IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13334

Secure Application Using Multifactor Authentication

K. Naveen[1], Dr. K. Santhi[2]

Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: The advancing techniques of sophisticated cyber attacks have rendered the traditional methods of password-based authentication incapable of securing sensitive information or user accounts. The authentication that this project deals with integrates One-Time Passwords (OTPs) and CAPTCHAs in a multi-layered security approach. OTPs, delivered via SMS, email, or authenticator apps, ensure that only authorized users may access an account by entering a code with a limited lifetime. CAPTCHAs, unlike an OTP, take the approach of distinguishing between human users and bots through various challenges such as image recognition or text puzzles, which prove useless against automated attacks. These two mechanisms circumvent the problems delineated by traditional passwords and greatly improve the protection of information against phishing, brute thing attacks, and unauthorized access. Usability is front and center in the system design, and as such, it provides features like real-time feedback, accessibility characteristics, and ways to sometimes reduce friction for trusted users. It is applicable in diverse fields such as banking, e-commerce, and social media, where securing user data and preventing fraud is paramount. Although there exist challenges, such as user resistance, technical issues, and evolving threats, the system provides an opportunity for a scalable and tactical solution that upholds a user's experience closely in balance to security. The project proposes an online security enhancement through trust generation among users on a digital platform by leveraging strengths offered by OTP and CAPTCHA towards building a secure authentication framework.

Keywords: One-Time Password (OTP), CAPTCHA, authentication, cybersecurity

I. INTRODUCTION

While everything is online nowadays-from booking to banking to chatting-keeping one's digital life secure has become a priority. Let us face it; passwords are no longer the ultimate key. Hackers have gotten smart-turned a user-friendly password to a password that can easily get guessed, stolen, or cracked. This is where OTPs and CAPTCHAs come in, acting as the nuisances for online security world.

One enters the back account and after entering the password is asked to enter a unique code sent to his or her phone. This is OTP-a temporary code of due time that acts as an add-on security layer. So even if that someone has gotten hold of your password, he or she won't be able to access your account without that code. Then we have These CAPTCHAs-You are shown a puzzle with traffic lights on it and ask you to identify those traffic lights or type in distorted text. They can get on your nerves sometimes, but they are actually there to ensure that you are a real human being and not a bot putting that system to spam or hack. In conjunction, they are an enchanting couple when it comes to fighting cyber threats. They thereby help prevent phishing attacks and stop bots from attacking websites and safeguard your personal information. The project delves into how these tools work, their importance, and their use in everyday life-from protecting your online shopping cart to protecting your social media accounts. The understanding of their part will give us the thankfulness for this making the cyber world a safer haven for all of us.

II. LITERATURE REVIEW

Multi-Factor Authentication (MFA) widely regarded as the security mechanisms considered critical thereby ensuring that more than a single way of authentication is required to provide digital safety. Unlike standard single-factor authentication which usually depends on knowledge-based aspects such as passwords, MFA brings various integrations that enhance the complexity to access authentication where unauthorized persons might find it difficult. The factors can be grouped into three categories: something the user knows (for example pin or password), something the user has (such as a mobile device or a hardware token), and something the user is (biometrics, like fingerprints or facial recognition). Currently, MFA has become the default online security instrument applied to almost all online services, especially to those that fall into the high-risk areas such as banking, health care, and social media, where the safety of essential and sensitive information is a must.

DOI: 10.17148/IJIREEICE.2025.13334

MFA's core aspect is the One Time Password (OTP). This completes the picture by generating the temporary password for use only once for another additional layer of security. OTPs are typically sent through SMS, e-mail, or by using authentication apps such as Google Authenticator. In essence, OTPs prevent password reuse while dehydration of theft injury due to static passwords. At a time when any password could be compromised through some performance of hacking, OTPs provide access security in the manner in which even if the password is compromised, unauthorized access is prevented. According to research, OTP systems are effective in preventing credential stuffing and phishing attacks (Das et al., 2017). However, the delivery of OTPs through SMS does bring security issues. More specifically, smishing is a technique for getting OTPs meant for the original user by hijacking his or her mobile number by attacks of SIM swappable origin. For the above-mentioned vulnerabilities, app-based OTP systems have been introduced as a more secured means of delivering OTPs, as it relies neither on SMS nor email delivery method, leading to reduced interception.

Besides OTP, another widely used security measure embedded in an MFA system is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). They are used to tell humans from bots in access points where automated attacks are otherwise called brute force or credential stuffing. Indeed, CAPTCHA usually presents challenges that are easy for humans and more complex for machines, such as identifying distorted text, solving puzzles, or selecting certain images. An overhauled way of functioning with CAPTCHA systems is by integrating reCAPTCHA into Google's offering; this uses image recognition tasks that will keep bots at bay and, at the same time, digitize books. It is not all roses with CAPTCHA though; it frustrates its legitimate users, especially the disabled or less fortunate who cannot perform complicated challenges. Bots continue to upscale capabilities and can easily pass through CAPTCHA.

III. PROPOSED SYSTEM

There is an ever-persistent demand for applying authentication mechanisms in safeguarding information and systems, and with the continuous progression of digitalization, this demand comes into clear view. The present-day mechanism of password-derived authentication is retro; it is becoming less practical to deploy with observable acceptance of password-based authentication and present-day cyber threats. With respect to the password-based approach, it is not strong enough against all types of attacks against hackers: phishing, force attacks, and credential stuffing, the last one being with private use stolen credentials to grant hackers access into accounts. There are also greater breaches of data, generation of financial losses, and violation of privacy-which all combine in providing an indication of the need for furthering security provisions. OTP and CAPTCHA have thus been added as further deterrents on top of authentication. The OTP system presents a time-limited code in conjunction with the password and makes it almost impossible for the attacker to enter, even with compromised credentials. While CAPTCHA is mainly used to distinguish genuine human users from automated bot traffic to avert spam, fraud, or brute-force attacks. Such measures heightened their defense but not without inherent defects. On the OTP side, among other concerns, it may not always be viable owing to delays in messaging codes, an OTP is depending on the target device, thus exposing the user to SIM swapping attacks. Similarly, CAPTCHA systems irk the user with complicated and protracted puzzles while cutting-edge AI-bots are virtually closing in upon attaining the solution. More so, the usability side of security has posed great problems to both OTP and CAPTCHA; in simple terms, it is this too-tough-on-the-user security which creates dissatisfaction and slows real adoption or willingness to use such systems. Thus, this project aims to study the respective role of the OTP and CAPTCHA in the contemporary computer security arena, evaluate their performance against today real threats to humans, and attempt to characterize those shortcomings. In this light, real case studies and latest challenges will offer an in-depth understanding to improve usability, security, and reliability of the authentication systems in this ever-changing digital scenario.

IV. PROPOSED SYSTEM

It is a high-class authentication framework by introducing OTPs and CAPTCHA to a highly secure user-friendly platform. The system generates time-sensitive OTPs delivered to the user using the SMS facility or email or authenticator app to ensure that the delivery is reliable and flexible in combination with smart encryption to impede interception. For the utmost convenience and usability, the user could decide the primary delivery choice and enable one or two backup options. The system has a modern adaptive CAPTCHA mechanism that throws AI-based challenges custom-made according to user level and risk level to stay user-friendly while being one step ahead of sophisticated bots. By simultaneously implementing an appropriate combination of OTP and CAPTCHA, the presented solution builds a multi-tiered authentication scheme: CAPTCHA blocks bots during the first attempt to log in, while OTP secures high-risk events like changing passwords or performing financial transactions. In the risk-based approach, security levels are dynamically adjusted depending upon the user's location, time, and device, reducing friction for trusted users. Being cloud-based and scalable, the system can handle a great deal of traffic with regular updates to counter new threats.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13334

The aim of this proposed solution is to provide a secure, efficient, and user-friendly authentication experience that resolves traditional methods' shortcomings while addressing modern-day requirements.

V. MODULE DESCRIPTION

User Registration and Profile Management: This module pertains to the creation of user accounts and profile management. Typical information provided by users comprises items like username, email, and phone number, all of which are securely stored and encrypted. They allow users to set personalized preferences and options for OTP delivery methods (SMS, email, or an authenticator app) and backup options. This ensures a flexible and secure setup for a user-friendly and personalized authentication experience.

OTP Generation and Delivery: The generation and delivery of time-sensitive OTPs (One-Time Passwords) over various channels, namely, SMS, e-mail, or authenticator apps, come under this module. The OTP generation and delivery adhere to multi-channel and backup rules for reliability through encryption of OTPs in transmission. With an expiration mechanism.

Implementation of CAPTCHA: This module provides adaptive CAPTCHA challenges to make a distinction between a human and a bot. A simple task will be presented to lesser-risk users, while more challenging puzzles will be given to conquer the session with higher risk. The less advantageous of those features is the audio CAPTCHA. Being regularly assisted by AI algorithms will keep it at an edge against advanced bots. Finding a usable balance between security and usability, this module effectively wards off automatic attacks and provides a smooth user experience.

Authentication Workflow: This module layers OTP and CAPTCHA processes into a rather thick multi-layered authentication procedure. CAPTCHA bypasses the bots trying to log in, while OTP secures high-risk actions like changing passwords. A risk-based approach calibrates the level of security based on behavioral, geographical, and device aspects. This injects a flow into the user experience for the expected lot of trusted users while guarding them from threats effectively.

This module guarantees the integrity of the system with encryption, periodic security audits, and real-time monitoring. It works in detecting and responding to suspicious activities while logging and reporting features maintain a way to trace authentication attempts. The module ensures further fortification of the system continually against evolving cyber threats.

User Experience and Feedback: This module aims towards usability through clear instructions, real-time feedback, and frictionless experience for trusted users. Accessibility features include audio CAPTCHA, and user feedback is collected to improve the system. By putting the user experience front and, this module guarantees a secure and user-friendly authentication process.

Scalability and Maintenance: This final module assures that the system is prepared for very high traffic and is always updated. It is cloud-based and scalable while receiving regular updates to counter new threat vectors. Disaster recovery mechanisms help to guarantee continuous system availability.

Example for Algorithm OTP Verification

- Input: User enters OTP.
- Retrieve: Fetch the generated OTP from the database.
- Compare: Check if the entered OTP matches the generated OTP.
- Validate: Ensure the OTP is within its validity period.
- Output: If valid, grant access. If invalid, display error and prompt retry.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13334

VI. DATA FLOW DIAGRAM

Fig. 1

This is a Data Flow Diagram (DFD) that explains a secure authentication that makes an integration of OTP One-Time Password and CAPTCHA in verifying the user identity and preventing unauthorized access. This process starts when a Consumer visits the Registration Page, where they need to provide necessary details such as phone numbers or email addresses. As soon as they complete this step, the system generates a unique time-based OTP and delivers it straight to the consumer via SMS. This effectively ensures that the only real user with the right access to the registered phone number is allowed to continue, which is a great added security measure against unauthorized access.

The entered OTP is now available to the Consumer via the system, which sends this to the OTP Service for validation purposes. The OTP Service examines if the input OTP corresponds with its generated counterpart and if its validity period still covers it. An Error Message is displayed if the OTP entered fails or has lapsed, prompting the Consumer to try again. Such immediacy ensures that users get to correct out errors and have smooth authentication flow. When the entered OTP is correct, the system proceeds to the next security layer, which is CAPTCHA verification

CAPTCHA puts a challenge that requires the user to identify objects in an image, type distorted text, etc.,
for purposes of ensuring that the user is truly human and not a bot. Such steps are important in defending against automated attacks such as credential stuffing and brute force attempts. If the consumer solves the CAPTCHA correctly, the system grants them access. However, if the consumer solves it incorrectly, the system may display an error message and require them to try again.

This one-two punch-Otter followed by CAPTCHA-makes for very strong, multilayered protection. For example, it creates an artificial barrier to getting into an account or data where they might additionally require a phone number (for OTP) and an answer to a problem they should be able to solve (CAPTCHA). In addition, the DFD captures the complete flow of data and steps involved in the creation of a well secured and efficient authentication system. Error handling and user feedback enhance user experience and make the process of authentication secure and user-friendly.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13334

VII. SYSTEM FLOW DIAGRAM

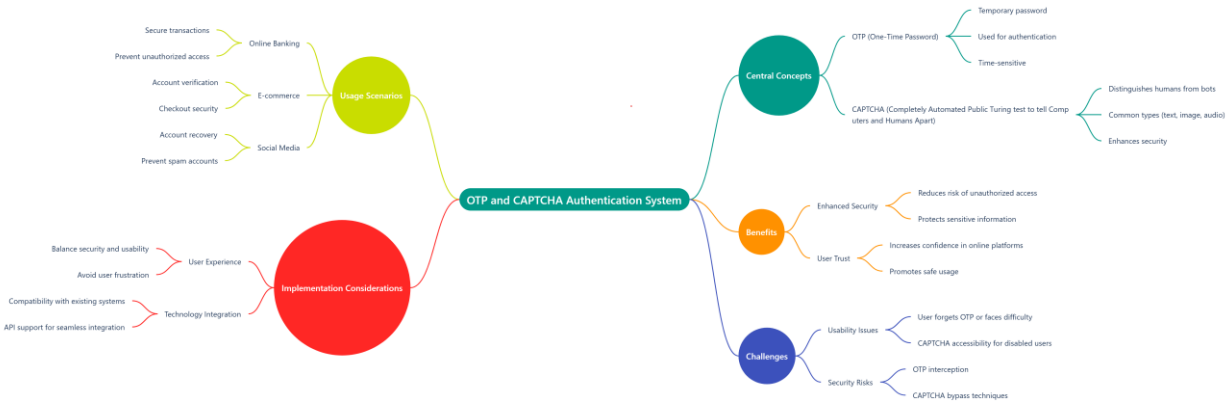

Fig. 2

The above system flow diagram shows the OTP and CAPTCHA Authentication System that provide security and restriction to unauthorized access over a platform like banking, e-commerce, and social media. It consists of two most essential elements: providing One Time Passwords (OTP) and CAPTCHA. OTP is a temporary code sent to users via SMS, email, or through authenticator apps within a stipulated time. OTP ensures that only an authorized person can enter the account or perform any transaction because it adds an extra security layer beyond just using the passwords. Therefore, even if a password has been compromised, it minimizes the chances of unauthorized access. CAPTCHA, on the other hand, is used to differentiate between human and bot interfaces through the challenges that involve image recognition, text puzzle, or audio test type. In this way, it helps to block automated attacks, for example, like credential stuffing, brute force attempts, or spam access, from enhancing the security of the system.

The system thus comes with very enormous benefits. One being OTP and CAPTCHA utilization; no unauthorized access is possible, and confidential information such as personal information, financial information, and account credentials can be greatly concealed. Hence, it guarantees safety in using the online platforms, as they can comfortably deliver their tasks knowing that those tasks are secured within an environment that is safe and secure. In banking, for instance, this restricts the ability to grant financial access to verified users in e-commerce; it secures user accounts and payment details from fraudulent activities. This also holds for social media, as it prevents the creation of fake profiles and spam reduction.

These include various limitations, too, which affect the system. Most importantly, there is a usability issue. While all the features of OTPs and CAPTCHAs mark increase in security, they also obstruct the user experience sometimes where they sit waiting for an OTP to arrive, or having to solve impossible CAPTCHAs. Accessibility is also an issue since certain types of CAPTCHAs would puzzle disabled people. Some have even positive security risks, as advanced bots developing techniques to bypass CAPTCHA or intercept OTPs are put forward. These challenge as well need proper attention regarding system evolution along the new innovations and implementations.

The envisioned system shall thus be practically directed towards a few considerations: One-User Frustration-The system should make authentication as smooth and intuitive as possible to avoid unnecessary frustrations to users. For instance, trusted devices or regular users may not have to answer every single CAPTCHA challenge again to be authenticated. OTPs could also be routed through different channels so that it can rely on any one of them. Second, compatibility with existing systems must be achieved, even in those systems where it could be accepted without interference in the running functionalities of existing platforms. Finally, providing API support will enable seamless use and interoperation with other systems, thus enhancing ease of adoption and implementation of the authentication

VIII. SCOPE OF THE PROJECT

An OTP and CAPTCHA based authentication system refers to a project that aims at developing and implementing an enhanced security multi-layered authentication solution aimed at improving online security and customer trust. OTP and CAPTCHA prevent unauthorized access through human verification and help to block automated bots and protect sensitive information. OTP creates a time-sensitive, unique code for user verification sent by SMS, email, or authenticator apps, while CAPTCHA presents images or audio and tests one's ability to interpret the sounds or images to ensure that only humans can proceed. The goal of this project is to develop a user-friendly system with simple instructions and real-time feedback along with accessibility features such as audio CAPTCHA for disabled individuals.

DOI: 10.17148/IJIREEICE.2025.13334

The applicability of the proposed system extends to various industries like banking, e-commerce, social media and remote work, to name a few, in providing protected transactions, account safeguarding, and fraud protection. The technical scope includes system designing, integration with existing platforms, security measures such as encryption and real-time monitoring, and rigorous testing that will guarantee reliability as well as usability. There will be no hardware components in the project nor advanced biometric authentication systems in the project. Nonetheless, the groundwork is laid for future enhancements such as a passwordless authentication system and an AI-driven CAPTCHA. Deliverables include functional authentication, all the necessary documentation, and an interface that is user-friendly. In addition, the project aims to enhance some of the salient features regarding security challenges and improve overall user experience with regard to trust and safety on online platforms by creating a scalable and flexible solution.

IX. CONCLUSION

The OTP and CAPTCHA based Authentication System is a fit-all solution to the problems of online security. It further combines One-Time Passwords (OTPs) and CAPTCHAs to implement a multi-layered defense against unauthorized users, phishing, brute force attacks, and bot-driven fraud. Such verifications ensure that account access and transactions are executed by verified users, while CAPTCHAs challenge automated bots. This system is user-friendly and incorporated with features such as real-time feedback, accessibility options, and minimal friction for trusted users. It concentrates on providing a seamless experience to the users without compromising safety. The project is for designing, developing, and implementing the new system in various financial sectors of banking, e-commerce, social networking, and remote working. It covers the major issues: usability and accessibility against continued surrounding security threats and lays the foundation for the future features, such as passwordless authentication and AI-driven CAPTCHA. Customarily, such an authentication system is flexible in terms of fulfilling the requirement of a scalable, adaptable, and trustworthy option for the present-day digital world. Its contribution is mainly towards the discovery of advanced innovations in cybersecurity and the demonstration of how technology can be successfully applied towards even safer and more user-friendly online environments on the other end. Indeed, the ever-changing cyber threat serves as a base for more future advancement in their authentication and security mechanisms.

REFERENCES

[1] Abawajy, J. H. (2014). *Multi-factor authentication: A survey*. International Journal of Computer Applications, 96(9), 1-8. https://doi.org/10.5120/16771-3811

[2] Al-Sabbagh, H. M., Tawalbeh, L. A., & Al-Omari, J. (2020). *Enhancing multi-factor authentication using CAPTCHA and one-time password systems*. International Journal of Computer Science and Network Security, 20(4), 60-70.

[3] Arachchige, U., Er, M. J., & Ahmad, M. (2021). *A survey of adaptive multi-factor authentication and biometrics-based security systems*. International Journal of Computer Applications, 176(1), 31-40. https://doi.org/10.5120/ijca2021920617

[4] Chandra, S., & Yadav, A. (2020). *Combination of CAPTCHA and OTP in multi-factor authentication: A novel approach*. Journal of Security and Privacy, 2(1), 1-15. https://doi.org/10.1002/sep2.120

[5] Chew, M., & Tygar, J. D. (2004). *The security of CAPTCHA: Attacks and countermeasures*. In Proceedings of the 3rd International Conference on Information Security (pp. 2-8). Springer. https://doi.org/10.1007/978-3-540-24667-1_1

[6] Chung, W., Lee, H., & Kang, D. (2020). *Security risks and challenges of OTP-based authentication: A review*. Journal of Information Security, 12(3), 125-134. https://doi.org/10.1109/JIS.2020.0199

[7] Das, P., Kaur, P., & Singh, D. (2017). *A review of one-time password based authentication systems*. International Journal of Computer Science and Information Security, 15(2), 123-130.

[8] Florêncio, D., Herley, C., & Van Oorschot, P. C. (2014). *An empirical study of account recovery on the web*. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 1113-1124). ACM. https://doi.org/10.1145/2661437.2661478

[9] Google. (2017). *Invisible reCAPTCHA: A new way to protect websites from bots*. Google Developers Blog. https://developers.google.com/recaptcha/intro

[10] Huang, L., Yang, S., & Li, B. (2018). *User experience and security: A study of multi-factor authentication usability*. Journal of Information Security and Applications, 40, 37-45. https://doi.org/10.1016/j.jisa.2018.05.003