A Highly Reliable User Authentication Using Imagen and Biometrische Key Values

[1]R. ArumugaArun, [2]F.M. Blessina Pearly, [3]K. Lizzy
[1,2,3]Dept. of CSE, Loyola Institute of Technology, Chennai, Tamil Nadu, India

Abstract
This paper provides highly reliable security mechanism in online process. This paper is fully concentrating on User Authentication .If we are allowing authenticated users only to access the process means most of the security problem will be solved .This paper increases the amount of authentication checking process .This paper introduces authentication verification process in two levels (L1,L2). In the authentication Level 1, it uses Imagen Values. Users are generating these Imagen key values by selecting hotspot positions on images. Authentication Level 2 uses two Alpha Numeric codes namely, TCG, ITC. These codes are highly secured and reliable because, these code values are created using users direct interference. On the success of authentication Level1 only ITC will be generated by using TCG and with the user's Biometrische key values. This ITC is valid only for particular time span. Using ITC Authentication Level 2 is verified.

Keywords
TCG- Transaction Code Generator, ITC- Individual Transaction Code, CAPTCHA-Complete Automated Public Turing Tells To Computer and Human Apart

I. Introduction
A foundation talk in security is to create cryptographic primitives based on hard mathematical problems that are computational intractable using hard AI (Artificial Intelligence) problems for security is initially proposed is an exciting new paradigm. Under this paradigm, the most important primitives invented is CAPTCHA which distinguishes humans from computers by displaying a challenge, (i.e.) a puzzle beyond the capability of computers but easy for humans CAPTCHA is now a standard internet security methodology to protect online attacks. In this paper, we implement two level of Authentication where Imagen Values and Biometrische values are used.

A. Imagen Key Values
Imagen values means that clue click points on the images. Generation of Imagen values is happened during registration phase. Here five Imagen values generated. This Imagen values are processed on the basis of x and y axis point values of the images. During the login phase if the Imagen values are wrongly selected or clicked it shows an error message and proceeds back to the login page.

B. Biometrische Key Values
Biometrische key value means user finger print values. These key values generated during the registration the process. And these bometrische key values are used to generate ITC. This Biometrische values are highly reliable because without users it cannot be created.

C. Transaction Code Generator
It is a 4 digit alphanumeric code. This TCG generated using the beneficiary name, account number and the transaction time. This TCG are needed to generate ITC.

D. Individual Transaction Code
It is 6 digit alphanumeric codes. This ITC generated using TCG and Biometrische values. This code is session based. Because it is valid only for particular time period (15 Minutes) and after that time period ITC will be expired. This ITC is highly secure it cannot be created without direct user presence.

II. Related Work
For the implementation of this paper, we have reference with below related ideas. First and foremost, the user is validated with a username. If the user name is already registered, then it displays the registered imagens and verifies the point values of the imagen [3]. If the imagen values are correct, and co-ordinates are verified, the user profile details are displayed. If the user is a new user, then registration should be done first. Otherwise the user name do not match with the user's name with the database then the page will be directed to the login page

A. Existing System
In the existing system, a security primitive based on hard AI problms which is called CaRP (Captcha as Graphical Password). CaRP is click-based graphical passwords where a hotspot s clicked in a sequence of images [1,4]. In CaRP, the user has to register their name, mail-id, password and five images where the user has to click the key point which is already registered. In this paper, only one authentication level is used which can be insecure in future times. In existing One Time Password (OTP) used as second level authentication. OTP is alphanumeric codes [11]. This OTP code is generated and sent to the registered mobile number, but the disadvantage is that if the mobile phone network is not available means OTP will not be received, even though the OTP is generated and sent. This OTP is session based Key. Due to the mobile network problem, sometimes it reaches the user after session period. So OTP becomes invalid. Another disadvantage is if the hacker theft the user mobile phone means hacker can use the users account. Even though OTP is a highly secure it can be hacked.

IV. Experimental Work

A. Proposed Work
In our proposed work, we are going to provide a hybrid security primitive to make the authentication more secure and reliable. We introduce two level authentication method where Imagen and Biometrische values are used.
In authentication L(1), the user has to login by their user name if they are already registered. During the login, registered images will be displayed to the user in order to view the user profile. If the first Imagen value is correctly selected means it proceeds with the next Imagen and also if the second Imagen values are also selected correctly means the user has to enter the text password that will be registered during registration. If the user has entered the wrong text password it shows an error message and redirects to the login page. If the user has entered the correct password, it displays the user profile details. The user profile has all the details

regarding the user account.

If the user opts for money transfer in the given options, they have to click generate TCG icon. TCG (Transaction code Generator) is a 4 digit alpha numeric code which is based on user account number, beneficiary account number and time & date. The TCG will be displayed in the screen within some seconds and a link will be sent the user's mail id. The user has to login into their mail and open that link. That link redirects to a page where the TCG code has to be entered and ask randomly two fingerprints. If the entered TCG and two finger prints are correct, it generates ITC (Individual transaction code). The ITC is an alpha numeric code which is completely based on TCG code, two finger prints and date & time of the transaction. The ITC will be generated for each and every transaction of the user. The ITC is similar to TCG code as it will valid till two hours from the time the code is generated.

In Authentication L(2), the user has to enter their account number, beneficiary account number, amount to be transferred, and ITC. If all the above details are entered correctly, the amount will be transferred to the beneficiary. But if any one of the details is entered wrongly it shows an error message and redirects back to the login page. It also sends a notification message to the user's mail id that your account was accessed. Only 3 attempts will be provided for each user, if login attempts are wrong the user's access will restricted for 24 hours.

V. System Design

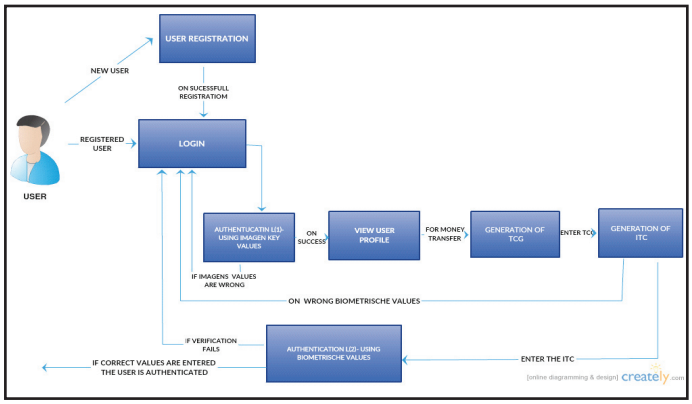

Fig. 1:

A. List of Phases

It contains six phases

- Registration phase
- Generation of Imagen key phase
- Authentication l (1)-using Imagen key phase
- Generation of TCG phase
- Generation of ITC phase
- Authentication l(2)-Biometrische key phase

B. Registration Phase

In the registration phase, the user has to register the primary details like user name, mail-id, mobile no, address, account number, branch number as well as user asked register the biometrische values. Biometrische values means that user's then finger print values. Here use mail id, contact number, account number and biometrische values are mandatory and user have to give the exact details. As in the upcoming phases, process will communicate with users through this. After the registration a notification message will be sent the user's mail id and mobile number that your registration is successful.

C. Generation Of Imagen Key Values Phase

After the registration, the users have to create Imagen key values. Users have to create 5 imagen key values. Imagen key values means that clue click points on images. So the users should click on the image to create key values in all the five registered Imagen key values. The key values will be processed based on the x and y axis values. At the time of login the users have to give the same imagen values what they have given during generation of Imagen values. The registered imagen key values information are stored in the database.

D. Authentication L(1) - Using Imagen Key Values Phase

The user has to login their profile using user name. If the user is registered already, it displays the Image registered during the registration. The user has to give the correct imagen values. In order to give the correct imagen values, it proceeds with the text password. And if the text password is correctly entered, it login into the users account and can view all the details like last transaction, available balance, credited amount, paid bills, money transaction, etc., Suppose the user the give wrong imagen values three times means, the account will be blocked for next 24 hours and the information will be sent to the user registered contact number and mail id. If the user has to transfer money from their account, they have to opt for money transaction option.

E. Generation of TCG Phase

The money transfer opens a new page and has an option as generate TCG which will be generated. The TCG is a 4 digit alpha numeric code which is based on the account number, beneficiary account number and time & date. The TCG code will be generated within some seconds and will be displayed in the user screen. During the generation of TCG, it will also dispatch a link to the user's registered mail. That link proceeds to a web page, where the user has to enter the TCG code and two Biometrische values have to be verified. The Biometrische values may be of any two fingerprints like left thumb, right index etc.

E. Generation of ITC Phase

If the user is verified successfully, it proceeds with the generation of ITC. ITC is generated for the individual money transaction of the user. The ITC is a 6 digit alpha numeric code which is completely based on TCG code, user biometrische values and date & time of the user's transaction. The ITC is also similar to TCG code which is valid only for particular time span.

F. Authentication L(2)-Biometrische Key Phase

In authentication L(2), the user has to enter the generated ITC, beneficiary account number, amount to be transferred. If all the details are correctly entered, mentioned amount will be transferred to the beneficiary. If not entered correctly, then user will be displayed with an error message and the page will be redirected to the login page. If the user is redirected to login page for more than 3 times, their access to login will be restricted for next 24 hours and the notification message will be sent to the user's id that your account was blocked.

VI Conclusion

In this paper, Two level of authentication checking is used. The imagen key values and biometrische key values plays major role in these two level of authentication verification process. These two key values are graphical passwords. In overall, this concept

one step ahead in existing security process because these two key values will not be created users direct interference.

References

[1] I.Jermyn, A. Mayer, F. Monrose, M. Reiter, A. Rubin, "The design and analysis of graphical passwords," In Proc. 8th USENIX Security Symp. , 1999, pp. 1–15.

[2] R. Dhamija, A. Perrig,"Déjà Vu: A user study using images for authentication," In Proc. 9th USENIX Security, 2000, pp. 1–4.

[3] G. Mori, J. Malik,"Recognizing objects in adversarial clutter", In Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit., Jun. 2003, pp. 134–141.

[4] H. Tao, C. Adams,"Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, Vol. 7, No. 2, pp. 273–292, 2008.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, N. Memon,"PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, Vol. 63, pp. 102–127, Jul. 2005.

[6] P.C.van Oorschot, J.Thorpe,"On predictive models and user-drawn graphical passwords," ACM Trans. Inf. Syst. Security, Vol. 10, No. 4, pp. 1–33, 2008.

[7] M. Szydlowski, C. Kruegel, E. Kirda,"Secure input for web applications," In Proc. ACSAC, 2007, pp. 375–384.

[8] G. Wolberg,"2-pass mesh warping," In Digital Image Warping. Hoboken, NJ, USA: Wiley, 1990.

[9] HP TippingPoint DVLabs, New York, NY, USA. (2011). the Mid-Year Top Cyber Security Risks Report [Online] Available: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-7045ENW.pdf

[10] S. Kim, X. Cao, H. Zhang, D. Tan,"Enabling concurrent dual views on common LCD screens", In Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 2175–2184.

[11] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi R. Schmitz,"Breaking e-banking APTCHAs," In Proc. ACSAC, 2010, pp. 1–10.

[12] H. Gao, X. Liu, S. Wang, R. Dai,"A new graphical password scheme against spyware by using CAPTCHA," In Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.

[13] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," In Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.

[14] J. Bonneau,"The science of guessing: Analyzing an anonymized corpusof 70 million passwords," In Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.

[15] John the Ripper Password Cracker [Online] Available: http://www.openwall.com/john/

Mr. R. Arumuga Arun, M.E Received his B.Tech degree in the department of Information Technology from Vel Tech Multitech Dr.RR and Dr.SR Engineering college, Chennai in 2011. And received his M.E. degree in the department of Computer Science and Engineering in PB college of Engineering, Chennai in 2013. Now he is an Assistant professor in Loyola Institute of Technology.

Miss. F. M Blessina Pearly. pursuing B.E degree in the department of Computer Science and Engineering from Loyola Institute of Technology, Chennai in the year of 2012-2016.

Miss. K. Lizzy, pursuing B.E degree in the department of Computer Science and Engineering from Loyola Institute of Technology, Chennai in the year of 2012-2016.