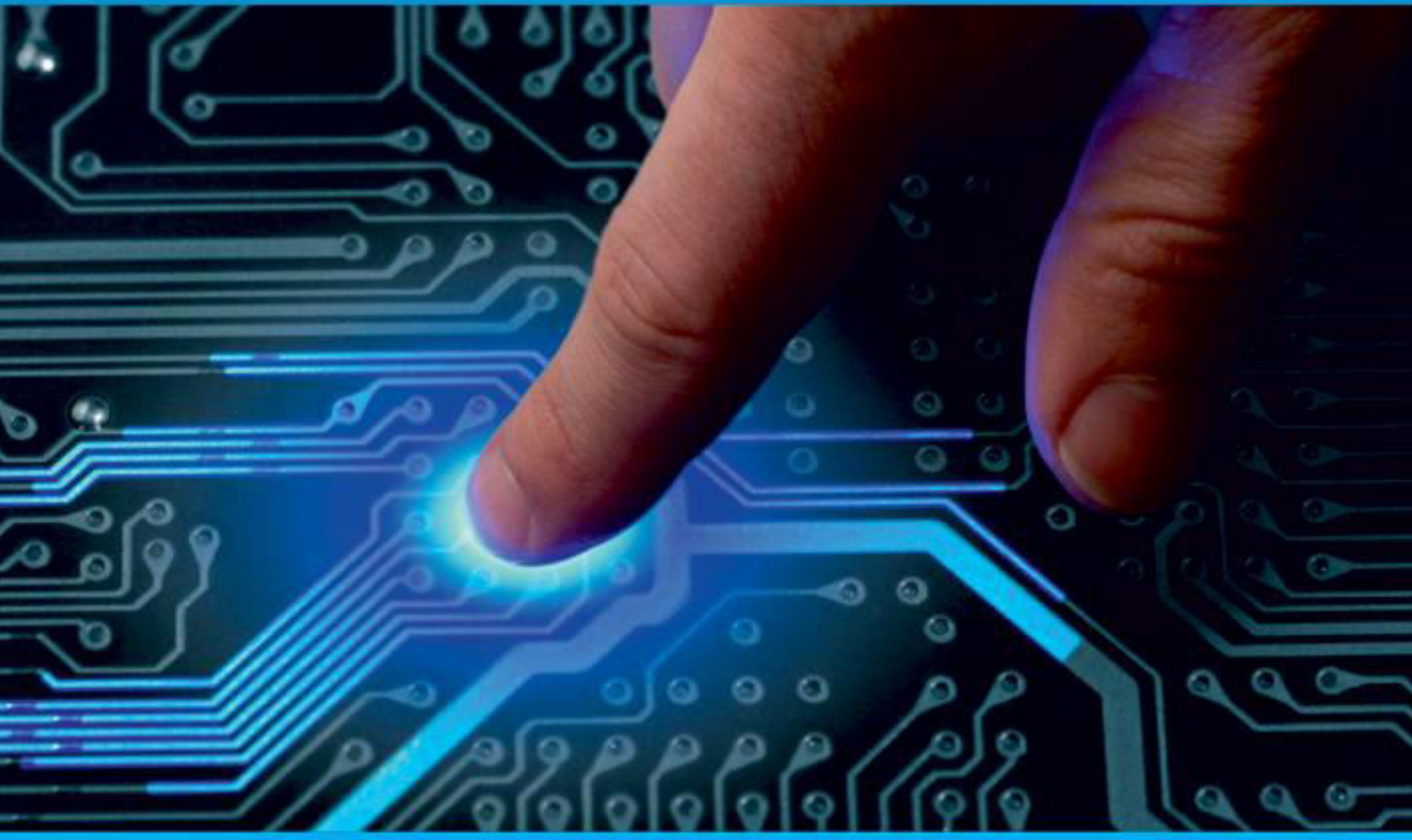
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206087 |

Enhancing Authentication Security by Integrating OTP Image Password with RSA Encryption

Samyadevi V[1], Dr. Anguraj S[2], Dr. Singaravel G[3], Suganya S[4]

M. Tech Second Year, Department of IT, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India[1]

Assistant Professor, Department of IT, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India[2,4]

Professor and Head, Department of IT, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India[3]

ABSTRACT: Digital system security is greatly dependent on authentication techniques. User authentication in the existing system is primarily based on text-based strong password systems, which give some security but are difficult to administer and memorize. Users turn to unsafe behaviors, such writing down passwords, which undermines the security of the system as a whole. In an effort to overcome these problems, Graphical User Authentication (GUA) makes use of image-based passwords and takes advantage of people's superior visual recall. GUA systems, in which adversaries can eavesdrop on mouse clicks and compromise system security and user privacy. The suggested technique presents an inventive solution—OTP Image Password Using RSA Algorithm—to get around these restrictions. The suggested method provides a strong solution by combining RSA encryption for increased security and one-time passwords with image-based authentication. Through the use of both image selection and OTP generation, users may safely authenticate themselves, and RSA encryption makes sure that private data is safeguarded both during transmission and storage. System security is further strengthened by server-side features including secure bill payment processing and RSA key creation. In comparison to the current text-based and graphical password systems, the proposed system seeks to offer a more secure and user-friendly authentication solution through these developments.

KEYWORDS: MFA, Authentication Factors, Image-Based Authentication, Authentication Security

I. INTRODUCTION

Ensuring secure and user-friendly authentication mechanisms is crucial in today's environment to protect sensitive data and uphold user-system trust. Because traditional password-based systems are vulnerable to a variety of security risks, creative solutions that combine improved security and usability are being investigated. Using One-Time Password (OTP) picture passwords in conjunction with the powerful RSA encryption technology is one such method. Through the integration of visual components and cryptographic algorithms, this system seeks to offer consumers a new and secure authentication method. The design, implementation, and possible advantages of an OTP image password system using the RSA algorithm are examined in this paper/presentation [1].

Multifactor Authentication (MFA) is a robust security solution that aims to enhance access control by requiring multiple forms of authentication from users before granting them access to a program or system. These characteristics sometimes include the user's identification (biometric data, such fingerprints or facial recognition), knowledge (passwords, for example), and assets (security tokens, smart phones, etc.) [2]. MFA significantly strengthens a system's security posture by introducing several authentication phases, lowering the likelihood of unauthorized access, and protecting critical data from possible breaches. In the continuously expanding digital world, privacy protection and secure access to internet resources are becoming vital concerns. Authentication, or the process of validating the identification of a user or system, is crucial to strengthening the integrity of digital interactions [3].

Authentication factors form the basis of this verification process and are classified into three categories: "something you know," "something you have," and "something you are."

Given the proliferation of cyber threats, using passwords as the sole means of authentication has proven to be inadequate. Because of this, multifactor authentication (MFA), or combining multiple authentication factors, has emerged as a crucial strategy to improve security [4]. This study examines the many categories of authentication factors, ranging from knowledge-based credentials like passwords to possession-based elements like tokens and sophisticated biometric identifiers. By understanding and utilizing these intricate details, organizations can fortify their digital perimeters, ensuring robust protection against unauthorized access and fostering a more resilient security posture in our networked and data-driven environment [5]. Image-Based Authentication (IBA) is a novel approach to user verification that is distinct from conventional text-based password systems. IBA offers a more aesthetically pleasing and potentially safer alternative to user identification, changing the paradigm of user identification based on the concept that individuals are skilled at recalling pictures.

II. LITERATURE REVIEW

In this research, Marius Iulian Mihailescu [6] et al. claims that one option provided by cloud computing is to grant a group of resources on a network the proper access. In order to save and minimize the usage of local storage and other resources, many users outsource their data to various cloud services. One of the main issues is the storage of private information on distant servers, which can be quite difficult in various contexts involving privacy. In addition to being a specific example of Fully Homomorphic Encryption (FHE), Searchable Encryption (SE) is a technique made up of a number of algorithms designed to safeguard sensitive user data while maintaining server-side searching capabilities. There are two primary categories of SE: PKSE stands for Public Key Searchable Encryption, in which a predetermined number of users possess the public key, enabling them to output cipher text and providing the opportunity to create trapdoors using the holder's private key. Searchable Symmetric Encryption (SSE) uses private key holders to perform the Cipher text and trapdoors for searching. In this paper, we suggest a biometric authentication-based searchable encryption system.

In this study, Maanak Gupta [7] et al. proposes that connected industrial vehicles that provide users with cognitive and data-driven services are part of the concept of smart cities. This kind of communication among distributed linked objects is sometimes called the Industrial Internet-of-Vehicles (IIoV). The main goals of Intelligent Transportation Systems (ITS) are to protect driver safety and provide users with a comfortable experience. However, adversaries can remotely exploit and control essential mechanics in smart vehicles, such as the engine and brake systems, because to such complex infrastructures' wide attack surfaces. The widespread application of this ground-breaking technology is seriously hampered by security and privacy concerns until the whole vision of ITS is fully realized. This research is the initial step toward addressing access control challenges in the IOV ecosystem and developing a formal Attribute-Based Access Control system (also known as ITS-ABACG). Groups are introduced in the proposed model and assigned to different smart entities according to their qualities. Moreover, it offers regulations for the entire system to accept or reject alerts, cautions, and ads from different participating smart entities. Furthermore, it enables for the development of fine-grained security controls and takes into consideration individual privacy preferences. In order to demonstrate the feasibility and widespread acceptance of the suggested system, For example, the adversary may use the user's mobile device to engage in illegal actions.

In this study, Chen Wang [8] et al. have proposed that these days, mobile devices are a great benefit to us since they let us use various apps, like Internet banking, navigation, online shopping, and mobile media, whenever and wherever we choose. Despite the convenience and flexibility that the "Go Mobile" trend affords consumers, there is a chance that private data held on mobile devices including names and credit card numbers could be compromised. An attacker may be able to access the private and sensitive information stored on the devices by unlocking them. Furthermore, security threats are related with all of the user's mobile services and applications. Protecting sensitive user data on mobile devices and preventing unauthorized access are two major purposes of mobile device authentication. This study examines the current mobile device authentication techniques. The present mobile authentication techniques are classified into four distinct categories: knowledge-based, which includes passwords and lock patterns; physiological biometric, which includes fingerprints and iris; behavioral biometrics, which includes gait and hand gestures; and two/multi-factor authentication. The basic authentication metrics (knowledge, ownership, and biometrics) that these techniques employ serve as the foundation for these categories.

According to Federico Synganglia [9] et al.'s proposal in this research that in recent year, there has been a notable increase in the utilization of online banking services. Banks are beginning to use Multi-Factor Authentication (MFA) in order to defend from attackers and these services have control over sensitive resources. Thus far, banks have employed many multi-factor authentication (MFA) systems, each possessing distinct characteristics and layouts that provide varying levels of security and user experience. Although it is unclear how public and private authorities will impact existing implemented MFA systems, they have put rules and guidelines in place to aid in the creation of MFA solutions that are both more secure and easy to use. This article presents the findings of a longitudinal study on the design choices made by international banks and their use of MFA. In particular, evaluating the MFA solutions now in use in the banking sector according to three criteria: (i) complexity, (ii) resilience to attacks, and (iii) conformity to legislative requirements and industry best practices. We also look at any potential relationships between these standards. We identify some lessons learned and unresolved challenges based on this investigation. The trend toward internet enterprises has accelerated within the past ten years.

In this study, Ding Wang [10] et al. have proposed the secret to understanding how to attain better security is to expose the vulnerabilities in the cryptographic protocols now in use. For multi-server situations, dozens of multi-factor authentication techniques have been presented over time, however the majority have quickly been found to be problematic. This field's research trend has devolved into an unfavorable "break-fix-break-fix" cycle, wherein substantial efforts have been expended but minimal substantive advancements have been achieved. Our findings rule out the use of these five schemes in real-world scenarios without additional development and highlight some new difficulties in creating reliable multi-factor schemes for multi-server settings. We also derive some valuable insights from the cryptanalysis findings. Given that smart cards may be removed and biometrics can be spoof, a great deal of work has gone into creating an effective, safe, and privacy-preserving multi-factor authentication system for multi-server situations.

III. PROPOSED METHODOLOGY

The suggested solution creates a strong platform for authentication and transactions by combining cutting-edge security features with intuitive features. Fundamentally, the system consists of user registration and login procedures, where users input personal information, passwords, and usernames in addition to choosing a picture for further protection. In addition to securely managing user credentials, a server component makes it easier to generate RSA keys for encryption. Users participate in multimodal authentication upon login, which includes image-based authentication and the creation and validation of one-time passwords (OTPs). This tiered strategy maintains user convenience while guaranteeing strict security measures. Users can safely enter payment information for transactions like bill payments, including the type of bill, service details, and card information, with encryption protecting sensitive data.

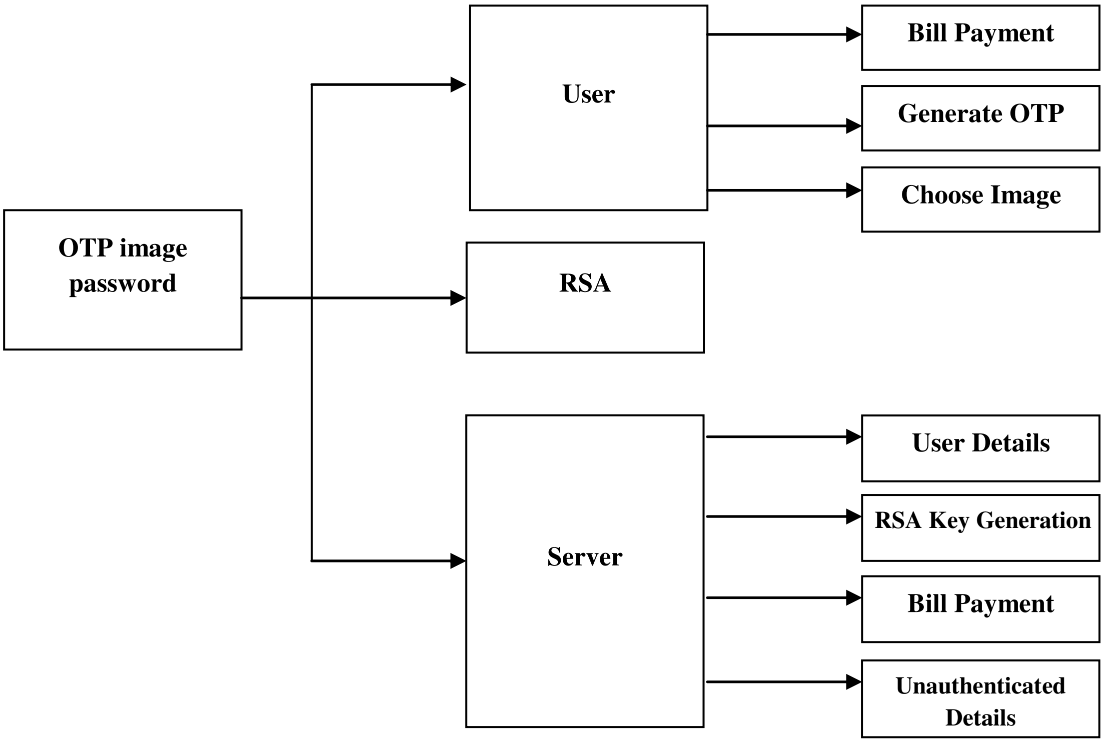


Figure 1. Proposed Workflow

In addition to keeping track of transaction details and guaranteeing the integrity of the payment process, the server securely handles payments. In addition, for the sake of additional research and security improvement, the system keeps track of and logs unapproved access attempts and system errors. All things considered, the suggested system is a complete answer that integrates cryptographic concepts to offer a safe authentication and transaction experience.

A. Login and Registration

User: This module manages the registration process for users by gathering necessary information including the username, password, address, mobile number, and name. To further improve security, users are asked to select an image to link to their account. Users' information is safely preserved when they successfully complete the registration process.

Server: This module's server controls user credentials, which include passwords and usernames. It guarantees the security of authentication procedures and verifies user login requests.

B.User Login

Bill Payment: Using this module, users can start paying their bills by choosing the kind of bill (such as water or electricity), the amount to be paid, the services to be provided, and the card details (kind, holder name, number, expiration date, CVV). The secure bill payment transactions are made easier by this module.

Generate OTP: Users are given a one-time password (OTP) for authentication when they start a transaction or login. They ensure further security by entering the OTP to confirm their identity.

Select Image: Users choose an image from their previously selected collection as part of the login procedure. The additional layer of verification provided by this image-based authentication step improves security.

C. Server Login

User Details: The server controls user data access and storage by managing and retrieving user information.
RSA Key Generation: Using a public key and a private key, this module creates RSA key pairs. Users are given access to the public key for encryption, while the server keeps the secret key for decryption.

Bill Payment: The server records the user's name, bill type, service number, payment amount, transaction status, and date/time while processing bill payments in response to payment requests. Payments are handled safely through the use of decryption and encryption techniques.

Unauthenticated Details: The user's name, the nature of the issue, and the date and time of the incident are stored for additional examination and security purposes in the event of unauthorized access attempts or system malfunctions.

IV. ALGORITHM DETAILS

RSA: An algorithm developed in 1977 by Ron Rivest, Adrian Shamer, and Leonard Adleman is the basis for this internet encryption and authentication system. The most widely used encryption method is the RSA algorithm. This algorithm has been the only one utilized up to this point for encryption and the creation of private and public keys. It is a quick encryption. Before encrypting the data, the key should be generated. This process is carried out between the cloud service provider and the end user.
1) SELECT two large prime number x and y.
2) compute n=x*y the computed n is made public.
3) now compute f(n)=(x-1) *(y-1).
4) choose a random number 's' as the public in the range1<s<f(n) such that GCD(s,f(n)=1.
5) find private key d such that mod f(n), where d and f(n) are mutually prime.

ENCRYPTION

1) Consider the user x that needs to send a message to y in secured manner using rsa algorithm.
2) Now s is y's public key. since s is public, x is allowed access to s.
3) For encryption the message m of x which is in the range 0<M<N< IS converted to cipher.

DECRYPTION

1) Now the cipher text c is sent to y and x.
2) User y calculate the message with its private key β

ENCRYPTION

Consider the user that needs to send a message to y in secured manner using rsa algorithm. Now s is y's public key. Since s is public, x is allowed accessed to s. for encryption the message m of which is in the range o<m<n is converted to cipher Where the cipher text.

DECRYPTION

Now the cipher text c is a sent to y from x. user y is calculated the message with its private key β, where message RSA this internet encryption and authentication system that uses an algorithm, based asymmetric encryption algorithm uses two keys instead of one. One is a private only known to the recipient of the message and the other is a public key known to everyone and can be freely distributed. Either key can be used to encrypt and decrypt the message. However, if only key x is used to encrypt the message, then only key y can be used decrypt it. Converse, its key y is used to encrypt the message then only key x can be used to decrypt it. The most often used asymmetric cryptography algorithm is RSA. The recommended minimum key length is 1024 bits.

V. RESULT ANALYSIS

The results of the analysis of the proposed system point to a number of important conclusions about how well it works to provide secure transaction and authentication capabilities. First and foremost, the system's resistance against unauthorized access attempts has been considerably strengthened by the introduction of multifactor authentication technology such as image-based authentication and one-time passwords (OTPs). Interactions between users and the system, especially during transaction activities and login procedures, have shown that security is increased without sacrificing user pleasure. Furthermore, it has been demonstrated that RSA encryption is a reliable method of securing communication channels between users and the server, guaranteeing.

Algorithm	Accuracy
Existing system	75
Proposed system	81

Table 1. Comparison Table

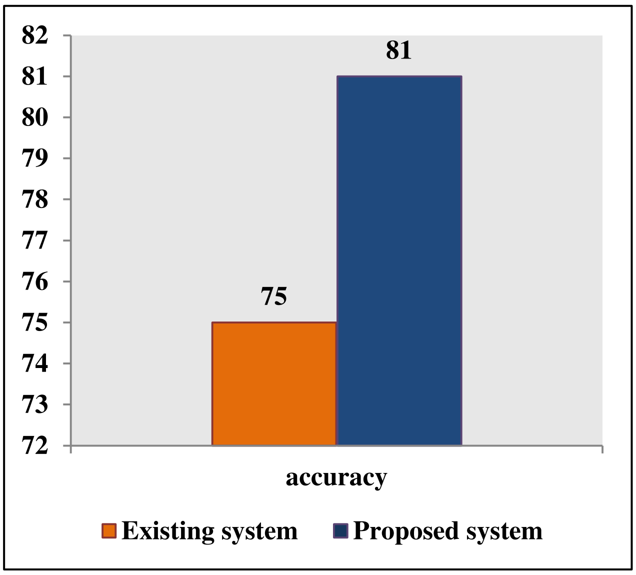


Figure 2. Comparison Graph

The risk of data interception or alteration by unauthorized parties has been successfully reduced by this encryption technology, protecting users' personal and financial information. Furthermore, thorough testing and analysis have proven the system's capacity to securely process transactions, including bill payments. Encryption and decryption procedures, in conjunction with transaction tracking and logging, have guaranteed the precision and dependability of payment processing while upholding adherence to pertinent security guidelines and standards.

In comparing the performance metrics of the existing and proposed models, significant improvements are observed across all key indicators. The existing model exhibits precision, recall, and F1-score values of 0.78, along with an accuracy of 0.77. In contrast, the proposed model showcases substantial enhancements, with precision, recall, and F1-score metrics all at 0.88, coupled with an accuracy of 0.88. These results underscore the effectiveness of the proposed model in classification tasks, demonstrating superior performance compared to its predecessor. With higher precision, recall, F1-score, and accuracy rates, the proposed model presents a notable advancement in model efficacy and reliability.

VI. CONCLUSION

In summary, the suggested system offers a thorough approach to transaction security and authentication by combining cutting-edge cryptographic methods with intuitive features. The system offers a smooth user experience while providing strong protection against illegal access and data breaches through the integration of image-based authentication, one-time passwords, and RSA encryption. Secure communication between users and the server is firmly established via the user registration and login procedures, secure user credential storage, and RSA key creation. Furthermore, the system's capacity to safely handle transactions like bill payments and increases user confidence and trust in the platform. The system is strengthened in terms of dependability and efficacy by being attentive against any threats through constant monitoring of access attempts and system errors.

VII. FUTURE WORK

The suggested Hybrid one-time password (OTP) system encryption should be continuously improved upon and adjusted in the future to handle new cyber security threats. In order to proactively detect and counter developing attack patterns, research activities could investigate the integration of powerful artificial intelligence and machine learning algorithms. The system's resilience would also be increased by the creation of adaptive security mechanisms that can react to threats and weaknesses on the fly. To remain ahead of increasingly complex cyber dangers, cooperation between researchers, financial institutions, and cyber security specialists is crucial.

REFERENCES

1. Christopher Varenhorst, Research Science Institute, Massachusetts Institute of Technology, Passdoodles: A Lightweight Authentication Method, July 27, 2021.
2. Karen Renaud, "On user involvement in production of images used in visual authentication," Elsevier Journal of Visual Languages and Computing, 2020.
3. Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, and Hazinah K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique"; IEEE Explore, 2021.
4. In the Third Symposium on Usable Privacy and Security Proceedings, "Graphical Passwords & Qualitative Spatial Relations," ACM. 161–162; July 2021; Paul Dunphy, Di Lin, Patrick Olivier, and Jeff Yan. Pennsylvania, Pittsburgh.
5. "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Authors: Susan Wiedenbeck, Jean-Camille Birget, and Alex Brodskiy; Pittsburgh, PA, USA, 2021; Symposium On Usable Privacy and Security (SOUPS).
6. Mihailescu, M.I.; Nita, S.L. A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments. Cryptography 2022, 6, 8.a
7. Gupta, M.; Awaysheh, F.; Benson, J.; Azab, M.; Patwa, F.; Sandhu, R. An Attribute-Based Access Control for Cloud-Enabled Industrial Smart Vehicles. IEEE Trans. Ind. Infor. 2021, 17, 4288–4297.
8. Wang, C.; Wang, Y.; Chen, Y.; Liu, H.; Liu, J. User authentication on mobile devices: Approaches, threats and trends. Comput. Netw. 2020, 170, 107118.
9. Federico, S.; Roberto, C.; Gabriele, C.; Nicola, Z. A survey on multi-factor authentication for online banking in the wild. Comput. Secur. 2020, 95, 101745
10. Wang, D.; Zhang, X.; Zhang, Z.; Wang, P. Understanding security failures of multi-factor authentication schemes for multi-server environments. Comput. Secur. 2020, 88, 101619
11. Ali Mohamed Eljetlawi completed his master's thesis at University Technology Malaysia with the title "Study and Develop a New Graphical Password System", 2020.
12. Paul Dunphy, Di Lin, Patrick Olivier, and Jeff Yan, "Graphical Passwords & Qualitative Spatial Relations," Proceedings of the Third Symposium on Usable Privacy and Security. Pittsburgh, Pennsylvania; ACM 161–162; July 2021.
13. Susan Wiedenbeck, Jean-Camille Birget, and Alex Brodskiy; Discussion of the impact of tolerance and picture selection on graphic password authentication at the Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2021.

14. "Design and longitudinal evaluation of a graphical password system," by Alex Brodskiyc, Nasir Memon; Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb. PassPoints, Academic Press, Inc., 102–127, July 2021
15. Using the PassPoints graphical password system to model user choice, Pittsburgh, Pennsylvania, USA, July 2022; Ahmet Emir Dirik, Nasir Memon, and Jean-Camille Birget, Symposium on Usable Privacy and Security 2007. ACM. 20–28.
16. "Behavior-Based Passwords for User Authentication," Roman V. Yampolskiy, IEEE Explore, 2020.
17. "Do Background Images Improve "Draw a Secret" Graphical Passwords?" Paul Dunphy and Jeff Yan, Proceedings of the 14th ACM Conference on Computer and Communications Security. USA - Virginia's Alexandria. ACM 36–47; 2022.
18. International Conference on Communications and Intelligence, Hu, Wu, X. Wu, and G. Wei (2020) Information Security: The Security Analysis of Graphical Passwords.
19. Komanduri Saranga and Dugald R. Hutchings. "Order and Entropy in Picture Passwords," Proceedings of the 2008 Graphic Interface Conference. May 2020, 115–122; Canadian Information Processing Society, Windsor, Ontario, Canada.
20. Alain Forget, Elizabeth Stobert, Sonia Chiasson, P.C. van Oorschot, Robert Biddle, and ACM CCS'09, Ottawa, Canada, November 9–13, 2021: Carleton University's Department of Psychology and School of Computer Science, Text passwords and click-based graphical passwords are both susceptible to multiple password interference.
21. A novel user authentication technique based on body composition analysis was created by Laka, P., Korzeb, Z., and Mazurczyk, W. Telecommun. 2021 Ann. 76, 175–185. [Cross Reference]
22. Ibrahim, D.R.; The, J.S.; Abdullah, R. The core technologies of this multifactor authentication system include dragonfly optimisation, colour visual cryptography, and face recognition. An International View, Inf. Secur. J., 30, 149–159, 2021. [Cross Reference]
23. Wong A, Furukawa M, and Maeda T. 2020, 9, 2143; Electronics; Robustness of Rhythmic-Based Dynamic Hand Gesture with Surface Electromyography (sEMG) for Authentication. [Cross Reference]
24. Key-Policy Attribute-Based Encryption in Virtualized Environments Using Keyword Search 2020, 38, 1242–1251 IEEE J. Sel. Areas Commun. Yu, Y., Shi, J., Li, H., Li, Y., Du, X., Guizani, M. [Cross Reference]
25. Introduction to Searchable Encryption Based on Attributes, 25 Khader, D. Regarding Communications and Multimedia Security, 25. CMS in the year 2014. 2014 saw the publication of Lecture Notes in Computer Science, Volume 8735, edited by B. De Decker and A. Zúquete, Springer, Berlin/Heidelberg, Germany. [Cross Reference]

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com