# A COMPLETE, SMART DEVICES-BASED VERIFICATION OF A SECURED GRAPHICAL AUTHENTICATION SYSTEM

[1]V ANITHA, [2]B HARI KUMAR, [3]PUNNA MAHESH, [4]RISHAB GAIKWAD
[1]Professor, [2,3]Assistant Professor, [4]Student, Dept. of Computer Science Engineering, Brilliant Institute of Engineering and Technology, Hyderabad, Telangana, India

**ABSTRACT**

Nowadays user authentication is one of the foremost in area of data security that is many ways to be connected for immemorial verification plans that apply strong content- based passwords which are traditionally been able to supply a few security confirmations. However committing these solid passwords to memory will demonstrate a very devastating assignment constraining clients to resort to composing them down on paper pieces or indeed putting away them in a computer record. Graphical confirmation has been recommended as a substitute for text-based verification as a way of obstructing these habits. The graphical confirmation method is utilized to supply a secured login for the clients. Verifying an application safely has gotten to be a major issue these days due to the hacking of passwords effectively by programmers. In this overview, an viable arrangement for giving secure login for an application has been made.

***Keywords*:** Authentication, Password, Information Security, Randomized algorithm, Attacks, Passpoint Scheme

## 1. INTRODUCTION

Authentication is an important process for accessing any application or important information in an mobile phone. Various authentication techniques have been created until now but still, provide all those techniques that are tough to memorize the password and provide poor authenticity for the users. Computer security programs must also take into account human factors such as ease of use and accessibility. With the advancement in technology, a secured and easily memorable password has to be designed for each user to have a secured login. Present safe systems fail because they mostly neglect the importance of human factors to security [3].

Generally, the process begins with the authentication, i.e. the user claims identity and the authorization where the user presents certificates to prove the alleged identity is followed by that [1]. The password can be of numbers, alphabets or alphanumeric. The user finds it difficult to remember the password which is in text form. They try to form a strong password which will be difficult for others to guess their password easily. Such types of passwords are difficult to remember as a user tries to pick a complicated key combination for greater security. On the other hand, when choosing a simple key combination, such passwords can be quickly memorized. Text password is easily prone to brute force attack.Now all those strong passwords also can be easily hacked by hackers [5].

In 2005, a team of computer for security has done a password cracker network, in that they can ableto find 80% of passwords in 30 seconds. The passwords are prone to different attacks namely Dictionary Attack, Shoulder-surfing Attack, Guessing Attack, Spy-ware Attack, Social Eng neering Attack and Brute Force Attack. In the event of an attack on the shoulder wave, an intruder may obtain information such as personal identification numbers (PINs), passwords, and other confidential data by looking over the shoulder of the victim [6].

In a knowledge-based technique, there are also graphical password schemes in it. Moreover, it is easy for users to remember images than text. It can be easily memorized by all age people. Graphical passwords [1] are more user-friendly and can provide protection and accessibility to users together. Besides all the benefits of graphical passwords, certain issues often occur over time, for instance, shoulder surfing is a familiar issue with graphical passwords [7]. The main reason to introduce a graphical scheme is the users can easily remember the pictures and the things which they see through their vision. As mentioned in the literature, there are various methods proposed to minimize these problems. This paper mainly focuses on providing secured login for users using different graphical scheme techniques.

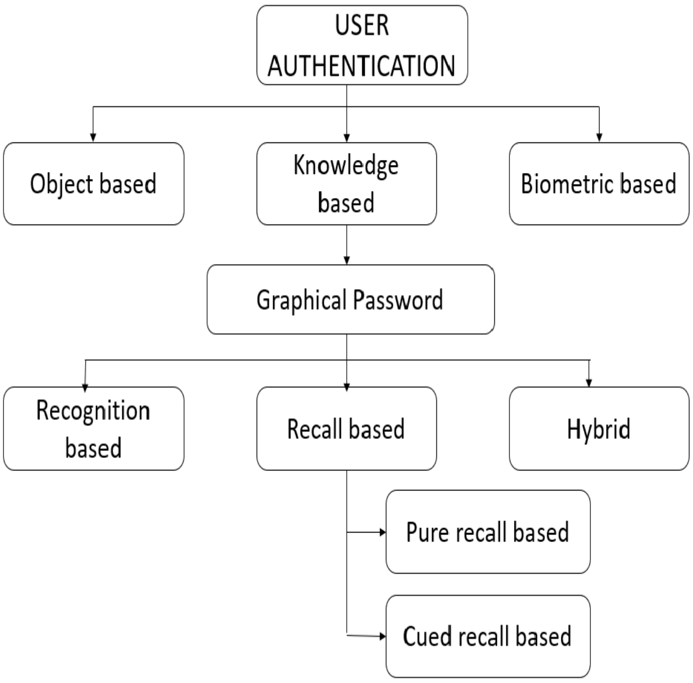

Fig.1: User authentication techniques

## 2. CATEGORIZATION OF GRAPHICAL PASSWORD-BASED SCHEMES

The Graphical authentication schemes are broadly classified into four classes, they are:

### *A.* Recognition-based Graphical Scheme

In this system, during the authentication process, all the users are requested to remember the images during the password generation. During the process, a series of images were displayed and request the userto recognize the set of images in the login section. All the images are selected in the appropriate order and this was discovered based on remembering the password. It was developed based on the authentication process that is easy and reliable for the user. It should not allow the user to have a weak password and it should be difficult to guess. It is based on three processes such as training, portfolio creation and user authentication. Normally, graphical schemes do not allow input in typewritten format instead of this it uses authentication which is more effective than passwords [4]. This provides extra security over passwords. In this scheme, it makes a story to the user in the form of images to remember the passwords. At last, it provides authentication to get authenticated.

Another method is the cognitive authentication scheme which is against shoulder surfing attacks and spyware. At the registration process, set of images provided to the users and they are requested to choose some images as a password for authentication. For accessing the particular system, a set of images is prescribed to choose and they choose around the screen by moving right, left and down the images. Users can try for a certain number of rounds, if the user has reached a certain limit then the login is failed. Another technique also based on the cognitive system which is also known as use your illusion. This provides recognition based on the selected images [8]. It also consists of three methods such as portfolio and authentication. During the process, a series of images is randomly selected by the user and the user can upload any images from the drive. After selecting the images then it is moved to the authentication deviceand distorted using a lossy filter. Once the portfolio is created, it runs for the memory improvement ofimages. All the users can see the original images during the session. If the user enters the wrong passwords thenthe system will provide feedback. In the authentication phase, the user needs to enter the correct password. It is difficult to recognize when the image is distorted [10].

### *B.* Pure-recall-based Graphical Schemes

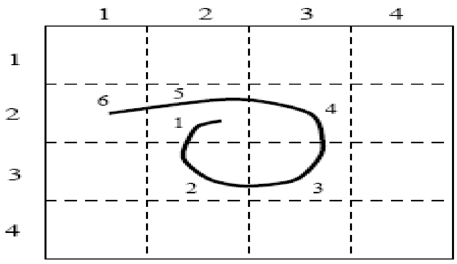

Fig.2: Draw-a-secret method

This scheme also referred to as the draw-metric system in which user recalls and produces a secret drawing. In this user draw their own selected passwords in the blank space. Then another technique isknown as Draw a secret (DAS) as in fig.2, this allows the user to draw the password in the blank space or inthe grid [9]. For authentication, it requests the user to redraw the password otherwise the access is denied. There are different methods in DAS such as PassShapes [11] in which the password is converted into alphanumeric characters. Moreover, DAS is redesigned differently and it is known as Qualitative Draw a Secret (DQAS) which uses the grid to hide the creation of a password and it is considered as the safe technique for Shoulder-surfing attack.

### *C.* Cued-Recall-based Graphical Schemes

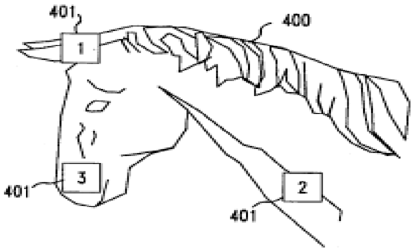

Fig.3:Blonder scheme

These schemes are mostly used to reduce the memory and usability and make the user to remember and to specify target locations within the images. For authentication, the user has to right-click the position. Then another technique is known as the Blonder scheme [12] which consists of predefined images on the screen and sets a particular point as a password. Then the PassPoint [2] technique used as the recent version of the Blonder scheme. In this method, the user can choose any picture as their password but here the pictureis not considered as the password. The point in which the user selects on the image is considered as secret. The user can choose any points on the image and for authentication, the user can click to any point on the picture for accessing.

### *D.* Hybrid Graphical Schemes

A hybrid scheme is normally used to overcome the defects by combining one or more techniques to design a new technique that is used to guard against some vulnerable attacks. It is considered as the combination of one or more techniques. This technique consists of images for creating the password. There are many methods in the hybrid scheme if the users want to strengthen the password it combines text with graphical passwords. An alternate method of a hybrid system for the authentication process consists of two steps i.e., authentication and registration. During the registration process, the user is requested to type the password and username and it is stored in the database. In the authentication phase, the user has to select a minimum of four objects for password creation. Another scheme known as GRAMAP which uses the map as password and it consists of three different methods for password authentication schemes such as click point selection, image selection, and map navigation [1]. The main highlight of this system the user can increase or decrease the number of levels as per the requirements of the user. So, the user can change their password at any time. While the creation of a password, the user has presented the map which has seven continents. In that, the user has to select one continent as their password and then the country is displayedfor selecting. Then the user has to select aminimum number of points for passwords. The user has tocomplete all the stages for authentication.

## 3. ALGORITHMS USED FOR GRAPHICAL SCHEMES

### *A.* Randomized algorithm

An algorithm that uses a degree of randomness as a logic. It has deterministic time complexity also. The Randomized algorithm is simple and faster and makes a good decision for a problem. Using the degreeof randomness which gives average-case behavior and efficient solutions for the problems. One has to differentiate between algorithms that use the random input so that they always end with the correct answer, but where the expected running time is finite, and algorithms that have the chance to produce an incorrect result by either signaling a failure or failing to stop. In some cases, the only practical means of solving a problem are probabilistic algorithms.

### *B.* Press touch finding algorithm

When a consumer receives a PT — it produces a peak. Thus, those two words are used interchangeably in the rest of the discussion. With some modifications, any appropriate 1-D Point finding algorithm could be used as Press Touch Finding Algorithm (PTFA). One noteworthy change is that thePTFA must always discover local maximum points, instead of discovering a global optimum value. Besides,it must also count the number of peaks, as it is the PTC given by the user during the authentication session. The PTFA algorithm here makes a simple assumption when it comes to finding the peaks, that if any pressure

$$\mu'_{t_{i-1}} < \mu'_{t_i} > \mu'_{t_{i+1}}$$

strength value exists,µ0 ti is greater than its adjacent neighbors, it is a peak.

The PTC is increased by 1 every time a peak is reached, which was initialized as 0 before theprocess commenced. Once all the peaks are found, they are called the PTC and stored in a register [13]. The PTC for this sequence is 10 since there are 10 peaks. Later, the user (who registered this PTC) has to rememberthe value during the authentication process and have to provide the same number of force presses on the computer. Therefore, this approach falls under the principle of knowledge-based authentication.

### *C.* VAP code

The vibration technique is currently available on most Android devices, and convert it into a newtype of code, called the Vibration Code, which is compatible with the authentication process. The VC couldbe used as a standalone authentication scheme where a user initially generates a verification signature η, which is essentially a single VC that is stored for future verification purposes within the program. When that user tries to unlock the screen, he/she must repeat the code next time. If and only if the VC obtained at the current session is equal to the one recorded before, the user will be able to unlock the screen, if and only if, the acquired VC at the current session, η' matches with the registered η, i.e., η' = η [14].

### *D.* Syukri algorithm

-

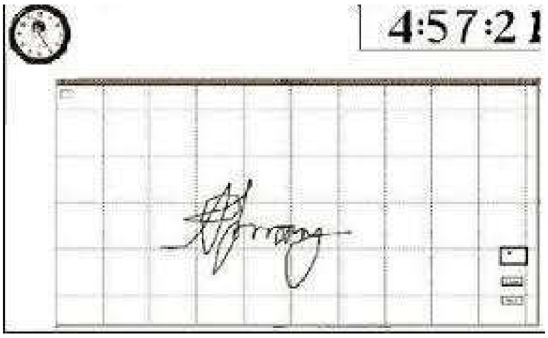

Fig.4:Syukri algorithm

The Syukri algorithm proposes a method in which the user obtains authentication using a mouse to draw his signature. This method is composed of two phases: registration and verification. To begin with, the user is asked to draw his signature with a mouse during the registration stage, this is followed by the system extracting the signature area and either expanding or scaling-down signatures and rotating if necessary [12].If possible, and rotating (also known as normalizing). After this, the data is stored in the database. The verification stage starts with obtaining the user input, on which the normalization is repeated; afterward, it extracts the signature parameters. The program essentially uses geometric mean and dynamic database changes for verification purposes. The rate of successful verification has been satisfactory, based on the study undertaken. The main benefit of this approach is that not only is there no memorization requirementfor one's signature, but it is difficult to come up with falsified signatures.

## CONCLUSION

There are some disadvantages with the text-based password, such as dictionary attacks and brute force attacks. Likewise, the shoulder-surfing attack is a major problem with the graphical password. The existing graphical password schemes are yet immature. To overcome all these drawbacks can be overcomeby using graphical authentication methods which can be easily adopted by all types of users.

The main purpose of this survey is to help people to know about the various graphical schemes that will be so easy to remember for authenticating an application securely. In case, if the user forgot password, it can also be easily changed in a secured manner by the proper authentication process.

## REFERENCES

1. Khan, M. A., Din, I. U., Jadoon, S. U., Khan, M. K., Guizani, M., & Awan, K. A. (2019). g-RAT| A novel graphical randomized authentication technique for consumer -smart devices. IEEE Transactions on Consumer Electronics, 65(2), 215-223.
2. Azad, S., Nordin, N. E. A. C., Ab Rasul, N. N., Mahmud, M., &Zamli, K. Z. (2019). A Secure Hybrid Authentication Scheme Using Passpoints and Press Touch Code. IEEE Access, 7, 166043-166053.
3. Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes.” in USENIX Security Symposium, vol. 13, 2004, pp. 11–11.
4. Weinshall, “Cognitive authentication schemes safe against spyware,” in IEEE Symp. Security and Privacy, 2006, pp. 6–pp.
    a. De Angeli, L. Coventry, G. Johnson, and K. Renaud, “Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems,” Int. jour. human-computer studies, vol.63, no. 1, pp. 128–152, 2005.
5. Hayashi, R. Dhamija, N. Christin, and A. Perrig, “Use your illusion: secure authentication usable anywhere,” in Proc. 4th ACM symposium on Usable privacy and security, 2008, pp. 35–45.
6. T. Pering, M. Sundar, J. Light, and R. Want, “Photographic authentication through untrusted terminals,” IEEE Pervasive Computing, vol. 2, no. 1, pp. 30–36, 2003.
7. W. Jansen, S. I. Gavrila, V. Korolev, R. P. Ayers, and R. Swanstrom, “Picture password: a visual login technique for mobile devices,” NIST Interagency/Internal Report (NISTIR)-7030, 2003
8. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and analysis of graphical passwords.” USENIX Association, 1999.
9. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, “Yagp: Yet another graphical password strategy,” in IEEE Computer Security Applications Conference (ACSAC2008), 2008, pp. 121–129.
10. Khan, W. Z., Aalsalem, M. Y., & Xiang, Y. (2011). A graphical password based system for small mobile devices. *arXiv preprint arXiv:1110.3844*.
11. Lashkari, A. H., Gani, A., Sabet, L. G., &Farmand, S. (2010). A new algorithm on Graphical User Authentication (GUA) based on multi-line grids. *Scientific Research and Essays*, *5*(24), 3865-3875.
12. Ranak, M. N., Azad, S., Nor, N. N. H. B. M., &Zamli, K. Z. (2017). Press touch code: A finger pressbased screen size independent authentication scheme for smart devices. *PloS one*, *12*(10).
13. Azad, S., Rahman, M., Ranak, M. N., Ruhee, B. K., Nisa, N. N., Kabir, N., ... & Zain, J. M. (2017). VAP code: A secure graphical password for smart devices. *Computers & Electrical*

*Engineering*, *59*, 99-109