iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35293

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: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Secured Application Environment using Enhanced Graphical Passwords

Ms. Prajakta Vikhe[1], Dr. M. R. Bendre[2]
[1, 2] *M.E Computer Eigg. Dept, P.R.E.C. Loni, Ahmednagar, Maharashtra-413736., Savitribai Phule Pune University.*

Abstract: ***Today computer and mobile based applications has become an integral part of our life. Thus, there arises a need of a reliable security while using these applications using authentication techniques that are most secured and hard to crack. Today many authentication techniques are introduced for better security and replace textual authentication technique. But these techniques are proving insufficient, so new ways should be studied and introduced for better security. So, we are concentrating on two such techniques, first we studied graphical authentication systems using images. The one such technique called gRat which uses set of images for authentication was found to be useful. The second for searching a different authentication technique we came across ENP which explains how to provide security using to an application by using hashing, ascii, negation and cryptography together for a secured application. So, we find out that one technique is insufficient and more than two techniques should be combined together. So, in this paper we are recommending a dual authentication technique. First technique will be used for login id and other will be used for login password. The first technique uses a set of images with specific border colors for authentication and is called Graphical random authentication technique (gRat). In this technique a set of images with different boundary colors are displayed for the user which are shown randomly each time a user attempts a login ID. The user has to select the same set of images with same boundary color in same format for login ID verification than only second technique for login password will be shown. The second technique uses encryption and negative password together called as Encrypted negative password (ENP). In this technique while deciding a password a plain textual password is accepted from the user and then it is converted to hash code using hashing algorithm. Then the hash code is converted to an ascii code od 0's and 1's. Then negation is applied to the ascii where we get a negative text. The negative text is then encrypted. This process is followed in reverse while authentication. After second correct verification main application will be started. Both authentication data will be secured by Advanced encryption standard (AES) algorithm and saved on cloud. We are using public cloud Google drive as our cloud as it is free and more secured. Thus, while testing the application for authentication using both techniques together our system becomes very secured and almost unbreakable.***

Keywords: Graphical Password, Authentication Technique, gRat, ENP, AES, Cloud Computing, Mobile Computing.

I. INTRODUCTION

As our life gets digital by more and more use of applications both on local computers and hand-held devices. A lot of information shared by an application user with organizations all over the world. As more and more data getting accumulated online it gives invitation for the hackers to misuse them. So many authentication techniques are introduced today to replace old textual authentication systems. But these techniques are also proving to be insufficient in securing the application environment as these techniques are used one at a time. So there arises a need of using more than one authentication techniques together. So, to achieve target we are studying the existing systems thar are released by various authors together. Thus, this paper studies and elaborated various graphical authentication and another authentication technique all together to design a more secured authentication technique. The various authentication techniques are shown in Fig.1.

Thus, by studying the various authentication techniques in Fig.1 we come to understand that no one authentication technique can be full proof but they have to combined to make a more powerful technique. So, two authentication techniques which we studied found to be useful, first was gRAt [1]. and second was ENP [2]. Which if combined together will create a very strong and more powerful authentication technique. So, in other words the main objective of this paper is to:

A. Focus on security features and usability of an authentication technique.
B. Study most better and promising authentication technique for security and which can be used easily by the user.
C. Propose a new authentication technique by combining one or more security algorithms together.
D. Implement new authentication framework for both mobile and local computer applications.
E. Evaluate and analyze the new authentication framework and its strengths.
F. Evaluate and analyze the new movie review system framework and its strengths.

Thus, the rest of the paper is organized as follows:

1) Section II. explains literature survey which studies various techniques with their advantages and drawbacks.
2) Section III. explains the methodology i.e., mathematical model and algorithms to be used by the system.
3) Section IV. explains proposed system with block diagram and working of the system.
4) Section V. shows the results and discussions and how it will be implemented.

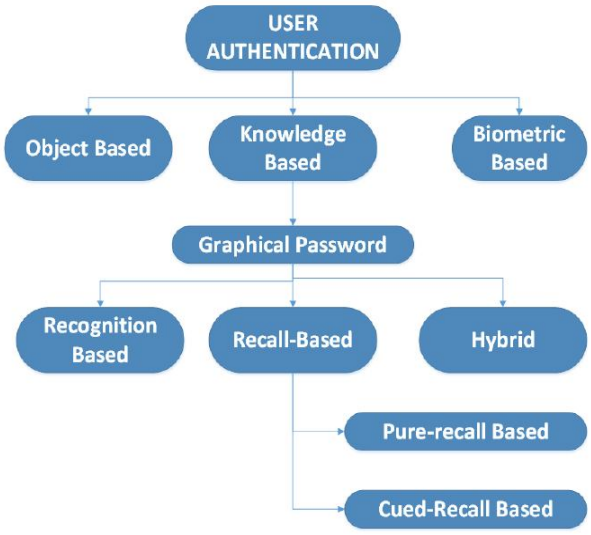


Fig.1. Existing authentication techniques

II. LITERATURE SURVEY

This section describes the fundamentals of various authentication techniques that can be used in designing a new more reliable and secured authentication technique. It helps in understanding various ideas put forward by various technical papers published by various authors and how they put forth a more accurate and concrete techniques. Some of the ideas with technique and drawbacks are mentioned below:

In 2018 Khan et al. [1] presented the paper focusses mainly on graphical randomized authentication for smart devices. This technique uses a set of random images for authentication. This technique is quite good and provides a secured authentication. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2019 Wazir et al. [2] presented the paper focusses mainly on doodle images-based authentication for smart devices. This technique uses a set of images for authentication. This technique uses a set of random doodle images for authentication. This technique is quite good and provides a secured authentication. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2018 Luo et al. [3] presented the paper focusses mainly on authentication by converting a text in to encrypted negative password. This technique combines hashing, negation and AES together. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2020 Khan et al. [4] presented the paper focusses mainly on captcha based graphical password. It uses captcha image with cued click point technique for authentication. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2017 Zaki et al. [5] presented the paper focusses mainly on secured pattern key-based password authentication. This sets a password by selecting numbers with a specific pattern and dummy numbers in it. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer. In 2017 Alese et al. [6] presented the paper focusses mainly on graphic based cryptographic model for authentication. This technique uses cued click and recall model. This technique uses a set of images for authentication. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2017 S.Sukanya et al. [7] presented the paper focusses mainly on image based graphical password for banks. This technique uses cued click point technique with a dragging property. This technique uses a set of images for authentication. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2017 Prakash et al. [8] presented the paper focusses mainly on graphical authentication technique using watermarking and QR code. This technique combines cued click point, watermarking and QR code together for authentication. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2017 Kaja et al. [9] presented the paper focusses mainly on graphical password using persuasive cued click points. This technique uses a set of images for authentication. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

In 2017 Tabrez et al. [10] presented the paper focusses mainly on pass matrix authentication technique. This technique uses a set of images for authentication with cued click points. This technique is quite good solves authentication problem. But main drawback of this system is that it on only a single layer of authenticate which is quite breakable as it does not have a backup layer.

III.METHODOLOGY

This section will study the mathematical conditions and algorithms to be used for designing a secured and multilayer authentication framework. These are explained as follows:

A. Mathematical Model

Our authentication technique can be explained in two sets with probability, success and failure conditions.

1) gRat

Set (G)= {G0, G1, G2, G3, G4, G5, G6}

G0$\in$G = Set login id.
G1$\in$G = Retrieve random set of images.
G2$\in$G = Select set of images in a pattern.
G3$\in$G = Save login id after encryption.
G4$\in$G= Select same steps of image pattern selection for verification.
G5$\in$G = Verify login id after decryption.
G6$\in$G = Authentication message.

2) ENP

Set (E)= {E0, E1, E2, E3, E4, E5, E6, G6}

E0$\in$E = Set login password.
E1$\in$E = Accept password and convert it to hash code.
E2$\in$E = Convert hash code to ascii code.
E3$\in$E = Apply negation on ascii to get negative password.
E4$\in$E = Save login password after encryption.
E5$\in$E = Reverse the steps for verification.
E6$\in$E = Verify login password after decryption.
G6$\in$E = Authentication message.

So, by studying the sets we come to notice that elements are common in both modules and used in coordination in both sets so they be placed as

$$x \in G \cap E \text{ if } x \in G \text{ and } x \in E$$

Thus, the probability of intersection of elements in both modules can be given as

$$P(G \cap E) = P(G)+P(E)$$

So, intersection of common elements can be shown as

$$G \cap E = \{G6\}$$

The conditional probability of both modules using the same element can be shown as

$$P(G \mid E) = \frac{P(G \cap E)}{P(E)}$$

Thus, we conclude that our authentication framework's success and failure will depend upon the internet as our authentication data is stored on cloud, i.e., if the internet connection is not good or not present the authentication frame work will not work, thus this is a case of failure, so our framework supports NP-Hard and not NP-Completes

B. Algorithms Used

Our authentication and registration process using following algorithmic steps.

```
1: procedure REGISTRATION
2:     images[]=Fetch images
3:     imageCount=images.length()
4:     if imageCount == 0 then
5:         load images in a 3X3 grid.
6:         selectionCount=getImageNo()
7:         if selectionCount > 0 then
8:             Save grid based password
9:             passText=getPasswordTex()
10:            if passText! = "" then
11:                passText=convertToHash(passText)
12:                passText=convertToBinary(passText)
13:                passText=convertToNegaive(passText)
14:                passText=encryptAES(passText)
15:                save passText as ENP password
16:            else
17:                Repeat Step 9:
18:            end if
19:        else
20:            Repeat Step 6:
21:        end if
22:    else
23:        Repeat Step 2:
24:    end if
25:    View registration status message.
26: end procedure
```

```
1: procedure VERIFICATION
2:     images[]=Fetch images
3:     imageCount=images.length()
4:     if imageCount == 0 then
5:         load images in a 3X3 grid.
6:         selectionCount=getImageNo()
7:         if selectionCount > 0 then
8:             verifyStatus=verify grid based password
9:             if verifyStatus == True then
10:                passText=getPasswordTex()
11:                if passText! = "" then
12:                    passText=convertToHash(passText)
13:                    passText=convertToBinary(passText)
14:                    passText=convertToNegaive(passText)
15:                    passText=encryptAES(passText)
16:                    Verify passText as ENP password
17:                else
18:                    result ←Exit procedure
19:                end if
20:            else
21:                Repeat Step 9:
22:            end if
23:        else
24:            Repeat Step 6:
25:        end if
26:    else
27:        Repeat Step 2:
28:    end if
29:    View verification status message.
30: end procedure
```

IV. PROPOSED SYSTEM

This This section is mainly divided in 4 parts with other sub parts in them. The text that follows explains the modules with a block diagram or system architecture as shown in Fig.2. to illustrate them. The working of the framework is explained as:

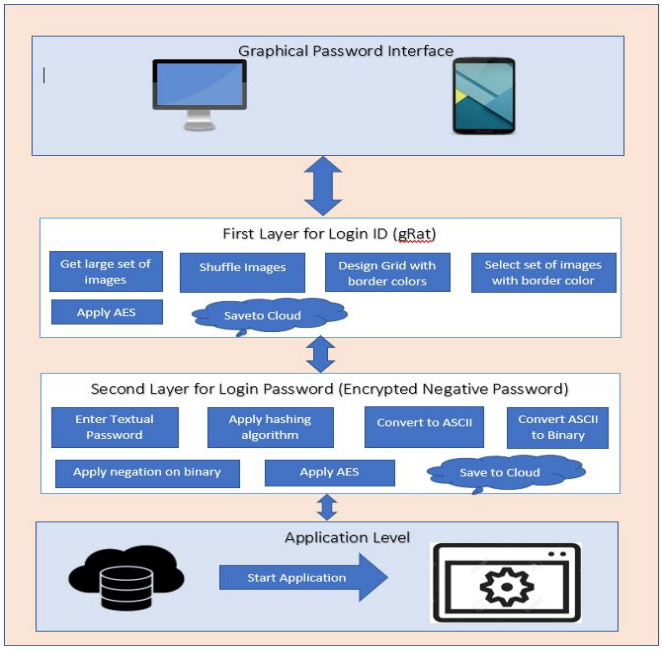


Fig.2. System Architecture Diagram.

A. *Graphical Password Interface*

This graphical user interface for the propose system will be both for a standalone application as well as for hand led smart devices. The system will provide authentication layers for both the application types i.e., it will not be limited for a standalone application or a mobile application. Thus, or application will have a dual layered authentication system.

B. *Layer First (gRat)*

This will be the first authentication layer in the dual layered framework. After successfully authenticating it the user can view the second layer. This layer will be used for inputting a login ID for authenticating the application. In this layer a large set of images will be fetched. The images will be shuffled and 16 images will be extracted from the set. The set of 16 images will then again be shuffled and shown in 4x4 grid. The grid boxes will have specific colors. After selecting a login ID during registration, the user has to select images in a pattern with a specific border color. The pattern will then be encrypted using AES. The encrypted login ID will then be saved on Google cloud. During authentication the user has to follow the reverse process for successful login ID authentication. After successful verification from the cloud after decryption using AES the second layer of login password will be visible for verification.

C. *Layer Second (ENP)*

This will be the second authentication layer in the dual layered framework. It will be visible for authentication only after first layered is verified. This layer will be used for login password. In this layer a user has to input a text. The text will be converted to a hash code. The hash code will then be converted to ASCII. The ASCII code will then be converted to binary. The binary code will then be negated i.e., in place of 0 1 will be instead and vice versa. Thus, we get a negative password. The negative password will then be encrypted using AES and uploaded to cloud during registration phase. The same process will then be followed for verification in a reverse process. After successful verification of the second layer an application window or menu will be shown where a user can perform operations needed by the application.

D. *Application Level*

This module will be any application where our authentication system will be applied. The application starts only after verification of dual authentication framework proposed in the paper.

V. RESULTS AND DISCUSSION

Thus, to explain the above proposed system we have created 1 application using java and python. We are using 2 SNPs for fetching movie reviews i.e., IMDB and Twitter.

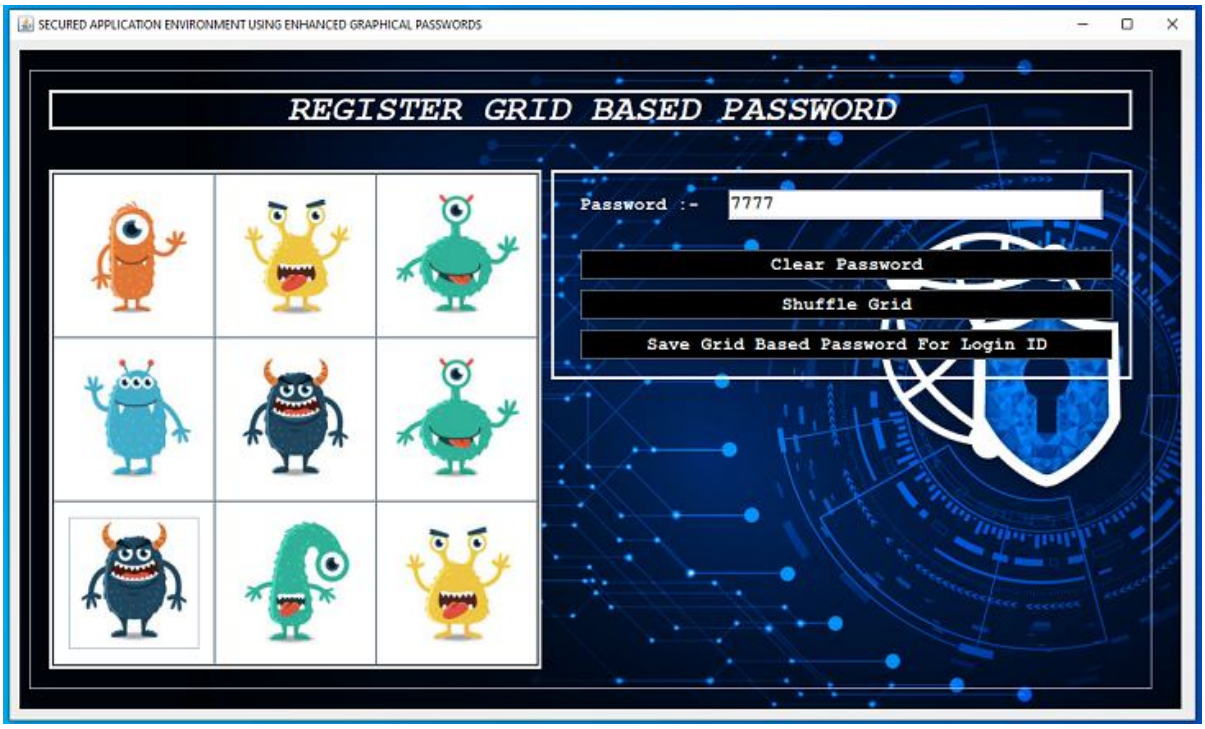


Fig.3. Registration process using Grid based.

In Fig.3 it shows how a user can select images and create password for login id of a banking application.

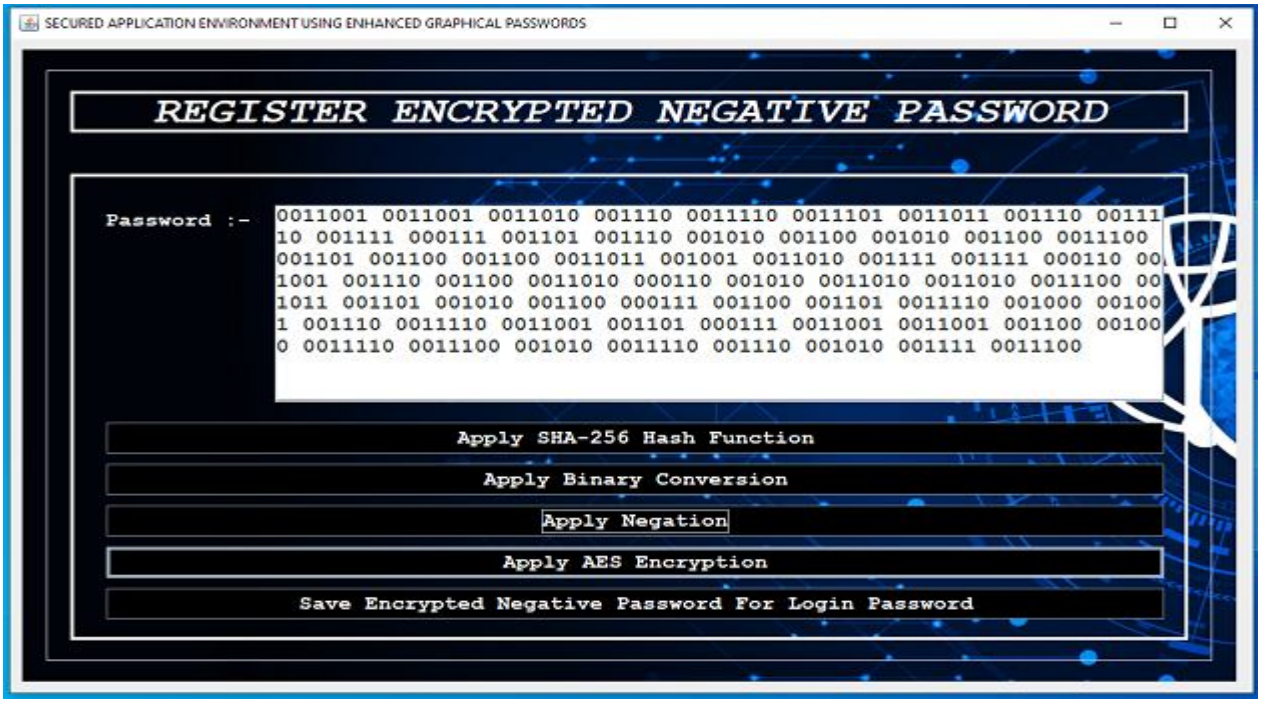


Fig.4. Registration process using ENP.

In Fig.4 it shows how a user can create an encrypted negative password by following various conversion layers for login password of a banking application.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Fig.5. Verification using Grid based.

In Fig.5 it shows how a user can verify first layer of banking authentication using Grid based password on mobile. The same is applicable for desktop application also.

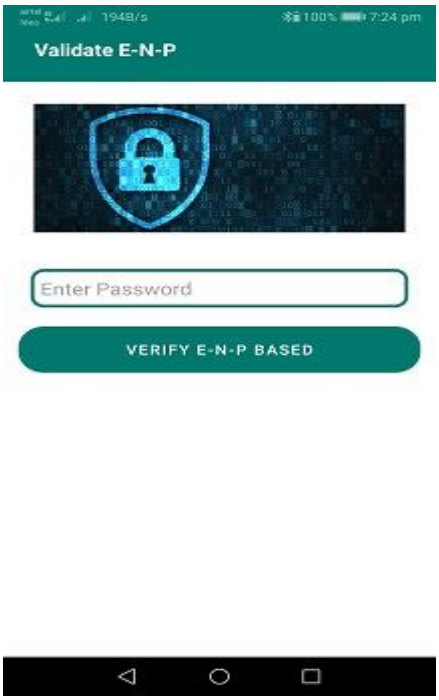


Fig.6. Verification using ENP

In Fig.5 it shows how a user can verify second layer of banking authentication using ENP based password on mobile. The same is applicable for desktop application also. After successful authentication of both passwords banking menu screen is shown where various banking operations can be performed.

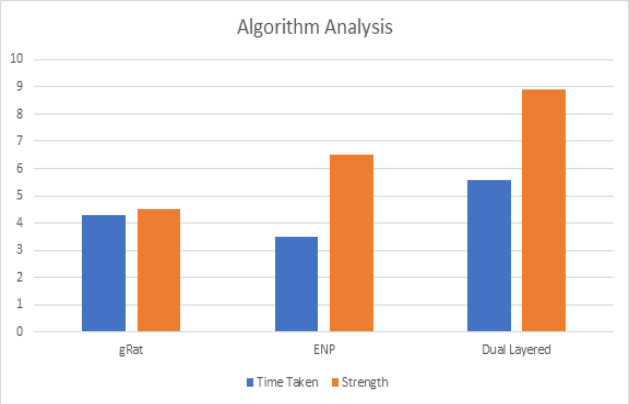


Fig.7. Comparison chart

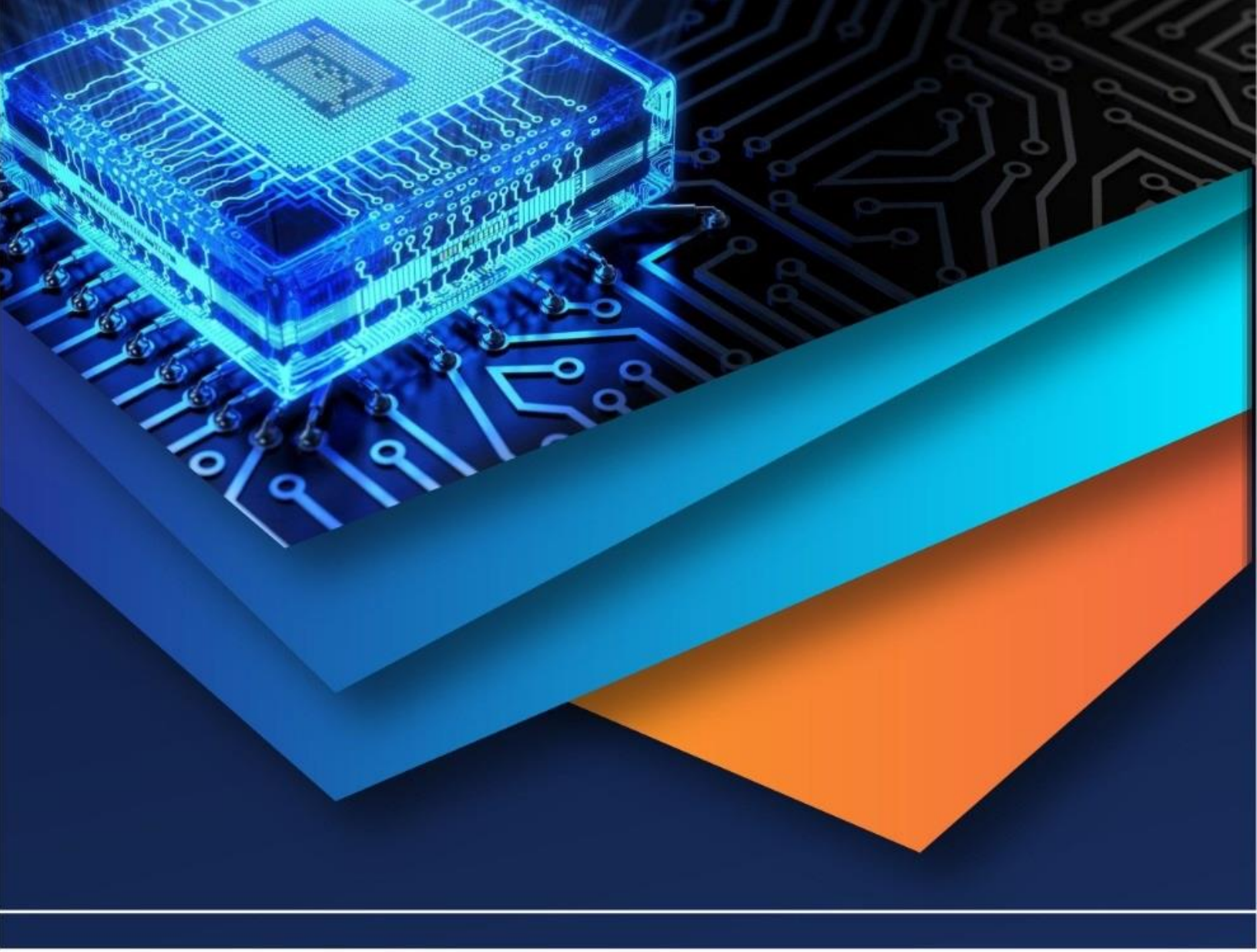
Thus, the results in Fig.7. suggests that strength of gRat is lower than ENP means ENP is more effective. But the third result shows that when both algorithms are combined and a dual layered authentication framework is formed it becomes a very strong authentication technique with more authentication strength than gRat and ENP.

VI. CONCLUSION

In this paper we conclude a novel approach to provide security to application using two techniques together to achieve a secured dual layered authentication technique. While proposing the system we came across various techniques mentioned by authors [1][2][3][4][5][10] mainly and understood the various aspects needed for a successful authentication technique. Thus, our technique will be tough to crack as we are using graphical passwords instead of textual passwords which are guessable thus making a unguessable and hard to crack system. Thus, we are going to provide the authentication on multiple platforms i.e., it can be used with a standalone application as well as a mobile application. Thus, we conclude that our system will be helpful in securing an application more securely than other authentication techniques.

REFERENCES

[1] Mudassar Ali Khan, Ikram Uddin, Sultan Ullah Jadoon, Muhammad Khurram Khan, Mohsen Guizani and Kamran Ahmad Awan, - g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices, IEEE-2018.
[2] Waqas Wazir, Hasan Ali Khattak, Ahmad Almogren, Mudassar Ali Khan and Ikram Uddin., - Doodle-Based Authentication Technique Using Augmented Reality, IEEE-2019.
[3] Wenjian Luo, Senior Member, Yamin Hu, Hao Jiang and Junteng Wang., - Authentication by Encrypted Negative Password , IEEE-2018.
[4] Altaf Khan and Dr. Alexander G. Chefranov, - A Captcha-Based Graphical Password With Strong Password Space and Usability Study, in IEEE 2020.
[5] M Hamza Zaki, Adil Husain, M Sarosh Umar and Muneeb H Khan, - Secure Pattern-Key Based Password Authentication Scheme, in IEEE-2017.
[6] Boniface K. Alese, Abimbola Akindele, Folasade M.Dahunsi, Aderonke F. Thompson and Tosin Adesuyi, - A Graphic-based Cryptographic Model for Authentication, in IEEE-2017.
[7] S.SUKANYA and M.SARAVANAN, - IMAGE BASED PASSWORD AUTHENTICATION SYSTEM FOR BANKS, in IEEE-2017.
[8] SREYA PRAKASH and SREELAKSHMY M K, - A SECURE GRAPHICAL AUTHENTICATION SYSTEM USING WATERMARK EMBEDDING, in IEEE-2017.
[9] Sachin Kaja and Divya Gupta, - Graphical Password Scheme using Persuasive Cued Click Points, in IEEE-2017.
[10] Shums Tabrez and Jagadeesh Sai D, - Pass-Matrix authentication solution to shoulder surfing attacks with the assistance of graphical password authentication system, in IEEE-2017.
[11] F. Tari, A. Ozok, and S. H. Holden, - A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords, in Proc. 2nd ACM symposium on Usable privacy and security, 2006, pp. 56–66.
[12] K. Gilhooly, - Biometrics: Getting back to business, Computerworld, May, vol. 9, p. 2005, 2005.
[13] G. Blonder and P. GRAPHICAL, - United states patent 5559961, Graphical Passwords, 1996.
[14] G. Ye et al., -Cracking android pattern lock in five attempts, Proc. 2017 Netw. Distrib. Syst. Secur. Symp., no. March, 2017.
[15] V. Venkateswara Rao and A. S. N. Chakravarthy, -Analysis and bypassing of pattern lock in android smartphone, IEEE Int. Conf.
[16] Comput. Intell. Comput. Res. ICCIC, pp. 1–3, 2017.
[17] B. B. Zhu, J. Yan, Guanbo Bao, Maowei Yang, and Ning Xu, -Captcha as graphical passwords: a new security primitive based on hard AI problems, IEEE Trans. Inf. Forensics Secur., vol. 9, no. 6, pp. 891–904, 2014.
[18] A. Khan, &A. G. Chefranov, -A new secure and usable captcha-based graphical password scheme, In International Symposium on Computer
[19] and Information Sciences, Springer, Cham., September, 2018, pp. 150- 157.
[20] H. Tao and C. Adams, -Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw. Secur., vol. 7, no. 2, pp. 273–292, 2008.
[21] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, -Enhancing security behaviour by supporting the user, Comput. Secur., vol. 75, pp. 1–9, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY