Multi-Factor Graphical Password for Cloud Interface Authentication Security

Ramandeep Kaur
Department of Information Technology,
CEC, Landran (Mohali)

Amanpreet Kaur
Department Of Information Technology,
CEC, Landran (Mohali)

ABSTRACT
As the trend of mobile devices is on the rise, every kind of internet application is being easily accessible locally using mobile apps. The proposed technique will be using one-level double-trap image based authentication for the login protection in cloud platforms on mobile devices. The one-level authentication scheme consists of various small images, which are made of single numerical or alphabetical characters each, in 3x3 point grid formation. The second level password is a 9 clue-points grid based password scheme for pattern passwords. The pattern password input grid is in the static arrangement and does not change at any point of time. The traditional 9 clue-point scheme will additionally allow the overlapping patterns, hence they are prone to the shoulder surfing attacks, whereas the proposed scheme is based on shuffling geometrical shape and the overlapping password pattern to mitigate the threat of shoulder surfing attacks.

Keywords
Graphical Authentication, Cue-points, pattern lock, pattern password, cloud authentication, mobile authentication.

1. INTRODUCTION
Cloud computing enables on-demand access to computing and data storage resources that can be configured to meet unique constraints of the clients with minimal management overhead. The recent rise in the availability of cloud services makes them attractive and economically sensible for clients with limited computing or storage resources who are unwilling or unable to procure and maintain their own computing infrastructure. The ever increasing need for computing power and storage accounts for the steady growth in popularity of companies offering cloud services. Clients can easily outsource large amounts of data and computation to remote locations, as well as run applications directly from the cloud. From the past few decades, there has been very fast advancement in computing technology. Systems have been designed which have high resource handling capability, capacity and computing power. All these online activity require some type of authentication. Authentication means to verify identity of the user, which means whether the person is same which he pretends to be. For authentication, various techniques are used, e.g. username-passwords, biometric face recognition, public key transportation and symmetric key based authentication schemes etc. At present, authentication is done in several ways: such as, textual, graphical, bio-metric, 3D password and third party authentication.

The popularity of the touch based devices is rising day by day. The touch based devices include the mobile devices, tablets, touch-based PCs and other personal gadgets. The number of internet users from the touch based devices is rising every day. The increase in the internet user from the touch-based devices is also producing the difficulty of typing, hence filling the alphanumeric passwords. The graphical passwords are getting popular as the best form of passwords for the touch-based devices. The recent and existing graphical password schemes are definitely better than the earlier schemes in terms of security and ease-of-use. The existing scheme being evaluated are Graphic Touch Gesture Feature (GTGF) scheme and Resistant Text-Based Graphical Password (RTBGP) scheme. The drawback of GTGF scheme may offer easy-to-use platform but it is prone to the guessing attacks. A hacker may try a large image set to crack into this scheme. On the other hand, the RTBGP scheme is not easy-to-use up to the desired level. Many layman users cannot easily understand the working of the scheme and they can face a problem in using this scheme. Both of the schemes cannot be considered very secure, efficient and adaptable in the today's real-time environment. In this research, the limitation of GTGR and RTBGP are to be overcome by developing an effective graphical password scheme in the multi-layered fashion. The proposed graphical password scheme, which is an effective and multi-layered graphical scheme, can be used in various applications for the multi-level authentication secure access. The proposed graphical scheme can be used for the most secure applications like internet banking, share-market applications, etc.

2. LITERATURE SURVEY
Abdulameer Hussain et. al. [3] [has developed an enhanced authentication mechanism using multilevel security model. The proposed scheme is aimed at protecting against the highly secure and confidential data. The proposed models divides the existing data access services into multi-level data access services based on the sensitivity of data being stored on the storage device. Some of the sensitive security levels are also sub-divided into sub-levels. Each level and sub-level is programmed with specific privileges and data types managed by Identity manager. The user is forced to provide and prove its identity on every level to gain the access of the data.

Maninder Singh and Sarbjeet Singh, et al. [8] have designed and Implemented of Multi-tier Authentication Scheme in Cloud. The proposed authentication scheme belongs to the multi-tier authentication paradigm. The proposed scheme focuses on the secure use of third party cloud servers. The proposed scheme consists of two authentication levels to protect against the malicious third party cloud servers. The first level authentication includes the text based username and password. The second level password includes the combination of pre-determined

steps. The decision logic is returned in the form of success (S) and failure (F).

Dinesha, H. A.et. al. [2] has developed the multi-level authentication technique for accessing cloud services. The authors have developed multi-level authentication scheme to generate passwords in multiple levels for user authentication purposes. The use of proposed scheme has been suggested as a middleware authentication scheme. This technique helps in generating the password in many levels of organization so that the strict authentication and authorization is possible.

Umanandhini. D.et. al. [13] has worked upon dynamic authentication for consumer supplies in mobile cloud environment. The proposed novel authentication method is based on the quick response (QR) code. The new authentication scheme has been proposed for the purpose of cloud computing environment for mobile users. The proposed scheme has been made easily accessible on the mobile devices, where typing becomes really a tough task. The proposed scheme has been made able to authenticate the products associated with the specific QR-codes.

Tanvi Naiket. al. [10] has worked on Multi-Dimensional and Multi-Level Authentication Techniques. A novel multi-level and multi-dimensional method of authentication has been developed in this research using the combination of text, biometric and graphical password scheme. The proposed method has been developed to protect against the dictionary based brute force attacks. The method is prominently focusing upon the use of non-dictionary based passwords, which are also easy to remember. The non-dictionary passwords are difficult to crack and cannot be cracked using the traditional dictionary based hybrid or brute force attacks. The techniques include many options for multi-level authentication, like Change position of object, Textual password, Graphical password, Biometric password, and Play audio. The user is free to choose between the combinations for his customized multi-level authentication scheme.

ShraddhaM.Guravet. al. [7] has proposed the graphical password authentication. The authors have tried to create a user friendly scheme to ease out the users of the application equipped with the proposed scheme. The capability of human mind to remember images more than the text data is being explored in the proposed scheme. The proposed scheme is the combination of username and image based password. The proposed scheme is based on the images of alphabets which generate a number series at the backend used for the matching and authorizing purposes.

3. IMPLEMENTATION

We have implemented the new shuffling points based pattern password scheme which is designed to prevent the security risks of the currently popular pass-go pattern scheme. In this research work, we have used HTML with JavaScript for the purpose of implementation of the proposed pattern password scheme. This scheme is designed using the HTML and CSS (Cascade Style Sheets) combination, because they are simple and used to create attractive & flexible designs. Also this pattern scheme is developed in the duo, because these two are widely used for the iPhone and Android application development purposes.

For the backend programming, i.e. the result retrieval, JavaScript is used. JavaScript is used to create the number sequence which acts as a numerical representation of the frond end pattern password and saved in the database. The users are provided with two types of graphical password authentication schemes. The first scheme is used to authentication the user for the first level, where the user will get the privileges to operate the cloud testing up to one to two instances (or cloudlets) of cloud, which may be used to run some specific small-sized or semi mid-sized applications on the cloud platforms. The second scheme is used to authentication the users for the more privileged interface, where the user can test all formations or setups for various types of applications. The first level password is based on a 3x3 password grid and irrespective of any pattern. It means the user can fill any combination using the first level graphical password scheme. The second password scheme is repeatable and overlapping password pattern scheme. The user will be capable of drawing an overlapping pattern which is always difficult for the hacking trying to crack the passwords using shoulder surfing attacks. When a user enters the pattern passwords, a numerical code for the pattern password is generated on the basis of the grid point indexing numbers. JavaScript code is divided into the various functions to perform the various types of functions.

The first-level graphical password is prompted in the form of 3x3 image grid as the password input method. The input pattern is irrespective of any pattern based password input in the image based password. The user is free to input any password combination; either it is a combination of one image as all four positions, or any two, three or four images in the all four placeholder for password combination .(Fig. 1,2,3 and 4)

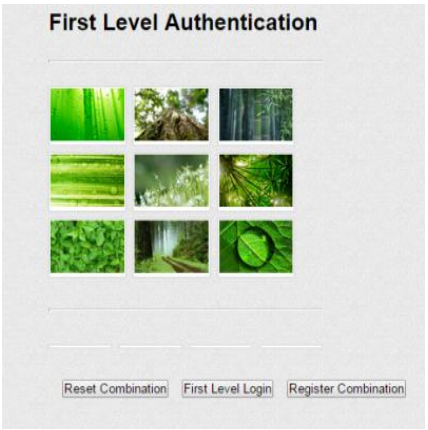

Fig 1: The difference image based password combinations in the graphical password scheme. The graphical password scheme before log-in.

Fig.2. the password input with four different images.

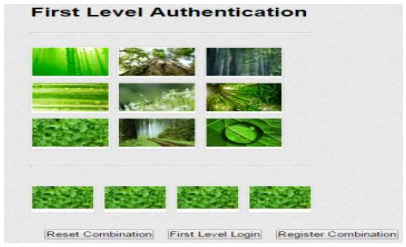

Fig. 3. The password input with one image at all four places.

Fig 4. The password input with two images in 2-and-2 combination of images.

The second level password is a 9 clue-points grid based password scheme for pattern passwords. The pattern password is a scheme where the patterns are drawn by combining the points in order to draw the password pattern for the purpose of authentication. The pattern password input grid is in the static arrangement and does not change at any point of time.

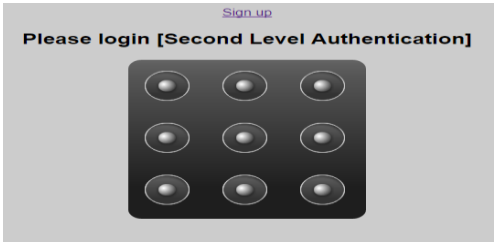

Fig.5. the pattern password scheme based on overlapping pattern, 9 clue-points grid based password scheme awaiting input.

Fig.6. the non-overlapping pattern password

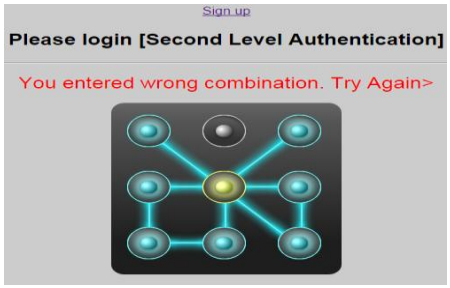

Fig.7. the overlapping pattern password

The traditional 9 clue-point scheme does not allow the overlapping patterns, hence they are prone to the shoulder surfing attacks, whereas the proposed scheme is based on the overlapping password pattern to mitigate the threat of shoulder surfing attacks. The shoulder surfing attacks are the attacks where the attacker copies the users by watching their input (Fig. 5, 6 and 7).

4. RESULT ANALYSIS

The implemented work includes the new multi-level graphical password scheme which is designed to prevent the security risks of the currently popular graphical password schemes. The new scheme has been proposed for its use in the power user portal for cloudlet testing for various testing levels from the IT administrator's touch-screen based devices. In this research work, HTML with JavaScript has been used for the purpose of implementation of the proposed pattern password scheme. This scheme is designed using the HTML and CSS (Cascade Style Sheets) combination, because they are simple and used to create attractive & flexible designs. Also this pattern scheme is developed in the duo, because these two are widely used for the iPhone and Android application development purposes. For the backend programming, i.e. the result retrieval, JavaScript is used. JavaScript is used to create the number sequence which acts as a numerical representation of the front end pattern password and saved in the database. When a user enters the pattern passwords, a numerical code for the pattern password is generated on the basis of the grid point indexing numbers. JavaScript code is divided into the various functions to perform the various types of functions. (Fig. 1, 2, 3 and 4)

The second level password is a 9 clue-points grid based password scheme for pattern passwords. The pattern password is a scheme where the patterns are drawn by combining the points in order to draw the password pattern for the purpose of authentication. The pattern password input grid is in the static arrangement and does not change at any point of time. The traditional 9 clue-point scheme does not allow the overlapping patterns, hence they are prone to the shoulder surfing attacks, whereas the proposed scheme is based on the overlapping password pattern to mitigate the threat of shoulder surfing attacks. The shoulder surfing attacks are the attacks where the attacker copies the users by watching their input (Fig. 5, 6 and 7).

Additionally, proposed pattern password scheme is designed in way to make use capable of drawing an overlapping pattern, i.e. user can draw can cross-line pattern, which adds more probability of pattern designs. In this way, more secure passwords can be generated, and also it may help one to generate a more visually complex patter password, which will be definitely difficult to guess

and will be less or not prone to the shoulder surfing attacks.

5. CONCLUSION

In case, somebody once see a user entering the graphical password can easily remember or guess the pattern and can take access to the device. Our major goal is to overcome this security issue and to use the password on the cloud platforms for the administrator panels for various cloud applications. Using this password scheme, the touch screen friendly secure administration interfaces can be developed to give the administrators an easy access to the administration panel. In this research, a multi-level password authentication scheme has been proposed for the administrator panels, where the administrators would be prompted to enter the first-level password at first and second-level password can be used to access more critical administration areas in order to protect the power user accounts from hacking attempts. A user when signup creates and stores a pattern by joining the number points or by selecting the images to create a password, the password is converted into a hash which is further sent to the server for the authentication purposes. The server returns the decision logic which is responsible to accept or deny the login request. To gain the access to the device, the user has to remember the graphical passwords and need to enter the same sequence every time drawing a pattern. The proposed scheme has been evaluated as effective, robust, ease of access and wide adaptability of the scheme for the various smart phone platforms. The proposed scheme has been evaluated under various situations. Both of the graphical password schemes have been evaluated individually with various password combinations. The new multi-level graphical password scheme can be considered as a secure scheme for cloud platforms.

6. FUTURE WORK

The drawbacks or limitations concerned with the existing multi-level graphical password scheme can be mitigated in the future researches, which can be considered as the critical enhancement or improvement in the proposed system. A new improved scheme can be developed following the design and pattern schemes of the proposed scheme.

7. REFERENCES

[1] Bashier, H. K., Hoe, L. S., & Han, P. Y. "Graphical Password: Pass-Images Edge Detection", In Signal Processing And Its Applications (CSPA), IEEE 9th International Colloquium , Pp. 111-116 , 2013.

[2] Dinesha, H. A., And V. K. Agrawal. "Multi-Level Authentica tion Technique For Accessing Cloud Services." Computing, Com munication And Applications (ICCCA), 2012 International Conference On.IEEE, Pp 1-4, 2012.

[3] Hussain, Abdulameer. "Enhanced Authentication Mechanism Using Multilevel Security Model." Int. Arab J. E-Technol. V.1.2 , Pp 49-57,2009.

[4] Ku, Wei-Chi, Dum-Min Liao, Chia-Ju Chang, And Pei-Jia Qiu. "An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme." In Communications In China (ICCC), IEEE/CIC International Conference On, Pp. 204-208, 2014.

[5] Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. "Are Graphical Authentication Mechanisms As Strong As Passwords" In Computer Science And Information Systems (Fedcsis), Federated Conference On Pp. 837-844, 2013.

[6] Revar, A. G., & Bhavsar, M. D. "Securing User Authentication Using Single Sign-On In Cloud Computing" In Engineering (Nuicone), Nirma University International Conference On Pp. 1-4, 2011.

[7] Shraddham. Gurav, "Graphical Password Authentication", ICESSPCT, Vol. 1, Pp. 479-483,2014.

[8] Singh, M., & Singh, S. "Design And Implementation Of Multi-Tier Authentication Scheme In Cloud" IJCSI International Journal Of Computer Science Issues, 9(5), Pp. 87-90.

[9] Tao, Hai, And Carlisle Adams. "Pass-Go: A Proposal To Improve The Usability Of Graphical Passwords." IJ Network Security 7, Pp.273-292.2 ,2008.

[10] Tanvi Naik, Sheetal Koul, "Multi-Dimensional And Multi-Level Authentication Techniques", IJCA ,Vol. 75, Issue 12, Pp.17-22, 2013.

[11] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, Dun-Min Liao, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password", ISNE, Vol. 1, Pp. 161-164,2013.

[12] Revathy Gangadaren M And Lijo V P.. Article: Cloud Based Spatial Cloaking For Mobile User Privacy Preservation. International Journal Of Applied Information Systems 4(5) , Pp. 39-432012.

[13] Umanandhini, D., Tamilselvan, L., Udhayakumar, S., & Vijayasingam, T. "Dynamic Authentication For Consumer Supplies In Mobile Cloud Environment" In Computing Communication & Networking Technologies (ICCCNT) ,Pp. 1-6,2012.

[14] Zhao, Xi, Tao Feng, And Weidong Shi. "Continuous Mobile Authentication Using A Novel Graphic Touch Gesture Feature." In Biometrics: Theory, Applications And Systems (BTAS), IEEE Sixth International Conference On, Pp. 1-6,2013.

[15] Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz, T. "Quantifying The Security Of Graphical Passwords: The Case Of Android Unlock Patterns" In Proceedings Of The 2013 ACM SIGSAC Conference On Computer & Communications Security ,Pp. 161-172.