DMPedia Lecture Notes in Computer Science & Engineering
Volume 1, pp. 453-464, 2026

International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

An XML transformed method to Enhancement effectiveness of Password Authentication System using Graphical Images

P. Divyarani, Rashed Ahmed, Sardar Savinder Singh, Omair Mukaram, Nihal Ansari

Department of Computer Science and Engineering, Vijay Rural Engineering College, Rochis Valley, Manikbhandar, Telangana, India

projectvrec07@gmail.com

Abstract

A crucial part of the security infrastructure is now set up for user authentication and data security. Most users choose text passwords as a means of protecting the security and privacy of their computer system. However, there is always a potential that someone will enter their password in an unsafe method or choose a weak or insecure one. By leveraging the simplicity of image recall over word memory for authentication, graphic passwords are an effective alternative to conventional text passwords. This study presents an XML-transformed Method for improving the Effectiveness of a password authentication system utilising graphical images. The server analyzes the password image with the graphical pattern when a user loads it, using drift and stroke length to confirm its authenticity. Several graphical pattern types emerge when the input pattern is made vulnerable to various changes. When a user enters a password image, the password pattern is extracted and mapped from the recovered pixel values, which are stored in an XML pattern database. Performance analysis parameters include authentication, security, and accuracy. Compared to other image password mappers, this method works better, according to the comparative performance test.

Keywords: *Authentication System, Graphical password, XML (eXtensible Markup Language), Security, Textual password.*

I. Introduction

Nowadays, computers play an important role in everyone's life. Computers can be used for personal and interpersonal communication in addition to business-related applications. In the majority of computer security scenarios, user authentication is an essential element [1]. It is the foundation of access control and user accountability [2]. Password authentication systems often use text-based passwords [3]. One of the functions of passwords is authentication, which verifies that a person is who they represent. (b) Finding out if a confirmed user is permitted access to particular data or services is done through the authorization process. [4] (c) Access Control (Authorization and authentication are part of access restriction). Whether a user chooses a text-based or graphical password, it is typically predictable. [5]. Although people are more inclined to create unique passwords, attackers can still easily guess them because they often follow standard patterns.

These passwords are vulnerable to multiple types of cyberattacks, including phishing, dictionary attacks, shoulder surfing, and brute-force attacks [6]. Numerous studies indicate that many users

select weak passwords, forget them, or write them down insecurely in an effort to remember them all, thereby increasing the risk of password compromise [7].

In recent years, graphical password authentication has become a more secure and user-friendly solution to these problems. With this method, users can select a single image, a group of images, or a sequence of images to serve as their password. It is also possible to use graphic passwords for images of faces, nature icons, and other objects. Recent years have seen an exponential increase in interest in graphic password authentication, and a large number of studies have been conducted to assess its effectiveness and security [8]. GPIs are authentication systems that allow users to choose specific images in a predetermined order [9]. The user is responsible for choosing an image's type, size, quality, accessibility, and other attributes. The recognition process's selection approach is also challenging because the input image is vulnerable to change. Some graphical password systems utilize multiple images as the password. Such images may be recorded consecutively to improve security. For server-side image management, there are two fundamental methods. The first step is to keep it in the database, and the second is to keep it as an image file. The query must be executed on a collection of images using an enhanced query mechanism that maintains the image data database current [10].

In recall-based systems, the chosen sequence functions as the password, and authentication keys are positioned across a still image [11]. Techniques that depend on memory and recognition are commonly used for graphic authentication. To authenticate the system, the user uses a mouse or pen to tap pre-programmed touch points (such as the left eye, mouth, and nose) in an organised manner. With the Pass Points system, which eliminates predefined content limitations and allows the use of arbitrary images, this idea has taken a different direction.

The user inputs the graphical password while utilizing recognition-based authentication, which recognizes a series of images [12]. "Concrete, nameable, and distinctive color images are easier to remember" [13] is the idea behind this graphical identification prototype. On a white background, the pictures depict fundamental, real, and important objects. It is suggested that this prototype be used as a substitute for PIN-based ATM (Automated Teller Machine) authentication, even though images are less effective and memorable than numbers, and customers are more likely to remember passwords based on recognition than on visuals.

To increase password authentication systems effectiveness, this study presents an XML-transformed method that makes use of graphic images. In this study, the server generates an image file using the graphical pattern, creates a graphical password using a pattern frame and gets pattern-adaptable picture data from an XML data form. The source pattern password image is the final file the user is provided. The remainder of the paper is structured as follows: the literature review is presented in Section II, and the use of graphical images for a password authentication system is examined in Section III. The comparative results are discussed in Section IV, and the paper's conclusion is presented in Section V.

II. Literature Survey

In [14], the security and usability of two geographic authentication techniques, GeoPass and GeoPassNotes, were evaluated by the author. To authenticate users, GeoPass displays a geographical password on a digital map. GeoPassNotes extends this process by adding identifying words to the password. The results show that both forms are very memorable, and because annotated location passwords are more secure and have less of an impact on usability than location passwords alone, they might be preferable.

In [15] to solve the problem of traditional password methods that ignore security and usability, in order to help users create safe and memorable passwords, Alphapwd is a novel password creation method that combines letter stroke sequences with mnemonic types. The results show that when it comes to resistance to unknown attacks, passwords based on alphapwd perform better than real password sets.

In [16], the three-dimensional password is shown and assessed, along with the contribution. Multi-factor authentication is a feature of three-dimensional passwords. In order to confirm the validity of the objects, the user can navigate and interact with them in our three-dimensional virtual environment. Users create their three-dimensional password by actions and interactions with objects in the three-dimensional world. Using the 3-D password, the majority of the existing authentication techniques, such as graphical passwords, text passwords, and other biometrics, might be included into a 3-D virtual world. The 3-D password key space is determined by the kinds of objects chosen and the layout of the three-dimensional virtual world.

In [17], for safe password storage, they offer an easy-to-integrate password authentication framework with existing authentication solutions. This architecture encodes the plain password that was sent to it by a client using a cryptographic hash method (like SHA-256). The ENP (Encrypted Negative Password) may be more safe against dictionary attacks and lookup table attacks, based on algorithm complexity comparisons and evaluations.

In [18] an authentication method that combines text and graphics and takes security and usability into consideration, and memorability issues of current approaches. This has been achieved by effectively integrating several approaches that address the problems of the current security solutions. By revealing various trends in the components utilized and the corresponding authentication timings, the password's usability and memorability have also been investigated. The evaluations and results demonstrate how well the recommended strategy worked. The planned plan's extensive use of novel methods presents many chances for security processes to progress.

In [19] SPHINX, a new password management technique, offers security even in the event that a password manager is hacked. SPHINX maintains that the user's master password has no effect on the data on the device. By providing browser plugins, mobile application prototypes, and they give a summary of the design, deployment, and performance analysis of SPHINX while supporting open device-client communication. Additionally, they compare SPHINX to other password managers using a systematic methodology that takes into account factors like usability, security, and deployability.

In [20], by analyzing the techniques utilized by some of the most well-known websites, they investigate potential online password recovery system threats, building on the results of previous studies. A useful open-source plugin that can be installed on any website is called Maildust, and they recommend, to provide a method for registered users to recover their passwords and to stop attacks at the mail service provider level. Finally, while the study was restricted to websites registered with the European Union (EU), the recommended methodology can be applied to any website.

In [21] uses an authentication mechanism that is based on a challenge-response password and is based on the fully automated public turing test to tell computers and humans apart (CAPTCHA) hard problem. The results of an investigation show how efficient the suggested system is in terms of both time and space. The indistinguishable security of the suggested approach against an adaptive chosen-challenge text attack (IND-ACCTA) is shown under the CAPTCHA AI hard problem whenever the hash function H is regarded as a random oracle.

In [22] In cyber-physical systems enabled by the Internet of Things, machine-to-machine (M2M) networks offer a safe and effective way to authenticate users, for safe and efficient data sharing, the suggested solution allows any two entities to mutually authenticate and select a session key. Making use of the widely used BAN (Burrows Abadi Needham) logic model for assessing authentication systems, examined is the suggested method's security. They assess the effectiveness of the proposed strategy by contrasting it with other recently proposed designs.

In [23] for the next-generation network based on the session-initiation protocol that depends on a reliable third-party system, an innovative self-enforcing authentication technique is presented: a low-entropy shared password. By evaluating its security features against current standards, the suggested solution successfully reduces threats including replay attacks, password guessing, and man-in-the-middle attacks.

In [24] develop an asymmetric password authenticated key exchange (PAKE) protocol that is immune to quantum attacks by utilizing smooth projective hash functions (SPHF) and commitment-based password-hashing schemes (PHS) in comparison with lattice-based encryption. This avoids the assumptions of the random oracle model, eliminates the costly Non-interactive zero-knowledge (NIZK) approach, and creates quantum resistance. They also demonstrate how an effective and safe asymmetric-PAKE protocol may be developed using the bellare-pointcheval-rogaway (BPR) paradigm. Lastly, they create a prototype implementation to test how described instantiation works in a real-world environment.

In [25], they develop The availability of motion, heart rate, and respiration audio signals is used by a hierarchical implicit authentication (HIAuth) system to identify a user. Our thorough investigation showed that the real rejection rate is approximately 0.93 ± 0.04 for adults who are sedentary and 0.97 ± 0.07 for those who are not. This radial basis function (RBF) kernel-based binary support vector machine (SVM) classifiers displayed an average accuracy of 0.98 ± 0.04 for sedentary people and 0.94 ± 0.03 for non-sedentary people. There is a non-sedentary F1 score

of 0.98 ± 0.03 and a sedentary F1 score of 0.94 ± 0.04. These outcomes show the possibility and feasible this task

III. Password Authentication System using Graphical Images

Figure 1 represents the block diagram of An XML-transformed technique for improving the efficiency of a password authentication system through graphical images.

To enhance the security element and provide safe authentication, a mixed-media architecture is offered. User-specific passwords and other server-side procedural modifications have been made by the structure to improve security at the media and pattern levels.

For the first time, the user selects their name and a collection of image pixels as their password. The registration method consists of two steps: first, a user must create a CCP (cued click point) password; second, the CCP password is constructed using either user-uploaded or pre-existing images, and email registration is required. using the RGB values of specific areas in images, the CCP password is created; this method is repeated during the verification process.

To generate the CCP, the user click area is used. The x and y axes are saved together with the click point data, and to generate a password, the system uses the RGB values of the clicked image areas.

Operating on a single curve dragging configuration with few limitations, the password system reflects user input using a graphic pattern and an image. The valid pattern must satisfy constraints, drag time, length, and coverage.

Through geometric transformation, it modifies the input pattern's positional aspect., and patterns are created by making small changes to size, shape, or location.

Using an XML file that includes details about the raster pattern pixel, relative pixel positions, and intensity is the third step in the process. To develop random bit sequences and pixel patterns, the input image is available on the server as an XML file with an N-pixel pattern, applying a random qualifier to this structured file is the final and fourth step. By hiding a random bit sequence inside a randomly selected pattern, three-bit data concealing creates a stego image that simulates the password pattern. For each user logout, the system creates a new password image on the server side and updates the client side.

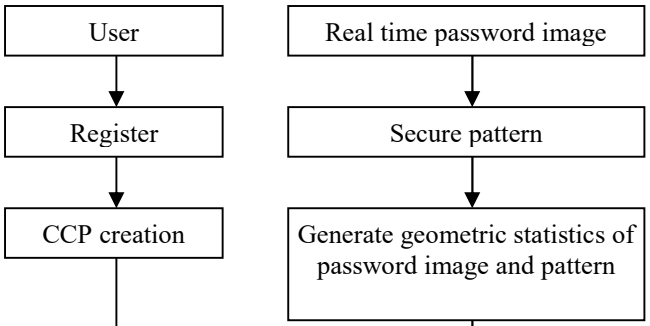

Figure 1: Block diagram of Password Authentication System Using Graphical Images

The server maps and authenticates passwords using the mapping technique, and the password image serves as the actual input into the system. In order to carry out the mapping procedure for recognizing the XML file and password image, the server uses the user's identification to find the matching password file and XML pattern. The position and intensity of each pattern are taken out of the XML file one at a time, and they are then transformed into a graphic pattern. The

user's identity is confirmed by mapping the password, this is a three-bit LSB (least significant bit) and is connected to the corresponding XML DB password via a graphical pattern. If the pattern cannot validate the password, it will extract the next pattern sequence in the XML file. If the pattern is mapped from the received, For every pattern sequence in an XML file, the process is repeated several times to confirm the system's authentication.

The updated password image is entered the next time to log in to the system or mobile. The pattern pixels are generated by mapping the user ID in an XML database, then sequentially overlaying each pattern over the password image. This covered password matches the corresponding XML DB pattern.

IV. Result Analysis

This section evaluates the performance of An XML-transformed technique for Improving the effectiveness of a Password Authentication system based on graphical images. High-resolution images are used to implement graphical pattern passwords in real-time. The framework is used by environment-based mobile and desktop applications. the proposed approach used the input image to generate a random graphical stroke pattern and store the stroke pixels in an XML file. Upon passing the password image, in the XML file, consumers will only see the extracted graphical pattern pixels not the entire image and performance analysis is predicated on authenticity, security, and accuracy.

Accuracy: It is a measure of the accuracy of the password authentication system.

Security: The purpose of a password security definition is to verify and authenticate a user's identity in order to limit access to accounts, devices, and data. To prevent identity theft and protect data, strong passwords are crucial.

Authentication: Verifying a user or device is the process of authenticating before granting access to a system or resources. When authentication is done through a graphical password system, shoulder surfing attacks are less likely to happen.

To improve the performance of password authentication systems that use graphical pictures (XML transformed-PASGA), biometric/token-based password authentication systems (biometric/token-based PAS), and pixel-based image mapping password authentication systems (pixel-based image mapping PAS), The provided XML transformed method's accuracy, security, and authentication settings are compared in Table 1.

Table 1: Comparative performance analysis

Parameters	XML transformed-	Biometric/Tok	Pixel based Image

	PASGA	en based PAS	Mapping PAS
Accuracy	98	87	84
Security	98	88	81
Authentication	99	87	82

A comparison of figure 2 displays the Accuracy parameter for the designated XML transformed-PASGA, Biometric/Token based PAS, and Pixel based Image Mapping PAS. Figure demonstrates the high accuracy of the described XML transformed-PASGA model in comparison to the other two models.

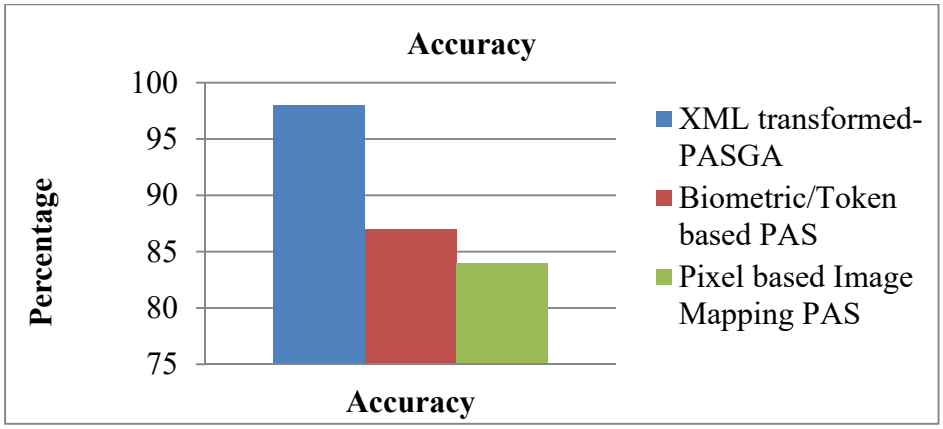

Figure 2: Comparative accuracy parameter analysis

A graphical comparison of security characteristics for pixel-based image mapping PAS, biometric/token-based PAS, and XML translated PASGA is shown in Figure 3, which emphasizes that the XML transformed-PASGA model delivers good security.

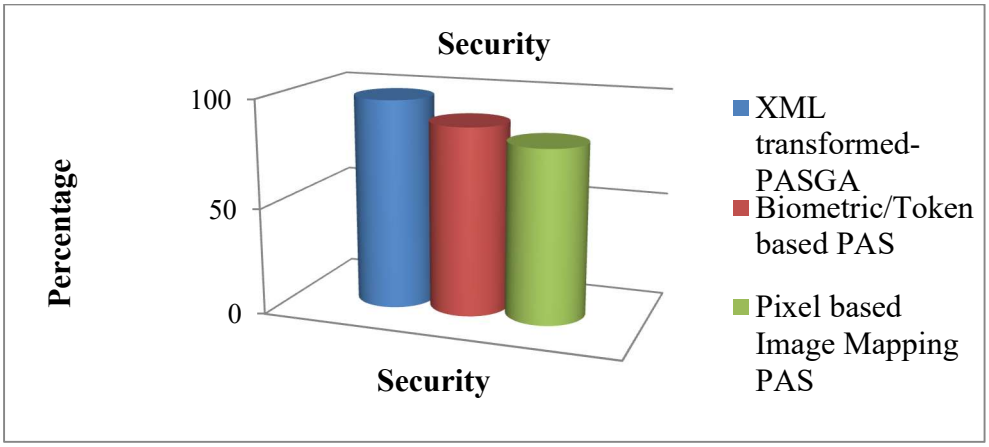

Figure 3: Comparative security parameter analysis

In Figure 4 below, the XML-transformed PASGA, the Biometric/Token-based PAS, and the Pixel-based Image Mapping PAS are the three models whose authentication analysis is shown

graphically. The results show that the described model's authentication is significantly higher than that of the other models.

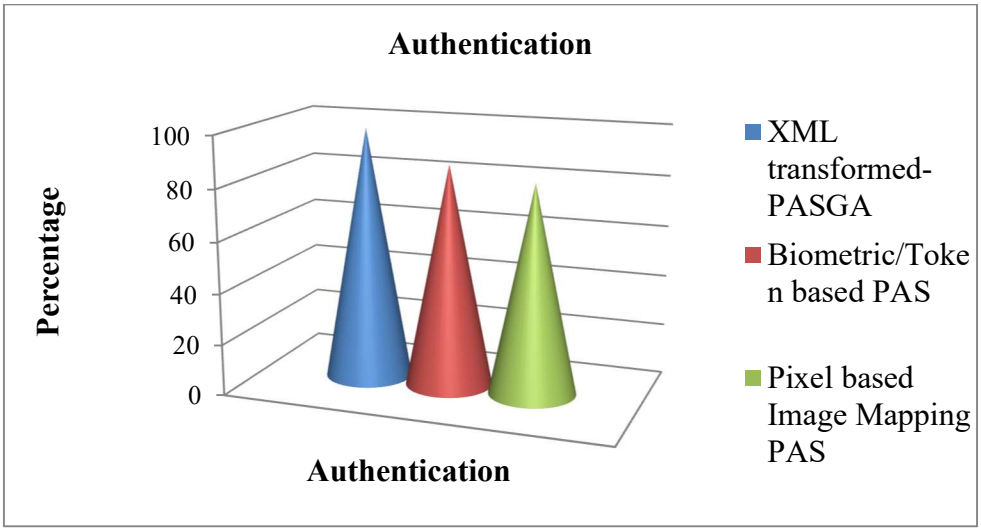

Figure 4: Comparative Authentication analysis

The overall results indicate that the XML-transformed method is more effective at enhancing the password authentication system's use of images. The stated model's achieved parameter values are 99% for authentication, 98% for security, and 98% for accuracy.

V. Conclusion

This study presents An XML (eXtensible Markup Language)-transformed Method for Improving the effectiveness of a password authentication system that uses graphics. This work presents a more efficient graphical image pattern password mapping approach that improves efficiency and incorporates security features. Following the server's verification and transformation process of the user-input patterns, which resulted in several changed patterns, this database was produced. The XML DB form is used to insert the extracted pattern using the LSB (Least Significant Bit) approach into the input image. After the password is verified, a image is produced, and the pattern values are saved for later retrieval in an XML pattern database. The following criteria are used in performance analysis: authentication, security, and accuracy. When using graphic images, the XML converted technique greatly improves the password authentication system's efficiency according to a number of performance criteria. The stated model's achieved parameter values are 99% for authentication, 98% for security, and 98% for accuracy.

VI. References

[1] J. Shen, A. Wang, C. Wang, J. Li and Y. Zhang, "Content-Centric Group User Authentication for Secure Social Networks," in IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 3, pp. 833-844, 1 July-Sept. 2020, doi: 10.1109/TETC.2017.2779163.

[2] S. Vhaduri and C. Poellabauer, "Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3116-3125, Dec. 2019, doi: 10.1109/TIFS.2019.2911170.

[3] KC Chaganti , SR Inta , SL Bandla , R Chilukuri , P Paidy , S Muthuveeran , N Dulam, "Cyber Threats in the Pharmaceutical Industry: A Deep Dive into Recent Attacks and Future Implications", IEEE Access. 2025 Jun 27.

[4] MA Hussain, VB Meruga, AK Rajamandrapu, SR Varanasi, SS Valiveti, AG Mohapatra, "Generative AI Sensor Fusion for Secure Digital Twin Ecosystems: A Standardization-Aligned Framework for Cyber-Physical Systems", IEEE Communications Standards Magazine. 2026 Feb 13.

[5] B. Yao, Y. MU, H. Sun, X. Zhang, H. Wang and J. Su, "Connection Between Text-based Passwords and Topological Graphic Passwords," 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 2018, pp. 1090-1096, doi: 10.1109/ITOEC.2018.8740702.

[6] H. Shin, D. Kim and J. Hur, "Secure pattern-based authentication against shoulder surfing attack in smart devices," 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo, Japan, 2015, pp. 13-18, doi: 10.1109/ICUFN.2015.7182486.

[7] N. Wakabayashi, M. Kuriyama and A. Kanai, "Personal authentication method against shoulder-surfing attacks for smartphone," 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2017, pp. 153-155, doi: 10.1109/ICCE.2017.7889266.

[8] Tripathi, Bhaskar, et al. "Deep learning-based facial recognition system with privacy-preserving features." U.S. Patent Application No. 19/214,023.

[9] M. Martinez-Diaz, J. Fierrez and J. Galbally, "Graphical Password-Based User Authentication With Free-Form Doodles," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 4, pp. 607-614, Aug. 2016, doi: 10.1109/THMS.2015.2504101.

[10] N. Lopez, M. Rodriguez, C. Fellegi, D. Long and T. Schwarz, "Even or Odd: A Simple Graphical Authentication System," in IEEE Latin America Transactions, vol. 13, no. 3, pp. 804-809, March 2015, doi: 10.1109/TLA.2015.7069108.

[11] H. Adamu, A. D. Mohammed, S. A. Adepoju and A. O. Aderiike, "A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication," 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, 2022, pp. 1-5, doi: 10.1109/NIGERCON54645.2022.9803122.

[12] A. B. Yazid, M. M. Boukar and S. I. Yusuf, "PandaLock: Variable-Pointer Rotary-Password Authentication Technique," 2018 14th International Conference on Electronics Computer and Computation (ICECCO), Kaskelen, Kazakhstan, 2018, pp. 1-6, doi: 10.1109/ICECCO.2018.8634700.

[13] M.K. Gaddam, "Edge-to-Cloud Security Fabric for AI Workflows in Regulated Industries." In *2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, pp. 549-555. IEEE, 2025.

[14] B. MacRae, A. Salehi-Abari and J. Thorpe, "An Exploration of Geographic Authentication Schemes," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1997-2012, Sept. 2016, doi: 10.1109/TIFS.2016.2570681.

[15] J. Song, D. Wang, Z. Yun and X. Han, "Alphapwd: A Password Generation Strategy Based on Mnemonic Shape," in IEEE Access, vol. 7, pp. 119052-119059, 2019, doi: 10.1109/ACCESS.2019.2937030

[16] F. A. Alsulaiman and A. El Saddik, "Three-Dimensional Password for More Secure Authentication," in IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 9, pp. 1929-1938, Sept. 2008, doi: 10.1109/TIM.2008.919905

[17] W. Luo, Y. Hu, H. Jiang and J. Wang, "Authentication by Encrypted Negative Password," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 114-128, Jan. 2019, doi: 10.1109/TIFS.2018.2844854.

[18] [18] S. Z. Nizamani, S. R. Hassan, R. A. Shaikh, E. A. Abozinadah and R. Mehmood, "A Novel Hybrid Textual-Graphical Authentication Scheme With Better Security, Memorability, and Usability," in IEEE Access, vol. 9, pp. 51294-51312, 2021, doi: 10.1109/ACCESS.2021.3069164.

[19] M. Shirvanian, N. Saxena, S. Jarecki and H. Krawczyk, "Building and Studying a Password Store that Perfectly Hides Passwords from Itself," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 5, pp. 770-782, 1 Sept.-Oct. 2019, doi: 10.1109/TDSC.2019.2902551

[20] S. Raponi and R. D. Pietro, "A Longitudinal Study on Web-Sites Password Management (in)Security: Evidence and Remedies," in IEEE Access, vol. 8, pp. 52075-52090, 2020, doi: 10.1109/ACCESS.2020.2981207.

[21] M. Alajmi, I. Elashry, H. S. El-Sayed and O. S. Faragallah, "A Password-Based Authentication System Based on the CAPTCHA AI Problem," in IEEE Access, vol. 8, pp. 153914-153928, 2020, doi: 10.1109/ACCESS.2020. 3018659.

[22] K. M. Renuka, S. Kumari, D. Zhao and L. Li, "Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems," in IEEE Access, vol. 7, pp. 51014-51027, 2019, doi: 10.1109/ACCESS.2019.2908499.

[23] M. A. Azad, S. Bag, C. Perera, M. Barhamgi and F. Hao, "Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network," in IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3606-3615, May 2020, doi: 10.1109/TII.2019.2941724.

[24] Z. Li, D. Wang and E. Morais, "Quantum-Safe Round-Optimal Password Authentication for Mobile Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1885-1899, 1 May-June 2022, doi: 10.1109/TDSC.2020.3040776.

[25] S. Vhaduri, S. V. Dibbo and W. Cheung, "HIAuth: A Hierarchical Implicit Authentication System for IoT Wearables Using Multiple Biometrics," in IEEE Access, vol. 9, pp. 116395-116406, 2021, doi: 10.1109/ACCESS.2021.3105481.