iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55838

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Data Security Using Unique Code Generation and Micro Pattern Analysis with GUA CCP Technique

M. Parvathi
Head of the Department, Computer Science, Latha Mathavan Arts and Science College, Tamilnadu, India

Abstract: ***This project is concentrated on the data security using various authentication mechanisms. This is to validate the user to enter into the system and to access the database by using password. The password techniques will differ and it may be vary from stage to stage. If the password is correct then only the user can get accessing rights. In this project three different types of techniques are analyzed. The project comprises of text password i.e. passphrase, image based password and graphical password for the three levels respectively. First one is unique one time password generation whenever the user gets into login. Second one is behavioral authentication. User has to upload their finger print at the time of registration. User has to import their finger print. If it matches with the database already stored then the access rights will be given to the user. Third one is graphical password. In this method CCP method is implemented. Set of images uploaded at the time of registration and a pixel coordinate is fixed on each image. At the time of login user has to enter the correct pixel coordinate in all the images then only user can get the accessing rights. In these methods nobody can crack all the three level passwords. In the first level it is dynamic password and in the second level unique identification password and in the third level multiple static key points are used as password. It is highly impossible to crack the third level authentication.***

Keywords: Dynamic password, CCP method, behavioral authentication

I. INTRODUCTION

Authentication and authorization are two vital information security processes that administrators use to protect systems and information. Authentication verifies the identity of a user or service, and authorization determines their access rights. Authentication is important because it enables organizations to keep their networks secure by permitting only authenticated users (or processes) to access their protected resources, which may include computer systems, networks, databases, websites and other network-based applications or services. Authentication methods include something users know, something users have and something users are. Not every authentication type is created equal to protect the network, however; these authentication methods range from offering basic protection to stronger security. Authentication is used to determine the identity of the user and verify and validate that identity. Authorization checks the permissions of the authenticated user and controls access to functions based on the roles that are assigned to the user.

II. EXISTING SYSTEM

Authentication method in the form of a password is created using letters, numbers, and special characters. Combinations that are created can use all three or only one (i.e. a combination of letters and numbers, a combination of numbers, etc.). Biometrics is a technology that uses a unique pattern of physical factors or user habits in authentication or identification. Biometric authentication can be divided into 2, namely Physiological Authentication and Behavioral Authentication. Biometric authentication is a method of authentication that has begun to be widely used, especially using fingerprints and faces. Physiological Authentication performs authentication using the physical features of the user. For example, fingerprint, palm print, hand geometry, face, eye, ear, ECG, EEG.

III. PROPOSED SYSTEM

First level is unique code generation and second level is finger print authentication, and the third level is graphical based authentication. In the third level CCP method is used. In proposed work a click based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click point per image. In addition user is asked to select a sound signature corresponding to click point this sound signature will be used to help the user to login. System showed very good performance in terms of speed, accuracy and ease of use. Users preferred CCP to pass points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably recalling the click points. In this method speed and accuracy is higher than that of other methods.

©IJRASET: All Rights are Reserved

IV. METHODOLOGY

A. Unique Code Generation

Generating random numbers involves computational algorithms that can produce apparently random results.

Why apparently random? Because the end results obtained are in fact completely determined by an initial value also known as the **seed** value or **key**. Therefore, if you knew the key value and how the algorithm works, you could reproduce these seemingly random results. Random number generators of this type are frequently called **Pseudorandom number** generators and, as a result, output Pseudorandom Numbers. Even though this type of generator typically doesn't gather any data from sources of naturally occurring randomness, such gathering of keys can be made possible when needed. Let's compare some aspects of true random number generators or **TRNG**s and pseudorandom number generators or **PRNG**s.

PRNGs are faster than TRNGs. Because of their deterministic nature, they are useful when you need to replay a sequence of random events. On the other hand, TRNGs are not periodic and work better in security sensitive roles such as encryption. A **period** is the number of iterations a PRNG goes through before it starts repeating itself. Thus, all other things being equal, a PRNG with a longer period would take more computer resources to predict and crack.

A computer executes code that is based on a set of rules to be followed. For PRNGs in general, those rules revolve around the following:

- Accept some initial input number, that is a seed or key.
- Apply that seed in a sequence of mathematical operations to generate the result. That result is the random number.
- Use that resulting random number as the seed for the next iteration.
- Repeat the process to emulate randomness.

1) The Linear Congruential Generator

This generator produces a series of pseudorandom numbers. Given an initial seed $\mathbf{X_0}$ and integer parameters **a** as the multiplier, **b** as the increment, and **m** as the modulus, the generator is defined by the linear relation: $\mathbf{X_n \equiv (aX_{n-1} + b) mod\ m}$. Or using more programming friendly syntax: $\mathbf{X_n = (a * X_{n-1} + b)\ \%\ m}$.

Each of these members have to satisfy the following conditions:

- $\mathbf{m > 0}$ (the modulus is positive),
- $\mathbf{0 < a < m}$ (the multiplier is positive but less than the modulus),
- $\mathbf{0 \leq b < m}$ (the increment is non negative but less than the modulus), and $\mathbf{0 \leq X_0 < m}$ (the seed is non negative but less than the modulus).

B. Biometric Representation

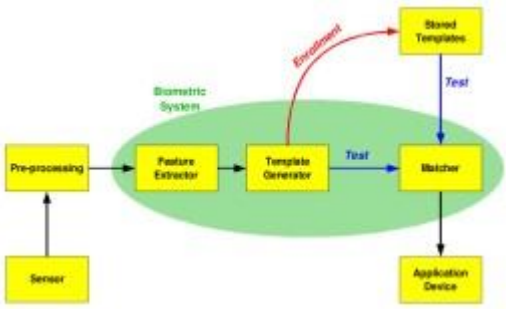
Although the various biometric technologies vary in what and how they scan, the principle of operation is very similar. A biometric system is a real-time identification system which identifies a person by measuring a particular physical or behavioural characteristic and later comparing it to a library of characteristics belonging to many people. Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and wherever the data is to be analysed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

C. Verification vs. Identification

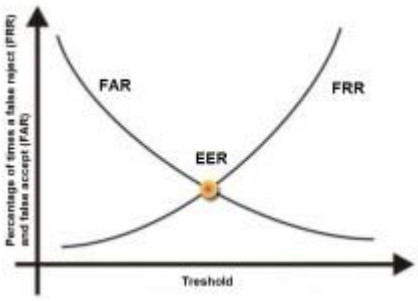
Depending on the application context, a biometric system can operate either in verification or identification mode.

In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. 'Positive recognition' is a common use of verification mode, where the aim is to prevent multiple people from using same identity.

In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person where the system establishes whether the person is who she (implicitly or explicitly) denies to be.



The basic block diagram of a biometric system



Threshold values for FAR a FRR

D. Performance of Biometric Systems

There are many characteristics which make it possible to compare the biometric systems. The following are the most used as performance metrics for biometric systems:

1) *False Rejection Rate (FRR):* The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
2) *False Acceptance Rate (FAR):* The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.
3) *Equal Error Rate (EER):* The rate at which both accept and reject errors are equal. The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the higher the accuracy of the biometric system

Fingerprint



Optical, capacitive or thermal fingerprinting
False Rejection Rate (FRR): <1%
False Acceptance Rate (FAR): from 0,0001% to 0,00001% depending on type
Verification time: 0,2 - 1 sec.

E. Cued Click Point Algorithm

By selecting all click point on single image introduces hotspots creation. In CCP user have to select different five images instead of selecting click point on same image. For every image user has to select only one click point. User has to click on a correct position on image, if so, next image will be displayed. In CCP address of next image is stored in previous click point. If click point is wrong then wrong image will be displayed. Users have to select sequence of click-point on correct images. CCP REGISTRATION After the first phase, user needs to login using user name and password. CCP registration needs to be done where user is asked to select number of images and splits. User needs to select images from the set of images.

CCP Registration. The user needs to select one point from each image for CCP registration. This point will be recorded in the database of the system. After that the user will have to wait for the approval/rejection from admin. The system designed consists of three modules: user registration module, picture selection module and system login module.

F. System Design Modules

In user registration module user enters the user name in user name. When user entered the all user details in registration phase, this user registration data is stored in data base and used during login phase for verification.

In picture selection phase there are two ways for selecting picture password authentication.

1) User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.

2) 2. System defines pictures: pictures are selected by the user from the database of the password system.

3) In picture selection phase user select any image as passwords and consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. Users must select a click-point in the image and proceed on the next image. During system login process, images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

V. CONCLUSIONS

Security is most important factor for any system authentication. we proposed a shoulder surfing resistant authentication system based on three level authentication mechanisms. Firstly random unique code generation technique will be implemented, next biometric finger print algorithm followed by graphical method. In graphical passwords using CCP technique more images with separate click point on it is used. The problem of shoulder surfing is solved. CCP offers an exceptionally secure option in contrast to existing frameworks. CCP builds remaining burden for assailants by driving them to initially obtain picture sets for every client and after that direct hotspot examination on every one of this pictures

REFERENCES

[1] Suo, Ying Zhu, G. Scott,Owen Xiaoyuan, “Graphical passwords: a survey”, (Department of Computer Science Georgia State University).

[2] 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, 2007

[3] Stalling, W. Cryptography And Netwrok Security,

[4] Ravi Saini, Sanjay Singh, Anil K Saini, A S Mandal, Chandra Shekhar “Design of a Fast and Efficient Hardware Implementation of a Random Number Generator in FPGA” CSIR- Central Electronics Engineering Research Institute (CSIR-CEERI) Pilani333031, Rajasthan, India 2013 International Conference on Advanced Electronic Systems (ICAES).

[5] Purushottam Y. Chawle and R.V. Kshirsagar, “Design of 8 and 16 bit LFSR with maximum length feedback polynomial using verilog HDL”.13th IRF international conference 20thjuly 2014, Pune, India

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

The heading of the References section must not be numbered. All reference items must be in 8 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]).

When referring to a reference item, please simply use the reference number, as in [2]. Do not use "Ref. [3]" or "Reference [3]" except at the beginning of a sentence, e.g. "Reference [3] shows …". Multiple references are each numbered with separate brackets (e.g. [2], [3], [4]–[6]).

Examples of reference items of different categories shown in the References section include:

- example of a book in [1]
- example of a book in a series in [2]
- example of a journal article in [3]
- example of a conference paper in [4]
- example of a patent in [5]
- example of a website in [6]
- example of a web page in [7]
- example of a databook as a manual in [8]
- example of a datasheet in [9]
- example of a master's thesis in [10]
- example of a technical report in [11]
- example of a standard in [12]

CONCLUSIONS

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

Causal Productions permits the distribution and revision of these templates on the condition that Causal Productions is credited in the revised template as follows: "original version of this template was provided by courtesy of Causal Productions (www.causalproductions.com)".

ACKNOWLEDGMENT

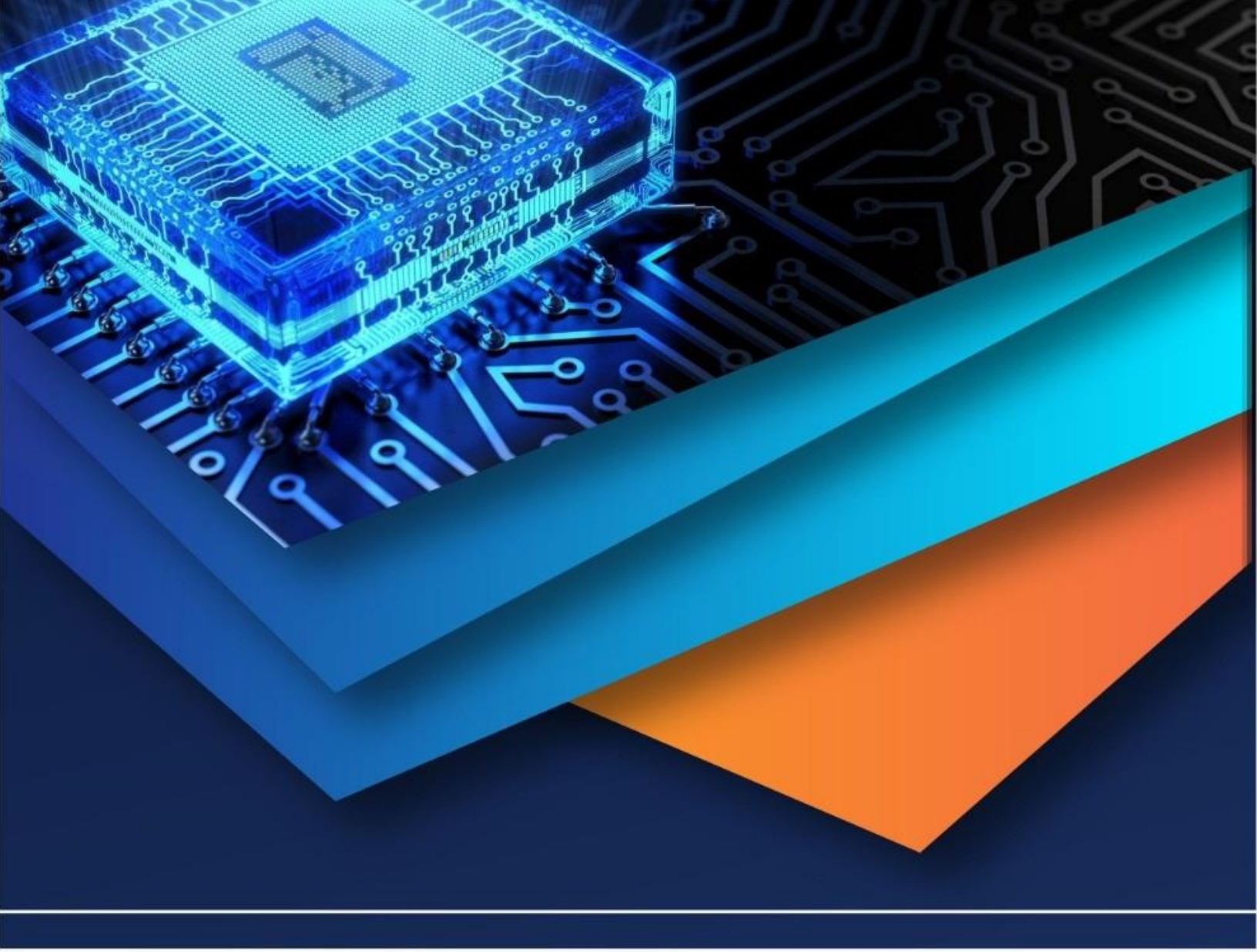
The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[2] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[3] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[4] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
[5] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[6] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
[7] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/
[8] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[9] FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
[10] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[11] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.
[12] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[13] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)