8th International Engineering Conference on advances in Computer and Civil Engineering Towards Engineering Innovations and Sustainability, ( IEC-2022), Erbil-Iraq

2022 8th International Engineering Conference on Sustainable Technology and Development (IEC) | 978-1-6654-7829-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/IEC54822.2022.9807472

# An Automated CAPTCHA for Website Protection Based on User Behavioral Model

Hoshang Qasim Awla
*Computer Science Department/ Faculty of Science/ Soran University*
*Soran, Kurdistan Regional Government, Iraq*
*IT Department, College of Engineering and Computer Science, Lebanese French* University, Erbil, Kurdistan Region,
hoshang.awla@soran.edu.iq

Arsalan Rahman Mirza
*Computer Science Department*
*Soran University*
Soran, Kurdistan Regional Government, Iraq
arsalan.mirza@soran.edu.iq

Shahab Wahhab Kareem
*Department of Technical Information Systems Engineering*
*Erbil Technical Engineering College*
Erbil Polytechnique University
Erbil, Iraq
shahab.kareem@epu.edu.iq

***Abstract*-CAPTCHA (Completely Automated Public Test to tell Computers and Humans Apart) currently is the standard security technology and has been used widely in applications on commercial websites. It is an automated method with human maintenance and intervention and it is used for protecting the websites from automated attackers. There exist different types of CAPTCHA, ranging from difficult/easy to complex/simple ones. The problem with current CAPTCHAs is most of them use one single layout and simple user interface to distinguish the human from the attacker. This mechanism will help the attacker to easily bypass by using an appropriate bot program. In this paper, the main objective is to make a survey regarding the available security technique and evaluate the existing ones according to a set of characteristics for defending against attackers. Upon the evaluation result, a new user behavioral model has been proposed based on the user activity. In the proposed method the user behavior is scored according to the characteristics needed by their web applications. Finally, the model is implemented by building a web application and validated using an experimental setup and achieved a score of 70.26 for the usability of the model and the proposed method compared with other CAPTCHA tests and with the experimental evaluations, the proposed method is easier to solve and more user-friendly.**

***Keywords: CAPTCHA, Website protection, Attack, Security Mechanism, Automated Machine, User Behavior***.

## I. INTRODUCTION

In the past 20 years, there has been a tremendous increase in the use of the internet. With the development of large open networks, security threats have increased significantly. Network security is constantly focused on protecting profitable services such as social media, banking systems, and websites [1]. Internet services are employed in numerous areas, so many daily tasks, such as sales and banking, are performed through the internet. Therefore, protecting internet services against attackers has become very necessary which may compromise a system in the absence of any secure applications protecting against such threats [6],[ 7].

Computer automated programs can run automated tasks over the network. The application layer is the most significant layer which is targeted in many attacks against the network. Protecting the network in the Application Layer Network will be an efficient method for preventing threats and stabilizing the network to provide services. The authors investigate the Application layer network which is a mechanism for resisting attacks on networks [3].

Application layer denial of service (DoS) attacks make up one of the major threats among the hardest security problems in today's internet. The DoS attack is the most common in network security with the progress of network and internet [3]. DoS attack detection technologies which include networks traffic detection and packet content detection are presented. These attacks obtain their goal by sending a victim a stream of packets that swamps his network or processing capacity thereby denying access to his regular clients. The most popular DoS attacks target the computer network's bandwidth or connectivity [3], [4].

On the other hand, Distributed Denial of Service (DDoS) attempts to make online services unavailable to users. It usually interrupts or suspends the services of its hosting server temporarily. Unlike a DoS attack, DDoS attacks in a group can be programmed by an attacker. It is divided into many computers that all carry a legal IP but are not legal users, which means they are zombie machines [4]. While attacking, much traffic is directed at the servers, and they can enter the website and obtain the data. The main goal of a DDoS attack is to cause damage to a victim either for popularity or for personal reasons. DDoS attacks consist of four elements; real attacker, handlers or masters, daemon agent or zombie hosts, and the victim or target hosts [2],[ 4].

Although most people are not familiar with the term CAPTCHA, many use them weekly or even daily. CAPTCHAs are the security tests that are most often found on websites that require the use of registration [3]. The purpose of CAPTCHA is to restrict access to a website and prevent the attacker to run

an automated program. For example, humans can read distorted text, but computer programs (bot and automated program) may not be able to [5, 10] while requiring a correct answer to a question, which only a human can answer rather than any better random guess. Humans have speed limitations, and hence, cannot replicate the impact of an automated program [11]. CAPTCHA is useful for several applications like preventing website registration, protecting against comment spam in blogs, protecting email addresses from web scrapper's online pols, preventing worm and spam in emails, and preventing dictionary attacks in password systems [7], [8],[ 9].

The remainder of this study is organized in the following manner: In section 2, different type of CAPTCHA and user behavior has been investigated. In section 3, the contribution of this paper is explained. In section 4, the proposed framework evaluated with result. Finally in section 5, is the conclusion of the paper.

## II. Related Works

In this section, the recent works and the previous research conducted on the user behavioral model and CAPTCHA mechanism tests, the techniques that are used for differentiating human users from automated programs will be considered.

In researches done by [12], [13] described the classification of current CAPTCHA, and the classification was based on text, images, voice, video, and puzzles. While Chow. Y, et al [12] illustrated the fundamental requirement of CAPTCHAs necessitates that they must be designed to be easy for humans but difficult for computers. Thus, it is well recognized that the trade-off between usability and security is difficult to balance. On the other hand, [14], [15] outlines a typical method in the text-based CAPTCHA. Chen. J, et al [14] used text-based CAPTCHA by breaking and proposing a framework of text-based CAPTCHA breaking technique which consists of preprocessing, segmentation, combination, recognition, postprocessing, and other modules. Also, UmaMaheswari. P, et al [15] proposed a dynamic approach to predict Text-based CAPTCHAs that challenges the supposition that they cannot be solved by computers. Three types of CAPTCHAs namely Rotated, Noisy Arc, Complicated Background has been taken. The CAPTCHAs are pre-processed based Erosion, Dilation, Binarization are used to remove the noise from the CAPTCHA. The pre-processed CAPTCHAs are then fed to the **Convolutional neural network (CNN)** which generates a feature vector. This feature vector is then passed to the long-short-term-memory (LSTM) which generates a sequence of characters. This sequence is displayed as an outcome to the user. The dataset for Rotated, Noisy Arc, Complicated Background CAPTCHAs consisted of 9,955, 1,070, and 1,000 images respectively. The model was also tested for CAPTCHAs involving a combination of different resistance mechanisms. The model was able to predict Rotated CAPTCHAs with an accuracy of 85.97%, Noisy Arc CAPTCHAs with an accuracy of 84.52%, and Complicated Background CAPTCHAs with an accuracy of 82.91%. While, Bostik. O, et al [16], compared several machine learning classifications algorithms for Optical Character Recognition of CAPTCHA by using Neural Networks, K-Nearest Neighbour (KNN), Support Vector Machine (SVM), and Decision Trees. Finally achieved success rates of 89% for all algorithms. Based on the data found, it is possible to choose the right algorithm for the particular algorithm.

Zhang. Y, et al [17] showed that the security of different schemes can be increased by adding font faces and noise to the text-based CAPTCHA. However, compared with other CAPTCHAs, these schemes require a more complex operation, and many of them are no longer safe. The image-based CAPTCHA is the most diverse type. Although some image-based CAPTCHAs are vulnerable to deep learning attacks, it still has a large development space. Audio/video-based CAPTCHAs are not common in the real world. While the Audio/Video-based CAPTCHA requires higher bandwidth and takes more time for users to pass. Anil. J, et al [18] proposed a new CAPTCHA model which is known as an image-based captcha generation system, a system that provides controlled distortions on a randomly chosen image for user-friendliness and attack resistance. The primary results of the survey that is conducted are %95 users were a correct response to the CAPTCHA compared with other CAPTCHA types. Alnfiai, M. [18], proposed a real-time audio-based CAPTCHA that enables easy access for users with visual impairments. The user must identify what the sound-maker is. After that, HearAct identifies a word and requires the user to analyze a word and determine whether it has the stated letter or not. The results of the study also show that the success rate of solving the HearAct CAPTCHA is 82.05% and 43.58% for audio CAPTCHA. Conti, M. [20] proposed CAPTCHaStar, which is a novel image-based captcha that leverages the human ability to recognize shapes in confusing environments. The work meets both security and usability requirements for a good captcha design. The success rate was higher than 90 %, which is better than the success rates of captchas currently used in websites such as mail.ru and Microsoft.

Rahman, [21] illustrated, text-based CAPTCHAs are the most widely used in web applications, there are some common weaknesses. The number of characters, classes, and digits is very small and it is possible to identify texts by using Object Character Recognition (OCR); when noise and distortion are added to the text-based CAPTCHA, they often create a problem in recognizing them. Some letters and digits become difficult to recognize when they are distorted. Chandavale, et al [22], and Elie, et al [23], proposed an approach to break text-based CAPTCHAs by using techniques such as Pre-processing, segmentation, post segmentation, recognition, and post-processing, then recognizing the characters depending on their features. Kameswara, et al [24] has illustrated a method to introduce new techniques for CAPTCHA tests, which is video-based CAPTCHA. Also, Kluever and Zanibbe [25] presented a technique in the case of using content-based video labeling as a CAPTCHA test. As shown in Table II , the success rate between human users and machine attacks is compared. In all instances, the human user achieved a better result in understanding what the CAPTCHA is in comparison to the machine attack. The significant part of. Table I is the success attack rate of machines

in video CAPTCHAs, which is less than the human success rate for these types of CAPTCHA. Beitollahi. H and Deconinck .G [26][27] proposes a four-step technique to tackle DDoS attacks. It is a cooperation method between routers of different parts of a network. The routers closed to the server adjust the leaky-bucket of upstream routers close to the source of attacks to stop the attack. And in [27] use the idea of hidden conception to protect a server from DDoS attacks. In fact, Ferris-wheel is an architecture that hides the server while the server provides the services to its users. DDoS attackers have no IP of the server to attack it.

TABLE I: COMPARISON OF SUCCESS RATE FOR HUMAN AND AUTOMATED MACHINES WITH DIFFERENT TYPES OF CAPTCHA.

| | Success Rate | |
|---|---|---|
| **CAPTCHA Types** | **Human** | **Machine** |
| Text-based Microsoft CAPTCHA | 0.90 | 0.60 |
| CAPTCHA based Baffle text | 0.89 | 0.25 |
| Handwriting-based CAPTCHA | 0.76 | 0.13 |
| Image-based CAPTCHA | 0.99 | 0.10 |
| Video-based CAPTCHA | 0.90 | 0.13 |

## III.PROPOSED FRAMEWORK

The proposed framework focuses mainly on two different phases that try to differentiate human users from automated programs. The first phase is the user behavioral model that only observes users' behavior. Each user accessing the website should enter into the user behavior model phase. In this phase, the system will track the user behavior and will record the activity for each user. If the user's behavior looks abnormal, it enters a process where the suspected user faces the second phase (ICAPTCHA Mechanism Test), which includes different types of CAPTCHA tests. The first phase controls user behavior and determines whether the user is a human user or an automated program. In the first phase, if the system recognizes the user as a human, it will allow the user to access the website and continuously track user activity and behavior. In the second phase, to ensure that the user is not a bot, the user will face a CAPTCHA test and if the user passes the test successfully, the user will return to the first phase. Phase one is designed for human users to be able to access the website, and phase two is for deciding on whether the user is a human or bot user.

### *A. Phase I: User Behavioral Model*

The main idea of the user behavior model phase is to collect statistical data about the user during normal conditions. Every user will be recognized based on behavior and recorded data on the website. In this phase, the attributes which are defined for the system are used to control the user activity and the data will be recorded for each user. These attributes and data are website-independent. The user behavior model phase predicts the legal connection with high probability in a feedback control process with the website. For the user behavior model, a scoring schema has been used to identify which type of user is online. The score value during the page loading will be changed based on the defined attributes. Each attribute may decrease the score value to decide whether the user is a human user or not.

The website considers various attributes and statistical data for each user. In the study, each attribute has a specific value, and each time when a user accesses a page on the website, the website will predict a score value for each user. The initial score value for all users when visiting the website for the first time will be 100 and, based on user activity, the score value will change according to the attributes that have been involved by the system during website access. In the user behavior model phase, the threshold value used to decide whether the user is a human or a bot is 50. The score value changes during user activity on the website. If it is less than the threshold value the system sends the user to the second phase, and if greater than the threshold value it allows the user to access the website. In this phase, the system for each attribute will measure its value based on its requirements. The requirements which are used for all attributes in this phase are time, cookie, session, IP address, and user status. Time refers to the duration between a user opening one page and the next page. A cookie is used for tracking the user activity on the pages and for interaction between page sessions. With IP address the system knows that the current user is either a new user or previously visited the website. Finally, the user status determines the current page which is used by the user and its activity.

### *B.Page Time Interval*

Page time interval is the time that each user spends visiting the website. The Page Time Interval shows the amount of time that each user stays on a specific page. If the number of requests for opening the pages happens in a short period, the website counts the user as a bot. For page time interval attributes, if the user tries to open many pages in a short period, the score value will be decreased.

### *C.Decoy Hyperlink*

Decoy hyperlink [28] is a type of fake hyperlink that the human user cannot access and cannot view. However, when the automated program accesses the source code tag of the website, it can easily be detected and opened. This is a factor that can be used to differentiate human users from automated programs.

*i. User Uptime*

The user uptime indicates the total time for each user when interacting with the website until the user session within the website ends [3]. The human user cannot stay on the website for a long time. For the user uptime attribute, if a user stays for a long time (a night, days, weeks) the system will make the user a candidate for a bot and the user score value will be decreased.

*ii. Direct URL Access*

In direct URL access when a user accesses a hidden or long URL within a page, the server can discern whether the URL is directly accessed or redirected to the website. The Website checks the URL validity and request rate for a specific page with different values. This attribute causes the score value to be decreased in case of finding an attempt of the user to append form-data into the URL If a user opens a direct URL from the website the score value will be decreased and if the user opens the pages normally there will be no effect on the attribute value.

*iii. Mouse Movement*

To access any website, a user is required to have control over the mouse cursor. Most users use the mouse pointer to open pages and navigate to specific pages by clicking on the hyperlink. In contrast, the bot program, which opens the links in source tag view, may not use the mouse pointer for opening the links. Mouse movement is one of the main factors for distinguishing the human user from the bot because of the position of the hyperlink changes in different devices and pages.

*iv. Keyboard Usage*

The keyboard will be used by humans when opening the website for data submission, page navigation, and scroll up/down, or using any other type of keyboard shortcut. If this attribute is used by the visitor, the system will distinguish the human user from the bot. When the user doesn't use the keyboard functions, the system detects the user as a bot and decreases the score value because of this attribute. For other cases, there is no effect.

### *D.Score Rate Calculation*

The scoring rate can significantly help the website to detect malicious connections. However, attackers are not aware of the scoring rate and thereby access the pages randomly. The website measures the scoring rate for each user during page visits. The key point is that the website classifies users based on their score rate value into four categories: low, medium, high, and very high rate. The score value will be measured continuously every time users try to open the pages. If the system in the first phase detects the user as an automated program, the score value will be decreased until the user behavior model identifies the user as a candidate for a bot. Whenever another page loads from the website the new value for score will be recorded. The first phase will make the decision based on the score value. The summary of this phase shows in table II .

TABLE II: SCORE VALUES FOR DIFFERENT TYPES OF USERS AND SYSTEM DECISIONS BASED ON THRESHOLD VALUES.

| Score value | Score Status | Type of user | Note |
|---|---|---|---|
| Score < 50 | Low | Bot | Guarantee bot |
| Score = 50 | Medium | Threshold | No decision, |
| 50 < Score < 60 | High | Candidate for a human user | Probability to be a human user |
| 60 < Score | Very high | Human user | Guarantee human |

### *E. Phase II: ICAPTCHA Mechanism Test*

In the ICAPTCHA test, the users have to think to pass the test and used it to protect the website against threats of attack or overloading. By using strong mechanisms like ICAPTCHA with new techniques the system can differentiate normal users from automated programs. Human users can solve ICAPTCHA tests easily but it is complex for automated programs. ICAPTCHA tests guard against threats of attack and are complex to analyze. ICAPTCHA tests are divided into four types, with one example for each kind illustrated in Fig. 1 : (i) IQ CAPTCHA Test; in this test, some numbers are arranged one by one, but one of them is omitted. Users have to find the omitted number. In IQ CAPTCHA tests new types of patterns are generated randomly every time, Fig. 2: (a) depicts one of the samples. (ii) Temperature CAPTCHA Test; illustrate in fig. 1:(b) this test shows an image that refers to a season and users have to select the appropriate temperature. To pass the TCAPTCHA test the user should click on the correct temperature levels. One of the TCAPTCHA is shown in fig. 1:(c), (iii) Order CAPTCHA Test; in this test, three different images are shown in one class. Users have to Drag and Drop the images to reorder correctly [3]. (iv) Velocity CAPTCHA tests; in this test, a picture of a moving car is shown to the user. Beside the road, there are some traffic speed signs. To pass the test, the user has to choose the correct answer which corresponds to the speed of the car, shown in fig. 1:(d).

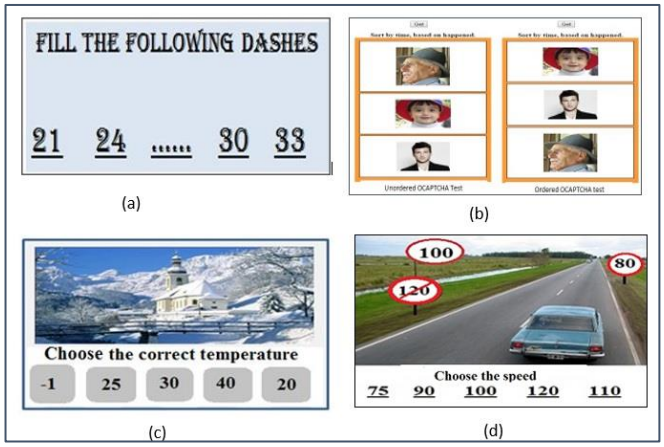


Fig.1: ICAPTCHA Mechanism Test Sample.

ICAPTCHA tests are employed when there is suspicious behavior of a user during the first phase when the user accesses the website. If a user fails to pass the test successfully the first time, the user is presented with another, different CAPTCHA test. Time is a significant factor in the ICAPTCHA test and the time is limited for every test. If the user is not capable of passing the test during the limited time, it renews and presents another different test. With every change, the new test employs a different technique, and thus it causes complexity for attackers to attack those tests. Changing tests in ICAPTCHA is random. Also, those users who face the ICAPTCHA test will have three chances to retake the tests. The target is to limit attempts for attackers. If they fail in all three attempts, they will directly be denied from accessing the website.

Figure 2 shows the "User activity flow chart diagram for ICAPTCHA system". The flow chart diagram is concentrated on the two phases (user behavior model) and (ICAPTCHA Mechanism Test). Opening the page of the website will activate the ICAPTCHA system and, as for the first time when users access a URL within the website, the system will account for the user in the first phase. Then, if the user's behavior is suspect, the user falls into the second phase because of a reduction in the scoring rate. In the second phase, there is an ICAPTCHA test. All users don't need to fall into the second phase unless the user is suspected. If the user could solve the ICAPTCHA tests successfully, the user goes back to the user active page and the

score value becomes 100 again. When a user solves the ICAPTCHA test, the user is considered a new user when accessing the website again. In addition, when the user fails in 3 test attempts, the user will be denied access to the website. The system checks the score value of all the visitors and compares it with the threshold value to determine whether the user has visited the website previously or not, and with the same score value for the attributes of each user.

## IV. Evaluation and Results

### A. Evaluation

To evaluate the proposed ICAPTCHA system for its ability to protect websites from attackers, a user study was performed. In particular, the proposed approach was evaluated in terms of usability from the users' perspective (i.e. user satisfaction). For this purpose, a survey was prepared to evaluate the ICAPTCHA system by users and to determine its efficiency. The survey obtained feedback from users about the system. Fig. 2 shows the ICAPTCHA test flow-chart diagram.

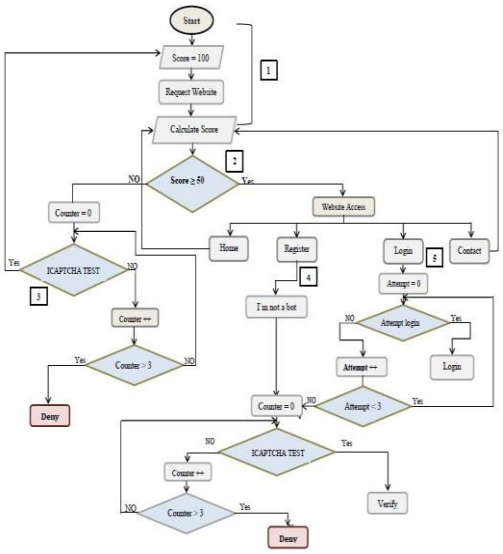


Fig. 2: ICAPTCHA test flow-chart diagram.

In our survey 47 users participated, most of them worked in academic institutions and had a good background in computer science. The results of the participating users are summarized in Table III . From this table we can see that 63.8% of all participants are males and 36.2% are females, most of them were older than 25 years old, 51.1% of the participants are under-graduate, 40.4% post-graduate, and 8.5% hold a Ph.D. As for the number of hours that they spent on the internet, more than 88% of all participants announced that they spent more than two hours on the internet each day.

93.6% of the participants in the survey have substantial knowledge about CAPTCHA tests, and they had already solved CAPTCHAs in the past. As shown in Fig. 3, 48.9% of them think that image CAPTCHA tests are more suitable and easier to solve, while 36.2% percent prefer text-based CAPTCHA. However, audio and video tests were desirable for only a few of the participants.

By using System Usability Scale (SUS) [29], the overall usability of the ICAPTCHA system can be determined. The ICAPTCHA system achieved an average SUS score of 70.26. The average value for the ICAPTCHA system Fig. 4, Q1 is 4.1, which most of the users said that they would like to use. In Q3 most of the participants announced that the system is easy to use. In Q4 most of the participants believe that they do not need the support of a technical person to use the system and in Q8 most of the participants think that the system is not very complex to use.

TABLE III: DEMOGRAPHIC DATA OF PARTICIPANTS' BACKGROUND

| Characteristic | Frequency | % |
|---|---|---|
| ***Gender*** | | |
| Male | 30 | 63.8 |
| Female | 17 | 36.2 |
| ***Age*** | | |
| 20-25 | 11 | 23.4 |
| 26-30 | 23 | 48.9 |
| 30+ | 13 | 27.7 |
| ***Academic position:*** | | |
| Undergraduate | 24 | 51.1 |
| Postgraduate | 19 | 40.4 |
| PhD | 4 | 8.5 |
| ***Hours spent on the internet daily*** | | |
| 0,1 | 6 | 12.8 |
| 2,3 | 18 | 38.3 |
| 4,5 | 19 | 40.4 |
| 6+ | 4 | 8.5 |
| ***Solving CAPTCHA*** | | |
| Yes | 44 | 93.6 |
| No | 3 | 6.4 |
| ***Suitable CAPTCHA*** | | |
| Text | 17 | 36.2 |
| Image | 23 | 48.9 |
| Audio | 2 | 4.3 |
| Video | 2 | 4.3 |

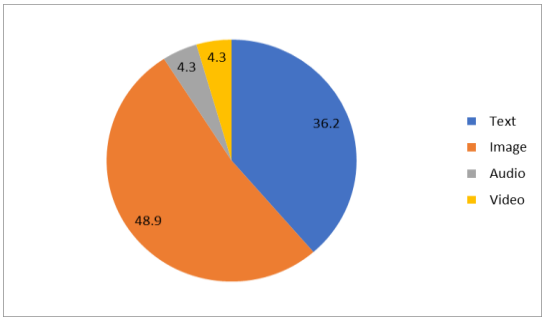


Fig. 3: Participants background on the type of CAPTCHA and suitable CAPTCHA for solving

### B. Results

SUS has proved to be a valuable evaluation tool, being robust and reliable. It correlates well with other subjective measures of usability. In this research, the SUS usability has been used

for ICAPTCHA system evaluations. The ICAPTCHA system SUS score (70.26) shows the usability of the system. The SUS score will help to improve the ICAPTCHA system in the future. The SUS score which was achieved by ICAPTCHA illustrates that the functionality of the user behavioral model and ICAPTCHA system tests are well integrated. The overall SUS score is the users' feedback to the system and the number of participants in the study highly affected the SUS score.

### C. *CAPTCHA Comparison*

In this section, we have evaluated our proposed CAPTCHA mechanism with respect to the different types CAPTCHA. As we can see, in table IV , our system uses the scoring rate while other types of CAPTCHA just ask one time for passing through login or form submission. Another most important feature for ICAPTCHA test is changing captcha types such as (VCAPTCHA, TCAPTCHA, OCAPTCHA, and IQCAPTCHA). While in the other hand our proposed CAPTCHA is much simpler and easier for solving for users.

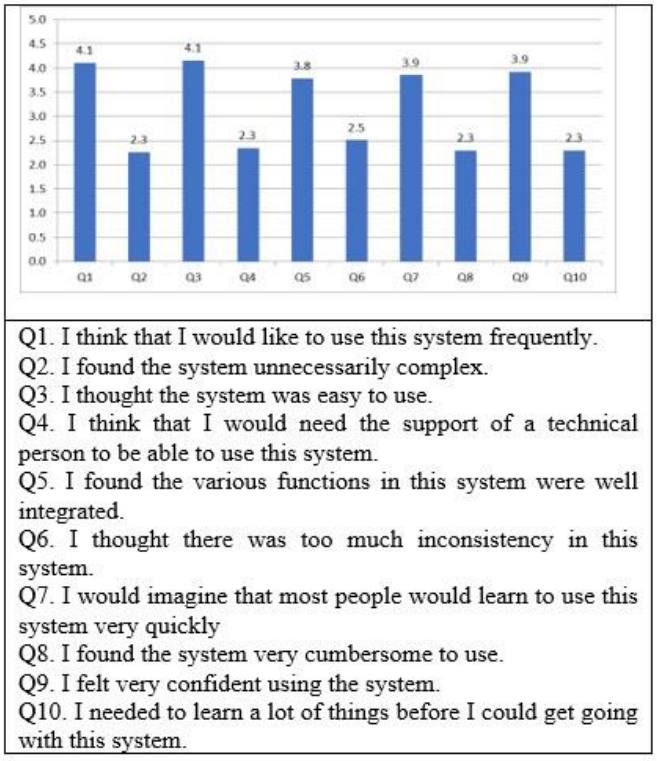


Fig. 4: System Usability Scale result for ICAPTCHA system.

TABLE IV: DIFFERENT TYPES OF CAPTCHA COMPARISON

| CAPTCHA TYPES | User Friendly | CAPTCHA Changing | Pattern CAPTCHA changing | Using Score | Easy or Difficult to use |
|---|---|---|---|---|---|
| ICAPTCHA System | YES | YES | YES | YES | Easy |
| reCAPTCHA | YES | NO | YES | NO | Average |
| Microsoft Text-based CAPTCHA | NO | NO | YES | NO | Difficult |
| Arithmetic CAPTCHA | NO | NO | YES | NO | Difficult |
| Game CAPTCHA | NO | YES | YES | NO | Difficult |
| Video-Based CAPTCHA | NO | NO | YES | NO | Difficult |
| Audio Based CAPTCHA | NO | NO | YES | NO | Difficult |

## V. CONCLUSION

In this research different types of CAPTCHAs were studied based on their popularity and efficiency for protecting the website. Many types of CAPTCHA were evaluated and a new methodology for protecting websites was investigated to prevent automated attacks. A new CAPTCHA method (ICAPTCHA) was proposed and implemented to meet the requirements of protecting the website as efficiently as possible. The ICAPTCHA system was built to defend against attacks from machines and to distinguish humans from automated attacks. Unlike all other types of CAPTCHAs, the ICAPTCHA system was built in two phases (User Behavioral Model and ICAPTCHA test). The ICAPTCHA system was tested in various situations and by many types of users and software. Finally, the proposed method has been evaluated by using the System Usability Scale to validate the ICAPTCHA and determine user satisfaction with the system. The most important feature which makes ICAPTCHA stronger compared to other types of CAPTCHA lies in its behavior. Each time the ICAPTCHA detects a user to be a Bot, it proposes a new pattern and style to the user which is completely random. The ICAPTCHA system can be integrated easily with any other website and will immediately start to control user behavior. The ICAPTCHA system can be implemented in many other types of web languages. Compared to other types of CAPTCHAs our proposed model was evaluated as easier and simpler to the user while on the other hand, the model used different types of CAPTCHA each time when user faced to solve a test.

## REFERENCES

[1] S. S. Baljit, . B.Anju, A Review of Bot Protection using CAPTCHA for Web Security, *Journal of Computer Engineering,* **8**, 36-42, (2013).

[2] Y. S. Patrice, S. Richard, B. Josh C. Julien , C. Iulian, Using Character Recognition and Segmentation to Tell Computer from Humans, (ICDAR'2003), 1, 418-423, (2003).

[3] H. Beitollahi., G. Deconinck. "ConnectionScore: a statistical technique to resist application-layer DDoS attacks", The Springer Journal of Ambient Intelligence and Humanized Computing, 5(3), 425-442, (2014).

[4] U. R. Rizwan, S. T. Deepak , D. Sujoy, Dynamic Image Based CAPTCHA, International Conference on Communication Systems and Network Technologies, 3, 90-94. (IEEE), (2012).

[5] K. Kiranjot, B. Sunny, CAPTCHA and Its Techniques: A Review, International Journal of Computer Science and Information Technologies, 5, 6341-6344, (2014).

[6] G. Prakhar, D. Rajesh , L. Palak, . A Review on Network Security Threats and Solutions, (IJSER), 3, 21-24, (2014).

[7] S. E Pawar , M. M. Bauskar. A security measure against spam attacks, International Journal of Research in Engineering and Technology, 02, 854-857, (2013).

[8] DAYANAND. Word grouping captcha-a novel approach for securing web services, International Journal of Electrical, Electronics and Data Communication, 1, 10-14, (2013).

[9] M. Sandeep , P. S. Varun, B. Devendra, B. A Survey of CAPTCHA based Web and Application Security Methods and Techniques, International Journal of Technology Innovations and Research, (14), 1-14, (2015).

[10] B. Elie, M. Matthieu, C. M. John, Text-based CAPTCHA Strengths and Weaknesses, Proceedings of the 18th ACM conference on Computer and communications security, 125-138, (2011).

[11] G. Moy, N. Jonesm, C. Harkless, R. Potter, Distortion estimation techniques in solving visual CAPTCHAs, Conference on Computer Vision and Pattern Recognition,(IEEE), 2, 23-28, .(2014).

[12] Y. W. Chow, W. Susilo, & P. Thorncharoensri, CAPTCHA design and security issues. In Advances in Cyber Security: Principles, Techniques, and Applications (pp. 69-92). Springer, Singapore, (2019).

[13] W. K. A. Hasan, A survey of current research on captcha. Int. J. Comput. Sci. Eng. Surv.(IJCSES), 7(3), 141-157, (2016).

[14] J. Chen, X. Luo, Y. Guo, Zhang, Y., & Gong, D. A survey on breaking technique of text-based CAPTCHA. Security and Communication Networks, 2017.

[15] P. Uma Maheswari, S. Ezhilarasi, P. Harish, B. Gowrishankar, & Sanjiv, S. Designing a Text-based CAPTCHA Breaker and Solver by using Deep Learning Techniques. (ICADEE) (pp. 1-6). IEEE, (2020).

[16] O. Bostik, ,& J. Klecka, . Recognition of CAPTCHA characters by supervised machine learning algorithms. IFAC-PapersOnLine, 51(6), 208-213, (2018).

[17] Y. Zhang, H. Gao, G. Pei, S. Luo, G. Chang, & N. Cheng, August). A survey of research on captcha designing and breaking techniques. 13th IEEE International Conference On Big Data Science And Engineering (pp. 75-84). IEEE, (2019) .

[18] J. Anil, G. S. Naveli, & Bhukya, S. Image based captcha generation system. International Journal of Pure and Applied Mathematics, 118(24), 1-9, (2018).

[19] M. Alnfiai, M. A Novel Design of Audio CAPTCHA for Visually Impaired Users. International Journal of Communication Networks and Information Security, 12(2), 168-179, (2020).

[20] M. Conti, C. Guarisco, & Spolaor, R. CAPTCHaStar! A novel CAPTCHA based on interactive shape discovery. In International Conference on Applied Cryptography and Network Security (pp. 611-628). Springer, Cham, (2016, June).

[21] U. R. Rizwan, SURVEY ON CAPTCHA SYSTEMS, Journal of Global Research in Computer Science, 3, 54-58, (2012).

[22] A. A Chandavale,., Sapkal, A. M., Jalnekar, R. M. A Framework to analyze the security of Text based CAPTCHA, International Journal of Computer Applications, 1(27), 127-132, (2010).

[23] B. Elie, M. Matthieu, C. M. John, Text-based CAPTCHA Strengths and Weaknesses, Proceedings of the 18th ACM conference on Computer and communications security, 125-138, (2011).

[24] R. Kameswara, R., Maniraj. Sneha, G. Improved Video CAPTCHA, Journal Of Emerging Technologies In Web Intelligence, 6, 416-419, (2014).

[25] K. A. Kluever, & R. Zanibbi, Video CAPTCHAs: usability vs. security, (2008).

[26] H. Beitollahi and G. Deconinck, "A four-step technique for tackling ddos attacks" in journal of Procedia Computer Science, Vol. 10, pp. 507-516

[27] H. Beitollahi and G. Deconinck, "Ferris wheel: A ring based onion circuit for hidden services" in journal of Computer Communications, Vol. 35, No. 7, pp. 829-841

[28] D. Gavrilis, I. Chatzis, E. Dermatas,)Flash Crowd Detection Using Decoy Hyperlinks, Proceedings of IEEE International Conference on Networking, Sensing and Control,London, 466-470, . (2007)

[29] B. John, SUS - A quick and dirty usability scale. Journal of usability study, 8(2), 29-40, (2013).

[30] S. T. ANDREW,., J. W. DAVID, Computer Networks, 5th edition, Upper Saddle River: Pearson, (2011).

[31] F. K. James., W. R. Keith (Computer Networking A Top-Down Approach, 6th edition, Pearson, (2013).

[32] W. Stallings. Data and Computer Communications. 8th edition. Upper Saddle River, NJ: Pearson/Prentice Hall, (2007).

[33] L. P Larry., S. D. Bruce Computer Networks a systems approach. 5th edition. A systems approach. San Francisco, CA: Morgan Kaufmann. (2012).