RES MILITARIS Social Science Journal

Improving Security through Image based Three Level Authentication Using SHA256 and Huffman Coding Algorithm for Web Based Applications

Dr. G. Murali [1], Dr. Saidaiah Bandi[2]

(1) Assistant Professor and Head of the Department, Department of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula

(2) Professor, Department of Electronics and Communication Engineering, NRI Institute of Technology (KP), Visadala (P), Guntur, A.P.,

Abstract:

This article discusses a cutting-edge three-level authentication system designed to elevate the security paradigm for user access controls. The initial level employs conventional passwords, establishing a foundational layer for user authentication. Building upon this, the second level introduces an additional safeguard through one- time passwords (OTPs) sent to users registered email addresses. Following the successful completion of the first two levels, users progress to the third tier, where they engage in a unique authentication process. In this final stage, users select two personalized images in a specific sequence, contributing to a robust defence mechanism against unauthorized access. By amalgamating the strengths of traditional passwords, email-based OTPs, and personalized image sequencing, this approach aims to significantly fortify security measures, providing a resilient defence against potential threats in the digital landscape.

Keywords:

Huffman coding technique, SHA-256, Image Based Authentication, OTP, Authentication, Security.

I. INTRODUCTION

The transition from offline to online society has necessitated the development of online user authentication technology [1]. In offline society, the identity of the user is verified face to face only on the basis of the user's personal documents (e.g. Social Security Number, Driver's License, or Passport). In online society, the requirement for user authentication is replaced by a technique that does not require the user to be identified face to face. As a result of these demands, a variety of user authentication techniques have emerged in the history of online use, and a representative type of user authentication technique is a password-based authentication technique. As technology progresses, so do the ways in which malicious actors attempt to access personal and confidential data [2]. Consequently, the demand for innovative and multi-layered authentication systems has become paramount. This research addresses this critical need by introducing a comprehensive three-level authentication system designed to enhance the security landscape of user access controls. However, the issue with password authentication is that it neutralizes keyboard data protection [4]. The increasing frequency and complexity of cyber-attacks highlights the need to go beyond traditional password authentication techniques. Traditional passwords, often susceptible to breaches through various means such as phishing attacks or brute-force attempts, present a vulnerability that needs to be addressed. Recognizing this challenge, our proposed system initiates the authentication process with conventional passwords as the first level of defence. This element serves as a foundational layer within the overall security architecture, providing both familiarity and essentiality. Image-based authentication is an authentication technique that shows a particular image on the screen (e.g. a keypad) and uses the click data on the image as the password [6]. The information that needs to be protected in image-based authentication is the image information that is shown to the output device as well as the mouse data information that is inputted by a mouse. Despite the limitations of passwords, several studies have demonstrated that many Database Service providers (DBs) store passwords in plaintext format [23], the second level of our authentication system incorporates a dynamic and

time-sensitive layer by introducing one-time passwords (OTPs). To provide an additional layer of verification that improves security and is flexible enough to respond to the ever-changing threat landscape, One-Time Passwords (OTPs) are emailed to the user's registered email address. Email-based OTPs serve as an additional layer of security, requiring users to verify their identity in real-time before proceeding to the next authentication level. This procedure lessens the possibility of unwanted access to sensitive data and helps to ensure a greater level of security.

Beyond conventional password and OTP mechanisms, the third level introduces a novel approach to user authentication. In this phase, users are prompted to choose and sequence two personalized images from a predefined set. This personalized image sequencing not only adds a layer of complexity for potential attackers but also aligns with the user's unique preferences, enhancing the overall user experience.

The amalgamation of these three authentication levels forms a cohesive and resilient defence against unauthorized access [7]. By blending the familiarity of passwords, the dynamic nature of OTPs, and the personalization of image sequencing, our proposed system aims to mitigate the vulnerabilities associated with singular authentication methods. This research sets out to contribute to the ongoing efforts in fortifying digital security, ensuring that users can confidently engage in online activities with a heightened level of protection against evolving cyber threats.

II. LITERATURE REVIEW

Several studies have explored the implementation of three-level authentication systems, incorporating factors such as knowledge-based, possession-based, and biometric authentication. In order to overcome flaws in conventional two-factor authentication techniques, researchers have concentrated on improving security through the integration of several layers of verification. Information can be protected and made chaotic by using encryption [21]. The literature highlights advancements in biometric technologies and cryptographic techniques to achieve robust and reliable three-level authentication systems.

While text-based or alphanumeric passwords stood out as prominent authentication methods, they were not without their drawbacks. Managing multiple text passwords for various accounts posed a significant challenge. As a result, other techniques like biometric data credentials [4] even token-based passwords have attracted attention as alternatives to traditional text-based passwords [3].

It's a well-known fact that achieving security and memorability simultaneously is impossible to do [22]. The limitations of text-based and token-based passwords are recognized in the study published by Shiv Narain Gupta et al. (2023), which led to the creation of pictorial passwords such as Pass Point, Cued Click Point (CCP), and Persuasive Cued Click Points (PCCP). Pass Point relies on selecting five dots on an image, facing security issues due to a common "hot spot." CCP improves on this by distributing points across different images, and PCCP enhances security further with additional tasks. Despite PCCP's innovation, there are still some security concerns, though considered less severe than other methods [1].

The security system consists of three levels: the first involves a text-based password with special characters for client-side entry. Successful completion of the initial stages leads to a unique numeric password sent to the registered email for the current session. The third level's one-time automatic password is unbreakable, even if a hacker manages to obtain the user's email address. After passing all three levels, the user gains access to stored data, enhancing overall system protection. Sharing passwords is prohibited, and after three unsuccessful attempts, the account locks, requiring administrator intervention, effectively thwarting automated attacks and physical force assaults [2].

Cued click points were developed in an effort to overcome the drawbacks of the pass-point authentication mechanism. The essential difference between cued click points and pass points is that the former require choosing five points from five separate frames [1][5].

The pass-point mechanism, conceptualized by its creator, involved a simple process: selecting five dots on an image, connecting them to form a pattern, and establishing a password. Users were required to choose five specific points from a given image, and during password creation and login, they had to replicate the selection process, ensuring consistency in the pattern across all chosen images [1][4].

Persuasive-Cued Click Points is a system that improves upon prompt tap points by allowing users to select more specific keywords. It includes tasks like repositioning and viewing, presenting a small

black-and-white image when a particular word is uttered. Programmers can utilize PCCP's intricate structure, which confines users within the viewport's bounds unless they choose to freely rearrange things by clicking the reorder button. Similar to the keyword period, users can generate passwords with an infinite number of rearrangements by using a viewport and reposition button. In the Post Emit-Word era, users can easily engage with graphical images, selecting the correct clickable area. While PCCP is a notable daily innovation, it does raise some security concerns, although they are less severe than those of alternative systems [1][6].

Three authentication approaches include biometric, token-based, and knowledge-based methods. Biometric utilizes face recognition, fingerprints, voice recording, and retina scanning. Token-based employs passports, badges, or smart cards but is susceptible to fraud. Knowledge-based relies on conventional passwords, pins, or images and is applicable both locally and remotely, demonstrating excellent performance [8][9].

In order to provide SMS OTP and two-factor authentication for e-transactions, this article uses SET. It generates time-limited OTPs that are issued by SMS to facilitate secure transactions in online banking, e-commerce, and ATMs. The Secured Cryptographic Algorithm validates OTPs. Successfully tested, it enhances electronic transaction security [10][11][13].

Graphical passcodes are proposed to overcome memory limitations of alphanumeric codes [15][16][18][20]. These strategies take advantage of the visual superiority effect, which states that people remember images better than words. Image data conveys more information than textual data [14]. Graphical information is an effective way to counter brute force attacks and provides a user-friendly authentication system.

After evaluating diverse authentication models proposed by researchers, we have formulated a streamlined three-level authentication system. This novel model excels in efficiency and security, empowering users to navigate a seamless authentication process. Leveraging a combination of traditional email-password validation, one-time password (OTP) verification, and image-based authentication, our system ensures a robust defence against unauthorized access.

In this advanced authentication model, user credentials are securely verified in the first level, followed by OTP validation for an added layer of security. The incorporation of image-based authentication adds a unique dimension, enhancing the overall reliability of user access. This three-tiered approach not only fortifies the authentication process but also aligns with contemporary security standards, establishing a trustworthy framework for user interactions within digital platforms.

III. METHODOLOGY

The Methodology consists of 2 parts namely Registration Phase and Login Phase.

A. Workflow :

The implementation of a three-level authentication system involved following a specific workflow, as outlined below in Fig1:

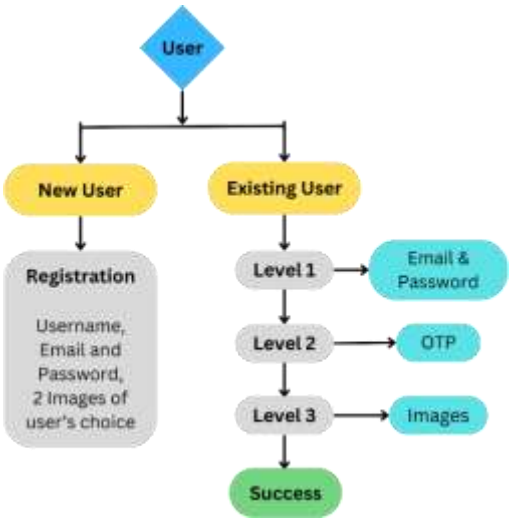


Figure 1. Workflow

Level 1: Email and Password

At the first level of authentication, users need to provide their registered email address and a secure password. This initial credential check ensures that only authorized individuals gain access to their accounts. The password should adhere to strong security standards, promoting a secure foundation for the subsequent authentication steps.

Level 2: OTP Verification

Following successful email and password entry, users proceed to the second level of authentication, which involves a one-time password (OTP) verification. The registered email address linked to the user's account receives an OTP. Users must input

the received OTP to confirm their identity. This adds an extra layer of security by requiring possession of a secondary device or access to a separate communication channel.

Level 3: Image-Based Authentication

The third and final level of authentication introduces image-based verification. After completing the email password and OTP steps, users are prompted to select two images associated with their account. This personalized image-based authentication enhances security by incorporating a visual element, making it more challenging for unauthorized entities to gain access. Users must correctly identify and match the selected images, providing an additional barrier against potential threats.

The combination of these three authentication levels – email-password, OTP verification, and image-based authentication – creates a robust and multifaceted security system. This approach aims to prevent unauthorized access, protect user accounts from various cyber threats, and ensure a high level of security for the users interacting with the platform.

B. Technology Stack :

The MERN stack, which consists of Express for server-side development, React for the user interface, MongoDB for database administration, and Node.js for server-side runtime, is used to construct the three-level authentication system. Additionally, Multer is employed to facilitate the seamless transfer of images from the client to the server end. This integration of technologies ensures a robust and efficient authentication process, combining the strengths of the MERN stack for web development with Multer for effective image handling, thereby enhancing the overall security and user experience of the authentication system.

IV. IMPLEMENTATION

The implementation of the three-level authentication system involves two stages: Registration and Login.

A. Registration:

To register in the application, new users must provide their username, email, and password. Additionally, they need to choose and upload two images of their choice, one at a time. The entered username, email, and password are stored in the MongoDB database. Utilizing FormData in React and Multer in Node.js, the images are transferred to the server side. Using the SHA-256 Cryptographic Hash Algorithm, a unique 64-byte string is generated for each image. The final hash string is created by concatenating both hashes obtained from the images. Once the final hash string is obtained, the images are deleted from the Multer storage. The non-human-readable final passcode for the images is generated using the Huffman coding technique, which employs standard ASCII values (0-256) for encoding. This generated passcode is stored in the MongoDB database along with user's email. Figure 2 will give you an overview.

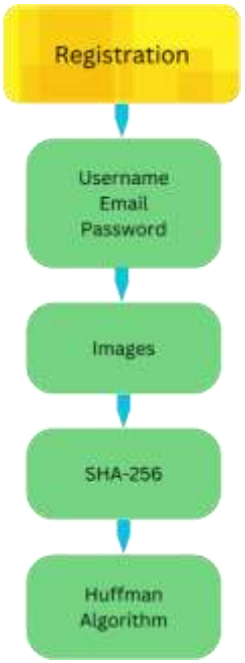


Figure 2. Registration

Algorithm:

1. Username, Email and Password are taken.
2. Images are taken from User.
3. Images are Converted into hashed strings using SHA-256.
4. Further Huffman algorithm is used to again encode the sting and also decreases the length of the hashed string.

SHA-256 Algorithm:

SHA-256, also known as Secure Hash Algorithm 256, is a cryptographic hash function that belongs to

the SHA-2 family. It produces a hash value that is 256 bits (32 bytes), which is commonly represented as a 64-character hexadecimal integer. The mathematical formula for SHA-256 involves several steps, including message padding, parsing the message into blocks, and applying a series of bitwise and arithmetic operations within a compression function. Below is a simplified overview of the SHA-256 algorithm:

1. Message Padding: The length of the input message is padded to make sure it is a multiple of 512 bits, allowing space for the appended length of the original message.

2. Parsing into Blocks: There are 512-bit chunks within the padded message. starting values for hashing Eight initial hash values, designated as H0 through H7, which are typically written as 32-bit words in SHA-256 are obtained from the first 32 bits of the fractional parts of the square roots of the first eight prime numbers.

3. Compression Function (SHA-256 Rounds): Each block goes through a series of 64 rounds of processing. In each round, the input block undergoes a series of bitwise and arithmetic operations, including bitwise logical functions (AND, OR, XOR), addition modulo 2^32, and circular shifts.

4. Final Hash Value: The final hash value is determined by concatenating the eight 32-bit words that are produced by the compression algorithm after all blocks have been processed.

$$W_i = \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16}$$

Huffman Coding Technique Algorithm:

1. Determine how often each character appears throughout the input string.

2. Using the character frequencies as a guide, construct the Huffman tree (Min Heap).

3. Use the tree to create Huffman codes for every character.

4. Enter the corresponding Huffman codes for the characters that were originally in the input string.

5. Add padding bits (at the end) to ensure the encoded string is divisible by 8.

6. Append the count of padding bits to the original encoded string (Just in case, want to decode)

Final Password Generation:

1. Read the Huffman-encoded string from left to right, treating each byte (8 bits) as a unit.

2. Convert each byte to its equivalent decimal integer.

3. Replace each decimal integer with its corresponding ASCII character

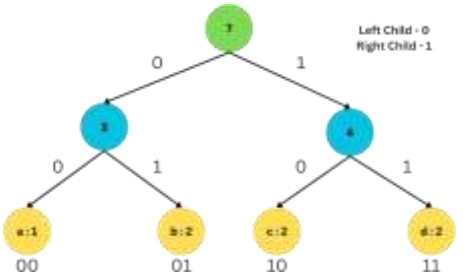
Time Complexity: O(nlogn) is the time complexity, where n stands for the number of distinct characters.

Example: Let's consider the string str = "abcdbcd" as the final concatenated hash generated by SHA-256 for images, and using Huffman encoding on this string will be as follows:

1. Character a b c d

Frequency 1 2 2 2

2.



3. Character Huffman code

a 00

b 01

c 10

d 11

4. Huffman encoded string = "00011011011011"

5. Padded Huffman encoded string = "0001101101101100"

6. Final Padded Huffman encoded string = "000000100001101101101100"

Final Password Generation:

1. 00000010 00011011 01101100

1. 2 27 108

2. SOH ESC l (ASCII)

B. Login:

During the login process, users must first complete the initial authentication level by providing the correct credentials, including the email and password assigned during registration. Upon successful verification at this level, users proceed to the second authentication level, which incorporates a one-time password (OTP) verification. In this step, users need to enter the OTP correctly, which is sent to their registered email address. Upon successful completion of the second authentication level, users are allowed to choose two images in the same sequence as during registration. Figure 3 will give you an overview.

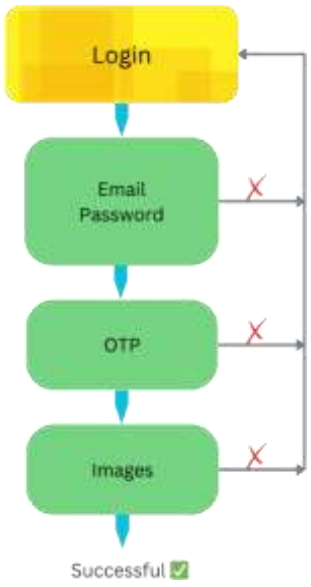


Figure 3. Login

Algorithm:

1. Email and Password should be provided.
2. OTP sent to email should be provided.
3. Same Images in the exact order should be provided.
4. Failure at any one of these levels will result in unsuccessful login.

Subsequently, these two selected images are transmitted to the server side using Multer. Employing the SHA-256 Cryptographic Hash Algorithm, the hashes for both images are generated and then concatenated. This final concatenated hash string undergoes encoding using Huffman encryption. Next, the compressed Huffman string and the one kept in the database linked to the enrolled email address are compared. The user is given permission to their account provided that there is a match; if not, access is refused.

IV. RESULT AND ANALYSIS

The proposed system employs a three-level authentication process for user registration and login. During registration, users provide basic details and upload two images. The system hashes and encodes the images, storing the resulting passcode alongside the user's email. For login, users enter their email and password, undergo OTP verification, and select the same two images. The system hashes and encodes these images, comparing the result with the stored passcode for access approval. This approach ensures robust security, utilizing encryption, hashing, and image-based authentication to safeguard user data.

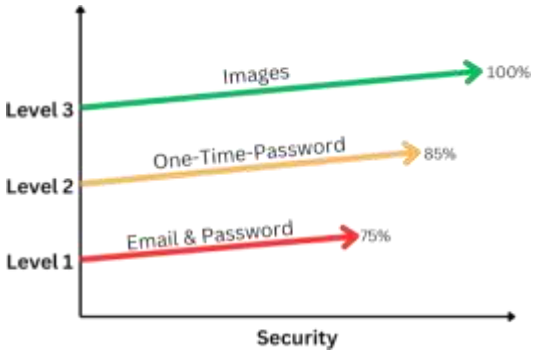


Fig. 4. Analysis

Sample Test Case:

Images:

Fig. 5. Image1

Fig. 6. Image2

SHA256 Output:

8d583606754b32de2c63b48e4d8917c2f5654f265f7
c678e3b5cfa2abc1c58f45d0b6ccb39fbdc279309af1
5939940622e8b4072e6e2ab2ef23654866237cc00

Huffman Output:

{ï"Z☻UÉÆ·ö(þÒw¤µæõ<¿9Ý³Q
9ýÙkX∟QlUôí[UòZr♣{↨áj7û‼þm;@

2 level Authentication vs 3 level Authentication:

Parameters	2 Level	3 Level
Time Complexity	Moderate	High
Security	Moderate	High
User Experience	Easy to Use	Not very Easy to Use
Risk Mitigation	Moderate Risk	No Risk

Time Complexity to Crack: The 3-level authentication is likely to have a higher time complexity due to the additional image upload and comparison step.

Security: The 3-level authentication is more complex and involves an additional factor, potentially making it more secure.

User Experience: The 2-level authentication is likely more user-friendly and easier to implement. The 3-level authentication may lead to user frustration due to the additional steps and potential issues with image uploads.

Risk Mitigation: Both methods provide additional layers of security, but the 3-level authentication has the potential to mitigate different types of risks, especially related to image-based verification.

The third level involves the application of the Huffman coding technique and the subsequent generation of the final password for images.

Limitation: Images should be carried along with user.

V. CONCLUSION

This paper discusses the creation of a sophisticated three-level authentication system, leveraging the MERN stack and Multer for secure user registration and login. The registration process involves hashing and encoding user-selected images, enhancing security by employing SHA-256 and Huffman encryption techniques. The login procedure incorporates multi-factor authentication, combining email-password validation, OTP verification, and image-based authentication. This comprehensive approach ensures a resilient defence against unauthorized access, emphasizing the importance of user data protection in today's digital landscape.

In conclusion, the proposed system not only provides a user-friendly interface but also prioritizes the paramount aspects of security and transparency. By integrating industry-standard encryption methods and innovative image-based authentication, the platform aims to set a new standard for safeguarding user accounts. The adoption of the MERN stack and Multer technology further enhances the system's scalability and efficiency, promising a robust solution for secure and seamless user interactions within the digital realm.

REFERENCES

[1] Karan Pandey,Amitesh Singh, Abhishek Kaushik, Ashutosh Anand and Shiv Narain Gupta, "Enhancement of Password Authentication System Using Vector (Graphical) Images", 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) | 979-8-3503-2230-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/AISC56616.2023.10085057.

[2] Ajmeera Kiran, Ben Sujitha B, Suragouni Nikitha, and Thakur Harshvardhan Singh, "Implementation of 3-Level Security System UsingImage Grid Based Authentication System", 2023 International Conference on Computer Communication and Informatics (ICCCI) | 979-8-3503-4821-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCI56745.2023.10128606.

[3] Vashek Mathyas, Zdenek Riha, "Security of biometric authentication system," International Journal of Computer Information System and Industrial Management Application, 2011.

[4] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, 2007.

[5] Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, Kalyani Pendke, "Cued Click Point techniques for graphicalpassword authentication," International Journal Of Computer Science And Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 166-172.

[6] Iranna A. M., PankajaPatil, “Graphical password authentication using peruasive cued click point,” International Journal Advanced Research in Electrical Instrumentation Engineering, July 2013.

[7] P. R. DaveleShrikala M. Deshmukh, Anil B. Pawar, “Persuasive Cued Click Points with click draw based graphical password scheme”, International Journal of Soft Computing and Engineering (IJSCE), May 2013.

[8] Chinnasamy P., Deepalakshmi P. (2018) Improved Key Generation Scheme of RSA (IKGSR) Algorithm Based on Offline Storageor Cloud. In: Rajsingh E., Veerasamy J., Alavi A., Peter J.(eds) Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing, vol 645. Springer, Singapore. https://doi.org/10.1007/978-981-10-7200-0_31.

[9] G. Vasanthi, P. Chinnasamy, N. Kanagavalli and M. Ramalingam, "Secure Data Storage Using Erasure-Coding In Cloud Environment," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402639.

[10] Chinnasamy, P., Deepalakshmi, P. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. J Ambient Intell Human Comput 13, 1001–1019 (2022). https://doi.org/10.1007/s12652-021-02942-2.

[11] Chinnasamy P., Praveena V. (2021) Secure and Efficient Data Sharing Scheme in Cloud for Protecting Data in Smart Cities. In: Al-Turjman F., Gowthaman N. (eds) Advanced Controllers for Smart Cities. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-48539-9_4.

[12] J. Nicholson, L. Coventry, and P. Briggs, ‘‘Faces and pictures: Understanding age differences in two types of graphical authentications,’’ Int. J. Hum.- Comput. Stud., vol. 71, no. 10, pp. 966–995, 2013.

[13] E. Stobert and R. Biddle, ‘‘Memory retrieval and graphical passwords,’’ inProc. 9th Symp. Usable Privacy Secur. (SOUPS), 2013, pp. 1–14..

[14] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, ‘‘Towards usable solutions to graphical password hotspot problem,’’ in Proc. 33rd A.

[15] D. Davis, F. Monrose, and M. K. Reiter, ‘‘On user choice in graphical password schemes,’’ in Proc. 13th Conf. USENIX Secur. Symp., vol. 13,2004, p. 11.

[16] T. Takada and M. Yoshida, Pict-Place Authentication: Recognition-Based Graphical Password Using Image Layout for Better Balance of Security and Operation Tim.

[17] W. A. J. van Eekelen, J. van den Elst, and V.-J. Khan, ‘‘Picassopass: A password scheme using a dynamically layered combination of graphical elements,’’ in Proc. CHI Exte.

[18] R. Biddle, S. Chiasson, and P. C. Van Oorschot, ‘‘Graphical passwords: Learning from the first twelve years,’’ ACM Comput. Surv., vol. 44, no. 4, pp. 1–41, Aug. 2012.

[19] J. Thorpe, M. Al-Badawi, B. MacRae, and A. Salehi-Abari, ‘‘The presentation effect on graphical passwords,’’ in Proc. SIGCHI Conf. Hum. Factors Comput. Syst., Apr. 2014, pp. 2947–2950.

[20] X. Suo, Y. Zhu, and G. S. Owen, ‘‘Graphical passwords: A survey,’’ in Proc. 21st Annu. Comput. Secur. Appl. Conf. (ACSAC), 2005, p. 10.

[21] G. J. Simmons, "Symmetric and asymmetric encryption", *ACM Comput. Surv.*, vol. 11, no. 4, pp. 305-330, Dec. 1979.

[22] C. Herley and P. C. van Oorschot, "A research agenda acknowledging the persistence of passwords", IEEE Security Privacy, vol. 10, pp. 28-36, Jan. 2012.

[23] M. Mohammadinodoushan, "Implementation of password manager with sram-based physical unclonable function", arXiv:2006.02562, 2020.