Balancing security and user experience in the evolving digital landscape

Kingsley Okoli, and Yana Bekeneva²*

Department of Computer Science and Engineering, Saint Petersburg Electrotechnical University "LETI", Saint Petersburg, Russia

Abstract. In today's digital landscape, the prevalence of automated threats poses a significant challenge to online security. This study addresses the evolving landscape of online security by investigating next-generation CAPTCHAs, which aim to strike a balance between heightened security and an enhanced user experience. The relentless arms race between automated threats and online security necessitates the development of innovative solutions capable of countering advanced technological threats while ensuring a seamless user experience. The primary objective of this research is to explore and evaluate the effectiveness the presented approach in enhancing online security and user satisfaction. We examine how the integration of behavioral biometrics, gamification techniques, and supplementary tools such as device fingerprinting, geolocation, and browser attributes can contribute to a more robust and user-friendly CAPTCHA experience. Our study employs a comprehensive methodology, including a thorough literature review, and data collection from diverse sources. We evaluate the authenticity of these advanced systems, taking into account their ability to adjust to ever-changing digital environments. However, challenges persist in striking the right balance between security and convenience, addressing privacy concerns, and adapting to evolving digital landscapes. These findings validate the critical importance of ongoing research and innovation technology to safeguard online platforms effectively.

1 Introduction

Over time, the internet has evolved into a crucial communication platform and a valuable research tool. Virtually everyone has internet access and employs it for socializing, acquiring knowledge, or seeking entertainment [1]. The widespread presence of the internet has brought about new difficulties in safeguarding online platforms from malicious activities, particularly from automated bots that can infiltrate websites and applications [2]. Bots, often referred to as web crawlers, spiders, or robots, are diligent software applications that navigate the internet to gather data, which is essential for the operation of services like search engines and platforms focusing on news, auctions, or reviews [3]. The majority of web application attacks originate from malicious web bots. These web bot attacks can range from minor activities such as click fraud, the creation of backlinks, to mass registration attempts [4]. Gilani et al.,

* Corresponding author: yabekeneva@etu.ru

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).
classified web bot activities into two categories: beneficial web bots and harmful web bots [5]. However, in real-world scenarios, the intent behind their development can be either positive or negative. As we navigate the digital landscape, the significance of strong security measures, designed to protect against malicious elements such as bots, has become of utmost importance. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), fulfill this role by playing a crucial part in verifying online interactions [6]. CAPTCHA was first introduced in 2003 by Von et al [2]. Since its inception, it has gained recognition as a system designed to differentiate between human users and automated bots, thus serving as a protective barrier for digital environments against potentially harmful activities. CAPTCHAs have served as the primary method for distinguishing between human users and automated bots in the realm of online platforms. These assessments commonly encompass activities such as deciphering distorted characters [7], choosing specific images [8], or tackling puzzles [9]. Nonetheless, despite their early success in thwarting bots, CAPTCHAs have gradually demonstrated shortcomings and user inconvenience in contemporary times. Traditional CAPTCHAs, which employ techniques such as text, sound, and image recognition, have traditionally served as the primary means of safeguarding against automated entities. For instance, Figure 1 illustrates a typical example of a CAPTCHA employing distorted characters to differentiate between human users and bots on the web.

As we delve into the literature review, we will explore the evolution of CAPTCHAs, their effectiveness, and the emerging technologies and strategies aimed at addressing the evolving threat landscape posed by automated bots in online platforms. This exploration will provide a comprehensive understanding of the current state of CAPTCHA technology and its role in mitigating security risks on the internet.

2 Related works

Numerous research endeavors have been conducted in the domain of CAPTCHA with the aim of discovering optimal methods suitable for our ever-changing world and the latest technological advancements. In 2014, Google unveiled that advancements in AI technology had the capacity to effectively decipher distorted textual variations with a remarkable accuracy rate of 99.8 percent, leading to the obsolescence of CAPTCHA systems reliant on text-based methods [10]. In a recent study by [11], they investigated the effectiveness and user perception of modern CAPTCHAs, which evolved to counteract advances in bot technology. The research assessed how long it takes legitimate users to solve these CAPTCHAs and how users perceive them. In a comprehensive investigation focused on the usability of CAPTCHA, the researchers found that the challenge in solving CAPTCHAs arises from their design, which prioritizes increasing complexity to thwart machine deciphering, often disregarding human perspectives [12]. This study sheds light on the persistent struggle faced by human users when dealing with CAPTCHAs, highlighting the unintended consequences of prioritizing machine resistance over user-friendliness in their design. A study by [8] aimed to assess the effectiveness of image-based CAPTCHA in safeguarding online services from automated scripts and malicious programs. The study introduced a system that utilized deep learning and machine learning techniques to break image-based CAPTCHAs, particularly Google's image reCAPTCHA. It revealed that these CAPTCHAs, while intended to enhance security, can be bypassed with an average accuracy of 85.32%, indicating potential vulnerabilities in their defense against automated threats.

Audio CAPTCHAs provide an alternative means of authentication, particularly designed to accommodate users with visual impairments [13]. One such instance is CAPTCHA instance (or C-instance) [14], an audio CAPTCHA generated by overlaying foreground utterances represented as a digital sequence over a background of the same voice
pronouncing English words, synthesized using a text-to-speech system (TTS). In contrast, image-based CAPTCHAs aim to overcome the limitations associated with text and audio CAPTCHAs. [15] introduced an image-based CAPTCHA method that effectively thwarts bot attacks, even when these bots benefit from robust heuristic learning algorithms and commonly-used commercial search engines.

However, these CAPTCHAs are not immune to evolving techniques employed by bots hence leading to research gaps which this study tends to address. The aim of this research is to investigate the advancement of next-generation CAPTCHAs that surpass the constraints associated with conventional text and image-based recognition. These innovative approaches integrate behavioral biometrics, machine learning algorithms, and gamification techniques into CAPTCHA design, utilizing cutting-edge technologies to enhance online security while delivering a user-friendly experience. Furthermore, this study explores the incorporation of device fingerprinting, geolocation data, and browser attributes as tools to verify user authenticity within CAPTCHA systems. By harnessing these multifaceted authentication methods, the research aims to develop CAPTCHAs that not only offer heightened security but also adapt to the evolving landscape of online threats and user preferences, thus ensuring a robust and user-centric approach to digital authentication.

3 Proposed approach

In our pursuit of comprehending the evolution and current state of CAPTCHA technology, we conducted a thorough literature review, meticulously analyzing academic research, industry reports, and online resources. This extensive review aimed to identify pertinent studies, technologies, and prevailing trends. This rigorous data collection process formed the foundation for shaping a promising trend in next-generation CAPTCHA technology. We meticulously gathered data from reputable sources, including journal articles, books, conferences, and similar scholarly outlets. The subsequent chapter will provide a comprehensive discussion of the outcomes derived from this study.

Next-generation CAPTCHAs incorporate behavioral biometrics and machine learning algorithms, a departure from static challenges. These CAPTCHAs can assess user behavior, such as keystroke dynamics and mouse movement, in real-time. The integration of behavioral biometrics and machine learning marks a notable advancement in CAPTCHA technology. It allows for a more dynamic and adaptive approach to user verification, making it increasingly difficult for bots to mimic genuine human behavior. However, the practical implementation of these technologies requires careful consideration of user privacy and ethical concerns. As depicted in Figure 1, several patterns in human activities makes up the behavioral biometrics.

![Fig. 1. Shows patterns on human activities in behavioral biometrics.](image-url)
Geolocation is the process of determining the physical location (latitude and longitude coordinates) of a device or user based on their IP address, GPS data, or other location-specific information. Geolocation data is employed in CAPTCHA systems to verify the user's physical location. It can help identify whether the user's location matches their claimed location, adding a layer of authenticity to the CAPTCHA verification process. Geolocation enhances CAPTCHA security by confirming that users are accessing services from the expected geographical regions. It can detect suspicious access attempts from unexpected locations, which may indicate bot activity or unauthorized access.

Browser attributes refer to specific characteristics and configurations of a user's web browser. This can include details such as the browser type, version, language settings, and enabled plugins. In CAPTCHA systems, browser attributes are analyzed to verify the legitimacy of the user's browser. By comparing the browser's attributes to known legitimate configurations, CAPTCHAs can determine whether the user's browser resembles a typical user's setup or deviates in suspicious ways. Browser attributes help CAPTCHAs distinguish between genuine users and automated bots based on the browser's characteristics. This can be particularly useful in identifying browser-based attacks and ensuring that users are accessing web services securely.

In summary, Device Fingerprinting, Geolocation, and Browser Attributes are supplementary tools that enhance CAPTCHA security by providing additional data points for user verification. Each tool has its unique strengths and considerations, and when used effectively, they contribute to a more robust and reliable CAPTCHA system. However, privacy concerns, false positives, and adaptability to changing conditions are important factors to consider in their implementation.

4 Results and discussion

The presented investigation into next-generation CAPTCHAs revealed a departure from traditional text and image-based methodologies. These novel CAPTCHAs leverage advanced technologies to address the shortcomings of their predecessors. The shift away from conventional CAPTCHAs shows the dynamic nature of online security. The emergence of next-generation CAPTCHAs represents a strategic response to the escalating sophistication of automated attacks. This transformation holds the potential to significantly enhance the security landscape while accommodating user expectations.

The evolution of CAPTCHA technology has led to the integration of various innovative methods and supplementary tools to enhance user verification and security while considering user engagement and privacy concerns. One significant advancement is the integration of behavioral biometrics and machine learning into next-generation CAPTCHAs. These CAPTCHAs can now assess user behavior, including keystroke dynamics and mouse movement, in real-time. This dynamic approach makes it increasingly challenging for bots to mimic genuine human behavior. However, while this technology offers improved security, it also raises important ethical and privacy concerns, as it involves collecting and analyzing user behavioral data. To make the authentication process more engaging and user-friendly, gamification elements have been introduced into CAPTCHAs. These interactive challenges, quizzes, or puzzles not only deter automated attacks but also provide a more enjoyable user experience. Constant innovation in gamification strategies is necessary to stay ahead of adaptive bots and maintain a balance between security and user engagement.

Supplementary tools such as device fingerprinting, geolocation, and browser attributes play crucial roles in enhancing CAPTCHA security. Device fingerprinting uniquely identifies a user's device based on hardware and software characteristics, adding an extra layer of security. Geolocation verifies the user's physical location, ensuring that access attempts match the expected geographical regions. Browser attributes help CAPTCHAs distinguish
between genuine users and automated bots based on the browser's characteristics, aiding in the identification of browser-based attacks. However, while these supplementary tools strengthen CAPTCHA security, they also come with considerations. Privacy concerns arise when collecting and analyzing user device and location data. False positives, where legitimate users are incorrectly identified as bots, can be a drawback of these methods. Additionally, adaptability to changing conditions and the ability to keep up with evolving bot tactics are ongoing challenges.

The integration of behavioral biometrics, gamification, and supplementary tools like device fingerprinting, geolocation, and browser attributes represents a multi-faceted approach to CAPTCHA security. While these advancements significantly enhance user verification and engagement, they also require a careful balance between security measures and privacy considerations to provide a robust and user-friendly CAPTCHA experience.

The significance of these results lies in the evolution of CAPTCHA technology, which is increasingly adaptable to combat advanced threats in the digital landscape. The integration of behavioral biometrics and machine learning enhances security by assessing user behavior, yet it raises ethical and privacy concerns. Gamification elements improve user engagement while deterring automated attacks, highlighting the importance of user-centric design. Supplementary tools like device fingerprinting, geolocation, and browser attributes contribute to robust security, but challenges include privacy issues and potential false positives. These findings underscore the critical need for ongoing innovation in CAPTCHA technology to ensure both enhanced security and a seamless user experience in the ever-changing online world.

5 Conclusion

In this comprehensive study, we have explored the evolution and current state of CAPTCHA technology, with a particular focus on its adaptation to counter advanced technological threats. The findings presented here underscore the pivotal importance of CAPTCHAs in safeguarding online spaces against automated threats while ensuring a seamless user experience. The significance of CAPTCHA technology lies in its ability to strike a delicate balance between security and user convenience. The evolution from traditional text-based and image-based CAPTCHAs to next-generation solutions incorporating behavioral biometrics, gamification, and supplementary tools represents a proactive response to the dynamic landscape of online security. These innovations promise not only heightened security but also a more engaging and user-centric online experience. However, this journey is not without its challenges. Achieving the right equilibrium between heightened security and user-friendliness remains an ongoing pursuit. Privacy concerns, potential false positives or negatives, and the need to adapt to the ever-changing digital ecosystem are all critical considerations.

The key takeaway from this study is that CAPTCHA technology must continue to evolve and innovate. As online threats become increasingly sophisticated, CAPTCHAs must adapt to thwart these threats while providing users with a seamless and enjoyable online experience. The integration of cutting-edge technologies, user-centric design, and ethical considerations is essential in shaping the future of CAPTCHA technology. In essence, CAPTCHA technology stands as a sentinel in the digital realm, guarding the gates of online platforms against malicious automation. Its continued development and adaptation to emerging challenges are imperative to ensure the security and usability of the ever-evolving digital landscape.

This work has been supported by Russian Federation President Grant MK-918.2022.1.6.
References