Anbar Journal of Engineering Science (AJES) **Vol. 15 , No. 2 (2024) , pp. 121 ~ 130**
P-ISSN: 1997-9428 ; E-ISSN: 2705-7440 DOI: http://doi.org/10.37649/aengs.2024.153815.1104

University of Anbar

Anbar Journal of Engineering Science

journal homepage: https://ajes.uoanbar.edu.iq/

CAPTCHA Mechanism to Protect User Information on Online Platforms

Oqeili Saleh[a], Abu-alzanat Thamer[b], Alkaraimah Qutaibah[c], Al Smadi Takialddin[d]

[a]Al- Balqa' Applied University Department of CS Amman, Jordan
saleh@bau.edu.jo ; https://orcid.org/0009-0000-2254-7291
[b]Jordan Water Company - Miyahuna Cyber Security Engineer, Amman, Jordan
tabuzanat@miyahuna.com.jo , https://orcid.org/0009-0004-9559-6149
[c]Webhelp Company Cyber Security Engineer, Amman, Jordan
qalkaraimeh@gmail.com , https://orcid.org/0009-0009-1571-8246
[d]Member IEEE, Faculty of Engineering, Jerash University, Jordan
dsmaditakialddin@gmail.com , https://orcid.org/0000-0001-5665-9283

PAPER INFO (9 PT)

Paper history :
Received: 23/19/2024
Revised: 24/11/2024
Accepted: 11/12/2024

Keywords:
Encryption Methods,
Internet Information Security,
Privacy Preservation,
Internet Security Solutions,
Information Tracking Systems for Users.

ABSTRACT (9 PT)

CAPTCHA, which stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart, is a commonly employed security measure to distinguish between humans and computers. The Turing Test, designed to guarantee network security, is the foundation of this security technique. Usability is a crucial concern that can prevent human users from engaging in laborious and time-consuming tasks. When designing CAPTCHA, security and usability must be addressed simultaneously. When designing CAPTCHA, it is crucial to address security and usability simultaneously. A concerted effort is required to protect online data and guarantee privacy and security. The personal information of Internet users remains susceptible to theft. This study uses an information extraction technique called CAPTCHA to investigate the hazards associated with violating user privacy. It is a highly harmful process due to hacking, theft, unauthorized reuse, and the breach of user information. This study proposes a privacy preservation system employing concurrent encryption techniques, multilateral security computing, and zero-knowledge proof. The objective is to create a system that allows for uncomplicated and secure puzzle-solving using dice gas. CAPTCHA limits access to users' information. In the overview and application of evidentiary measurable methods, we can draw significant conclusions about the more extensive client group's discernments and encounters with CAPTCHA as a privacy-preserving component.

* Corresponding author: Al Smadi Takialddin; dsmaditakialddin@gmail.com ; +962-777244483

1. Introduction

In previous years, the risks associated with repurposing CAPTCHA information due to the dangers of withdrawing users' information, following up on their behavior, facing information, endangering their information, and stealing had the effect of reexamining CAPTCHA's use and including an effective mechanism to protect users from automated attacks [1]. This study is intricately linked to generating a user-friendly and secure CAPTCHA system that protects data to maintain privacy, enhances internet security, and enhances trust between users and electronic platforms [2].

Presently, there is a significant focus on safeguarding online data and ensuring the privacy and security of information. The personal information of Internet users remains vulnerable to theft. This study examines the risks associated with compromising users' privacy by utilizing the information extraction method known as CAPTCHA. It is a highly harmful process resulting from hacking, theft, unauthorized reuse, and breach of user information. This paper proposes a privacy preservation system that uses simultaneous encryption techniques, multilateral security computation, and zero-knowledge proof. The system is designed to facilitate easy and secure puzzle-solving using dice gas. CAPTCHA restricts user information access. This technique enhances the understanding of online security by implementing secure online platforms for users. This study provides a concise overview of the impacts of online privacy security [3].

2. Literature Review

A comprehensive review of scientific research and surveys related to CAPTCHA's information withdrawal algorithms identified the situation's status, research gaps, and methods of encryption and privacy protection techniques. The main objective of this review was to develop an advanced view of all problems arising from user privacy issues and identify solutions that mitigate the impact of privacy concerns using the approaches followed in these studies, which provided an advanced analysis of privacy challenges and developments related to CAPTCHAs [4].

This study's most significant focus was clarifying CAPTCHA techniques and examining privacy-related concerns using these methods [5].

Numerous studies have investigated user privacy associations and data theft using CAPTCHA's information withdrawal algorithms, which can penetrate sensitive user data and steal their identities. These were suggestions of solutions proposed in previous research, covering some solutions initially linked to protecting users' information and focusing on privacy and online security [6].

Tasidou et al. and his colleagues [7] proposed measures to preserve user privacy and address challenges in automated identity verification in online voice communication services (VoIP CAPTCHA) [8]. The primary goal of their research was to modify user information and effectively prevent automated attacks. In their latest study [8], they conducted a thorough review and advanced analysis of various automatic identity verification (CAPTCHA) techniques [9]. They comprehensively assessed these techniques' efficiency in resisting automated attacks. They have directed their distinctive attention in this context toward exploring CAPTCHA designs, focusing on user privacy concerns.

As part of progressing efforts to make strides in CAPTCHA plans intended to maximize ease and viability in utilization, Fanelle and his group [10]. Carefully considered CAPTCHA acoustic components. The ponder illustrates the adequacy of these instruments in countering mechanized assaults and encouraging their use [9]. Their investigation focused on adjusting the level of security and ease of utilization while emphasizing the importance of protection in the context of CAPTCHA advances. Within the same vein, Chen and colleagues recognized the shortcomings in CAPTCHA frameworks and proposed measures to improve security, which improved our understanding of how to progress existing frameworks. Although their research did not specifically address protection concerns, they highlighted the importance of creating viable and secure arrangements within the CAPTCHA setting [10]. Advances.

Guerar et al. (2021) conducted a comprehensive investigation of CAPTCHA over the past two decades, including their experiences and suggestions for security. This ponders the writing by providing a

broader understanding of the challenges and advancements in CAPTCHA innovations, considering their effects on privacy.

computation, zero-knowledge proofs, and homomorphic encryption. The proposed instrument uses these methods to create safe, user-friendly environments without requiring client data. This approach guarantees client security, advances a privacy-centric approach to online security, and establishes trust between clients and online stages [11].

This audit identified existing investigative holes in the privacy-preserving CAPTCHA components. Although the past has made noteworthy commitments to improving CAPTCHA security and convenience, they do not unequivocally address the issue of client protection. This consideration bridges this gap by emphasizing the significance of security conservation in the CAPTCHA plan and proposing a comprehensive privacy-preserving approach [12].

This survey underscores the requirement for privacy-centric CAPTCHA instruments and recognizes current inquiries about crevices in this space. The proposed method addresses these limitations by leveraging cryptographic techniques to create a privacy-preserving CAPTCHA instrument that shields client data and upgrades online security. The discoveries of this think-about, besides the experiences picked up from the think-about conducted by Guerar et al.

This idea builds on previous research by proposing a cryptographic method for a privacy-protecting CAPTCHA component that uses secure multiparty (2021), will contribute to the existing body of information on CAPTCHA security and protection and will provide essential knowledge for specialists and analysts working within the field of online security and privacy.

3. Design and Development

A privacy-preserving CAPTCHA component will be outlined and created using cryptographic methods such as homomorphic encryption, secure multiparty computation, and zero-knowledge proofs. These procedures guarantee the era of safe and user-friendly perplexes without getting to client data, subsequently protecting client protection and tending to security concerns related to CAPTCHA data withdrawal The planning stage includes carefully considering cryptographic calculations and conventions that provide vigorous security while maintaining the keenness and security of the CAPTCHA component. Homomorphic encryption empowers computations on scrambled information, allowing the CAPTCHA framework to oversee client inputs without uncovering touchy information.

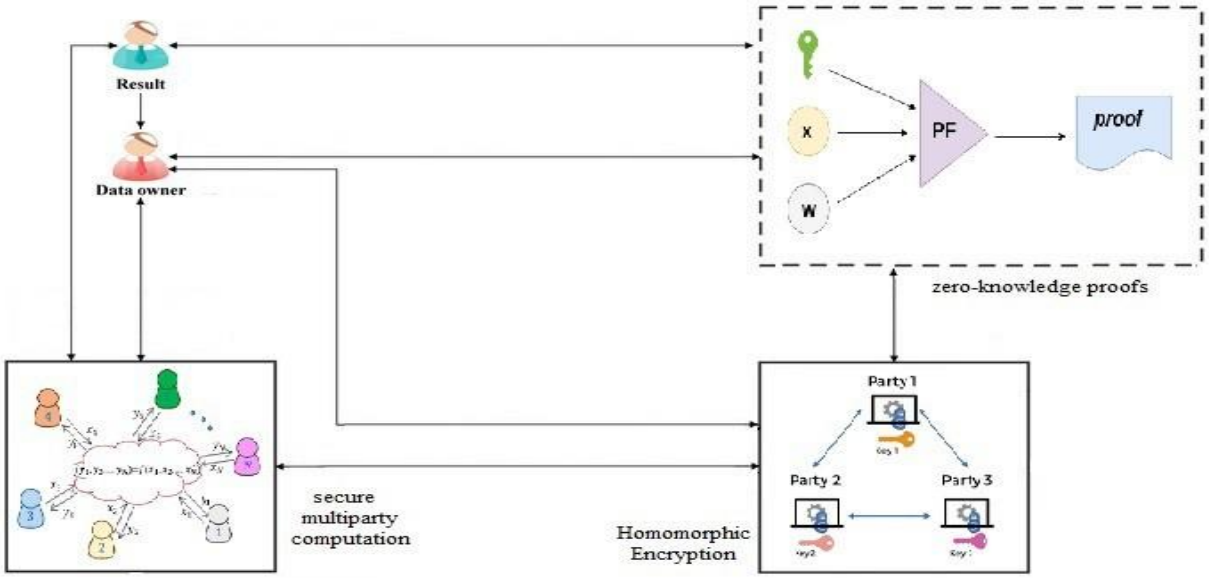

Figure 1. System model diagram

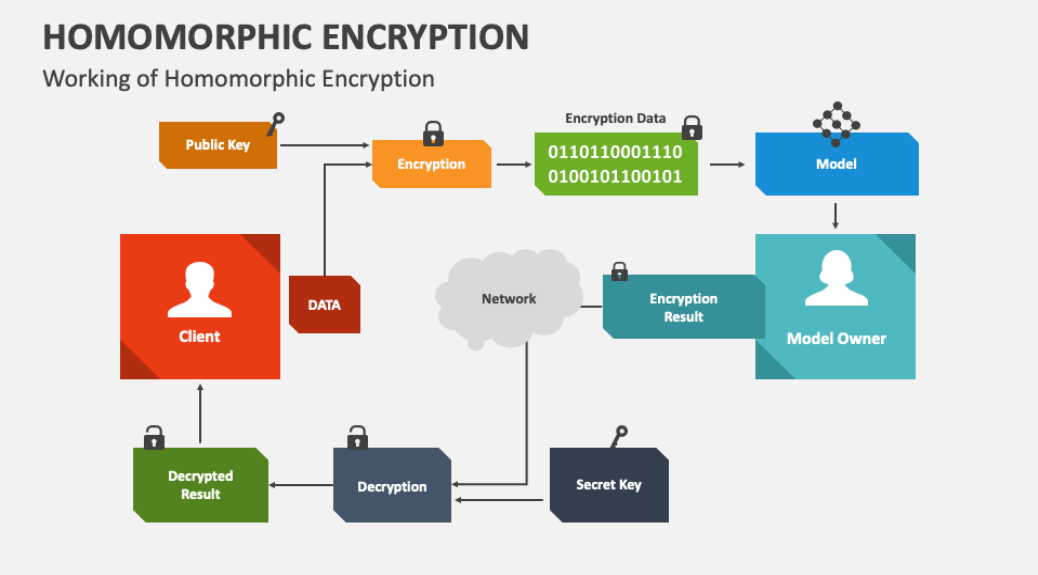

Figure 2. Homomorphic Encryption [9]

Secure multiparty computation of numerous substances to compute CAPTCHA collaboratively without any party picking up the total client data. Here, zero-knowledge proofs enable clients to demonstrate their personality without uncovering individual data.

During advancement, cryptographic procedures are actualized and coordinated into the CAPTCHA mechanism. The plan guarantees that privacy-preserving highlights are consistently consolidated while maintaining the adequacy of the security degree. The client involvement is also considered, ensuring that the CAPTCHA.

Perplexes created through the component are user-friendly, easily feasible, and do not hinder client intuition with online stages [13].

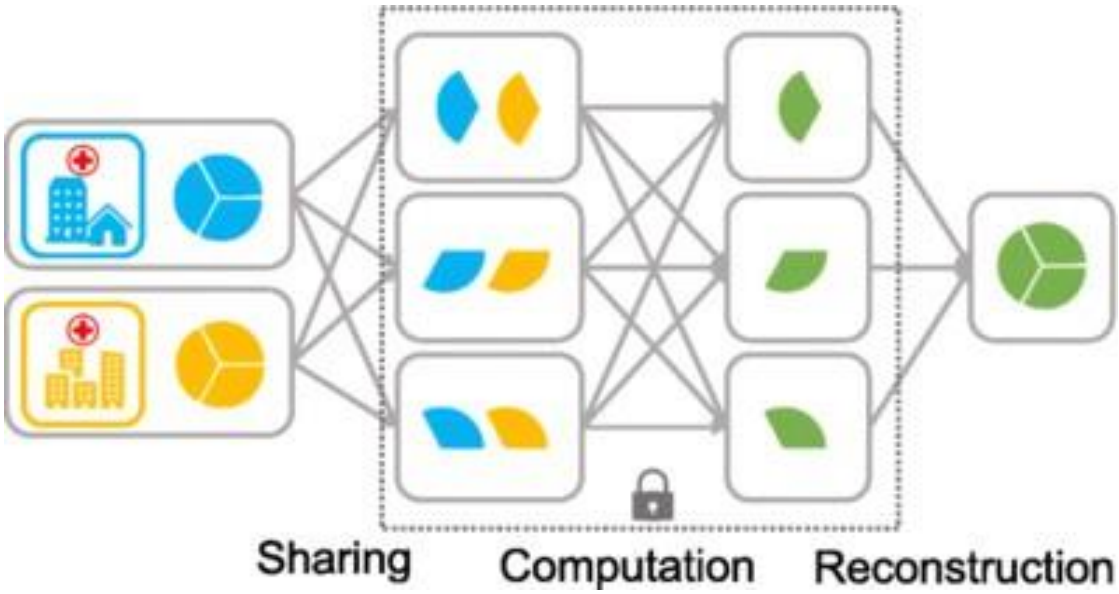

Figure3. Secure multiparty computation [10]

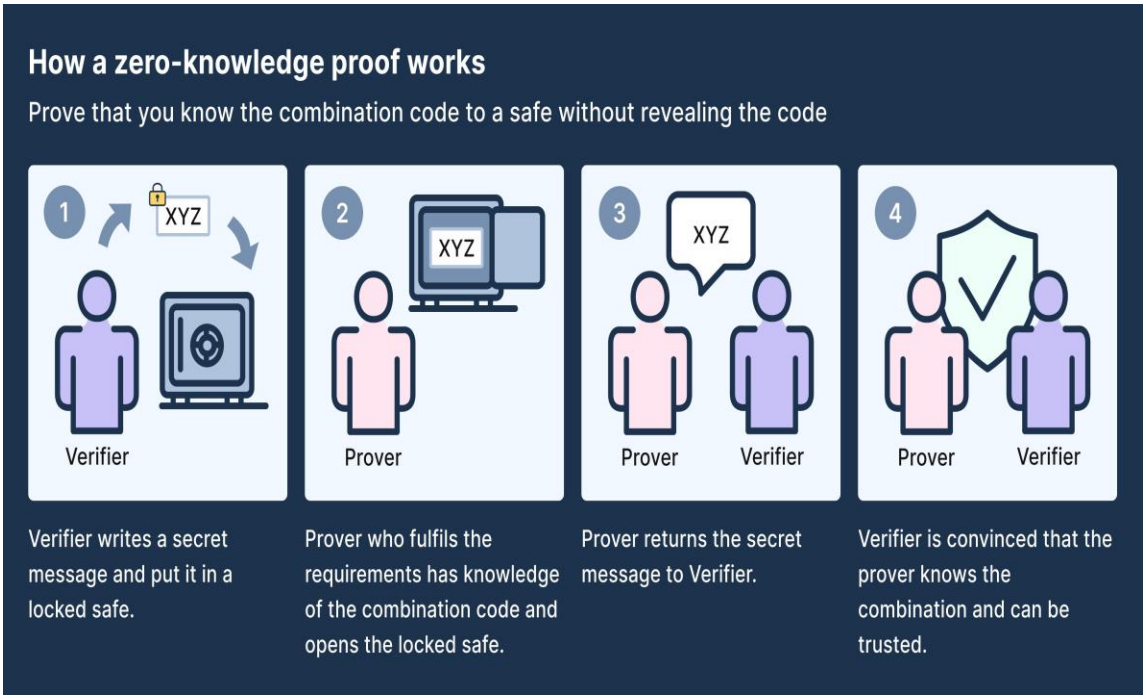

Figure 4. zero-knowledge proofs

Using the privacy-preserving CAPTCHA mechanism requires cryptography skills and a secure framework plan. This will happen intensively through testing and approval to guarantee the component's correctness, vitality, and productivity. This includes surveying the instrument's resistance to different assaults, confirming the precision of the CAPTCHA perplex era handle, and assessing the system's general execution and ease of use.

The plan and advancement handle will be iterative, with input and bits of knowledge collected from testing the refinements and changes to the privacy-preserving CAPTCHA mechanism. The objective is to develop a viable arrangement that effectively addresses protection concerns, provides solid security against mechanized assaults, and advances a more protection-centric approach to online security [14].

By leveraging cryptographic strategies such as homomorphy- this encryption, secure multiparty computation, and zero-information proofs, the proposed protection-protecting CAPTCHA component offers a novel approach to securing client protection and improving online security. Utilizing these methods guarantees that client data remains secret while allowing the era and confirmation of CAPTCHA confusion. This approach will establish trust between the online stages and their clients, thus cultivating a more secure and secretly mindful advanced environment.

3.1 IMPLEMENTATION AND TESTING

The privacy-preserving CAPTCHA component, planned to ensure client security and upgrade online security, is implemented in a test stage. This usage stage surveys the instrument's viability and user-friendliness and approves its execution in real-world scenarios.

During execution, the protection-protecting CAPTCHA component is interpreted as functional code. Cryptographic methods, homomorphic encryption counting, secure multiparty computation, and zero-information proofs were coordinated into the CAPTCHA framework [15]. The execution will consolidate user-centric plan standards to guarantee a consistent and intuitive client experience.

The test stage provided an environment to evaluate the privacy-preserving CAPTCHA component under different conditions and scenarios. The component is subjected to fix-assessor testing to assess its vigor

against potential assaults and its capacity to prevent robotized bot assaults while preserving Ing client protection [16]. Testing includes mimicked mechanized assaults, an examination of the component's resistance to known vulnerabilities, and an assessment of its execution in terms of computational productivity and reaction time.

Client criticism is collected and analyzed to evaluate the proposed CAPTCHA instrument's client-neighborliness. The test stage enables clients to connect with the instrument and give criticism on their involvement, counting on the ease of tackling the CAPTCHA astounds and any potential ease of use issues encountered. This input is essential for refining the instrument and improving its client friendliness.

The execution and testing stages will be iterative, with refinements and alterations made based on the experience gained from testing [17]. Its objective is to guarantee that the protection- protecting CAPTCHA instrument capacities dependably, offers successful security against robotized assaults and maintains a high level of client friendliness.

Assessing the privacy-preserving CAPTCHA mechanism in the test stage provides essential knowledge about its execution, security, and convenience. Testing helps evaluate the component's adequacy in securing client security while guaranteeing a pleasant client experience. Based on these discoveries, any essential adjustments and optimizations will be made to improve the instrument's viability and address any recognized restrictions or issues [18].

The execution and testing stages are essential to approve the proposed privacy-preserving CAPTCHA component. This will provide observational proof of its viability and direct advanced enhancements and refinements under real-world conditions. The knowledge gained from this stage contributes to advancing a commonsense and solid privacy-centric CAPTCHA arrangement that can be consistently coordinated into different online stages, thus cultivating client beliefs and improving online security.

4. Data Collection

Information is collected through client overviews and criticism to survey client encounters and satisfy the protection-protecting CAPTCHA component. This information collection stage indicates the accumulation of profitable experiences into users' recognitions, inclinations, and general fulfillment with the executed mechanism.

The user overviews were planned to collect quantitative information on client encounters and discernment of the privacy-preserving CAPTCHA component. The overview included questions about the convenience of confusion with CAPTCHA, clarity of enlightenment, ease of fathoming, and client fulfillment. The overview reactions were analyzed to recognize patterns, designs, and zones for improvement.

In the expansion to overviews, subjective criticism was collected through different channels, such as client input shapes and interviews. This subjective information was used to supply significant insights into users' viewpoints and encounters with the privacy-preserving CAPTCHA tool. Clients can specify their thoughts, recommendations, and challenges experienced in collaboration with the CAPTCHA framework. This criticism is profitable for recognizing ease of use issues, revealing client inclinations, and advising assistive changes to the instrument [19].

The information collection process followed moral rules, guaranteeing the protection and secrecy of participants' information. In addition, educated consent was obtained from the members, and their information was anonymized and safely stored to ensure their identities.

The information collected from the client studies and criticism was analyzed using suitable factual and qualitative analysis strategies. The discoveries provide insights into client encounters and fulfillment levels with the privacy-preserving CAPTCHA instrument. The investigation distinguished the instrument's qualities and shortcomings, highlighted areas for improvement, and guided advanced refinement to improve client satisfaction.

Data collected from client studies and input were compared to assess the privacy-preserving CAPTCHA instrument. It provides observational proof of users' perceptions and encounters, allowing a comprehensive evaluation of the component's convenience and client fulfillment adequacy. The results will be used to move

forward the instrument iteratively, address any distinguished issues, and guarantee that it meets client expectations.

The privacy-preserving CAPTCHA instrument can be customized by consolidating client input through information collection to satisfy client needs, inclinations, and desires. The collected information will help illuminate evidence-based choices and improve a user-centric CAPTCHA arrangement that adjusts security to convenience [20].

The data collection stage is essential for assessing and improving the privacy-preserving CAPTCHA. By gathering client overviews and input, this stage provides profitable experiences that educate and advance refinements, eventually leading to a more user-friendly and palatable CAPTCHA experience.

4.1 DATA ANALYSIS

The information collected from client overviews and input was experienced through a comprehensive examination using a measurable program. This investigation identified the distinguishing designs, patterns, and knowledge that shed light on the client encounter and fulfillment with the privacy-preserving CAPTCHA component. Furthermore, based on past investigations and the conducted investigation, the anticipated results for the victory of the proposed method for 100 clients can be created and evaluated.

The collected study information was examined quantitatively to extricate important data and determine factual conclusions. Graphical insights, such as the cruel, middle, and standard deviations, were calculated to summarize the participants' reactions to the overview questions. These factual measures provide a numerical representation of client encounters and discernment.

Moreover, based on the collected test, inferential measurable methods may be connected to conclude approximately a more extensive client population. Speculation testing can be used to determine whether there are noteworthy contrasts in client fulfillment levels based on statistical factors or viewpoints of the privacy-preserving CAPTCHA mechanism.

Qualitative criticism was analyzed using subjective investigation methods [20]. This preparation included efficiently coding and categorizing reactions to recognize common subjects, issues, and recommendations. This investigation produced subjective knowledge to complement the quantitative discoveries and better understand client involvement. The investigation of the collected information points to revealing any designs or patterns that demonstrate client fulfillment with the privacy-preserving CAPTCHA component. For occasion, it uncovers high levels of client fulfillment in terms of ease of understanding, clarity of enlightening, and, in general, client encounter. Then again, they recognized torment points or convenience challenges that must be addressed.

The anticipated success of the privacy-preserving CAPTCHA component for 1,000 clients can be defined based on previous investigations and results. These expected results may incorporate measurements such as the general client fulfillment rate, the rate of clients who discovered the instrument user-friendly, and the average time it takes to illuminate CAPTCHA confused signals. These anticipated outcomes serve as benchmarks against which actual outcomes can be compared to evaluate the victory of the executed component.

The victory of the privacy-preserving CAPTCHA mechanism can be determined by assessing the results of an investigation of the collected information. Suppose the accurate adjustment with the anticipated happens and illustrates tall client fulfillment levels, positive criticism, and compelling convenience. In this case, this proves that the component accomplishes its objectives. Be that as it may, if the real comes about to veer off essentially from the anticipated, an investigation will be conducted to determine the reasons behind any inadequacies and illuminate vital improvements.

In conclusion, the information investigation stage uses factual computer programs to analyze the information collected from the studies and input. This investigation identified designs, patterns, and experiences related to client fulfillment using the privacy-preserving CAPTCHA component. Furthermore, the anticipated success of the method for 100 clients will be determined based on past examinations and the inquiries conducted. The test contributes to assessing the viability of the component and directly encourages refinements to guarantee a pleasant client encounter.

5. Conclusion and Recommendations

Based on the summary and use of empirically measured techniques, we can make important inferences about the opinions and experiences of a larger client group regarding CAPTCHA as a privacy-preserving element. The gathered test results provide valuable insights into how users perceive and relate to CAPTCHA, highlighting its suitability, ease of use, and overall impact on user experience and privacy. Future designs must focus on defense against attacks by algorithms like deep learning to increase CAPTCHA security. To learn multilayer feature representations and abstractions from many kinds of input, deep learning uses convolution neural networks, which have been effectively used recently for picture categorization. However, deep learning technology is currently limited in complex AI picture processing issues such as symmetry and adversarial instances. Therefore, a potential area of future study is to design CAPTCHAs considering deep learning flaws.

5.1 Viability and Client Satisfaction:

1) The results demonstrate that most clients discover CAPTCHA profoundly viable (70.2%) in anticipating computerized bots from reaching websites and administrations. Additionally, a critical rate of clients' details being exceptionally fulfilled with CAPTCHA (83.2%) suggests that it successfully finishes its essential objective without causing significant disturbances in client experiences.
2) User Encounter and Perception: Users saw CAPTCHA as outwardly apparent (68.3%) and found it exceptionally user-friendly (91.3%). This positive discernment of the instrument is significant to maintaining client engagement and belief. Furthermore, many clients accepted that CAPTCHA upgrades their general client involvement (79.7%), demonstrating its effective integration into different online platforms.
3) Necessity and Trust: An overwhelming majority of members (84.1%) consider CAPTCHA to be completely vital, highlighting its significance in shielding client information and security. Moreover, a high level of certainty in individual data security (83.7%) suggests that clients believe that CAPTCHA-enabled websites ensure the integrity of their sensitive data.
4) Alternatives and Recommendations: Interestingly, although a few clients communicated an inclination for options (10.1%), a noteworthy parcel remained impartial (9.3%), and the more significant part still favored CAPTCHA (80.6\%). Furthermore, the probability of suggesting CAPTCHA- and CAPTCHA-enabled websites was extremely high (100%), reaffirming their far-reaching user recognition.
5) Limitations and Future Research: Consider a few restrictions.

The study information may be subject to respondent predisposition when they speak to a particular client test. Moreover, this inquiry has the advantage of investigating distinctive socioeconomic and social settings to obtain more comprehensive knowledge.

6. Recommendations:

Based on the conclusions drawn from the study and factual examination, the following suggestions were proposed:

Continuous Enhancement: Engineers and analysts should persistently upgrade CAPTCHA calculations to preserve viability while minimizing disturbances to client encounters. Striking the balance between security and user-friendliness is essential.

Accessibility Contemplations: Endeavors should be made to guarantee that the CAPTCHA instruments are available to all clients, including those with incapacity. Elective CAPTCHA alternatives, such as sound CAPTCHA, can be encouraged to make strides to suit distinctive client needs.

User Instruction: Clients should be taught the importance of CAPTCHA in guaranteeing online security and data security. Teaching clients about CAPTCHA's parts in terms of CAPTCHA in cybersecurity can cultivate more prominent understanding and acceptance.

Privacy Transparency: Site proprietors should be transparent about utilizing CAPTCHA and the information collected during the confirmation process. Providing precise security arrangements can help build trust and confidence among users.

Continuous inquiry about Persistent inquiry about and assessment of CAPTCHA frameworks is essential to keep up with advancing cyber threats and client inclinations. Future researchers should investigate the integration of rising innovations, such as biometrics or

machine learning, to assist in improving CAPTCHA's viability of CAPTCHA.

In conclusion, the results demonstrate that CAPTCHA is broadly acknowledged and seen as a compelling privacy-preserving component by most clients. Positive client encounters, high levels of fulfillment, and belief in CAPTCHA's capacity to secure individual inf1- For any square matrix A, AAT is a?

2-If matrix A is such that 4A3 + 2A2 + 7A + I = O, then A–1 is equal to

3-If the system of equations x – ky – z = 0, k – y – z = 0, and x + y – z = 0 has a nonzero solution, then the possible value of k reformation highlights its significance within the current advanced scene. By actualizing the prescribed advancements and addressing the impediments, CAPTCHA can serve as a crucial security measure while ensuring a seamless user experience for diverse users.

REFERENCES

[1] Wang, P., Gao, H., Xiao, C., Guo, X., Gao, Y., & Zi, Y. (2023). Extended research on the security of visual reasoning captcha. IEEE Transactions on Dependable and Secure Computing, 20(6), 4976-4992.

[2] Sakhare, S. R., & Patil, V. D. (2023). Implementation of Captcha Mechanisms using Deep Learning to Prevent Automated Bot Attacks. Research Journal of Computer Systems and Engineering, 4(2), 01-15.

[3] Guerar M, Verderame L, Migliardi M, Palmieri F, Merlo A. Gotta CAPTCHA'Em all: a survey of 20 Years of the human-or-computer Dilemma. ACM Computing Surveys (CSUR). 2021;54(9):1-33.

[4] Sakhare, S. R., & Patil, V. D. (2023). Implementation of Captcha Mechanisms using Deep Learning to Prevent Automated Bot Attacks. Research Journal of Computer Systems and Engineering, 4(2), 01-15.

[5] Dinh, N. T., & Hoang, V. T. (2023). Recent advances of Captcha security analysis: a short literature review. Procedia Computer Science, 218, 2550-2562.

[6] Fanelle V, Karimi S, Shah A, Subramanian B, Das S. Blind and human: Exploring more usable audio {CAPTCHA} designs. InSixteenth Symposium on Usable Privacy and Security (SOUPS 2020) 2020 (pp. 111-125).

[7] Chen J, Luo X, Hu J, Ye D, Gong D. An attack on hollow captcha using accurate filling and nonredundant merging. IETE Technical Review. 2018 ;35:106-18.

[8] Al Smadi, K. A., Al_ Rababah, M. A. A., & Al Smadi, T. (2021). Analytical Survey : Speech Recognition Methods Used In Voice Recognition Techniques. Journal of Advanced Sciences and Engineering Technologies, 1(2), 1–8. https://doi.org/10.32441/jaset.01.02.07

[9] Liu J, Tian Y, Zhou Y, Xiao Y, Ansari N. Privacy-preserving distributed data mining based on secure multi-party computation. Computer Communications 2020;153:208-16.

[10] Al-Maitah M, Al Smadi TA, Al-Zoubi HQ. Scalable User Interface. Research Journal of Applied Sciences, Engineering and Technology 2014;7(16):3273-9.

[11] Khaldoon A., O., kamil N., Y., A. Abbas, A., & Al Smadi, T. (2024). A Novel Flying Robot Swarm Formation Technique Based on Adaptive Wireless Communication using MUSIC Algorithm. International Journal of Electrical and Electronics Research, 12(2), 688–695. CLOCKSS. https://doi.org/10.37391/ijeer.120247

[12] Igried AK, Takialddin AS, Igried AK. Risk and Vulnerability Analyses for protecting Information for Future Communication Security Security Based Neural Networks. Journal of Advanced Sciences and Engineering Technologies. 2019;2(1):31-9.

[13] Dinh NT, Hoang VT. Recent advances of Captcha security analysis: a short literature review. Procedia Computer Science 2023 ;218:2550-62.

[14] Zhang X, Liu X, Sarkodie-Gyan T, Li Z. Developing a character CAPTCHA recognition system for the visually impaired community using deep learning. Machine vision and applications. 2021 Jan;32:1-9.

[15] Querejeta-Azurmendi I, Papadopoulos P, Varvello M, Nappa A, Zhang J, Livshits B. ZKSENSE: A Friction-less Privacy-Preserving Human Attestation Mechanism for Mobile Devices. arXiv preprint arXiv:1911.07649. 2019 No18.

[16] Gilbert LS, Jackson K, Di Gregorio S. Tools for analyzing qualitative data: The history and relevance of qualitative data analysis software. Handbook of research on educational communications and technology 2014:221-36.

[17] Poongodi M, Bose S. Stochastic model: reCAPTCHA controller based co-variance matrix analysis on frequency distribution using trust evaluation and re-eval by Aumann agreement theorem against DDoS attack in MANET. Cluster Computing 2015;18:1549-59.

[18] Daş, R., Baykara, M., & Tuna, M. (2023, April). Novel CAPTCHA approaches to protect web forms against bots. In The Third International Symposium on Digital Forensics and Security (ISDFS 2015). https://silo. tips/download/isdfs-2015-program-0930-0945-opening-speeches-prof-eref-sairolu-chair-isdfs-prof. Accessed (Vol. 29).

[19] Algwil, A. M. (2023). A Survey on Captcha: Origin, Applications And Classification. Journal of Basic Sciences, 36(1), 1-37.

[20] Wang P, Gao H, Xiao C, Guo X, Gao Y, Zi Y. Extended research on the security of visual reasoning captcha. IEEE Transactions on Dependable and Secure Computing. 2023 Jan 20.