ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
Your ult-MATE Research Paper !!!

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5,May 2024

Web-Based Graphical Password Authentication System

P. Sai Charitha[1],P. Nagesh[2],Ch. Harish[3],P. Soniya[4],Ch. Sai Tarun[5]
AssociateProfessor[1],Student[2][3][4][5]
SRKInstituteofTechnology,DepartmentofInformationTechnology[1][2][3][4][5]
Vijayawada,India
MailId:paladugusaicharitha456@gmail.com[1],
nageshpalakurthi13@gmail.com[2],chinthalapudiharish@gmail.com[3]
,soniypasupuleti27@gmail.com[4],tarunchalasani13@gmail.com[5]

Abstract—*Alphanumeric passwords are being replaced with safer, more user-friendly ones. These alternatives are growing in popularity. One prominent option is a graphical password authentication system. This study examines a web-based graphical password authentication system that aims to improve security and usability. The system is kept user-friendly throughout the study. This method reduces the hazards of alphanumeric passwords. Combining picture memorability with text-based passwords achieves this. This research emphasizes the usefulness and practicality of graphical password authentication for online application security. This study will concentrate on the efficacy of these methods. This is achieved by thoroughly examining the system's design, implementation, and user experience.*

Keywords—*Graphical password authentication, multi-factor authentication, usability, security, feasibility, user experience, intuitive interface, encryption, open-source technologies, accessibility.*

I. INTRODUCTION

User authentication is the most crucial part of cybersecurity since it prevents unauthorized access to critical data and resources in web-based systems. Because it considers user authentication. However, alphanumeric passwords are becoming increasingly susceptible to brute-force assaults and password guessing. Examples of hazards include. Due to the weaknesses, other authentication methods that mix security and usability are gaining popularity. This attention is spurred by the vulnerabilities revealed. Bringing out flaws has sparked this attention. Graphical password authentication solutions are intriguing because they avoid the limits of alphanumeric passwords. This is a response to password constraints. Graphical passwords may simplify client authentication and increase security. They use human cognitive talents better at recognizing and remembering visuals than words. This paper analyses a web-based graphical password authentication system designed for secure and easy authentication. The article's eventual objective is a complete system study. This method is supplied to improve safety and user convenience. This assignment may be completed using graphical and text-based components. This study will examine the architectural, implementation, and user experience aspects of the graphical password authentication system. This study aims to contribute to the ongoing conversation concerning web-based authentication solutions.

II. LITERATURE REVIEW

Graphical password authentication systems have garnered attention as a viable alternative to alphabetic and numeric passwords in recent years.

Some credit this interest for the creation of these systems. The paper reviews all graphical password research in this section. This research examinesseveral tactics, including recognition and recall methods and recognition methods, in addition to Passfaces and PassPoints.

A. A Shoulder Surfing Resistant Graphical Password Scheme

Rajarajan and Priyadarsini (2021) created SelfiePass, a photo-based password system. To prevent password-related shoulder surfing attacks. An attacker is "shoulder surfing" when they watch a real user's login procedure, which might compromise their password. Malicious actors invented shoulder surfing. Sometimes shoulder surfing is called shoulder surfing. SelfiePass solves this with selfie-based authentication. This authentication technique uses the user's familiarity with their face to reduce the possibility of unauthorized viewing. To engage in a SelfiePass, users must take a selfie on their phone. Users must meet this to participate. This occurs multiple times during event registration. To authenticate, users must respond to randomly generated screen prompts using actions or gestures. These instructions are on the screen for convenience. These cues may include smiling, blinking, or hand gestures. This ensures that the authentication process is secure and simple [1].

SelfiePass reduces shoulder surfing attacks by authenticating users based on their looks rather than alphanumeric passwords or graphical patterns. This is done using face-based authentication instead of passwords. This strategy boosts system efficiency and security. People remember facial movements better than random photos or patterns. This is because people recall face-related motions. SelfiePass also adds security measures to prevent unauthorized access. These components are officially called "security features." To prevent an attacker from copying the authentication process, the system may force users to perform a specified sequence of gestures or provide time-based challenges. To prevent authentication replication, this is done. Both measures ensure that the authentication method cannot be easily replicated [2].

This study assessed SelfiePass's effectiveness using a range of tests. These tests showed that the service resists shoulder surfing attacks and maintains client satisfaction. SelfiePass is more secure than existing photo password generators without sacrificing simplicity. This makes it a rival for the role of an alternative in the protection of sensitive information in many online applications. The introduction of SelfiePass has greatly improved graphical password authentication. It achieves this by providing a shoulder surfing-resistant solution, which increases system security and interface usability. Innovative solutions like SelfiePass authentication are needed to secure sensitive data and retain consumer trust in digital contexts. Given the growing online threats, this is becoming more critical.

B. A Graphical Password Authentication Scheme

Adebimpe introduced graphical password authentication in 2020 to speed up logins while retaining security. Graphical password systems have been studied because users may have trouble remembering regular alphabetic passwords, despite their popularity. The brain remembers graphical passwords better than random text. This is because graphical passwords employ pictures. The finding that many earlier graphical password systems had lengthy login times inspired the invention of this system. This may cause consumers to get frustrated, reducing the authentication process's usefulness. Thus, the system was created to simplify authentication to address this problem [3].

This technique offers a streamlined graphical user interface for password generation and authentication. Users may quickly pick and check graphical components using this interface, eliminating unneeded complexity. This program intends to increase efficiency, usability, and security by reducing user cognitive burden. User research and performance analysis were used to verify the system's efficacy. The findings showed that the system logged in faster than graphical passwords. Due to its implementation, the system was highly secure against unauthorized access.

The work balances security and usability, making it a potential graphical password authentication advancement. Considering everything, this work is promising. However, innovative solutions are becoming more important in sustaining digital system integrity and improving user experience. Secure authentication will likely become more important [4].

C. Graphical passwords: Behind the attainment of goals

In "Graphical Passwords: Behind the Attainment of Goals," Vaddeti et al. (2020) examine the motivations behind graphical password authentication methods. Traditional alphanumeric passwords are flawed despite their popularity. These include being vulnerable to brute force attacks and making it hard for users to memorize long strings of characters. Due to the problem, graphic passwords are an alternate authentication method. These passwords employ images instead of alphanumeric sequences, making them simpler to remember. Graphical password authentication systems aim to increase digital system security while maintaining or improving end-user usability. These methods generate easy-to-remember passwords that withstand the most prevalent assaults. Graphical passwords promise to boost user engagement and satisfaction by making login easier and more personalized. This might boost user satisfaction and thus, client satisfaction may grow.

In designing and implementing graphical password systems, Vaddeti et al. (2020) emphasize the need to balance security and usability. Consider this critical point. Security is crucial to preventing unauthorized access to sensitive data, but usability is crucial to ensuring that users can easily generate and remember their passwords without too much hassle. This should be considered. This research examines many aspects that affect graphical password authentication system efficacy. These include choosing graphical components, designing user interfaces, and adding security. If academics and practitioners understand the motives behind graphical password use, they may be able to create more robust and user-friendly authentication solutions.

Vaddeti et al. (2020) discuss the adoption of graphical password authentication systems and the importance of security and usability in their design and implementation. This study's findings are remarkable and educational. Graphical passwords, which are becoming more prevalent as digital systems proliferate, might improve security and simplify authentication.

III. METHODOLOGY

A conference paper's methodology section describes the research strategy, methods, and processes utilized to design, develop, and test the proposed graphical password authentication system. The paper includes this section since it will be presented at the conference. Most individuals find it easier to start publishing with this section. This section explains the systematic methods used to meet the study's goals. To complete the study, the following approaches were used. After system design and installation, data collecting, user testing, data analysis, and ethical considerations follow.

Research Design:

The research strategy focused on qualitative and experimental data collecting and analysis methods to achieve its aims. This technique covers creating and building a graphical password authentication system prototype. User testing evaluates the computer system's usability and efficacy. Additionally, the investigation analyzes the available literature. This research seeks adequate theoretical frameworks and methods. This study seeks to achieve this objective while guiding progress.

System Design and Development:

Besides defining the architectural structure of the graphical password authentication system, "system design" includes the system itself. The system, user interface, and interaction techniques are all determined by this criterion, which entails many options and issues. Executing the system prototype takes precedence during development. This ensures system functionality. HTML, CSS, JavaScript, and a server-side framework like Django are needed to do this.

Data Collection:

User input and system performance indicators are used to gather data for this study. This inquiry requires these components. Metrics for system performance include login time, authentication success rate, and authentication issues. Number of successful authentications is another measure. The total number of successful authentications is another metric. There are many ways to assess user happiness, system simplicity, and perceived security. The methodologies include usability testing, surveys, and user interviews. Usability testing sessions gather client input.

User Testing:

User testing evaluates the efficacy and usability of the graphical password authentication system to be installed. Therefore, it is crucial to choose participants from a variety of user groups to guarantee that the input is representative of the user population. Participants are assigned system tasks during testing sessions. They get these responsibilities throughout sessions. They're responsible for these. Individuals must register, present ID, and change passwords. These steps are needed to meet the criterion. Several observations are obtained of system-person interactions throughout the operation. Feedback is also collected via organized questionnaires and open-ended interviews.

Data Analysis:

Data and information analysis involves understanding and interpreting data to get insights. This will provide critical information. This task is crucial for learning. Statistical methods are used to find patterns and trends in quantitative data, which may include system metrics. This helps the system work better. This step is necessary to draw facts-based judgments. Theme analysis is used to evaluate qualitative user feedback. This method seeks recurring themes and insights regarding the system's usability and efficacy. The strategy seeks themes and insights.

Evaluation Criteria:

The presented graphical password authentication method is being evaluated based on many characteristics. Security, simplicity of use, and user satisfaction are among these criteria. Security assessments include the system's resilience against dictionary and brute force assaults. Dictionary and brute force assaults are examples. Dictionary and brute force attacks exist. Dictionary assaults increase. System usability evaluation considers many variables. These characteristics include usability, learnability, and authentication efficiency. In user testing sessions, participants' opinions and assessments are gathered to determine customer satisfaction with the product.

Ethical Considerations:

Every step of the research process involves ethical considerations. To protect participants' privacy and confidentiality, many steps are taken before data collection. Participants may provide informed permission before data collection. Participants are advised of their right to withdraw from the study at any time without penalty and given the choice to do so. This permit has no requirements. This study follows regulatory agencies' and organizations' ethical guidelines. Following these norms and values, the research is conducted. This is done to ensure research credibility and integrity.

The methodology section describes a methodical way to build, implement, and assess the graphical password authentication system. The research being conducted with the stated goal aims to advance digital authentication technology. This will be achieved by providing detailed system usage, effectiveness, and safety information. The research will employ qualitative and experimental methodologies to attain this goal [6].

A. System Architecture:

User Interface: The system is simple and intuitive and this simplifies graphic password creation and authentication. Users choose a personal picture and provide words to parts.

Authentication Engine: Login credentials are verified by the authentication engine. The chosen text and places are compared to the stored password.

Database: A database stores graphical passwords and other data and this database stores data. This protects sensitive and dependable data.

Integration with Web Frameworks: It interfaces nicely with Django, easing online application setup and scaling. This solution supports several frameworks.

B. Key Features:

Multi-Factor Authentication: Multi-factor authentication prevents unauthorized access. They encompass physical and digital identities. This is possible with graphical and text passwords.

Personalization and Memorability: Users may build memorable passwords using their photos and languages. This allows users to create simple, memorable passwords.

Flexibility in Password Creation: The number and order of picture parts may be customized. Including locations is up to the users. Users may secure passwords with greater control.

Secure Storage: To protect user data, a database is used and the purpose is information restriction. This is done using encryption, hashing, and other methods.

C. Authentication Process:

Password Creation: Passwords are created during authentication. User photos and section displays are selected at registration. Now they must connect each webpage using the right terms. The system database protects this data [8].

Login Authentication: Login authentication requires users to choose picture portions and write text. For authentication, the engine checks passwords to places and text. You are comparing during authentication. This is needed to validate user permission.

Security Measures: Multiple security measures safeguard and authenticate user credentials. They include encryption, hashing, and session management. These approaches provide safe authentication.

D. Usability and User Experience:

User-Friendly Interface: It's password-setting and authentication interface is easy and beautiful. These improvements improve system usability and experience.

Memorability: Users forget and reuse pictures less than alphanumeric passwords because they remember them better. Since images are easier to remember than alphanumeric passwords.

Usability Testing: To increase usability, the proposed system is extensively tested and researched. This assesses system performance. By doing this, customers may enjoy authentication.

It overcomes alphanumeric password issues with its website-based graphical password authentication. Graphical and text-based components secure web applications. The technology allows multi-factor and other authentications. This preserves accessibility and user experience while enhancing internet security [9].

IV. IMPLEMENTATION

A. Implementation

VB.NET, a flexible programming language for Windows-compatible applications, was used to create the system. Implementation classes include LoginInfo, GraphicalPassword, and SelReg. All of these classes help the platform.

1) LoginInfo stores user authentication info. The class has it. Login, graphical password, and other methods exist in this database. The system may separately authenticate users every time they log in using this class, which simplifies user credential storage and retrieval. It now handles user authentication effectively.
2) GraphicalPassword controls graphical passwords. Users may choose POIs in a photo and correlate them with similar text-based passwords. The system allows multi-factor authentication using graphics and text. This enhances security and system functioning [10].
3) SelReg handles select POIs and displays passwords visually. POIs may be linked to words or phrases at will. They may define location order and amount to increase authentication. The system's versatility lets users construct one-of-a-kind, memorable passwords.

The client-side interface of VB.NET communicates with a backend server to authenticate and save data. Management is simplified, concerns are segregated, and scalability is increased using this design [12].

System design

One of the goals of the web-based graphical password authentication system is to offer authentication that is both secure and simple to understand. In this part, the planning and implementation of the system are discussed in depth. The instructions on how to finish the project and make use of the interface are provided inside.

Accessing the User Interface:

Establishing a connection via the user interface As soon as the Django server is up and running, the user interface of the system will become accessible. Launch your web browser and enter the following URL into the address bar: http://127.0.0.1:8000/index.html. By doing so, the process of accessing the user interface is initiated [13]. When users press the enter key, they are sent to the login screen, as seen in the following example:

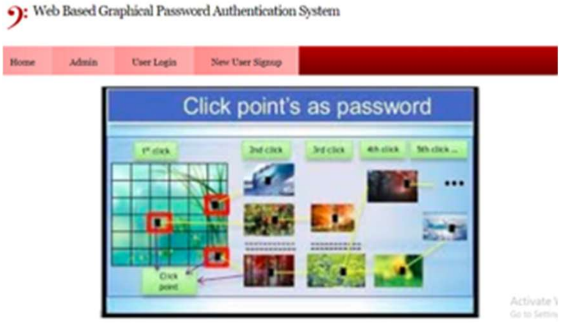
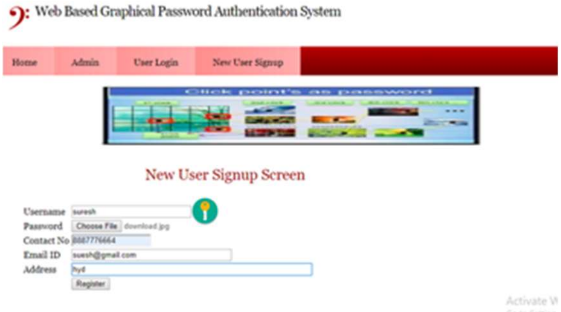


Fig. 1: New User Signup

User Signup:

To finish the registration process, new users are required to choose the "New User Signup" option on the login page. This is necessary to create an account. After that, visitors will be sent to the registration page, where they will be able to submit their information and choose a graphical password image, as seen in the snapshot that follows:


Web Based Graphical Password Authentication System
Home
Admin
User Login
New User Signup
Click point's as password

New User Signup Screen

Username suresh
Password Choose File download.jpg
Contact No 8887776664
Email ID suesh@gmail.com
Address hyd
Register

Fig. 2: Register

Graphical Password Creation:

To generate a graphical password, users are required to choose certain areas within their registered account picture. This guarantees that the password is generated correctly. The graphical password for them is generated by this [14]. Users can pick a region of the picture by clicking on any portion of the image, and the system displays the current location of the mouse to assist them in selecting the appropriate area. As may be seen in the graphic that follows, client registration is possible once they have chosen their fit places:

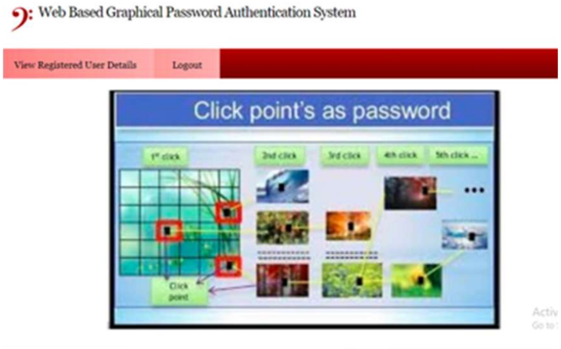
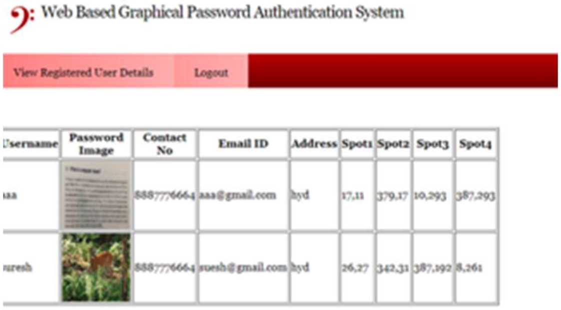

Web Based Graphical Password Authentication System
View Registered User Details
Logout
Click point's as password
1st click
2nd click
3rd click
4th click
5th click ...
Click point

Fig. 3: Registered with image password

Registration Confirmation:

Following the completion of the registration process, users are sent a message that serves as a confirmation. The message will show up when the online registration has been completed. After that, users can enter the login page and complete the authentication process by using the graphical password that they have just set. Because they have just set the password.


Web Based Graphical Password Authentication System
View Registered User Details
Logout

Username	Password Image	Contact No	Email ID	Address	Spot1	Spot2	Spot3	Spot4
aa		8887776664	aaa@gmail.com	hyd	17,11	379,17	10,293	387,293
uresh		8887776664	suesh@gmail.com	hyd	26,27	342,31	387,192	8,261

Fig. 4: users details after Registration Confirmation

User Authentication:

Users may authenticate themselves by entering their username and selecting areas from their graphical password picture (also known as "user authentication").

The user can access their account and by doing so, they can access their account. A word that might be used to describe this process is "user authentication." It is the responsibility of the system to validate the user's credentials once they have selected the appropriate fit places and clicked the authentication button [15]. If the provided places correspond to the locations of the database password, the user is granted authorization, as seen in the screenshot that follows:

A graphical password authentication solution that is web-based makes the process of logging in secure and simple from the very beginning. The system makes use of both graphical and text-based components, which results in an improvement in both accessibility and security. Because of this, it is a desirable alternative to passwords that are composed of alphabetic and numeric letter combinations.

V. CONCLUSION

Finally, its web-based graphical password authentication solution improves the safety and usefulness of enterprise user authentication operations. The approach overcomes the constraints of alphanumeric passwords by providing a more secure and user-friendly login experience. Innovative solutions like graphical passwords and multi-factor authentication do this. It created a system that meets modern security standards and is accessible to a broad variety of users. Simple user interfaces, strong security, and thorough feasibility studies achieve this. The system's user-friendly design and fluid navigation pathways increase the user experience while protecting sensitive user data with multi-factor authentication and encryption.

Throughout the project, a feasibility study validated the system's economic, technological, and social viability, confirming its broad adoption and acceptance. By showing system viability, this was achieved. This allows a secure, user-friendly authentication system that can be simply set up and modified to suit the demands of many sectors and organizations. This goal was achieved by integrating open-source technology, reducing costs, and prioritizing user demands. In a dynamic security environment, the system will need continual monitoring, review, and adjustment to be effective and relevant. This is needed to keep the system successful and current. If the system continues to monitor user input, new threats, and technical changes, it may improve its security and remain a trusted authentication solution in the digital age.

VI. FUTURE STUDY

Even though the present research offers useful insights into the design, development, and assessment of the proposed graphical password authentication system, several other routes may be examined and studied in the future about this particular issue. In the future, these potential paths may be investigated and investigated further. To further improve the safety, usefulness, and efficiency of graphical password authentication systems, the purpose of these prospective topics of future research is to provide further research opportunities. Taking into account the interests of consumers, tackling new issues, and capitalizing on technological improvements is how this objective will be realized. [5] proposed a system in which FASTRA downloads and data transfers can be carried over a high speed internet network. On enhancement of the algorithm, the new algorithm holds the key for many new frontiers to be explored in case of congestion control. The congestion control algorithm is currently running on Linux platform. [7] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation.

1. Advanced Security Features:

In the future, research may concentrate on incorporating advanced security features into graphical password authentication systems toincrease the systems' resistance to growing cyber threats. This is done to strengthen the systems' ability to withstand cyber attacks. Specifically, this is done to improve the systems' ability to resist the increasing amount of cyber assaults. There is a possibility that this will include the use of biometric authentication techniques to give extra levels of security and authentication. The scanning of fingerprints and the detection of facial traits are two examples of procedures that fall under this category.

2. Optimization of Usability:

Potentially, more research might investigate methods that can improve the usability of graphical password authentication systems by making them more user-friendly and intuitive. A term that might be used to describe this would be "usability optimization." There is a possibility that this will include the modification of the graphical user interface, the simplification of the technique of logging in, and the implementation of customized authentication methods that are suited to the preferences and routines of individual users. Not a single one of these things is impossible.

3. Multi-Modal Authentication:

In the future, research may study whether or not it is possible to include multi-modal authentication schemes into graphical password systems and whether or not this would increase the efficiency of these systems. Moreover, the research may also investigate whether or not this would be practical. The creation of hybrid authentication methods that provide improved security and usability may include merging graphical passwords with other authentication components, such as text-based passwords, biometrics, or token-based authentication. This may be done to create hybrid authentication methods. The development of hybrid authentication techniques might be accomplished by this action. The use of graphical passwords in combination with other authentication procedures may be necessary in this particular setting.

4. User-Centric Design:

In the future, research may use a user-centric design approach to get a better understanding of the requirements, preferences, and behaviors of users in connection to graphical password authentication systems. This is expected to be accomplished via the application of this method. It may be necessary to arrange user-centered design workshops, usability testing sessions, and user input surveys to accomplish this goal. To facilitate the development of authentication solutions that are more user-friendly and intuitive, these activities are intended to collect information and provide direction.

5. Cross-Platform Compatibility:

Additional studies might investigate various approaches to guarantee the cross-platform compatibility and interoperability of graphical password authentication systems across a variety of devices and operating systems on your computer. This would be an attempt that would be beneficial. Consequently, the development of standardized protocols and interfaces may be necessary to enable the integration and deployment of the system in a variety of digital settings. This is because of the conditions described above.

6. Behavioural Analysis:

In the future, more studies may examine the deployment of techniques that are based on behavioral analysis to identify and prevent efforts to get unauthorized access to graphical password authentication systems. This is being done to protect against the possibility of unauthorized access being gained. To do this, it may be necessary to investigateuser interaction patterns, keystroke dynamics, and other behavioral biometrics to discover any abnormalities and possible security issues.

VII. REFERENCES

[1] Rajarajan, S. and Priyadarsini, P.L.K., 2021, August. SelfiePass: A Shoulder Surfing Resistant Graphical Password Scheme. In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT) (pp. 563-567). IEEE.

[2] Adebimpe, L.A., 2020. TrimT: A Graphical Password Authentication Scheme. Journal, Advances in Mathematical & Computational Sciences, 8(3).

[3] Shammee, T.I., Akter, T., Mou, M., Chowdhury, F. and Ferdous, M.S., 2020. A systematic literature review of graphical password schemes. Journal of Computing Science and Engineering, 14(4), pp.163-185.

[4] Khodadadi, T., Javadianasl, Y., Rabiei, F., Alizadeh, M., Zamani, M. and Chaeikar, S.S., 2021, December. A novel graphical password authentication scheme with improved usability. In 2021 4th International symposium on advanced electrical and communication technologies (ISAECT) (pp. 01-04). IEEE.

[5] Christo Ananth, A. Ramalakshmi, S. Velammal,B. Rajalakshmi Chmizh, M. Esakki Deepana, “FASTRA – Safe And Secure”, International Journal For Technological Research In Engineering (IJTRE), Volume 1, Issue 12, August-2014,pp: 1433-1438.

[6] Chuen, Y.S., Al-Rashdan, M.A.E.N. and Al-Maatouk, Q.U.S.A.Y., 2020. Graphical password strategy. J. Crit. Rev, 7(3), pp.102-104.

[7] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, “Reconstruction of Objects with VSN”, International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20.

[8] Abraheem, A., Bozed, K. and Eltarhouni, W., 2022, May. Survey of various graphical password techniques and their schemes. In 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA) (pp. 105-110). IEEE.

[9] Khan, M.A., Din, I.U. and Almogren, A., 2023. Securing Access to Internet of Medical Things Using a Graphical-Password-Based User Authentication Scheme. Sustainability, 15(6), p.5207.

[10] Raptis, G.E., Katsini, C., Cen, A.J.L., Arachchilage, N.A.G. and Nacke, L.E., 2021, May. Better, funner, stronger: a gameful approach to nudge people into making less predictable graphical password choices. In Proceedings of the 2021 CHI conference on human factors in computing systems (pp. 1-17).

[11] Shah, A.N., Anand, D., Samanta, S. and Dey, D., 2021. Graphical password authentication system using modified intuitive approach. Int. J. HIT. TRANSC: ECCN, 7(2A), pp.64-71.

[12] Chu, X., Sun, H. and Chen, Z., 2020. Passpage: graphical password authentication scheme based on web browsing records. In Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24 (pp. 166-176). Springer International Publishing.

[13] Kaka, J.G., Ishaq, O.O. and Ojeniyi, J.O., 2021, February. Recognition-based graphical password algorithms: A survey. In 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA) (pp. 44-51). IEEE.

[14] Abdalkareem, Z.A., Akif, O.Z., Abdulatif, F.A., Amiza, A. and Ehkan, P., 2021, February. Graphical password based mouse behavior technique. In Journal of Physics: Conference Series (Vol. 1755, No. 1, p. 012021). IOP Publishing.

[15] Jaffar, J.A. and Zeki, A.M., 2020, December. Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability. In 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT) (pp. 1-5). IEEE.

[16] Juneja, K., 2020. An XML transformed method to improve effectiveness of graphical password authentication. Journal of King Saud University-Computer and Information Sciences, 32(1), pp.11-23.

[17] Quadry, K.M., Govardhan, A. and Misbahuddin, M., 2021. Design, Analysis, and Implementation of a Two-factor Authentication Scheme using Graphical Password. International Journal of Computer Network & Information Security, 13(3).

[18] Jirjees, S.W., Mahmood, A.M. and Nasser, A.R., 2022. Passnumbers: An approach of graphical password authentication based on grid selection. IJSSE, 12(1), pp.21-29.

[19] Fong, J. and Poet, R., 2020, November. Creating graphical passwords on a mobile phone: graphical passwords on a mobile. In 13th International Conference on Security of Information and Networks (pp. 1-6).

[20] Singh, U.P., Chouhan, S.S. and Jain, S., 2020. Images as graphical password: verification and analysis using non-regular low-density parity check coding. International Journal of Information Technology, pp.1-41.

[21] Kenneth, M.O. and Olujuwon, S.M., 2021. Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password. Journal of Computer Science Research, 3(3), pp.29-41.