IJSRTM
https://www.ijsrtm.com
Vol.3 Issue 1 March 2023: 16-20
Published online 11 Mar 2023
E-ISSN: 2583-7141

International Journal of Scientific Research in Technology & Management

Secure Authentication for Input Credentials using CAPTCHA as a Graphical Password (CaRP)

Utkarsh Dubey
Department of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India
utkarshdubey7@gmail.com

Arun Pratap Singh
Department of Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha, Madhya Pradesh, India
singhprataparun@gmail.com

***Abstract*— One of the most popular methods used by web services to protect their system against unexpected relay attacks is CAPTCHA. In essence, CAPTCHA is a Turing test that determines whether a human or a robot is accessing the system. Today's CAPTCHAs come in a variety of forms, and each has a different level of authentication. The CAPTCHA performs a crucial function in preventing spam entries and unauthorized access to a website. To securely authenticate the user in the proposed system, CAPTCHA is utilized to input the correct pairs of credentials. Proposed system prohibits input through keyboard and enhances security by dragging letters through mouse. In this system, CAPTCHA shows distorted alphabets of different colors and some colored bubbles are placed below. User needs to drag desired letter on the same colored bubble. Here in the developed method, identical shades of color are considered as same and every reload shuffles the color of letters and bubbles. A machine is not able to identify the identical shades for dragging up to desired one. System confuses bots by shuffling alphabets along with its colors and its shading. This is a new era of securing authentication system from various attacks using CAPTCHA.**

Keywords*— *CAPTCHA, Authentication, Graphical Password, Image processing, Game, Robot.

I. INTRODUCTION

Nowadays internet is extensively used to access various applications like mails, social networking sites, shopping websites and so on. To operate these applications on web, user requires to get registered on those websites by creating username and password for individual access. By using input credentials, user can safely access the web services on internet. Every sites or applications on web have their respective security levels and it varies according to the services provider. While registering in website, sometimes malicious program is used by the hackers to misuse the data and to create the fake account in that website and apply attacks to crack secured credentials [1].

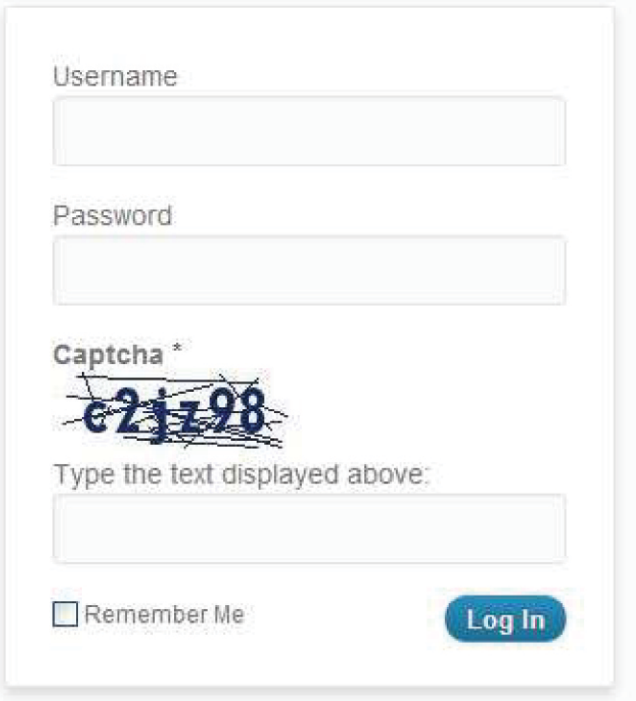

Fig. 1. Tradition CAPTCHA as a Turing Test [1]

There are so many techniques developed by the researchers to secure the web services from the attacks of robots. CAPTCHA, a kind of Turing test which is widely used to differentiate the user whether it's a human or a robot. Due to various techniques developed in this field, there are wide variety of CAPTCHA is available. Like Text CAPTCHA, where distorted alphanumeric letters are shown in an image and user needs to identify those letters.

Flash games are often used in the form of CAPTCHA where user needs to play that game for successful submission of datasets. CAPTCHA increased the security of websites from various attacks and if it is used to generate the input credentials, then definitely it can enhance the security level that oppose from various attacks.

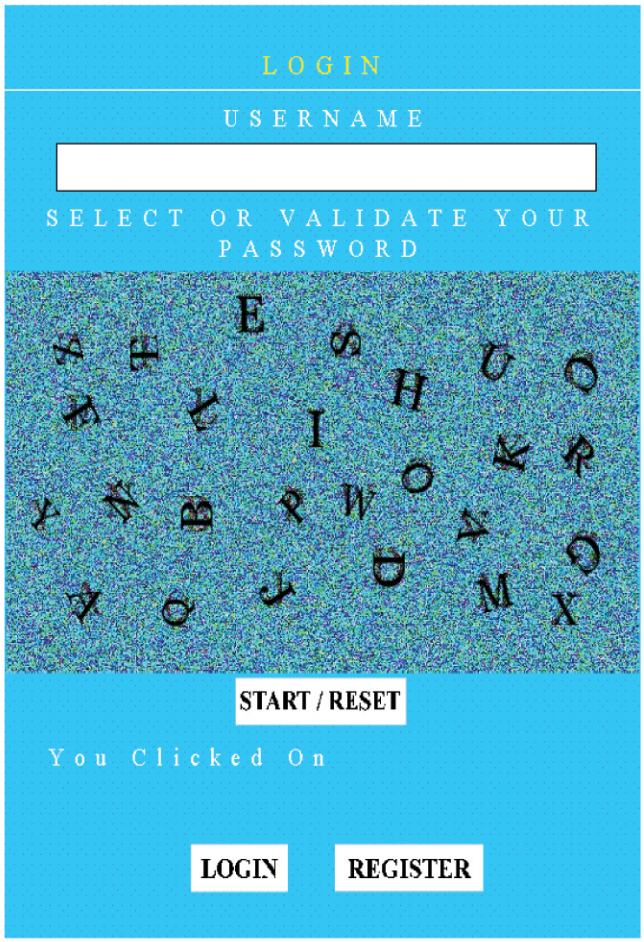

Fig. 2. Earlier System [6]

II. Related Works

Bin B. Zhu et al [2] proposed a graphical CAPTCHA which is based on hard AI problem. Here the system provided a CaRP where certain objects including animals are there along with coordinates and when user click on any animal or objects then it recorded the coordinates and store that for future reference. User is required to remember the animal as well as the position where he clicked. Each and every animal is assigned a grid where user is required to click and remember for future login. There are two kinds of CaRP proposed here first one is AnimalGrid based and another one is Click Text based. Silla Nirosha [3] et al. proposed a CaRP which is also based on hard AI problem. Here the system is also based on coordinates. User is required to click on a particular area of his choise while registration and remember to click there after to successfully login as legitimate user. Here the problem is that; user is required to remember the position or objects where is to be click for success login. Shraddha S. Banne et al. [4] proposed a survey on CAPTCHA as a graphical password. CaRP is a graphical password that uses Captcha. Using CAPTCHA and a graphical password in combination can solve a variety of security issues. User authentication in information security is a significant issue in every system. And every system relies on a password for authentication, whether it be a text-based password or a graphical password. The CAPTCHA test was created by computer programmes, but only humans can successfully complete it. In this article, we compare the advantages and disadvantages of each technique and provide a CaRP and graphical password strategy that is resistant to typical attacks on existing authentication schemes. Kalyani S et al. [5] proposed a technique to intervene as legitimate user by using CAPTCHA as a graphical password. Author uses AI based problem to challenge the bots to breach the security. It also uses the objects and animals or some time alphabets along with their coordinates where user is required to click on these coordinates and at the time of sign in; it is mandatory to remember the clicks or objects to resubmit the coordinates to get access successfully. It challenges to save the users from various attacks such as brute force attack, shoulder surfing attack and many more. It has been consider that an attacker can detect the objects, animals and alphabets but not able to recognize the coordinates. But it is also harder for human or legitimate user to remember the clicks.

III. Problem Identification

Priyanka P. et al [6] proposed a system which is based on clicks over distorted letters which only can be recognized by human. But some attacks can affect the system by recognizing its representation of letters on behalf of coordinate values. Some hard AI problems confuse users to recognize similar faces or sequence of faces and hard to remember at the time of login. A sequence of animal is often hard to remember for login authentication. We require a system which can secure the input credentials and password should be on user's choice. This credential should be secured while registering or authenticating it at all. The previously proposed system is based on layers where each alphabet is a layer that reflects its value. If motion has been stopped then all layers become still or in a static position.

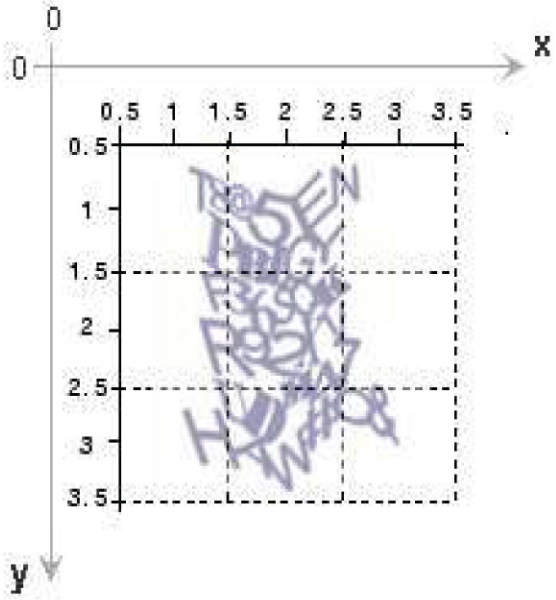

Fig. 3. Coordinates based CAPTCHA [6]

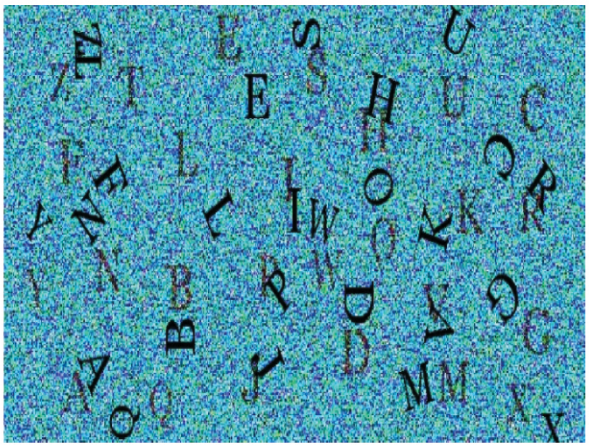

Fig. 4. Dynamic Position based CAPTCHA [6]

Fig. 5. Replica Alphabets [6]

Sobel Edge detection method can recognize edges through which layers will be highlighted and identified.

Fig. 6. Sobel Edge Detection [6]

IV. Proposed Work

Due to the various flaws found in the prior developed technique, the proposed system is aimed to prevent authentication from different attacks by securing input credentials that can differentiate human and robots. Proposed method provides an Artificial Intelligence problem in the form of CAPTCHA through which valid pair of input credentials need to feed to authenticate particular web application. It stated that if a robot is not able to make any input then it is impossible to break the security threat of authentication. The proposed system aimed to oppose machine fraudulent activities in the form of CAPTCHA. Developed system denies those inputs which are made through keyboard. Proposed technique operates in a form of virtual keyboard along with AI problems. In the proposed method, a CAPTCHA is appeared in the form of AI problem which is used to input the username and password to access the application. Following steps are required to solve the CAPTCHA and fill the credentials for authentication: User will have to drag desired alphabets with the same color of circle. After each selection the color of alphabets will get changed and the position will also get shuffled. Colors appearances are not color sensitive where user will have to recognize identical color shades that cannot differentiate by bots. There are no co-ordinates values behind the alphabets, which can be extracted by image processing. Background is complex that cannot be easily understood by bots but possible to observe by human. There is an intellectual efforts required at every selection where as present system is only based on clicks that return respective alphabets. Proposed system differentiates human and bots at every aspect of security.

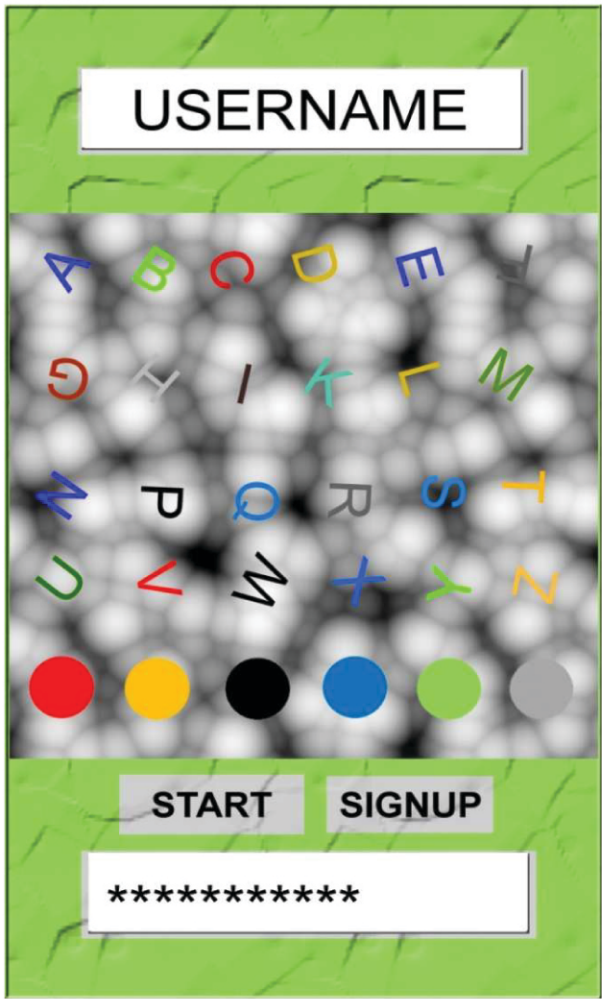

Fig. 7. Proposed System

Action script plays an important role to instruct the game logically and control the user intervention. In shock wave file; the reverse engineering is much difficult and hard to intervene in the server and breach the security. At the time of registration or enrollment user will have to choose username and select desired password, but password can only be selected through CAPTCHA that is only possible by human not by bots. Once the registration has been done, a user can login with the same process which has been done at time of registration. User will have to select password from CAPTCHA and password field will be disabled that does not allow keyboard entries.

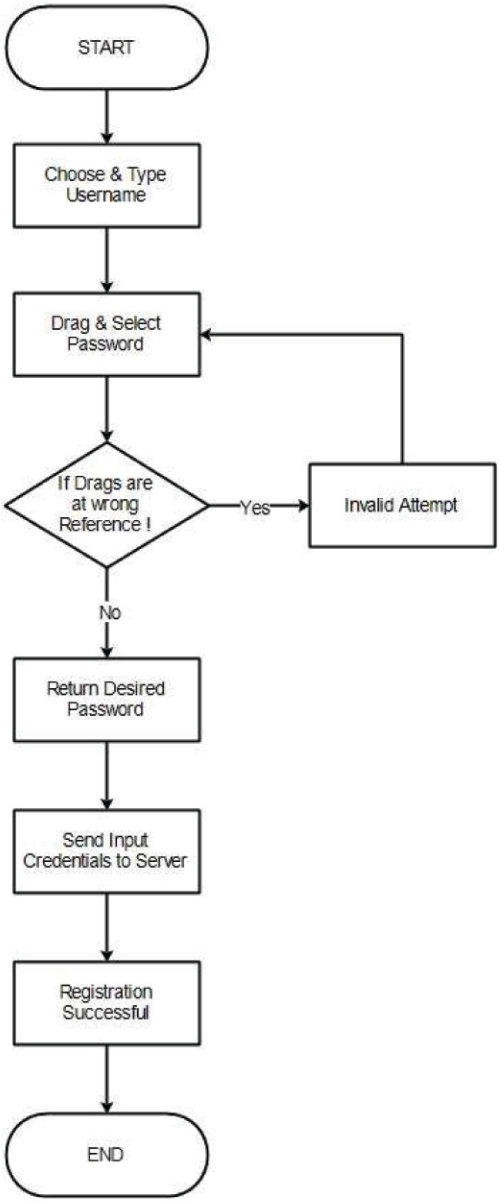

Fig. 8. Flow Chart for Enrollment

As per the flow chart of enrollment, first of all user will choose username and a password will be selected through dragging alphabets to the target position or color. If drag is at the empty area or at wrong references or target then it will return invalid attempt and it will be continue till right selection has not been made. A combination of valid username and password send to the authenticating server.

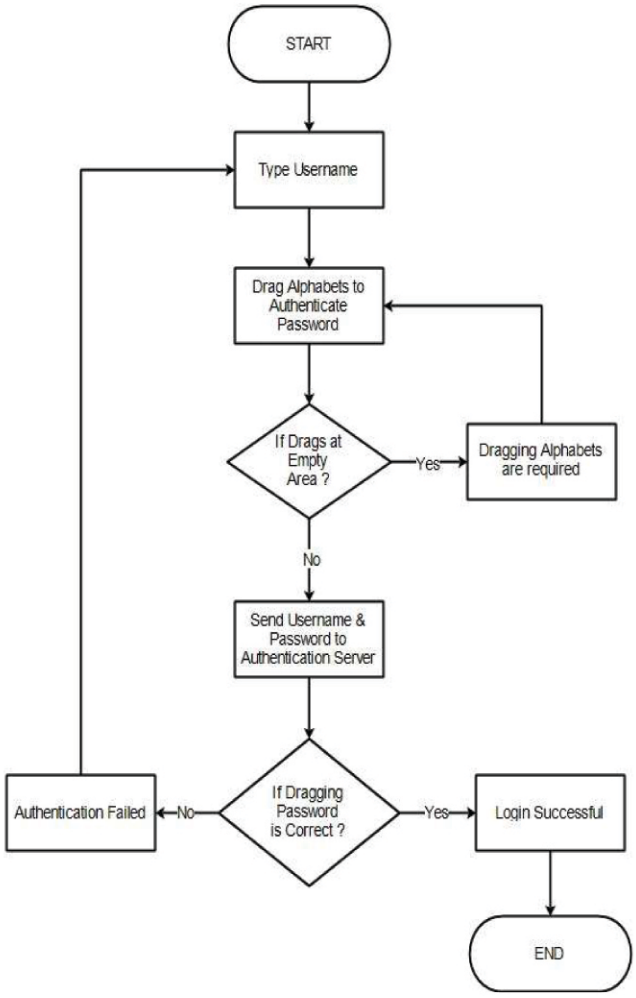

Fig. 9. Flow Chart for Authentication

At the time of login authentication, the same process will be repeated to enter username and password and user will be authenticated accordingly.

A. ET (Enigma Theory) Algorithm

Required: The target color set C_n, alphabets position A_s, alphabets updated position A_c, target position C_s, updated target position C_c, start button B_n, alphabet A_n, current state s, steps m, target object O, target position T, time t and non-target position n.

Input: Drag & Drop

Output: Object (x, y) hits Target (x, y)

1: Steps ← 0 //Initialize the steps
2: t ← 0 // Seconds
3: Dragging the Alphabets ← False
4: //Check if start button has been clicked
if B_n has been clicked **then**
Drag Alphabets ← True
goto step 5
5: (t=0; t≤3; t++); // 3 minutes
6: **if** $A_n(x, y)$ hits $C_n(x, y)$ **then**
A_n.return ← true
else
A_n.return ← false
end else
end if

7: **while** (timer t > 0) **do**
Drag Alphabets ← True
end while
8: **if** t = 0 **then**
$A_s \leftarrow A_c$
$C_s \leftarrow C_c$
end if
9: End

V. Result Analysis

Here the result is based on various users' interventions including enrollments and authentication stages. Here the total number of users are 30 where 2 users get failed to attempt successful login and 28 users get accessed successfully. Table I shows the user logs such as time taken by the user to get logged in and it also shows the password strength whether it is weak, moderate or strong. The mean time for all users is 34.03 which is bit lesser than the earlier system and the standard deviation is recorded as 10.87 which is also lesser than the earlier implemented system.

Table I Result Analysis

Users U_n	Time Taken t	Failed Users F_u	Successful Users S_u	Password Length
U_1	22	0	1	Moderate
U_2	15	0	1	Weak
U_3	19	0	1	Moderate
U_4	29	0	1	Moderate
U_5	35	0	1	Strong
U_6	28	0	1	Weak
U_7	45	0	1	Moderate
U_8	40	0	1	Moderate
U_9	19	0	1	Weak
U_{10}	24	0	1	Weak
U_{11}	49	0	1	Moderate
U_{12}	43	0	1	Strong
U_{13}	37	0	1	Weak
U_{14}	-	1	-	Failed
U_{15}	47	0	1	Strong
U_{16}	51	0	1	Strong
U_{17}	18	0	1	Weak
U_{18}	26	0	1	Moderate
U_{19}	29	0	1	Moderate
U_{20}	39	0	1	Moderate
U_{21}	50	0	1	Strong
U_{22}	22	0	1	Weak
U_{23}	32	0	1	Moderate
U_{24}	-	1	-	Failed
U_{25}	44	0	1	Strong
U_{26}	51	0	1	Strong
U_{27}	31	0	1	Weak
U_{28}	41	0	1	Strong
U_{29}	38	0	1	Strong
U_{30}	29	0	1	Moderate
Total U_n	μ (s) = 34.03	2	28	W – 8, M – 11, S – 9

Table II Result Comparison

Scheme	Priyanka [6]	Proposed
μ (s)	38.75	34.03
σ(s)	12.85	10.87
Max(s)	59	51
Min(s)	25	15
Failed Users (F_n)	Not Mentioned	2
Successful Users (S_n)	Not Mentioned	28

VI. Conclusion & Future Scope

Thus the proposed work is able to secure the authentication system from machine based attacks that can break the data confidentiality. Attack is a programming loop that can attempt all possible stabs to break the authenticity of the system. Proposed system can deny these machine entries to getting registered and prohibits them during authentication. So, the proposed work overcomes the previously implemented problems that affect the security premises. The present systems get enhanced in future by turning it in hard AI problems which can only solved by human.

References

[1] PNG Image, CAPTCHA Code PNG 1, Accessed. 06-Dec-2022, Available. https://pngimage.net/captcha-code-png-1/.

[2] Zhu, Bin & Yan, Jeff & Bao, Guanbo & Yang, Maowei & xu, Niu. (2014). Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems. IEEE Transactions on Information Forensics and Security. 9. 891-904. 10.1109/TIFS.2014.2312547.

[3] SILLA NIROSHA, URLAM SRIDHAR, Captcha As Graphical Passwords—A New Security Primitive Based On Hard AI Problems, (IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH, Volume No.5, Issue No.4, June – July 2017, 7030-7035.

[4] Shraddha S. Banne1, Kishor N. Shedge2, CARP: CAPTCHA as A Graphical Password Based Authentication Scheme, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 1, January 2016.

[5] Kalyani S Kumar, Captcha as Graphical Passwords, International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 1975-1985.

[6] Advanced CAPTCHA as a graphical password for better secure authentication, proposed by Priyanka Pipersaniya and Jijo S.Nair, in 2017 of IJIET.

[7] Click and Session Based—Captcha as Graphical Password Authentication Schemes for Smart Phone and Web proposed by Vikas K. Kolekar and Milindkumar B. Vaidya in 2015 on IEEE.

[8] Captcha As Graphical Passwords-Enhanced With Video-Based Captcha For Secure Services proposed by Anjitha K and Rijin I K in 2015 on IEEE.

[9] The Graphical Security System by using CaRP proposed by Pooja Jaiprakash Kulkarni and Dr. G. M. Malwatkar in 2015 IEEE.

[10] Captcha As Graphical Password For High Security proposed by Devina Vinod1, Anjana S.2 in 2015 of Global Journal of Advanced Engineering Technologies .

[11] Review Paper on Improved Security Using Captcha as Graphical Password proposed by Priyanka J. Charde, Prof. M. S. Khandare in 2016 IJSRSET.