International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Color Channel CAPTCHA: A Secure Scheme for Cloud Environment

PL. Chithra, K. Sathya,

Abstract: ***Abuse of cloud services consequently unauthorized access to cloud data by malicious software automation is prevented by CAPTCHA. The secure usable mechanism is mandatory for resilience to automate attacks accordingly to create pleasant challenges. In this paper, we propose a novel image-based graphical Color Channel CAPTCHA scheme to distinguish between malware and humans for data security in the cloud environment. This color channel CAPTCHA is designed with 2 X 2 grids of different color channels with micro invisible circles or less visible moving circles. This simple challenge is completed by click on the specified circles in the given order with very less solving time, while compared to the state of the art. The experimental study has been conducted among 41 participants on both usability and performance of color channel CAPTCHA.***

Keywords: Color channel, graphical, micro, invisible.

I. INTRODUCTION

Data storage in the cloud is a service design in which data is managed, backed up and maintained remotely and always make available to users through the network. Some specific reasons are there to store data in the cloud, the user can access the data anytime and anywhere, high data protection, low cost, scalability and flexibility and gives high-performance processing. This cloud storage does face some insecurity like files are not encrypted, transfer of data is not protected, and mainly poor password practices. The best cloud service provider is who keeps their client's accounts and data safe. Hence this remote database service provider is abruptly in the need of multi-level authentication to protect the backed up data. Color channel CAPTCHA is used as second-level authentication in the cloud database site to access and store the data whether by human or by automated software. User's data are exploited by automated programs like mimicking the human action for criminal activities. Some other examples of abuse done by the automated applications (i) register 'n' number of free accounts at a time (ii) posting inflammatory comments on social media (iii) automatic voting in online polls. (iv) Create a password iteration for the whole space to find the exact password (v) click on the advertisement to get revenue (vi) creating the illusion of a physical presence.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Dr.PL.Chithra*, Professor, Dept. of Computer Science, University of Madras, TN, India. Email: chitrasp2001@yahoo.com.
K.Sathya, Research Scholar, Dept. of Computer Science, University of Madras, TN, India. Email: sathyabalaji33@gmail.com.

The potential of cloud services abuse can be reduced by this proposed scenario whether the request has been initiated by a human or by the automated software. CAPTCHA (completely automated public Turing test to tell Computers and Humans Apart) distinguish between humans and computer programs, this is designed to be easy for humans but hard to solve for computers.

Google's reCAPTCHA is the most widely adopted CAPTCHA by popular websites which is difficult for computer programs but easy for a human. reCAPTCHA has taken multiple forms over the years as text, image, and audio challenges but it has been solved by automated applications with high accuracy [1]. Then Google introduced NoCAPTCHA reCAPTCHA in 2014 to overcome the difficulties in the existing reCAPTCHA model [2]. In NoCAPTCHA, the user should click on the box to enable 'I am not a robot'. Google is secretly monitoring the behavior of the clicking over the checkbox to distinguish whether human or not before allowing access to online services.

In CAPPTCHA (Completely Automated Public Physical Test to tell Computers and Humans Apart) [3] asks the user to tilt the smartphone to a certain degree to identify humans. But this CAPPTCHA can be applied only in mobile phones, not suitable for all devices which are connected to the network. In recent days, the storage of large data (cloud storage) in a secure place is a very big issue like protection against automated abuses. This proposal of color channel CAPTCHA gives an enormous level of security and usability while using along with existing first level authentication (user ID and password). Captcha is a reverse Turing test given by the service provider to a service requestor, based on the submission of the response; the server will provide the access or deny it. Captcha-challenge response tests that aim at preventing unwanted machines, including bots from commenting spam in blogs, registering at websites, harvesting email addresses and conducting dictionary attacks, among others[4].Several big companies have suggested and applied captchas [5] including Google's reCAPTCHA [6] eBay captcha, yahoo mail captcha and Microsoft's ASIRRA [7].

The remaining parts of this paper are organized as follows. Related Works is in section 2.Proposed work is in section 3 as Color channel CAPTCHA, Click or Tap Attribute, Color Channels and Color channel click partition based on integer partition. Security Analysis is in section 4 as Relay attacks by the human – solver, Reverse Engineering attack and Password replay and Brute force attack. This proposed work is investigated the usability perspectives systematically in section 5. Finally, the conclusion is given in section 6.

II. LITERATURE REVIEW

Text-based CAPTCHA is widely used CAPTCHA, which is displayed as a distorted text. This text-based CAPTCHA challenge is easily solved by artificial intelligence technology with 99.8% accuracy [8]. Pinkas et al. [9] proposed a scheme that is a combination of a password with CAPTCHA against online dictionary attacks. To protect cloud servers against malicious registration and logins, Yeh et al. [10] introduced a CAPTCHA for user authentication. Pequegnot et al.[11] insisted to use CAPTCHA to enhance the security of PIN codes against automated attacks in mobile devices. To improve the protection of passwords against various attacks Althamary et al. [12] proposed a CAPTCHA based authentication in the cloud environment.

[19] Proposed a CAPTCHA, this method authenticates the original user based on the timing differences in the entered keystrokes and movement of the phone while entering the password. This method is designed based on 3-dimensional sensors such as the accelerometer, the orientation, the magnetometer, the gravity sensors, and the gyroscope. Tap Logger [13], a Trojan application collects the data through an accelerometer (detect the number of taps) and orientation sensors (find position of the taps). This detected data are enough to log the screen on, detect credit card numbers and PIN numbers. Hence tap information on soft keywords is gathered from accelerometer and gyroscope readings in smartphones and tablets. This information is sufficient to enter into the smart devices. Image-based CAPTCHAs need a vast number of images with interpretations otherwise can be broken by visual object recognition algorithms.

Knowledge-based cognitive CAPTCHA is an image-based [14] which requires very specific knowledge in particular discipline during verification processes. ADAMAS CAPTCHA [15] proposed a model of interweaving Unicode and color to enhance CAPTCHA security. This model offers a multi-layered approach, Unicode as an input space, virtual keyboard as the input device, randomization, homoglyphs and correlated usage of colors in foreground and background. Farett-Gender, Farett-gender & age [16]two novel face-recognition CAPTCHAs are proposed. This model is required to click on the 5 female images among 25 images for Farett-Gender CAPTCHA and among 16 images click on 3 women images then need to find the youngest women for Farett-Gender & Age CAPTCHA.

FaceDCAPTCHA [17], the user must identify visually-distorted human face embedded in a complex background without selecting any non-human face. Confident CAPTCHA [18] asks the user to click on all the images according to the symbols such as cat, bird, and dog which are displayed by the scheme. PL. Chithra and K. Sathya [20] developed a secure system like PixCAPTCHA random pictures have been displayed with the content of crop properties and instruction of how much pixels to be cropped and in pixcaptcha graphical password[21], user should select an image in the image pool, then selected image is cropped with size in the ratio of 1:1,2:1,3:2,5:4,6:5,7:5 and etc. and the cropped image is pasted in the specified place.

III. PROPOSED WORK

In this paper, LCC proposes a new graphical CAPTCHA. It combines the existing knock code technique by transforming it into a new type of click with a modified knock code password system for all smart devices, applications, and websites. It provides multiple steps of resilience against multiple attacks. The details of this proposed scheme are presented in the following sections.

A. *Color channel CAPTCHA*

To prevent automated access of the web resources, remote cloud applications or sensitive mobile services, the user should perform a challenging task in order to prove that he is a human. For this motive, color channel CAPTCHA asks the user to click or tap on the micro invisible or less visible moving dots that are hidden or visible in the 2 x 2 color channels. Each channel contains 4 micro invisible dots in each channel namely left top (L_t), right top (R_t), right bottom (R_b), left bottom (L_b). In this scheme, the user needs to click or touch on the color channel in two circles where the annotation says as the CAPTCHA challenge. The user interface for color channel CAPTCHA is shown in Fig 2. There is no additional task to be performed by the user, only thing users should understand the annotation carefully.

The user may feel a little difficult for the first time; complete it within a few seconds if they get trained with it. The working principle flow of color channel CAPTCHA is shown in Fig 1. If the user wants to get access to the cloud service through a browser or web service, the color channel CAPTCHA's hidden microdots or less visible moving dots need to be clicked for the second level authentication. If the rest of the place which is not covered with dots gets the click more than 2 times, authentication cannot be given to the particular user moreover the user is considered as a malicious program.

B. *Click or Tap attribute with less visible moving circle*

Totally 16 numbers of invisible or less visible concentric dots are hidden or visible with moving in 4 color channels each consists of 4 dots which is shown in Fig 5 and Fig 3. These dots appear as the pattern lock dots which is currently used in smartphones but relatively bigger than pattern dots. To identify humans from the malicious, tap with one or two wrong taps around the concentric circles are considered as human conversely more than two wrong clicks in and around the concentric circles are considered malicious. Two wrong taps nearer to the specified circle's boundary are allowed. 100 tap data were collected from 41 participants of different age groups. To increase the usability, the number of circles is reduced and the visibility of the circle is increased with one annotation as depicted in fig 3.

C. *Color channels*

The color channel is displayed with random colors for each and every new CAPTCHA as depicted in Fig 4. This novel CAPTCHA model appeared with a different color pattern for every time and every user accompanied by the randomized hint that says the number of clicks and sequences; the user should do to complete the CAPTCHA test. According to the hint or annotation, the user should complete the process to pass the test. If the user's number of clicks and order equals to the hint which is produced at the time of online transaction or registration, the user is authenticated as a human, thus the captcha test is completed.

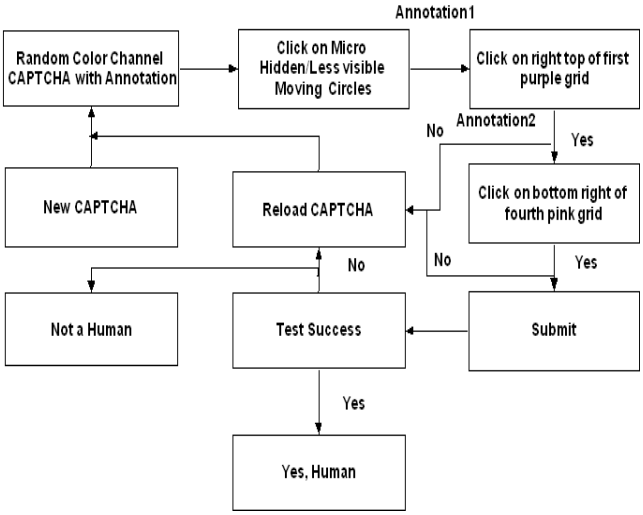

Fig 1. Working flow of color channel CAPTCHA

Total area of a channel (T_c) is (2cm * 2cm) 4cm^2 and area of single hidden micro circle (C_{di}) is 0.196cm^2 (π * 0.25cm(r)*0.25cm(r)) which is approximately 0.2cm and total area of 4 circles (target area) is 0.784 cm^2 (4* 0.196 cm^2). Then the non-target area (W_c) is the difference between the total area and target area, which is equal to 3.216cm^2 as in eqn.2. Every single circle dot is bounded with square area (S_c) which is nearly 0.44cm^2 including the circle dot area (C_{di}) (0.196cm^2=0.2cm^2).Without C_{di} the single bounded area (B_c) is nearly 0.244cm^2.Eqn.1 describes the circle dots (C_d) of every channel.

$$\left\{C^{n}_{d\,i=1}\right\} = \{d\} = \{L_{t1} / R_{t1} / R_{b1} / L_{b1}\} \ldots \{L_{tn} / R_{tn} / R_{bn} / L_{bn}\} \quad \ldots (1)$$

Total Wrong Tap area / non-target area in a channel

$$(W_c) = [T_c - (4 * C_{di})] \quad \ldots (2)$$

C_{di} and C_{di+1} are any two adjacent circle dots among 4 circles. The distance between two circles (C_{di}) is considered as wrong tap area. Then the Square bounded area (S_c) with C_{di} is calculated using eqn.3 and the absolute nontarget area of a single C_{di} (B_c) is calculated with eqn.4.

$$S_c = \left\{\left[(SideofColorChannel - (r*2)*2)/2\right] + (r*2)\right\}^2 \quad \ldots (3)$$

Bounded square area of a single

$$C_{di} = (B_c) = [S_c - C_{di}] \quad \ldots (4)$$

If the click area is more than the value of (B_c / W_c) to the corresponding C_{di}, then it will be considered as a failure of challenge hence CAPTCHA will be refreshed. The human solving rate and solving time is compared with other solutions, which is depicted in Table 1.

Table 1. Comparison with other solutions

Website / CAPTCHA Scheme	Human solving rate (%)	Solving Time (sec)
reCAPTCHA	85	9.6
eBay	96	6.3
Microsoft	86	9.5
Yahoo	91	8.6
Cognitive CAPTCHA	89	7.3
Google	92	7.7
Color Channel CAPTCHA (proposed work)	98	4.5(less than 5 sec)

D. *Color channel click partition based on integer partition*

An integer partition of n Ɛ N is a unique way of writing 'n' as the sum of integers. Partitions that differ in the order only are considered to be the same partition. Restricted partition is a partition that is restricted under specified conditions. The total number of clicks spread into the 4 channels according to the integer partition function p (n) represents the number of a possible partition of a natural number 'n' which is to say the number of distinct ways of representing 'n' as a sum of natural numbers.

$$P(n) \cong \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) - 1 \quad \ldots (5)$$

This formula in eqn.5 is used to find the approximate partition of integer but it gives weak approximation value. The partition function gives the value of every integer like p(1) = {1}, p(2) = {(2) and (1,1) }, p(3) = {(3), (2,1) and (1,1,1)} and so on. So the final absolute value of integer partition of p(0)=1, p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5 and for rest of the value refer in table 2.

Table 2. Integer Partition

N	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(n)	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

IV. SECURITY ANALYSIS

The security of this model against prominent threats and attacks is discussed in this section.

A. *Relay attacks by human – solver*

The main aim of the CAPTCHA is to distinguish between human and malicious programs. Here, the challenges are done by the remote solver, not by automated software to get unauthorized access by cracking the password. CAPTCHA challenges are relayed to some remote human solver; hence, the security provided by the CAPTCHA is by-passed. The difference between the legitimate user and remote human solver cannot be identified, thus the relay attack is considered as a most effective attack than others.

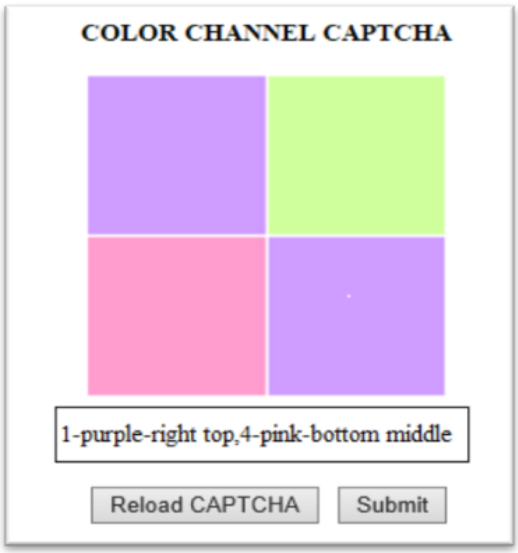

Fig.2. User interface for color channel CAPTCHA

In color channel CAPTCHA, only two annotations are given to the legitimate user, the user is asked to solve it in 5 seconds (because the average time taken to solve the color channel CAPTCHA by 41 participants is less than 5 second). If the user fails to pass the test within 5 seconds, then the new color channel CAPTCHA appears. Hence, the relay attack by a human solver cannot be performed on the color channel CAPTCHA. The time limit (5 seconds) is not enough to send the challenge to a different location for the remote human solver.

A. *Reverse Engineering attack*

Obfuscation of code is, transform a program into another program difficult to understand and read by either applying cryptographic key, the design of the software or algorithm used in the software. In this color channel CAPTCHA, source code formatting of layout obfuscation and compression is applied to protect the code from reverse engineering attack. Hence, de-obfuscation could not be achieved in any practice. A minifier eliminates the comments and unnecessary whitespace from a program. Depending on how the programming code is written, this can minimize the size.

Fig.3. Color Channel CAPTCHA with less visible moving circle.

Fig 4.Color channels

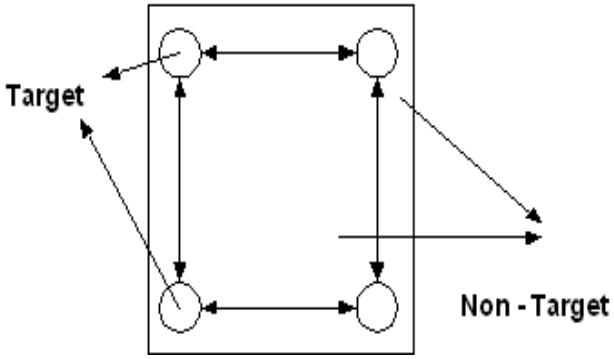

Fig 5. Single channel with target and non-target area

An obfuscator also minifies, but it will also modify the program, changing the names of variables, functions, and members, making the program much harder to understand, and further reducing its size.

Digital assets and intellectual property like source code are secured by obfuscation, but this is not the only approach to protect the code, defeatable at the same time harder for the code cracker. Obfuscation comprises the following features, name obfuscation, code flow obfuscation, minification and compression, dead code insertion, string encryption, and powerful locking. Minification and compression reduces the size of code and helps to load it quicker and minimizing bandwidth consumption. Dead code insertion is some unexecutable code inserted to the source code to avoid modification and theft. To secure this color channel captcha code, some of the features of obfuscation are applied and the result is shown below.

Obfuscator

```
var
_0xfef0=["\x3C\x69\x6D\x67\x20\x73\x72\x63\x3D\x22\x43\x3A\x2F\x55\x73\x65\x72\x73\x2F\x57\x65\x6C\x63\x6F\x6D\x65\x2F\x50\x69\x63\x74\x75\x72\x65\x73\x2F\x73\x68\x61\x70\x65\x34\x2E\x6A\x70\x67\x22\x3E","\x73\x75\x63\x63\x65\x73\x73","\x6E\x6F\x74\x20\x73\x75\x63\x63\x65\x73\x73"];var img1;function check1(){img1=_0xfef0[0];var _0xf25dx3=1;if(_0xf25dx3===1){alert(_0xfef0[1])}else {alert(_0xfef0[2])}}
```

Compressor

Before Compression

```
//function check1()
  //{
   //var
img1='<imgsrc="C:/Users/Welcome/Pictures/shape4.jpg">';
/varcol1=document.getElementById('slotID-1').style.backgroundColor;document.getElementById("demo").style.color = "red";
  //}
var img1;
```

```
//s=document.getElementById('img').src;
function check1()
 {
 img1='<imgsrc="C:/Users/Welcome/Pictures/shape4.jpg">';
var s=1;
if(s === 1)
            //document.getElementById("img1").src =
"C:/Users/Welcome/Pictures/shape4.jpg";
alert("success");
else
alert("not success");
  //var s1=document.getElementById("image");
 // alert(s1);
 }
```

After compression

```
Varimg1;function
check1(){img1='<imgsrc="C:/Users/Welcome/Pictures/shap
e4.jpg">';alert("success")}
```

After compression and Obfuscation

```
var
_0x8ec3=["\x3C\x69\x6D\x67\x20\x73\x72\x63\x3D\x22\x4
3\x3A\x2F\x55\x73\x65\x72\x73\x2F\x57\x65\x6C\x63\x6F\
x6D\x65\x2F\x50\x69\x63\x74\x75\x72\x65\x73\x2F\x73\x6
8\x61\x70\x65\x34\x2E\x6A\x70\x67\x22\x3E","\x73\x75\x
63\x63\x65\x73\x73"];Var;img1;function check1(){img1=
_0x8ec3[0];alert(_0x8ec3[1])}
```

Dead Code Insertion

```
{
  "color-change and moving": {
    "document.getElementById('img').src":
"getElementById",
    "document.getElementById('img').src1":
"getElementById"
  },
  "document.getElementById('img').src2": "style.color",
  "document.getElementById('img').src3": [
    {
      "backgroundColor": "style.color"
    }
  ]
```

B. *Password replay and Brute force attack*

Brute force attack is the trial and error method to find the correct password by trying all possible combinations. In order to secure the password from discovering it through a brute force attack, color channel CAPTCHA is used to access the service by the legitimate user. If malicious software successfully catches the correct password but cannot get access of the service, thus color channel CAPTCHA provides the security of passwords against password replay and brute force attack. Brute force attack or AI-based attack can break the CAPTCHA by using a machine learning algorithm with the probability in excess of 1% are considered as insecure which was proved in existing methodologies. Here Google's reCAPTCHA was taken as a benchmark for all the CAPTCHAs to compare the security with this proposed CAPTCHA system. reCAPTCHA's probability of success was calculated for 'p' length of characters from 'q' set of total characters (A-Z,a-z,0-9) as in Eqn 6.

$$SP_{reCAPTCHA} = \frac{1}{q^p} = \frac{1}{62^7} = 2.84.\ 10^{-13} \quad \ldots \quad (6)$$

This SP (success probability) value is below 1%, hence the reCAPTCHA is considered as secured. For this system, 'p' is 2 annotations which consist of 2 channel numbers, 2 colors, 2 micro circle dots position and 'q' is total number channels with microdots (4 x 4), number of random colors(32). Based on this method SP is calculated for this proposed methodology for the visible dots as in Eqn 7.

$$SP_{ccCAPTCHA} = \frac{1}{48^6} = 8.17\ .\ 10^{-11} \quad \ldots \quad (7)$$

If the microdots are visible, then the success probability of brute force or AI-based attack's value is 8.17 x 10^{-11}. Brute force attack on color channel captcha, an attack has to guess 'i' micro invisible circle dots out of a set of 'j' dots. One solution out of $\binom{j}{i}$ options, hence attackers success probability rate is calculated as in Eqn 8.

$$SP_{ccCAPTCHA} = \frac{1}{\binom{j}{i}} = \frac{i!(j-i)!}{j!} = \frac{1}{\binom{48}{6}} = \frac{6!(48-6)!}{48!}$$

$$= 0.0000000814\% \quad \ldots \quad (8)$$

This amounts to approximately 8.14 x 10^{-8} for j=48 i=6, which can be considered more secure than existing captcha systems of reCAPTCHA and Farett-gender CAPTCHA. According to this methodology, $SP_{ccCAPTCHA}$ value is considered as a minimum and it exceeds tremendously because of its invisible nature.

V. USABILITY STUDY

The experimental study has been conducted among 41 participants, 40 (98%) participants solved the color channel CAPTCHA successfully which is shown in Fig.6. According to their statement, this proposed scheme is user-friendly. Solving time is evaluated among various age group people (18-30, 31-45, 46-55); the average time to solve this CAPTCHA is 4.5 seconds as depicted in Table.3 consequently in Fig.7. To compute average accuracy for human responses using the Eqn.9

$$\text{Accuracy} = \frac{Total Number of Correct Tap}{Total Number of Tap} \text{ x } 100 \ldots \quad (9)$$

Here a correct response means that in a given CAPTCHA, microdots are correctly tapped with other challenges including channel number, color, and invisible attribute.

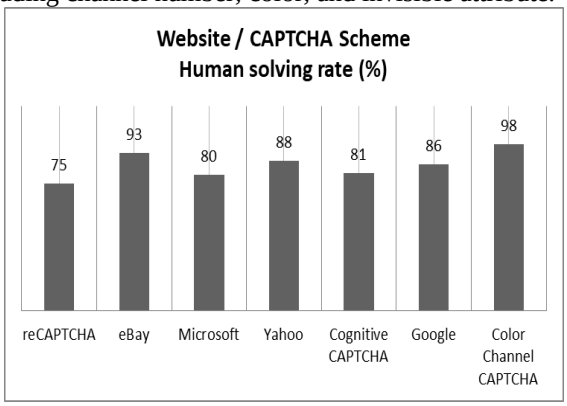

Fig 6. Comparison of Color Channel CAPTCHA's Human solving rate with other schemes

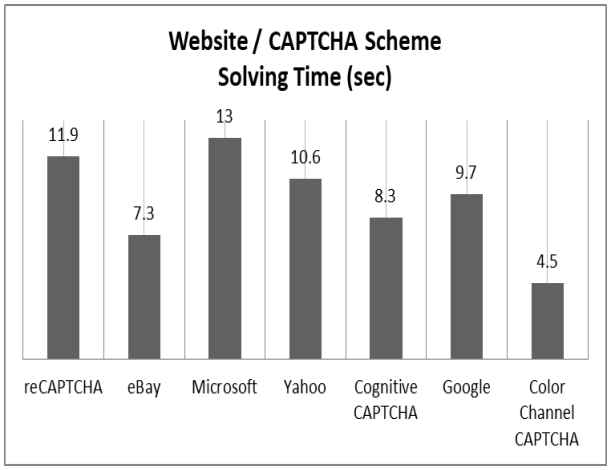

Fig 7.Comparison of Color Channel CAPTCHA's solving time with other schemes

Table.3 Participants average Solving Time

No. of Participants	Age	Solving Time(sec)
18	18-30	3.8
14	31-45	5.4
9	46-55	4.3

VI. CONCLUSION

CAPTCHAs are one of the main security services to protect the cloud service from automated abuses. In this paper, the color channel CAPTCHA is proposed, a novel technique that can potentially eradicate CAPTCHAs low-security issues. This proposed CAPTCHA is difficult for automated software to pass the challenge rather than a human can complete within 5.5 seconds (average 4.5 sec). The performance of this work was evaluated through experiments among 41 participants. As per the result, its user-friendliness, success probability, and time- solving rate are feasible than other existing CAPTCHA challenges.

ACKNOWLEDGMENT

We would like to thank all the participants for their support and involvement to carry out the experimental analysis successfully. This work has been supported by the University of Madras (India) under University Research Fellow Grant No; GCCO/URF/Comp.Science/2019-20/323.

REFERENCES

1. I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, V. D. Shet, Multi-digit number recognition from street view imagery using deep convolutional neural networks, CoRR abs/1312.6082. arXiv: 1312.6082. URL http://arxiv.org/abs/1312.6082
2. Google Inc., recaptcha: Easy on humans, hard on bots (January 2018). URL https://www.google.com/recaptcha/intro/
3. M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, B. Messabih, A completely automatic public physical test to tell computers and humans apart: A way to enhance authentication schemes in mobile devices, in: 2015 International Conference on High Performance Computing Simulation (HPCS), 2015, pp. 203–210. doi:10.1109/HPCSim.2015.7237041.
4. Carnegie Mellon University, (2010), captcha: Telling humans and computers apart automatically, http://www.captcha.net.
5. Bursztein E., Martin M., Mitchell J., Text-based captcha strengths and weaknesses. Proceedings of the 18th ACM conference on Computer and communications security - CCS11, (2011) 125.
6. Von Ahn L., Maurer B., McMillen C., Abraham D., Blum M., recaptcha: Human-based character recognition via web security measures. Science, 321 (2008) 1465–1468.
7. Elson J., Douceur J., Howell J., Saul J., Asirra: a captcha that exploits interest-aligned manual image categorization, CCS, 7 (2007) 366–374.
8. I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, V. D. Shet, Multi-digit number recognition from street view imagery using deep convolutional neural networks, CoRR abs/1312.6082. arXiv:1312.6082. URL http://arxiv.org/abs/1312.6082
9. B.Pinkas, T. Sander, Securing passwords against dictionary attacks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS '02, ACM, New York, NY, USA, 2002, pp.161–170.doi:10.1145/586110.586133. URLhttp://doi.acm.org/10.1145/586110.586133
10. H.-T. Yeh, B.-C. Chen, Y.-C. Wu, Mobile user authentication system in cloud environment, Security and Communication Networks 6 (9) (2013)1161–1168.doi:10.1002/sec.688.
11. URL http://dx.doi.org/10.1002/sec.688
12. D. Pequegnot, L. Cart-Lamy, A. Thomas, T. Tigeon, J. Iguchi Cartigny, J. L. Lanet, A security mechanism to increase confidence in m-transactions, in: 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2011, pp. 1–8. doi:10.1109/CRiSIS.2011.6061836
13. I. A. Althamary, E. S. M. El-Alfy, A more secure scheme for captcha based authentication in cloud environment, in: 2017 8th International Conference on Information Technology (ICIT),2017,pp.405–411.
14. doi:10.1109/ICITECH.2017.8080034.
15. Z. Xu, K. Bai, S. Zhu, Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors, in: Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC '12, ACM, New York, NY, USA, 2012,pp.113–124.doi:10.1145/2185448.2185465.URL http://doi.acm.org/10.1145/2185448.2185465
16. Ogiela MR, Krzyworzeka N, Ogiela L. Application of knowledge-based cognitive CAPTCHA in Cloud of Things security.ConcurrencyComputatPractExper.2018;e4769.https://doi.org /10.1002/cpe.4769
17. Narges R, James M, ADAMAS: Interweaving Unicode and color to enhance CAPTCHA security. In: Future Generation Computer Systems,2016,55.p.289-310.
18. Guido S, Gerit W, Alexander S, Development of two novel face-recognition CAPTCHAs: A security and usability study. In: Computers and security, 2016, 60. p.95-116.
19. Gaurav G, Brain M.P, Mayank V, Richa S, Afzal N, FaceDCAPTCHA: Face detection based color image CAPTCHA. In: Future Generation Computer Systems, 2014, 31.p59-68.
20. Confident Technologies. Confident CAPTCHA.
21. <http://http://confidenttechnologies.com/confident-captcha//>;2019.
22. A. Buriro, S. Gupta, B. Crispo, Evaluation of motion-based touch typing biometrics for online banking, in: 2017 International Conference of the Biometrics Special Interest Group (BIOSIG), 2017, pp. 1–5. doi:10.23919/BIOSIG.2017.8053504.
23. P.L.Chithra, K.Sathya, PixCaptcha A Novel Genre Captcha For User Dexterity, fourth International Conference on parallel, distributed grid computing(PDGC),IEEE,2016.pp.301-305.
24. P.L.Chithra, K.Sathya, Pristine PixCaptcha as Graphical Password for Secure eBanking Using Gaussian Elimination and Cleaves Algorithm, 2nd International Conference on Computer, Communication, and Signal Processing (ICCCSP),IEEE,2018.

AUTHORS PROFILE

Dr. PL. Chithra is the Professor in the Department of Computer Science at the University of Madras. She received her M.C.A and Ph.D. degrees from Alagappa University, Tamil Nadu, India and University of Madras, Tamil Nadu, India respectively. She has more than 29 years of experience in teaching. She has been serving as Organizing Chair and Program Chair of several International conferences, Program Committees of several International conferences and she is awarded UGC FIP program for two years.

Ph.D. and M.Phil. research supervisor for Guiding Image Processing Techniques, Big data analytics and Network Security. She has conducted several refresher courses and published more than 65 papers in national and international journals with 42 citations and 4 h-index. She is one of the Computer science staff selection committee members for various affiliated colleges of University of Madras.

Mrs. Sathya. K is a Research Scholar in the Department of Computer Science at the University of Madras. She received M.C.A, M.Phil degree from Madurai Kamaraj University and Thiruvalluvar University, Tamil Nadu, India respectively. She has qualified National Eligibility Test (NET). She is specialized in Information Security and her main research topic is secure online communication through encryption and development of novel CAPTCHAs.