session. This penalty and reward function will keep track of behaviour of user overall time that decide the user to lock out or not. An experiment was conducted on normal daily business domain. Results proved 25 systems would never lock out a genuine user, while intruders were locked out fairly quickly. Future work can be focused on the performance of continues authentication system with mouse usage along with keystroke dynamics.

Chen (2007) in [7] proposed methodology for implementing Bayesian network model in knowledge-based authentication. Knowledge-based authentication metrics like memorability and guess ability are calculated by maximum likelihood estimator. Results showed the superiority of BN-KBA incorporating dependency modelling. Future work can be focused by implementing algorithms for factor id selection based on theoretical values. D. Tan, P. Keyani (2005) in [8] designed a unique spy-resistant keyboard to allow users to enter private text without revealing it to the attackers. This keyboard contains 42 characters with 2-Interactor lines, a textbox for feedback, enter button, a space button. Results of implementing this keyboard indicates that though users take longer time to enter their passwords it has drastic increased their ability to protect the passwords from a watchful observer. Future works can be proposed to provide a better usability and user friendly device.Darabseh (2015) in [9] done a research to advance the user activation using keystroke dynamics. Based on the duration of a key, latency of flight time, digraph time, and latency performance of keystrokes feature is calculated. Machine learning techniques are used for calculating each item. Future work can involve more classifiers using fewer sample sizes and impact on performance accuracy.

Dasgupta D (2016) in [10] developed a framework based on authentication features and surrounding conditions. Trustworthy values are calculated with the probabilistic constraints like authentication modules (n), classifications (e), features (I) for authentication decision. The main advantage of the proposed system provides better security for online application, in the banking sector during transactions and no prior information to attackers about the authentication factors.Deutschmann (2013) in [11] performed an analysis on continuous authentication system including movement of mouse, usage of application, keystrokes in office environment. Analysis is done on 99 users in 10 week period. A trust model was proposed for detection or verification based on scores. Further Future work can be done on mobile devices and can focus on real attackers. Emanuel von Zezschwitz (2014) in [12] established results of the study that compared the authentication performance mobile devices along with password composition. A study was proposed in lab (n = 24) and the results gave a poor performance for entering the password for mobile devices like smart phones. Core study on (n = 450) proved that passwords which are alphanumeric are increasingly used on smart phones, tablets, etc. An adverse effect on password security is proved where users prefer easier passwords to enter on the respective devices. Limitation is analysis of keystroke mentioned that speed of input becomes very slow if complexity of string increases.

Fridman L (2015) in [13] developed a sensor for each modality. These sensors are organized in parallel binary decision fusion architecture, in this paper mouse movement patterns, keystroke dynamic features are considered. Each feature is tracked by using Navie-Bayes classifier. False rejection rate (FAR) and False acceptance rate (FAR) was calculated with interaction devices. The limitation is performance of system gets degraded for large size dataset.I.Oakley (2012) in [14] described about Multi-touch lock that is based on google- android pattern lock authentication system. It improves the security by mixing the tapes and strokes for the use of Mt Lock. Experimental results state that this method provides better security for mobile devices but the user is facing complexity during log-in. Future works can be done on feedback of user for the usage of MT-lock.

Hung-Minet (2016) in [15] developed an authentication method using pass matrix and pass images along with one time login indicator that is useful for pointing the location of pass square. Main advantage of this proposed work is no need of remembering password. Since there is a lack of user friendliness with the proposed work, random guess attacks may happen at the time of authentication. Janakiraman (2005) in [16] proposed a face verification system that continually verifies the presence of logged-in user. A Bayesian Framework was used to compute probability of verification for 10 seconds. If the probability falls below a threshold, it prevents the unauthorized user.Further analysis was made between verification accuracy, processor overhead, and system security. Results showed that both processor speed and face detection techniques had improved considerably. Future work can be done by deploying in student daily tasks to better, investigate the trade-offs between security, usability, and computational overhead.

K. Gilhooly (2005) in [17] dealed with problem of traditional username and password approach, and implemented biometrics. The main limitation in biometric authentication is the systems are not 100 percent accurate and it requires an additional hardware and it cannot be reset once done. Wang (2010) in [18] developed by combining both graphical passwords with text based CAPTCHA to provide better security against spyware attacks. In the proposed method password space is calculated and compared with text based password. But the ultimate drawback is user has to remember the pass images along with letter position. Future work can be focused on login time. Liu (2009) in [19] proposed a framework for multimodal biometrics for continuous authentication and intrusion detection to detect system security state. A Markov model scheduling algorithm was used for both intrusion detection and continuous authentication. Here Intrusion detection is considered as noisy sensors that can detect system security state. Simulation results were presented that proves effectiveness of proposed scheme. Further research is going on to study the complexity of the combined system and to consider other responses initiated by an IDS in this framework.Locklear (2014) in [20] proposed an experiment was conducted on continuous authentication performance based on the parameters like availability and authentication performance of user based on equal error rate and genuine vector. A Scaled Manhattan verifier was used for computing score on keystroke authentication. Results proved that based on behavioural features, 486 users have higher availability and Lower authentication rate in keystroke dynamics authentication. Martinez-Diaz (2013) in [21] presented a doodle database and pseudo signature. The performance was compared between pseudo and hand written signature. An acquisition protocol that enables the user devices to request permission is being implemented. Experimental results state that this method provides better security against forgeries. The verification principle itself is unverifiable: it isn't a tautology nor can it be

proved via experience. Future works can be based on the complexity of skilled forgeries.

Maghsoudi (2011) in [22] determined the accuracy of authentication on Android phones. Classification algorithms like support vector machine, k-nearest neighbour and naive Bayes classifiers are implemented to calculate accuracy. Results supported the importance of using behavioural biometrics in user authentication with standard authentication like a password. Future work can be done on performing test trails after analysis.Ms.GrinalTuscano (2015) in [23] focused on inventing a strong authentication method based on image distortion technique that is developed with the use of filters. In the proposed work both original and distorted images are displayed to user. Results proved that further research can be done to provide better security against random guess attacks.

Ninuma (2010) in [24] proposed a new method for continuous user authentication that monitors user's face and clothing color in addition to Face information. A continuous authentication algorithm was proposed as an enrolment template. This color distribution was used in automatic video context indexing. A new framework was proposed to achieve usability, cost, and security. Results showed that system captures color regardless of user posture. Future work can be done to find position and size between the face, body, EER, FRR, FAR.Patrick Boursa (2009) in [25] proposed a dynamic authentication to verify the current user was same who performed the initial static authentication by monitoring the typing behaviour. Differences between static and continuous authentication using keystroke dynamics. A concept of penalty and reward function is proposed to measure the difference that user was not changed during session. This penalty and reward function will keep track of behaviour of user overall time that decide the user to lock out or not. An experiment was conducted on normal daily business domain. Results proved 25 systems would never lock out a genuine user, while intruders were locked out fairly quickly. Future work can be focused on the performance of continues authentication system with mouse usage along with keystroke dynamics.Primo (2014) in [26] developed a framework of two stage authentication i.e., accelerometer-based gait authentication was proposed that identifies phone position and location to improve performance of classification. Results showed that this model is helpful to improve the security layers and authentication performance in smartphones.R.N. Shepard (1967) in [27] discussed the most frequently used authentication method in computer is user name and password. There are several vulnerabilities in this method that are known to all. The crucial step in this approach is to remember the passwords and then recall them during the authentication process. Studies proved that users every time prefer to choose short passwords or passwords that can be remembered easily. Unfortunately, these passwords are broken very easily. Ron Poet (2011) in [28] developed an attack exploiting predictability system called as the Semantic Ordered Guessing Attack (SOGA). The SOGA attack is applied on two different schemes (a standard recognition-based scheme and the Doodles scheme that uses photographic images). Outcome of the experiment shows that predictability in case of graphical passwords has varying degree of security levels (this depends on the type of distractor algorithm that is selected). Whereas the traditional pass images scheme shows that the guess ability has increased to maximum 18 times when compared to the usual reported guess ability. Hence to maximize security of the recognition-based graphical password method, the author recommends preventing or avoiding user choice of images.

S. Gurav (2014) in [29] enhanced the graphical authentication in cloud by describing the image authentication. Data integrity is calculated based on key generation technique. Future work can be focused on securing large data using efficient token generation techniques.Saini (2017) in [30] mainly focused on the analysis of best possible numeric input for authentication using keystroke dynamics. Random forest and Navie Bayes classifiers are used for yielding the result when a random number is taken as input. Results showed that combination of hold time and latency gave best results. Future work can be done by comparing different combinations of input.Stewart, (2011) in [31] proposed a robust system to authenticate users in online tests in keystroke and stylometry. Performance was considered from 40 students. Results proved that best equal error rate was 0.5%. Compared to stylometry, keystroke dynamics was far better. Future work can focus on Fraction of misspelled words, long text in different topics.Susan Wiedenbeck (2005) in [32] records an interesting analyzing on the use of Pass Points on passwords which are alphanumeric. The users participated in this study created and implemented alphanumeric, graphical password. The users must try three longitudinal trials to enter password for a time period of 6 weeks. Results of this experiment showed the users who use graphical passwords were able to create a valid password with less difficulty compared to alphanumeric users. Results also show that graphical users consumed longer time and committed several wrong password inputs compared to the alphanumeric users. On considering longitudinal trials, both methods performed equally on the bases of memory of their password. The group took much time to type the correct password. The limitation is results showed that 1/5th users are facing difficulty in inputting password.

T. Takada (2008) in [33] discussed a solution for fake pointer authentication technique against peeping attack. In the proposed work pointers are added as background to keypad and on screen. The ultimate drawback is there is a chance of camera based attacks since pointers are added in background.V.Roth (2004) in [34] proposed a new technique called steganography technique. The secrete message is protected or safe guarded using another message so as to avoid shoulder surfing attack. He discussed about semagrams that is used for hiding the PIN from attackers. Here the PIN is secured using signs and symbols. Two keypads are provided one is regular keypad and other is a challenge keypad which is used for OTP. Limitation is two keypads results in confusion to user.Zheng (2009) in [35] proposed an authentication scheme based on stroke concept on the grid as origin password. The main aim of this technique is to map the strokes against grids as original password and later enter the characters in the authentication process. Limitations in this method is that users adapt weak strokes as their passwords and hence creating passwords is vulnerable than login. Future studies can be based on providing security against camera based and brute force attacks.

3. Proposed Work

In this proposed framework non biometric authentication modalities like OTP, CAPTCHA, Graphical password and Textual password are implemented. User can randomly select the authentication modalities to access the information. After login, feedback form was collected from 20 users. For each and every authentication modality user interface time, number of failure attempts, Failure verification time (after login) is captured. Comparison of performance is done by considering number of users versus authentication modalities, user's interested modality in percentage and finally number of seconds versus authentication modalities. *Figure: 1* explains the brief description of proposed framework.

3.1 Non Biometric Authentication Modalities

User has to register with his personal details like name, password, mail id and address.

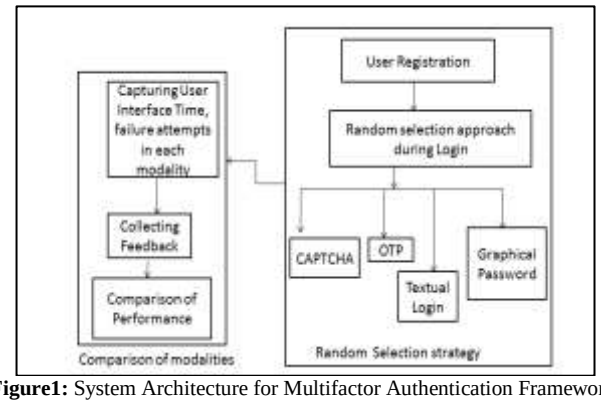

Figure1: System Architecture for Multifactor Authentication Framework

After the completion of successful registration, within these existing authentication modalities like OTP, CAPTCHA, Graphical Password and Simple Login, user can randomly choose these modalities for Login to access information. Below *Figure: 2*represents authentication modalities during login.

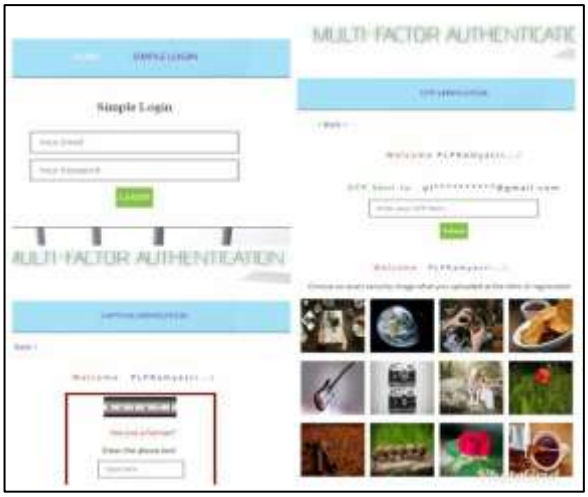

Figure2: Authentication modalities like OTP, CAPTCHA, Graphical Password, Textual Login

3.2 Capturing User Interface Time and Failure Verification Time

During login when the user selects the authentication modality randomly, user interface time(how much amount of time user takes to login),Number of failure attempts, Verification count, Failure Verification Count(for Graphical Password, Captcha, OTP) is captured and stored in the database.

3.3 Collecting Feedback from Users

After capturing number of failure attempts and user interface time for each authentication modality, a feedback form is displayed in a questionnaire form. Questionnaire Feedback form is displayed to user is shown below:

1. How easy is to enter the information in proposed authentication modality?
2. Which Authentication modality you are interested to login?
3. How easy is to select these authentication methods randomly?
4. To what degree you feel proposed authentication framework was secure to user?
5. Time was satisfactory when you are entering information wrongly?

3.4 Comparison of Performance

After collecting the feedback form from 20 users, Performance of the users for each authentication modality was compared by adding total number of seconds taken by user to login in each modality. Comparison is done by considering different combinations such as authentication modalities vs login time (Total number of seconds), Number of Users (based on Feedback) vs Modalities is performed and finally displayed in a graph and pie chart.

4. Results

Based on the Feedback from 20 user's comparison of performance for each and every authentication modality is done. Results showed that total number of seconds taken for Graphical Authentication is 180 seconds, for Textual Login is 90 seconds, for Captcha is 262 seconds, for OTP is 273 seconds. Based on the feedback, 20% users has chosen graphical authentication modality, 25% has chosen both Textual Login and Captcha, and 30.02% users has chosen OTP. Further Results are shown in graph and pie chart as below in *Figure no: 4.1* user interested modality versus Authentication modalities, *Figure no: 4.2* User interested modality in pie chart and *Figure no: 4.3* number of seconds versus authentication modalities.

Fig 4.1: User interested modality versus Authentication modalities

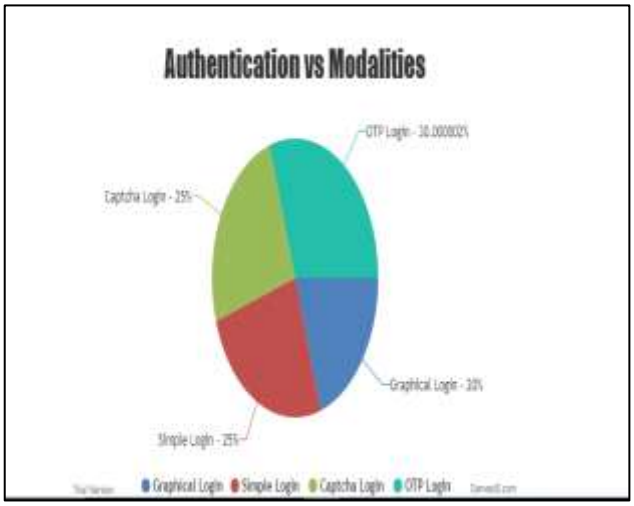

Fig4.2: User versus modality in pie chart

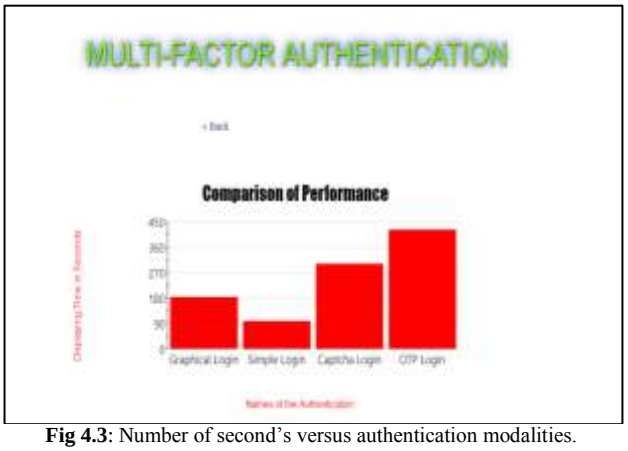

Fig 4.3: Number of second's versus authentication modalities.

5. Conclusion

In this paper a multi factor authentication framework was developed that includes non-biometric authentication modalities like OTP, CAPTCHA, Graphical Password and Textual Login. For each and every modality user interface time, number of failure attempts and failure verification count was captured. Further feedback form from 20 users is considered, based on the user's interest and time based constraint comparison of authentication modalities was performed. Based on these time constraints user can choose authentication modality. Further this proposed framework can be deployed in any social and web applications where user can choose his/her authentication modality for login to access any information.

References

[1] 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.

[2] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA: ACM, 2010.

[3] Abramson, Myriam, and David W. Aha (2013). "User Authentication from Web Browsing Behaviour." FLAIRS conference.

[4] Antonella, Angeli et al. "Usability and user authentication: Pictorial passwords vs. PIN." Contemporary ergonomics (2003): 253-258.

[5] Bianchi, Andrea, et al. "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices." Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction. ACM, 2011.

[6] Bours, Patrick, and Hafez Barghouthi. "Continuous authentication using biometric keystroke dynamics." The Norwegian Information Security Conference (NISK).Vol. 2009. 2009.

[7] Chen, Ye, and DivakaranLiginlal (2007). "Bayesian networks for knowledge-based authentication." IEEE Transactions on Knowledge and Data Engineering 19.5 (2007): 695-710.

[8] D. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens," in Proceedings of OZCHI-Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press, 2005

[9] Darabseh, Alaa, and Akbar SiamiNamin (2015). "On Accuracy of Keystroke Authentications Based on Commonly Used English Words." Biometrics Special Interest Group (BIOSIG), 2015 International Conference of the. IEEE.

[10] Dasgupta, Dipankar, Arunava Roy, and Abhijit Nag. (2016) "Toward the design of adaptive selection strategies for multi-factor authentication." computers & security 63 (2016): 85-116.

[11] Deutschmann, Ingo, and Johan Lindholm (2013). "Behavioural biometrics for DARPA's active authentication program." Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. IEEE.

[12] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey,i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Conference on Human-Computer Interaction: Fun, Fast, Foundational, New York, NY, USA: ACM, 2014.

[13] Fridman, Lex, et al (2015). "Multi-modal decision fusion for continuous authentication." Computers & Electrical Engineering 41 (2015): 142-156.

[14] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the ACM Conference on Ubiquitous Computing, New York, NY, USA: ACM, 2012.

[15] Janakiraman, Raj Kumar, et al. "Using continuous face verification to improve desktop security." Application of Computer Vision, 2005.WACV/MOTIONS'05 Volume 1.Seventh IEEE Workshops on.Vol. 1. IEEE, 2005.

[16] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[17] Khamis, Mohamed, et al. "GTmoPass: two-factor authentication on public displays using gaze-touch passwords and personal mobile devices:" Proceedings of the 6th ACM

[18] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme," in 24th International Conference on Advanced Information Networking and Applications, IEEE,2010.

[19] Liu, Jie, et al. "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks." IEEE transactions on wireless communications 8.2 (2009): 806-815.

[20] Locklear, Hilbert (2014) "Continuous authentication with cognition-centric text production and revision features." Biometrics (IJCB), 2014 IEEE International Joint Conference.

[21] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "The doodb graphical password database: Data analysis and benchmark results," Access, IEEE, 2013.

[22] Maghsoudi, Javid, and Charles C. Tappert (2011). "A Behavioural Biometrics User Authentication Study Using Motion Data from Android Smartphones. "Intelligence and Security Informatics Conference (EISIC), 2016 European. IEEE.

[23] Ms GrinalTuscano "Graphical password authentication using Pass faces" Int. Journal of Engineering Research and Applications March 2015.

[24] Niinuma, Koichiro, and Anil K. Jain (2010) "Continuous user authentication using temporal information." Biometric Technology for Human Identification VII.Vol. 7667. International Society for Optics and Photonics.

[25] Primo, Abena, et al. (2014) "Context-aware active authentication using smartphone accelerometer measurements." Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on. IEEE.

[26] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning, February 1967.

[27] Rosanne, and Ron Poet. "Measuring the revised guess ability of graphical passwords" 5th International Conference on. Network and System Security (NSS), IEEE, 2011.

[28] S. Gurav, L. Gawade, P. Rane, and N. Khochare, Graphical password authentication: Cloud securing scheme," International Conference on, in Electronic Systems, Signal Processing and Computing Technologies (ICESC),IEEE Jan 2014.

[29] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, 2005

[30] Saini, Baljit Singh, NavdeepKaur, and Kamaljit Singh Bhatia (2017). Keystrokedynamics based user authentication using numeric keypad." Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on. IEEE.

[31] Stewart, John C., et al. (2011)"An investigation of keystroke and stylometry traits forauthenticating online test takers." Biometrics (IJCB), 2011 International Joint Conference on. IEEE.

[32] **[32]** Sun, Hung-Min, "A shoulder surfing resistant graphical authentication system." IEEE Transactions on Dependable and Secure Computing (2016).

[33] T. Takada, "fake pointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, and Technologies, Second International Conference on IEEE 2008.

[34] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM conference on Computer and communications security, ACM, 2004.

[35] Zheng, Ziran, "A stroke-based textual password authentication scheme." Education Technology and Computer Science, 2009.ETCS'09.First International Workshop on.Vol. 3. IEEE, 2009.

[36] K. Vijayakumar, C. Arun, Analysis and selection of risk assessment frameworks for cloud based enterprise applications", Biomedical Research, ISSN: 0976-1683 (Electronic), January 2017.

[37] K. Vijayakumar C. Arun, Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC, Cluster Computing DOI 10.1007/s10586-017-1176-x, Sept 2017.