FMDB *Transactions on Sustainable Computer Letters*

Enhanced CAPTCHA Mechanism for Securing Online Social Networks and Web Pages Using Extended Finite Automata

M. Karthikeyan[1,*], A. R. Arunachalam[2]

[1]Department of Computer Science, Dr M.G.R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India.
[2]Department of Computer Science, Dr M.G.R. Educational and Research Institute, Adayalampattu, Chennai, Tamil Nadu, India.
mkeyan1990@gmail.com[1], arunachalam.cse@drmgrdu.ac.in[2]

Abstract: The internet has become essential to our daily lives, fundamentally changing the way we communicate and access information. However, this reliance has also introduced new challenges, such as automated behaviours that violate terms of service. These include activities like auto-sharing content, spamming friend requests, and submitting bulk forms. Such actions are primarily driven by bots—automated programs that imitate human behaviour online. The misuse of bots poses risks to website security, user experience, and resources. To combat these threats, CAPTCHA systems were developed to distinguish between human users and automated programs. CAPTCHA, which stands for "Completely Automated Public Turing test to tell Computers and Humans Apart," involves challenge-response tests that are difficult for bots to solve but manageable for humans. Traditional CAPTCHA methods, often relying on distorted text or images, are increasingly challenged as bots become more sophisticated at recognizing and bypassing these tests. Additionally, the growing number of online services has created more opportunities for bots to exploit platforms, resulting in increased spam and decreased user trust. To address these evolving threats, this paper introduces an innovative CAPTCHA system based on Extended Finite Automata (XFA), which creates dynamic, adaptive challenges that are more difficult for bots to overcome while remaining user-friendly for humans.

Keywords: CAPTCHA and BOTS; Extended Finite Automata; Security and Effectiveness; Computers and Internet; Online Resources; Security Protocols; Evolving Threats; Machine Learning; Social Networks.

Received on: 20/09/2024, **Revised on:** 24/11/2024, **Accepted on:** 28/12/2024, **Published on:** 03/06/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2025.000423

Cite as: M. Karthikeyan and A. R. Arunachalam, "Enhanced CAPTCHA Mechanism for Securing Online Social Networks and Web Pages Using Extended Finite Automata," *FMDB Transactions on Sustainable Computer Letters*, vol. 3, no. 2, pp. 76–84, 2025.

1. Introduction

Online resources and services are increasingly threatened by bots automated programs that imitate human behaviour, complicating the identification of genuine users. These bots can perform various tasks, both helpful and harmful. For instance, social bots have targeted networking platforms, resulting in hacking incidents involving unauthorised access to email accounts through weak password combinations and Facebook integration. The exponential increase in bot sophistication has led to a

*Corresponding author.

surge in cybercrimes, ranging from credential stuffing to account takeovers, making online interactions more vulnerable than ever before [21]. Cybersecurity experts face the dual challenge of enhancing digital user experience while maintaining robust security protocols against such threats [22]. To counter these threats, CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) has become essential for securing emails and webpages. CAPTCHA mechanisms are deployed across millions of websites to ensure that access is granted only to human users, effectively acting as gatekeepers to online resources [23]. This mechanism presents challenges that are easy for humans but difficult for bots to solve. They typically exploit differences between human cognitive abilities and machine processing, making tasks such as pattern recognition and interpreting distorted text a hurdle for automated scripts [24]. CAPTCHA not only serves as a filter but also functions as an early warning system for abnormal or suspicious behaviour on digital platforms.

Various CAPTCHA techniques exist, including text-based, image-based, video-based, and audio-based options, each designed to enhance user experience while preventing malicious actions [25]. Text-based CAPTCHAs involve presenting distorted alphanumeric characters that users must transcribe correctly. Image-based CAPTCHA prompts users to identify specific objects in a set of images, testing their visual processing skills. Video-based CAPTCHAs, though less common, require users to interpret motion or temporal patterns in short video clips. Audio-based CAPTCHAs offer an alternative for visually impaired users by presenting distorted audio clips that must be transcribed. While effective to a certain extent, these methods have drawbacks. Text-based CAPTCHA can be challenging for users with dyslexia or visual impairments, and image recognition tasks may become too complex or time-consuming, resulting in user frustration. Moreover, advances in machine learning and artificial intelligence have significantly reduced the effectiveness of traditional CAPTCHA systems [26].

In this paper, we propose an innovative CAPTCHA technique, XFA CAPTCHA, designed to enhance the security of webpages and social networks against attacks. XFA combines traditional finite-state automata (FSAs) with finite scratch memory to store important information for signature matching. This enhancement allows XFA to recognise regular languages while operating more efficiently than conventional FSAs, making it a powerful tool against online threats. Finite state automata are mathematical models that represent computational processes, consisting of states and transitions between these states based on input symbols. Traditional FSAs are limited by their inability to retain memory beyond the current state, which restricts their capacity to handle more complex tasks that require contextual awareness. XFA addresses this limitation by integrating finite scratch memory, which acts as a temporary storage area for relevant data during processing. This enables the system to retain and utilize contextual information, significantly enhancing its ability to distinguish between human and bot interactions. For example, XFA can monitor the sequence of user inputs, identify patterns indicative of automated scripts, and adapt its challenge mechanism accordingly. The dynamic nature of this approach makes it more likely that bots, which typically follow predefined scripts, will be detected and blocked.

Implementing XFA CAPTCHA involves a multi-layered process. Initially, the system generates a challenge according to predefined rules encoded in the finite-state automata. The challenge could involve a sequence of tasks that require understanding context, such as following a specific path through a grid based on textual clues or completing a pattern based on prior elements. During user interaction, the scratch memory records input data and evaluates it in real-time against expected behaviour models. If discrepancies indicative of bot activity are detected, such as unusually fast response times or repetitive patterns, the system can escalate the challenge or deny access. One of the primary advantages of XFA CAPTCHA is its adaptability. Unlike static CAPTCHA systems that present the same challenge to all users, XFA can generate personalised tasks based on user behaviour and interaction history. This makes it more difficult for bots to predict and circumvent the system. Furthermore, integrating scratch memory enables the system to learn from prior interactions, refining its challenge-generation algorithm over time. This continuous learning loop ensures that the CAPTCHA evolves in tandem with emerging threat vectors, maintaining its effectiveness in a rapidly changing digital landscape.

Another significant benefit of XFA CAPTCHA is its potential to enhance user experience while maintaining security. By tailoring challenges to individual users and leveraging contextual data, the system can reduce the complexity of tasks for legitimate users while increasing difficulty for suspected bots. For instance, a user who consistently demonstrates human-like behaviour may be presented with simpler challenges, whereas anomalies in interaction patterns may trigger more stringent verification steps. This balance between usability and security is crucial for the widespread adoption of any CAPTCHA system. In addition to its core functionality, XFA CAPTCHA can be integrated with existing authentication systems to provide multi-factor security. For example, it can be used in conjunction with biometric verification or one-time passwords to add a layer of protection. This modularity ensures that XFA can be seamlessly incorporated into diverse digital environments, from e-commerce platforms and banking portals to social media networks and content management systems. Its flexibility and scalability make it a valuable asset for organisations seeking to fortify their digital infrastructure.

The robustness of XFA CAPTCHA is further enhanced by its resistance to common bypass techniques employed by bots. Traditional CAPTCHA systems are often vulnerable to image recognition algorithms, audio processing tools, and even human-farm services where real individuals solve CAPTCHA challenges for bots. By introducing context-dependent challenges and

leveraging memory-based evaluation, XFA raises the barrier for automated systems attempting to spoof human behaviour. Moreover, the system can detect and respond to suspicious activity in real-time, such as multiple failed attempts from a single IP address or rapid-fire submissions, thereby mitigating the risk of brute-force attacks. To evaluate the effectiveness of XFA CAPTCHA, extensive testing was conducted across various platforms and user demographics. Metrics such as challenge completion time, error rates, user satisfaction, and bot detection accuracy were analysed. The results indicated a significant improvement in security without a corresponding increase in user burden. Users reported a smoother experience due to the challenges' contextual relevance, while bot-detection rates surpassed those of conventional CAPTCHA systems. These findings underscore the potential of XFA as a next-generation security solution.

The rise of bots and automated threats necessitates the development of more sophisticated and adaptive security measures. Traditional CAPTCHA systems, while effective in the past, are increasingly being circumvented by advanced algorithms and human-assisted attacks. The proposed XFA CAPTCHA represents a significant advancement in this domain, combining the theoretical rigour of finite state automata with the practical utility of scratch memory to create a dynamic, context-aware security mechanism. Its adaptability, user-centric design, and resistance to bypass techniques position it as a robust defence against the evolving landscape of online threats. As digital interactions continue to grow in complexity and volume, innovations like XFA CAPTCHA will play a crucial role in safeguarding the integrity and security of online ecosystems. The integration of advanced computational models with user-friendly design principles marks a new era in cybersecurity, where protection and usability are combined to ensure a safer and more seamless digital experience for all users.

2. Related Work

In this section, we will examine different types of CAPTCHA, categorised into optical character recognition (OCR)-based and non-OCR-based methods. Rather than providing an exhaustive review, we will highlight key approaches. CAPTCHAs are divided into two main categories: text-based CAPTCHAs, which require users to recognize and interpret text, and image-based CAPTCHAs, which require users to identify and interact with images. Recently, Google introduced the "No CAPTCHA" system, which uses advanced risk analysis to assess user interactions and prompt challenges that may involve text or images, enhancing security while improving the user experience. CAPTCHAs that involve text typically display an obscure word in an image, prompting users to identify and type it into a text box. Bursztein et al. [1] introduced the first text-based CAPTCHA in 2002, and since then, researchers have focused on improving these designs to balance flexibility and resistance to automated attacks [2]; [3]. Notable examples include CAPTCHA Star [4], ICAPTCHA [5], and DDIM-CAPTCHA [6]. CAPTCHA Star allows users to select responses without typing. ICAPTCHA [7] counters relay attacks [8] where spammers hire human workers to solve CAPTCHA.

It presents users with obscure words and requires answers formed from selected letters, validating responses by checking accuracy and analysing time intervals between button presses. However, time calculations can be unreliable due to network latency. ICAPTCHA also provides selectable characters, enhancing usability and challenging OCR systems. DDIM-CAPTCHA resembles traditional CAPTCHAs but asks users to select overlapping characters for a "solution box," increasing difficulty for bots while maintaining accessibility [9]. ReCAPTCHA remains a widely used benchmark for text-based CAPTCHA. Features of Text-Based CAPTCHA. Usability: The early text-based CAPTCHA was quick to complete, with high success rates, requiring only basic reading and typing skills. However, usability can decline on smartphones [10]. Vulnerabilities: Automated attacks often rely on OCR technology, and the ongoing battle between CAPTCHA designers and spammers has led to significant advancements in this area. Additionally, relay attacks, in which human workers solve CAPTCHA for spammers, achieve high success rates. To effectively protect online environments from spam, it's crucial to understand the strategies spammers use to bypass text-based CAPTCHA. These include:

- **Human Solvers:** Spammers often hire workers to manually solve CAPTCHA.
- **OCR with Dictionaries:** Optical Character Recognition (OCR) paired with dictionaries decodes CAPTCHA words.
- **Single-Character OCR:** Recognising individual characters helps spammers incrementally solve CAPTCHA.
- **Word Segmentation:** Breaking words into letters simplifies spammers' process.
- **Line Removal:** Eliminating added lines makes CAPTCHA easier to decode.
- **Letter Filling:** Filling gaps in letters enhances OCR accuracy.
- **Outline Repair:** Repairing broken outlines helps reconstruct CAPTCHA characters.

In response, CAPTCHA designers continually enhance security measures. Text-based CAPTCHA is essential for defending websites and social networks against spam. Advanced techniques such as shape recognition and image segmentation have enabled innovative CAPTCHA designs, ensuring a safer online experience for users. Image-based CAPTCHA is an innovative solution that invites users to engage with images or interact with displayed objects to find the correct answer. Unlike traditional text-based CAPTCHA, their unique designs require users to take a moment to understand how they work. Research shows that

users prefer image-based CAPTCHA due to its higher success rates and reduced frustration. They can be categorised into three subtypes: static, motion, and interactive. Static Image CAPTCHA: Asirra asks users to identify cats and dogs from a selection of images. Collage CAPTCHA [11] requires users to pick a specific image from six options, while Deep CAPTCHA [12] challenges them to arrange 3D models by size. Motion-Based CAPTCHAs [13]: These incorporate videos; for example, Motion CAPTCHA prompts users to identify actions in random videos, while YouTube Video CAPTCHA [14] requires interaction with short clips. Interactive CAPTCHA: These engage users through tasks. Play Thru CAPTCHA [15], for instance, presents mini-games that require users to complete specific actions, making the process more enjoyable. In summary, image-based CAPTCHAs enhance security and provides a more engaging user experience than text-based ones, making them the preferred choice for developers and users alike.

2.1. Features of Usability

Image-based CAPTCHA is popular for its user-friendly design, especially on smartphones and tablets, as it eliminates the need for keyboard input [16]. Game-based CAPTCHAs offer an enjoyable and intuitive alternative, engaging users with simple games like CAPTCHA Star and GISCH CAPTCHA, thereby enhancing both security and the user experience. VIKAS CAPTCHA utilises a virtual key system to generate alphanumeric characters of varying lengths [17]. While it streamlines the verification process by avoiding noise and distortion, this may make it easier for bots to bypass. Hear-Act CAPTCHA engages users through audio challenges, where participants listen to numbers or words amid background noise and type their responses, thereby enhancing accessibility. Gesture-based CAPTCHAs are specifically designed for mobile devices, allowing users to recognise and match patterns through hand gestures, creating a more interactive experience [18]. The Four-Dimensional Usability Investigation of Image CAPTCHA assesses usability across effectiveness, eye-tracking, efficiency, and satisfaction [19]. Although tested on a small sample of 35 users, it aims to improve real-world applications. 3D CAPTCHAs require users to interact with three-dimensional objects, blending creativity with challenge (Table 1).

Table 1: Compare the speculation rate of other CAPTCHA types

Mechanism of CAPTCHA	Probability of Success Rate of Speculation Attack
Collage-CAPTCHA	17.70%
Deep-CAPTCHA	21.10%
Motion-CAPTCHA	24.00%
Video-CAPTCHA	29.00%
Jigsaw-CAPTCHA	7.76%
CAPTCHAStar!	8.00%
Videop-CAPTCHA	2.77%

3. The Proposed XFA CAPTCHA

This section presents XFA CAPTCHA, a revolutionary solution that significantly enhances web page security against spammers [20]. It incorporates two powerful strategies: 1. XFA Automata Graph: A sophisticated tool for crafting CAPTCHA tests. 2. Clickable CAPTCHA: Features engaging interactive elements that require user involvement. XFA CAPTCHA not only increases test complexity but also prioritises usability and participant satisfaction, effectively fortifying defences against bots. Architecture of XFA CAPTCHA: The system is built on two key components: XFA CAPTCHA Generator. This component randomly selects puzzles from a specially designed database tailored for secure online services, ensuring rich diversity and unpredictability in challenges. XFA CAPTCHA Verification: This element rigorously validates user responses by comparing them against correct answers derived from the stored XFA automata graph. Design and Mechanism leveraging the principles of Extended Finite Automata (XFA), XFA CAPTCHA generates letter-based puzzles in multiple languages. Arrows guide users to pinpoint answers, and they must click three correct buttons within 3 minutes. If a wrong selection is made or insufficient answers are provided, a fresh puzzle emerges. By seamlessly blending advanced automata theory with engaging interactive features, XFA CAPTCHA offers robust security while ensuring an enjoyable user experience.

4. Methodology

This section outlines the methodology used in designing, implementing, and evaluating the proposed XFA CAPTCHA system (Figure 1). The methodology consists of three primary phases:

- System design,
- Implementation, and
- Evaluation

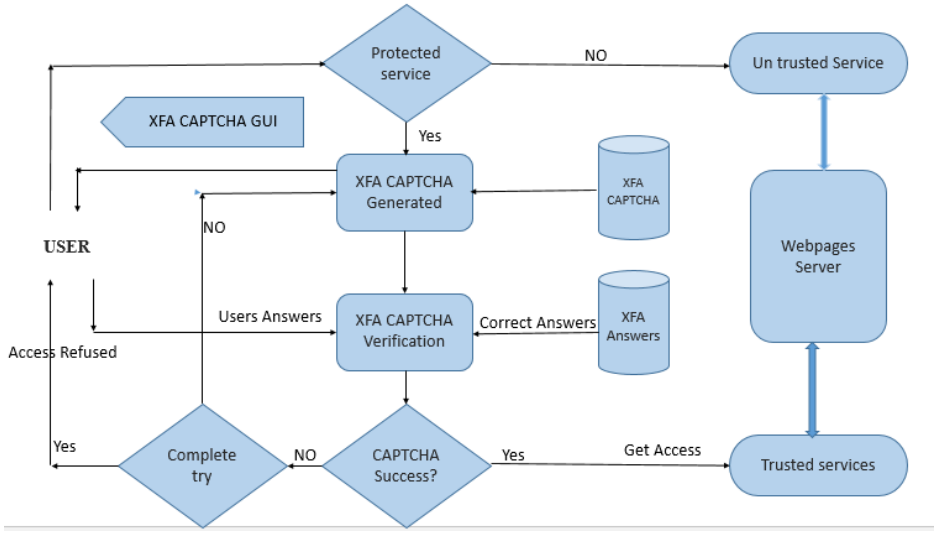


Figure 1: Flowchart of XFA CAPTCHA verification and access control process

5. Implementation and Evaluation of Experimental Results

For every proposed CAPTCHA system, it is essential to evaluate its security, usability for participants and robustness against bots. A well-designed CAPTCHA should strike a balance between robustness to prevent automated attacks and usability to ensure a smooth user experience.

5.1. XFA CAPTCHA Implementation

This algorithm model provides a clear, structured approach for implementing an XFA CAPTCHA system, ensuring robustness and usability in a login scenario.

- **Step 1:** Start the process.
- **Step 2:** Gather user details (username, email address, and age).
- **Step 3:** Generate an XFA CAPTCHA based on user details.
- **Step 4:** Display the CAPTCHA challenge and prompt the user to select three correct answers.
- **Step 5:** Check if the user's selected answers are correct. If incorrect, erase their selection.
- **Step 6:** User submits their answers.
- **Step 7:** If the answers are correct, the user passes the test.
- **Step 8:** If the answers are incorrect, the user can try another CAPTCHA.
- **Step 9:** End the process for that login attempt.

5.2. Calculate Usability

To evaluate the usability of XFA CAPTCHA on webpages, we conducted an assessment comprising 9 CAPTCHA challenges (Q1-Q9) with 255 participants, grouped by demographics: staff members, students at various levels, and across different age ranges. Participants were divided into educational categories: Intermediate education (ages 14-18, 70 users), Higher education (ages 19-26, 110 users), and University graduates (ages 27-55, 75 users). We invited participants through a public link shared online. Our analysis followed the ISO/IEC 9126-4 standard for usability metrics, focusing on Satisfaction, Efficiency, and Effectiveness. This approach ensures a reliable assessment of XFA CAPTCHA's usability.

Effectiveness: can be evaluated by calculating the CAPTCHA challenge completion rate. This is measured by assigning a value of 1 if the participant completes the CAPTCHA challenge and zero if they do not (Figure 2). The Completion Rate can be expressed as follows:

$$\text{effictiveness} = \left(\frac{\text{SU}}{\text{N}}\right) \times 100 \quad (1)$$

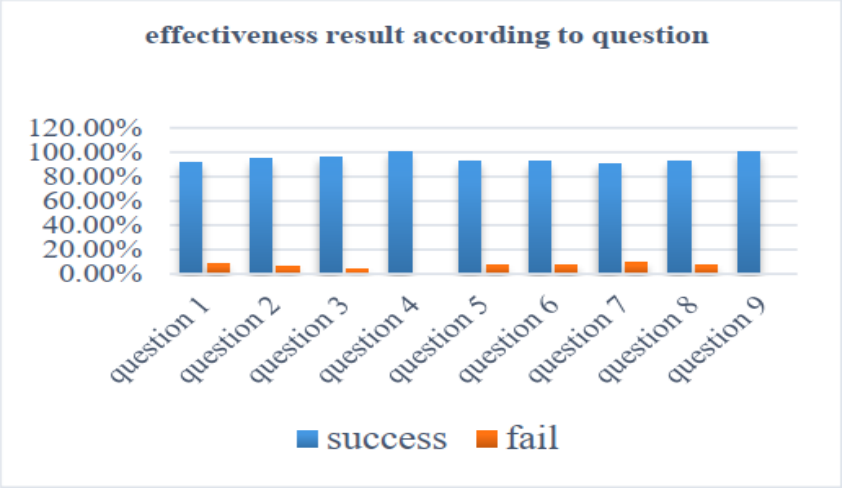


Figure 2: Performance breakdown across questions

Efficiency: the CAPTCHA system is calculated based on how quickly participants can solve our proposed CAPTCHA within a given period. The total relative efficiency is determined by the ratio of the time spent by participants who successfully pass the test to the overall time taken by all participants. This can be expressed as:

$$\text{Efficiency} = \frac{\sum_{i=1}^{R}\sum_{j=1}^{N} n_{ij}t_{ij}}{\sum_{i=1}^{R}\sum_{j=1}^{N} t_{ij}} \times 100 \qquad (2)$$

Whereas, (R) is the number of all participants, (N)represents all numbers of CAPTCHA challenges, (nij) represents the result of answering CAPTCHA, the identifier (j)represents tests by participant (i); if the participant passes the challenge successfully, then (nij) will be one, if the user can't pass the test, then the value of (nij) will be zero, and (tij) storing spent time of the participant (i) to finish the task (j) (Figure 3).

Figure 3: Efficiency progression over nine quarters

Satisfaction: can be measured by presenting a series of questions to a group of users to gauge their perception of the system's usability. In this research, we utilized the System Usability Scale (SUS), which comprises 10 questions that assess users' perceptions of the XFA CAPTCHA system. Forty participants were divided into three categories: intermediate education, higher education, and university graduates. Each participant rated their level of agreement on a scale from 1 (strongly disagree) to 5 (completely agree) (Figure 4).

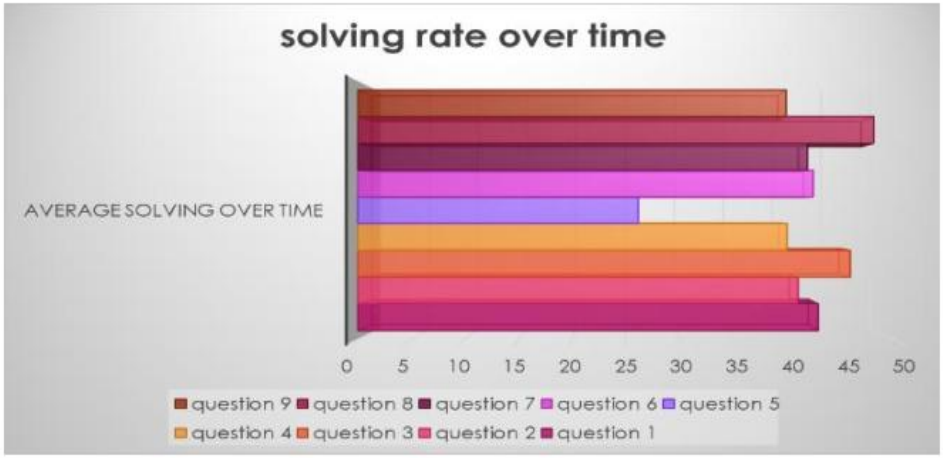


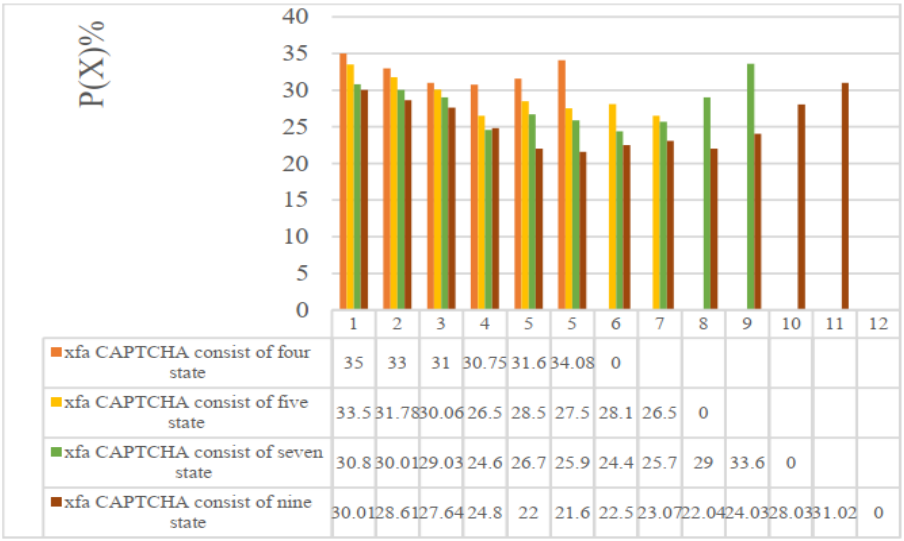
Figure 4: Average solving rate by question

The results were then analysed using the SUS algorithm to calculate satisfaction. The XFA CAPTCHA demonstrated high satisfaction among participants, as evidenced by the score curve exceeding the strict satisfaction limit of sixty-eight according to the SUS measure. Our findings for effectiveness, satisfaction, solving time ratio, and efficiency of the XFA CAPTCHA are visualised in Figure 4, respectively.

5.3. Security and Robustness Evaluation

The strengths and weaknesses of any CAPTCHA system are calculated by how easily a spammer can solve the CAPTCHA. Due to this challenge, we assess the robustness of XFA CAPTCHA against attack speculation using the Binomial Distribution function, as described in Section 3.

$$p(x) = \frac{N!}{X!(N-X)!} P^X Q^{N-X} \quad (3)$$



	1	2	3	4	5	5	6	7	8	9	10	11	12
xfa CAPTCHA consist of four state	35	33	31	30.75	31.6	34.08	0						
xfa CAPTCHA consist of five state	33.5	31.78	30.06	26.5	28.5	27.5	28.1	26.5	0				
xfa CAPTCHA consist of seven state	30.8	30.01	29.03	24.6	26.7	25.9	24.4	25.7	29	33.6	0		
xfa CAPTCHA consist of nine state	30.01	28.61	27.64	24.8	22	21.6	22.5	23.07	22.04	24.03	28.03	31.02	0

Figure 5: Probability distribution across CAPTCHA state configurations

Where NNN represents the total number of words that can be provided to solve the XFA CAPTCHA automaton, XXX is the number of correct words representing the solution of the test, PPP is the probability of passing the test, and QQQ equals 1−P1-P1−P, which represents the probability of failure in any test. Each result is evaluated by calculating the Binomial Distributed Function for the nine XFA graphs of the XFA CAPTCHA, as shown in Figure 5. The values in the yellow column indicate the smallest number of speculative attempts for each XFA CAPTCHA graph's probability level. The Binomial Distribution is used to estimate the probability of a correct answer for a specific word in the XFA CAPTCHA model, which requires each word to

be arranged in the correct order. Unlike simple bots that may struggle to guess correct words, the challenge lies in sorting every word accurately to pass the CAPTCHA test. To achieve a balance between security and usability, it is necessary to challenge users to correctly predict three words to pass the CAPTCHA test. This is reflected in Table 1, which compares the results of XFA CAPTCHA with those of other CAPTCHA approaches in terms of difficulty and the probability of passing a speculative attack.

$$\mathrm{NP}(X) = \frac{\mathrm{P}(X)}{X!} \tag{4}$$

6. Conclusion

We are excited to introduce a groundbreaking method for transforming traditional text-based CAPTCHA into engaging, image-based, clickable formats, enhancing user experience and security. Our proposed system, XFA CAPTCHA, fundamentally changes user interaction by replacing distorted or complex text challenges with intuitive, interactive visual tasks that are easier for humans to solve but remain resistant to automated attacks. The user study demonstrates that XFA CAPTCHA enables users to resolve challenges significantly faster than other CAPTCHAs currently in use. Importantly, it achieves this improved efficiency without relying on a static database of pre-stored images, thus ensuring dynamic adaptability and enhanced security by preventing pre-training or database-based attacks. The security of XFA CAPTCHA matches that of conventional text-based CAPTCHAs, effectively eliminating common issues such as wasted time and high failure rates, which often frustrate users and reduce platform accessibility. Our experimental evaluation revealed a remarkable success rate of up to 95.8% in solving XFA CAPTCHA, indicating its high accuracy and minimal error rates.

Furthermore, it achieved an impressive System Usability Scale (SUS) score of 90.5%, demonstrating that users overwhelmingly preferred XFA CAPTCHA over traditional text-based and other image-based methods due to its quick resolution time, simplicity, and engaging visual design. As we look to the future, there is immense potential for further research to enhance both the usability and security of XFA CAPTCHA. This development paves the way for its wide-scale adoption across diverse online platforms, ensuring a seamless balance between effective user authentication, security robustness, and enhanced user satisfaction in real-world deployments.

Acknowledgment: We sincerely thank Dr. M.G.R. Educational and Research Institute for providing the resources and support that made this research possible. The authors collectively appreciate the institution's encouragement and guidance throughout the study.

Data Availability Statement: The research presents a mechanism for Securing Online Social Networks and Web Pages Using Extended Finite Automata.

Funding Statement: The authors confirm that no external funding or financial support was received for conducting this research or preparing the manuscript.

Conflicts of Interest Statement: The authors declare that there are no known financial or personal conflicts of interest that could have influenced the results or interpretation of this study. All citations and references have been appropriately acknowledged.

Ethics and Consent Statement: Ethical approval was obtained from the relevant authorities, and informed consent was secured from all participants involved. The authors collectively affirm adherence to ethical research standards throughout the study.

References

1. E. Bursztein, M. Martin, and J. Mitchell, "Text-based CAPTCHA strengths and weaknesses," *Proc. 18th Conf. Comput. Commun. Secur.,* Illinois, United States of America, 2011.
2. H. D. Truong, C. F. Turner, and C. C. Zou, "iCAPTCHA: The next generation of CAPTCHA designed to defend against 3rd party human attacks," *Proc. Int. Conf. Commun. (ICC),* Kyoto, Japan, 2011.
3. Q.-B. Ye, T.-E. Wei, A. B. Jeng, H.-M. Lee, and K.-P. Wu, "DDIMCAPTCHA: A novel drag-n-drop interactive masking CAPTCHA against the third party human attacks," Proc. *Conf. Technol. Appl. Artif. Intell. (TAAI),* Taipei, Taiwan, 2013.
4. A. A. Chandavale and A. Sapkal, "Security analysis of CAPTCHA," in Recent Trends in Computer Networks and Distributed Systems Security, *Springer*, Berlin, Germany, 2012.

5. I. Akrout, A. Feriani, and M. Akrout, "Hacking Google reCAPTCHA v3 using reinforcement learning," *arXiv preprint arXiv:1903.01003*, 2019. Available: https://arxiv.org/pdf/1903.01003 [Accessed by 08/06/2024].
6. H. Gao, D. Yao, H. Liu, X. Liu, and L. Wang, "A novel image-based CAPTCHA using jigsaw puzzle," Proc. *13th Int. Conf. Comput. Sci. Eng. (CSE),* Hong Kong, China, 2010.
7. H. Nejati, N.-M. Cheung, R. Sosa, and D. C. Koh, "DeepCAPTCHA: An image CAPTCHA based on depth perception," Proc. *5th Multimedia Syst. Conf.,* New York, United States of America, 2014.
8. K. A. Kluever and R. Zanibbi, "Balancing usability and security in a video CAPTCHA," Proc. *5th Symp. Usable Privacy Secur.,* Mountain View, CA, United States of America, 2009.
9. S. Usuzaki, K. Aburada, H. Yamaba, T. Katayama, M. Mukunoki, and M. Park, "Interactive video CAPTCHA for better resistance to automated attack," *2018 11th Int. Conf. Mobile Comput. Ubiquitous Netw. (ICMU),* Auckland, New Zealand, 2018.
10. Are you a human, "Game-based CAPTCHAs." 2013. Available: http://areyouahuman.com [Accessed by 18/06/2024].
11. M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, and P. Wang, "Research on deep learning techniques in breaking text-based CAPTCHAs and designing image-based CAPTCHA," *IEEE Trans. Inf. Forensics Secur.,* vol. 13, no. 10, pp. 2522–2537, 2018.
12. A. Siripitakchai, S. Phimoltares, and A. Mahaweerawat, "EYE CAPTCHA: An enhanced CAPTCHA using eye movement," *2017 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, 2017.
13. H. Gao, D. Yao, H. Liu, X. Liu, and L. Wang, "A novel image-based CAPTCHA using jigsaw puzzle," *Proc. 13th Int. Conf. Comput. Sci. Eng. (CSE),* Hong Kong, China, 2010.
14. S. GlobalStats, "Canvas (basic support)," 2021. Available: http://caniuse.com/#feat=canvas [Accessed by 28/06/2024].
15. G. Ranjith, R. Parvathy, V. Vikas, K. Chandrasekharan, and S. Nair, "Machine learning methods for the classification of gliomas: Initial results using features extracted from MR spectroscopy," *Neuroradiology J.,* vol. 28, no. 2, pp. 106–111.
16. C. Shi, X. Xu, S. Ji, K. Bu, J. Chen, R. Beyah, and T. Wang, "Adversarial CAPTCHAs," *IEEE Trans. Cybern.,* vol. 52, no. 7, pp. 6095–6108, 2021.
17. N. Dinh, L. D. Ogiela, K. Tran-Trung, T. Le-Viet, and V. T. Hoang, "A comprehensive analysis of cognitive CAPTCHAs through eye tracking," *IEEE Access,* vol. 12, no. 3, pp. 47190–47209, 2024.
18. P. Wang, H. Gao, C. Xiao, X. Guo, Y. Gao, and Y. Zi, "Extended research on the security of visual reasoning CAPTCHA," *IEEE Trans. Dependable Secure Comput.,* vol. 20, no. 6, pp. 4976–4992, 2023.
19. A. O. Adesina, P. S. Ayobioloja, I. C. Obagbuwa, T. J. Odule, A. A. Afolorunso, and S. A. Ajagbe, "An improved text-based and image-based CAPTCHA based on solving and response time," *Comput. Mater. Contin.,* vol. 74, no. 2, pp. 2661–2675, 2023.
20. N. Dinh, T. Nguyen, and V. T. Hoang, "zxCAPTCHA: New security-enhanced CAPTCHA," *2023 15th Int. Conf. Knowl. Smart Technol. (KST),* Phuket, Thailand, 2023.
21. S. Alkasi, S. Surya, S. Tohir, S. Alpiah, and S. Oktapiana, "Community service journal: Promoting ethics and responsibility in social media use for high school students," *AVE Trends in Intelligent Social Letters*, vol. 1, no. 4, pp. 177–186, 2024.
22. L. Nurlaili, S. Anwar, and M. Ikhwanuddin, "Implementation of positive organizational behaviour to support the adaptation of the independent curriculum," *AVE Trends in Intelligent Techno Learning*, vol. 1, no. 2, pp. 97–106, 2024.
23. M. A. Raj, M. A. Thinesh, S. S. M. Varmann, A. R. Pothu, and P. Paramasivan, "Ensemble-based phishing website detection using Extra Trees classifier," *AVE Trends in Intelligent Computing Systems*, vol. 1, no. 3, pp. 142–156, 2024.
24. S. T. Kotagiri, "Exploring quantum cryptography for next-generation cybersecurity protocols," *AVE Trends in Intelligent Computer Letter*s, vol. 1, no. 1, pp. 21–30, 2025.
25. A. R. Pothu, "Behavioural analysis of end-users for enhancing cybersecurity awareness and prevention," *AVE Trends in Intelligent Computer Letters,* vol. 1, no. 1, pp. 31–40, 2025.
26. K. D. Jasper, M. N. Jaishnav, M. F. Chowdhury, R. Badhan, and R. Sivakani, "Defend and Secure: A strategic and implementation framework for robust data breach prevention," *AVE Trends in Intelligent Computing Systems*, vol. 1, no. 1, pp. 17–31, 2024.