Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Authentication System Using Human Behaviour against Objects

Ratna Deepthi Dasika*
Department of CSE
Geethanjali College of Engineering & Technology
Hyderabad, India

Sujanavan T
Department of CSE
MVSR Engineering College
Hyderabad, India

Abstract— We introduce a novel authentication system utilizing the psychological behaviour and/or attitude of human beings to solve many open authentication issues of the current scenario. The proposed system involves the reaction of a human being against different objects at a given situation. The features & status of the objects interacted with are then converted into a virtual password, which is used for authorization. At present, many authentication systems have major backdrops as they utilize a uni-variable dependency e.g., textual passwords, biometrics, graphical passwords etc., In this paper, we present an authentication system with a password dependent on multi-variable which is simple-to-use, more secure and a solution for various authentication issues.

Keywords— Authentication system; psychological behaviour; textual passwords; biometrics; graphical passwords

I. INTRODUCTION

The current authentication systems are unable to solve the security issues, as they are totally dependent on a single token or a variable. This not only increases the risk of intruders but also decreases the trust of the users on the industry [1-3]. There are different kinds of security mechanisms that are developed in the past which are vulnerable as they rotate around a single variable dependency e.g. textual passwords, graphical passwords, token based systems (RF-ID) & even biometrics [4-9]. Hence, we are in need of a multi-variable system that could solve the present situation.

Authentication has become an essential part of the life that we come across, not only at the WWW (World Wide Web) but also at bank ATMs and even in home security systems. It became a very difficult task for the user to remember all such passwords used. Sometimes a user needs to remember more than just a password to authorize, which leads to an increase in unsatisfactory complains. Our system solves this issue of forgetfulness and dissatisfaction of the users as the user does not require remembering anything [10], [11]. The system implemented is linked with the psychology of a human against reacting towards different things [12], [13]. The attitude of a human does not change frequently which creates an optimal solution for the issues faced in the past authentication systems.

The past authentication systems involve a kind of reproducing a secret which was solved by the biometrics model. The biometrics model also had its own disadvantages of consistency (trouble in identifying the legitimate user when his finger had a cut or a foreign material), uniqueness & acceptability [14], [15].

The system proposed and implemented in this paper does not involve a direct recall (user does not even know that he is recalling his past memory) and could also involve the entire past authentication systems, so far developed. Hence, the system suggested is a break-through idea in the revolution of authentication systems, which includes indirect intelligent behaviour of the end-user.

The remainder of this paper is organized as follows: Section II discusses related work. In Section III, we introduce the system and its implementation. Section IV is an elaborate discussion on security analysis including possible attacks and countermeasures. Section V presents the experimental conditions. Finally, in Section VI, we conclude and confer the future work.

II. RELATED WORK

After the degradation and dissatisfaction of the textual passwords, there was a sudden change brought by the graphical passwords methodologies. They could be differentiated based on two mechanisms, either recall or recognize e.g. Pass-faces[16], pass-points, DAS (Draw a sketch) etc., Though the graphical password was a great invention, it could not withstand the shoulder surfing attack [17], [18].

The popular apple I-phone application for authentication “Pass-faces” is a famous graphical password that involves in selecting a face (that is mentioned previously through a secure channel) from a set of faces projected on the mobile screen.

The pass-point method is a recall method where the user needs to select different points on a picture that resembles his password. The DAS (Draw a sketch) method also falls in this category where the user needs to draw his login sketch on a grid (5x5, 10x10 or 25x25). The login involves in identifying the lines that pass through the different grids present on the screen.

© 2014, IJARCSSE All Rights Reserved

Biometrics authentication system even though became popular with a short start, still, people are afraid of using it as it involves in recording the user's physical aspects posing a threat to his/her privacy. In addition, some users resist the idea of low intensity infrared light or any other kind of light directed to their eyes, such as in retina recognition systems. Moreover, biometrics cannot be revoked, which leads to a dilemma in case the user's data have been forged. Unlike other authentication schemes where the users can alter their password at the time of threat to privacy the user's biometrics cannot be revoked.

Many authentication systems are based on tangible objects and are referred to as token-based systems. Many token-based systems are vulnerable to theft and loss [2]; therefore, most token-based systems require a personal identification number followed by a textual password for authentication e.g. a debit or a credit card.

The proposed system has a great flexibility to involve all the above systems along with the psychological characteristics of the human being.

III. IMPLEMENTATION

The construction of the system involves the training of two different parameters followed by the final convergence with the programming.

A. Training the human psychology

To understand the human behaviour / attitude [12], [13] a keen observation has to be made by the system designer while preparing the questionnaire for which the user gives responses for his authorization process.

The humans do possess a change in behaviour while approaching new processes. When there is a new process the human begins with a pessimistic stage, undergoing different stages towards his successful goal reaching the optimistic stage.

The beginning of every process does involve learning and facing-complexities for the human mind to undergo due to which one either succeeds the goal or fails in approaching it. There are different intermediary stages that are between the start and the end in the life cycle of pessimism-optimism chart, shown in Fig. 1 (from [12]). Hence, our methodology should involve intermediary stages where the human could be easily successful and build confidence to approach for the next.

The system is designed in such a manner that the human could develop his attitude in a step by step process leading towards a stage of optimism. Indirectly the system is developed on the user choice of a password [11] projecting the relationship between his/her attitude and the authentication process. The person first starts accepting the situations that could occur then realizes some expectations of convenience that builds up belief, in the progress leading to the successful completion of a comfortable [10] authorization process, see depicted diagram in Fig. 2 (from [13]). If the above discussed sequential flow is to be achieved then a lot of effort is involved in developing the interface for the user.

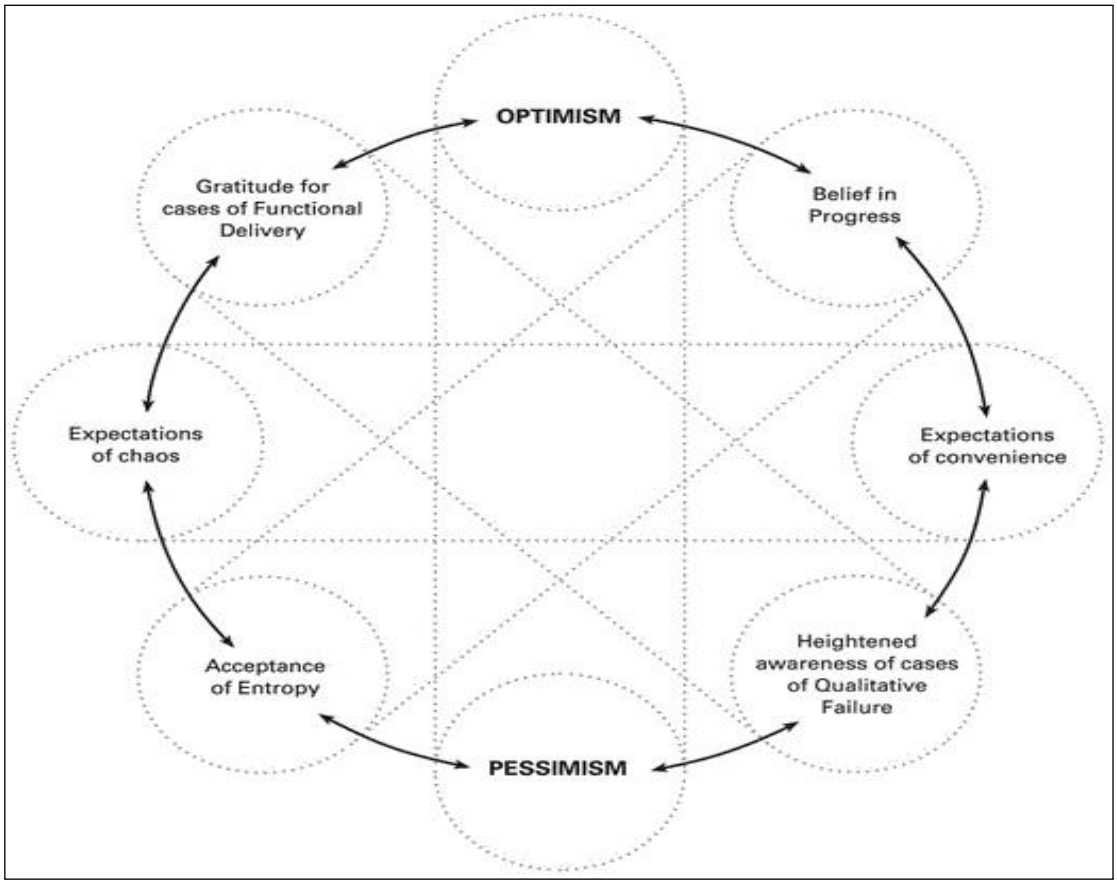

Fig. 1 The pessimism-optimism cycle of a human behavior and the different intermediary stages involved among the two.

© 2014, IJARCSSE All Rights Reserved

Fig. 2 The progressive motivation cycle of the human behavior against both good and bad effects towards an approach to goal.

B. Training for design & placement of objects

The interface development, unlike any other application involves the thorough knowledge regarding psychology of human attitude failing which could lead to the behavioural flow of the human back towards the pessimism stage. The design and placement of objects on the interface screen not only involves a comfortable authentication procedure but also helps the system to easily detect the genuine access.

Selection of the scenario also plays a major role in building the artificial environment. There are different aspects that should be taken care off while considering an environment and its relative objects. The environment singly does not reveal a scenario but the objects it contains reveals a thought in the human mind e.g. a group of objects involving cutlery and cooking electronics reveals that it is a scenario of a kitchen and not of a bathroom. Hence, choosing and lying of the objects reveals the scenario of the environment and the vice-versa is never true.

In order to develop a virtual environment (Fig. 3 depicts different stages involved in designing the interface of the system) about selected scenarios the following steps are to be executed in sequence.

1) Gathering the objects: Objects gathered for different scenarios are to be grouped in such a manner that it does not cause any confusion in the human mind while looking at them on the interface.

The objects selected are also required to follow the basic principles of view, which includes inclination [19], height and possible existence at a location e.g. a door cannot open from a ceiling and a window cannot open up from a floor.

The following principles are to be maintained

1. Objects should be represented as a part of the environment
2. Objects when projected together as a group should reveal a scenario
3. Objects should be recognizable
4. Object's features should be easily understandable
5. Objects should not be alien in nature
6. Object's existence should contribute a purpose
7. Objects should not be duplicated in larger quantity

2) Merging objects for setting the resolution: A group of objects are considered to build one scenario. Different scenarios could have the similar objects related to other group e.g. lights and fans are seen in a bedroom, an office and a drawing room.

The following steps are self-regulated that are to be completed in a sequence

1 Load the objects on a blank image file

© 2014, IJARCSSE All Rights Reserved

2 Setup the scenario using the objects
3 Adjust the heights and inclination of the objects
4 Adjust the required resolution of the scene (either mobile / desktop)

After completing the above steps successfully, the scenario is to be keenly observed for any misperceptions that could take place.

3) Partitioning the scenario: The system involves the "divide and conquer" mechanism where the objects are, at first, divided into different parts and later loaded together. The scenario that forms with the merging of the objects is interfaced independently by the user for the final authentication process. Hence, partitioning the scenario plays an important role in user access.

Partitioning is done so that the following requirements are fulfilled

1. Object along with the empty space up to the division is a single file
2. No specific object is left un-partitioned except for the last
3. Division is done so that reload does not involve noise in the scenario
4. Image storage compatible standards must be followed

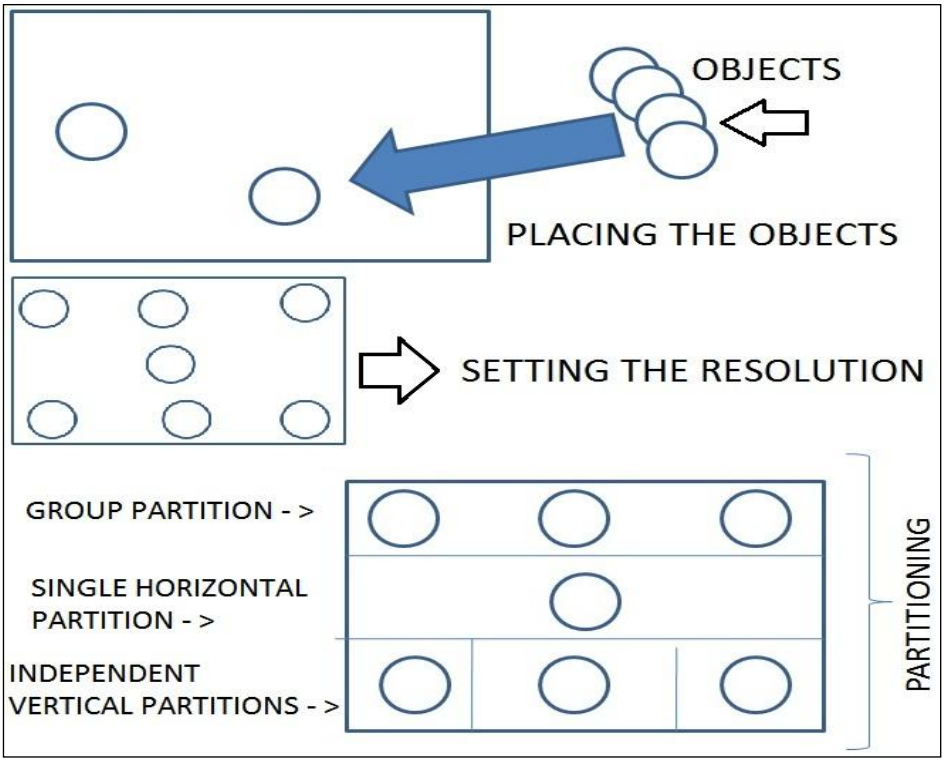

Fig. 3 Different stages involved in designing the interface of the system. (a) Involves placing of the objects according to their view and inclination principles (b) setting up the resolution i.e. either required for a desktop or a mobile (c) represents partitioning and the different partitioning methods that could take place.

C. Final Convergence

The psychological factors are merged with the graphical objects in the environment. This environment in turn acts as an interface towards the human behaviour and sample of such an environment is shown in Fig. 4.

Each object is related to a set of features it includes e.g. a fan could involve features like switching it on / off or varying its different speed levels. Features differ from object to object and dissimilar objects are distinct not only in the number of features and the differences exist in their features but also on the variation of their access. Consider a scenario where a set of electronic devices e.g. a television connected with a music system and a disc player be present in a single partition but the method of access would vary.

Convergence does not only involve simply loading the images, but it also carefully observes how a user approaches to access a partition, followed by accessing the features involved behind it. Hence, programming such confusing situations includes a broad mind and training behind the accessing algorithms. User easy access indirectly projects a major effort involved behind the scenes in positioning the objects and capturing the behaviour. The system flow is depicted in Fig. 5.

Later, the status of different objects captured (in a temporary database) is compared to the user's initial preferences (in the main database) and a final conclusion regarding authorization is taken.

© 2014, IJARCSSE All Rights Reserved

Fig. 4 A sample virtual environment from the implementation of the system

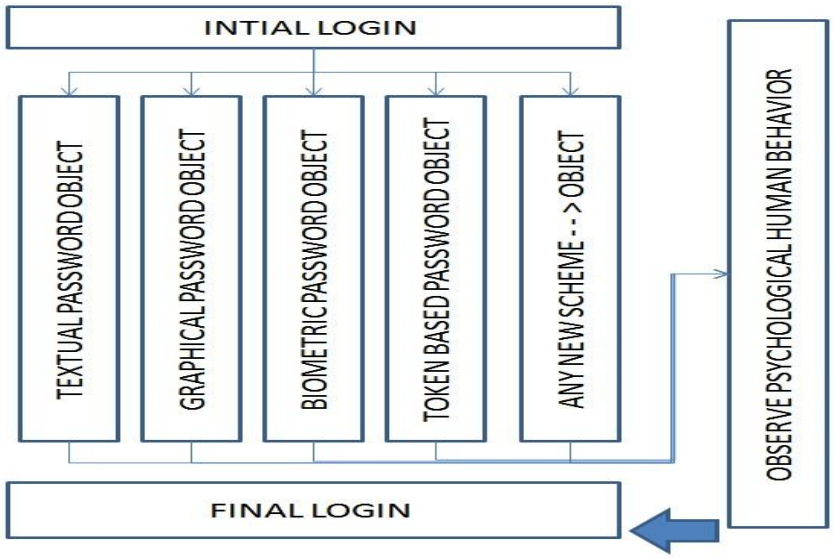

Fig. 5 System flow - The flow of sequence of the background process involved in the system. At first the user faces an initial login followed by selecting objects and changing their features. The different authentication systems that could be involved as objects are shown as above. Finally the observation program captures the psychological behavior and generates a final login decision.

IV. SECURITY ANALYSIS

In order to analyze how tough is a security algorithm, the best way is to crack it, open without knowing the password. Even though the proposed system looks simple, it is very hard to knock it down as it results in equally cracking down all the security programs possessed by the system. Still the hacker needs a huge amount of knowledge and data to gain that is impossible, as the state and attributes of the items are kept hidden even to the legitimate user and sequence is hidden from the administrator/working staff at the security company. There are also some organizations that provide a validation process for the authentication systems.

Still referring back to the standard principles of estimating the crack time by just looking at the password size even then, as the size of the password generated is huge compared to other algorithms, it makes impossible to be cracked.
The password size of the proposed system is explained below.

Consider,
PS(max) = maximum password size
S(a)= selections made over an item ‘a’
SC(a)= item ‘ a’ state changes undergone
S(b)= selections made over an item ‘b’
SC(b)= item ‘ b’ state changes undergone
So on…
S(n)= selections made over an item ‘n’
SC(n)= item ‘ n’ state changes undergone
Mii= Maximum objects involved behind an item
Mf= Maximum features of an item

© 2014, IJARCSSE All Rights Reserved

Then, the total number of passwords that could be generated can be calculated using the following formula

$$\prod(PS(max)) = \sum_{np=1}^{np=Mii(a)} (S(a))np \;.\; \sum_{np=1}^{np=Mf(a)} (SC(a))np$$

$$+$$

$$\sum_{np=1}^{np=Mii(b)} (S(b))np \;.\; \sum_{np=1}^{np=Mf(b)} (SC(b))np$$

So on…

$$+$$

$$\sum_{np=1}^{np=Mii(n)} (S(n))n \;.\; \sum_{np=1}^{np=Mf(n)} (SC(n))n$$

When, the above is compared to the rest of the algorithms, it could be observed that though the length of the password is small, the size of the password is very huge.

V. EXPERIMENTAL CONDITIONS

The project requires a large amount of data to be transported. In order to have a high speed data transfer for communication, we reduce the overhead by utilizing Java server pages concept. The object environment also does not require any high-end graphics, as they are manually selected images positioned at different angular views.

The back-end database has no much relation with the intermediate program and could be easily constructed over other platform. The server requests are managed by apache tomcat, which also could be replaced by any of the available industrial server software and has no role in the intermediate code [20].

A simple web-browser that supports the http / https protocols with Java support (found in many of mobiles e.g. Opera mobile, tea shark, fire-fox mobile, bolt etc…) could be enough for handling the authentication program.

VI. CONCLUSION AND FUTURE ENHANCEMENTS

The human behaviour / attitude never changes, hence, it provides a typical & simple method to detect the uniqueness of psychology in solving the present authentication issues.

The simplicity of the foreground reflects the complexity and effort at the background development. This shows that the algorithm is difficult to crack-in, as it does not involve any direct input. The change of the scenarios also confuses the attacker in solving the actual password. This leads to a better approach in avoiding breakage of the system by any external or internal intruders.

There could be enhancements performed on this project involving more graphical movement i.e. involving active component than passive ones.

The present system solves all the issues related to the past algorithms ([2],[10],[14],[15] and [18]) by efficiently utilizing them, keeping in mind their disadvantages, hence, building a user friendly, safe, secure and easy to use authentication system that could be applied to all fields.

Many of the major authentication systems do suffer a lack of confidence against shoulder surfing attacks. Our present system has the option to easily introduce any new scheme as a part of the environment to avoid such vulnerability thus, solving the present major authentication problem.

The discussion made in the above paragraph could be a matter of future work, involving a research in overcoming the attack that could be an enhancement of the present work.

REFERENCES

[1] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.
[2] ATM fraud- Banking on your money - Dateline NBC - Consumer Alert available on http://www.msnbc.com
[3] Shopping Scams - CBS News - Nov 16, 2010
[4] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.
[5] Norman Fraser Ph.D. "The usability of picture passwords" Tricerion Group
[6] Regunathan Radhakrishnan, Nasir Memon "On The Security Of The Sari Image Authentication System " 2002 Polytechnic University, Brooklyn.
[7] Ankesh Khandelwal, Shashank Singh, Niraj Satnalika "User Authentication by Secured Graphical Password Implementation " *International Journal of Computer Applications* (0975 - 8887) Volume 1 – No. 25, 2010
[8] Fabian Monrose and Michael k. Reiter "Graphical Passwords" ch09.10346 Page 161 Friday, August 5, 2005
[9] What is 3D Password Scheme available on http://www.technospot.net

© 2014, IJARCSSE All Rights Reserved

[10] Anne Adams and Martina Angela Sasse "Users Are Not The Enemy. Why users compromise computer security mechanisms and how to take remedial measures" *Communications of The ACM* /Vol. 42, No. 12 December 1999

[11] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th USENIX Security Symp., San Diego, CA*, pp. 1–14, Aug. 2004.

[12] William McDougall *Psychology: the study of behaviour* , 1914.

[13] William James *The Principles of Psychology*, 2007.

[14] Duc Nguyen – BKIS, Vietnam, Your face is not your password available on http://www.bkav.com.vn

[15] VIRDI- How to make the fakefingerprints available on http://www.shareshare.com

[16] Hugh Davies - Inventor of the Pass faces user authentication system available on http://www.passfaces.com

[17] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Proc. 21st Annu. Comput. Security Appl. Conf*erence, pp. 463–472, Dec. 5–9, 2005

[18] Jinhai Wu1, Bin B. Zhu2, Shipeng Li2, Fuzong Lin, " New Attacks on Sari Image Authentication System" State Key Lab of Intelligent Technology and Systems, Beijing, Microsoft Research Asia.

[19] Brøderbund (1990) 3D Home Architect available on http://www.3dhaonline.com/

[20] RACCOON (the mobile apache tomcat) available on http://sourceforge.net/projects/raccoon/

© 2014, IJARCSSE All Rights Reserved