International Journal of Development Mathematics Vol 1 Issue 3, Page No. 186 - 195

INTERNATIONAL JOURNAL OF DEVELOPMENT MATHEMATICS
ISSN: 3026-8656 (Print) | 3026-8699 (Online)
journal homepage: https://ijdm.org.ng/index.php/Journals

Enhancing Data Warehouse Security: An Encrypted Cued-Click-Points Authentication Approach

Yakubu H. Zali[a,b*], Gregory M. Wajiga[a], Faru A. Abdullahi[b], Yusuf M. Malgwi[a], Adamu L. Mohammed[c]
[a]*Department of Computer Science, Modibbo Adama University, Yola, Adamawa State*
[b]*Department of Computer Science, Federal Polytechnic Kaura Namoda, Zamfara State*
[c]*Command Science Secondary School (Girls) Miringa, Biu, Borno State*

ARTICLE INFO

Article history:
Received 17 May, 2024
Received in revised form 05 August, 2024
Accepted 29 August, 2024

Keywords:
Data warehouse, Password, Security, Vulnerability.

MSC 2020 Subject classification:
94A60, 68P25, 68P20, 68P15
94A62, 68M25

ABSTRACT

This research study focuses on developing an Encrypted Cued-Click-Points (ECCP) Authentication Scheme for a Hybrid Data Warehouse. The primary aim is to enhance encryption techniques used in the authentication process through a cued-recall-based technique. The study implements cued-click-points as a secure method of user authentication using Python programming language and tests the new authentication scheme for effectiveness. Additionally, it provides a user-friendly interface for accessing data securely using Tkinter (GUI Designer). The Unified Software Development Process (USDP) is employed as the software development approach. The ECCP scheme leverages specific cued-recall techniques where users select click-points on an image as their password. These points are encrypted and stored securely. To authenticate, users must correctly click on their chosen points in the correct sequence. This method capitalizes on the human brain's superior ability to recognize and remember images over text, enhancing both usability and security. Security aspects of the ECCP includes encryption of the click points, Dynamic image Management and Graphical Password Complexity. The study concluded that ECCP offers a usable and secure graphical user authentication scheme that is simple to create, learn, and use. The implemented system employs possible click points on a given image, and though increasing these can enhance security, the focus remains on maintaining usability. Usability studies performed on ECCP indicate favorable results for both usability and security. Thus, the study strongly recommends that data warehouses adopt the ECCP graphical password scheme to further strengthen their security. By improving the usability without compromising security, ECCP stands out as a robust and user-friendly authentication method suitable for hybrid data warehouse environments.

1. Introduction

Text passwords and other traditional security measures have been the mainstay of current data warehouse content security techniques. Due to the growing computational capability of information systems, security requirements, especially for the selection of secure text passwords, have changed throughout time. Because database administrators are either unaware of these changes or are overburdened by the magnitude of the adjustments necessary to remedy them, these vulnerabilities are typically invisible to them. As a result, research on usable authentication schemes have picked up steam, with the goal of developing the best authentication techniques and precautions. The most widely used form of user authentication in information systems is text passwords, yet these have security and usability issues. Advancements like passphrases (Sannihith, 2023) and mnemonic passwords (Kiesel *et al.*, 2017) have not been as successful because of their predictability issues and lack of adequate research on security. Although biometric authentication solutions have also been suggested (Sarkar & Singh, 2020). Note that there are some usability problems and privacy concerns with these issues. We suggested to develop an information systems authentication system that uses click-points on a series of pre-displayed graphics. Because it is impractical to expect users to precisely target a single pixel, click points that are presented utilizing the region surrounding an original click-point are considered as

* Corresponding author. Tel.: +2347035581155
E-mail address: zali2kida@gmail.com (Yakubu H. Z.)
https://doi.org/10.62054/ijdm/0103.14

correct. The click-point coordinates on each image are recorded in a database and encrypted before being saved for later use and comparison. For the click points while forwarding and even within the database, the application will offer encryption capabilities. As a result, the system offers a strong security framework that can significantly increase security regarding access to a data warehouse and lessen the susceptibility of the stored warehouse contents.

An integrated repository made up of both operating and historic databases is called a data warehouse. Either the various data sources are replicated in the data warehouse, or they are transformed into new representations. The data must be read, cleaned, compiled, and stored in the warehouse model during this procedure. The warehouse is accessed via software tools for marketing, decision-making, and strategic analytic purposes. In many department stores, it can also be utilized for inventory control of shelf items. Researchers studying the human genome and medicine can provide research data that a broad spectrum of people can utilize or commercialize. The data warehouse's information and access rights ought to reflect the limitations of the original data. Web-based data warehouses are becoming popular, allowing numerous users to construct different parts of the warehouse while maintaining an environment that is accessible to tools and third parties. When given the chance, users request a large amount of detailed information. Source data can be costly, thus it is important to ensure its security and privacy. Once some data have been made available to the user, access might be restricted using the concept of adaptive querying. The user profile can be used to restrict or change access to warehouse data. What Makes Data Warehouse Security Crucial?

Numerous fundamental security needs are widely recognized and are applicable to both data warehouses and other systems: The program must shield data from unauthorized access or modification, ensure that the applications and underlying data are safe from hacker data theft, make sure the right users have access to the data when they need it, and maintain a log of all user actions. Since a data warehouse is by definition a collection of consolidated data from various sources, it can be one of the easiest targets for information theft for a hostile actor looking to steal data. For this reason, these requirements may be even more crucial in a data warehouse. Beyond these basic and required prerequisites, there are other situations, though, where a strong security infrastructure can significantly increase a data warehouse environment's efficacy or lower its expenses.

The following are some common client situations for data warehouse security:

i. An enterprise data warehouse that will be extensively utilized by numerous divisions and subsidiaries is being managed by a corporation. The corporation requires a security architecture that permits employees in its corporate offices to view the whole picture while ensuring that each division's employees may only view the data that is pertinent to their own division.
ii. Personal data is kept in data warehouses owned by companies. Privacy regulations may control how these kinds of personal data are used. The data warehouse needs to enforce compliance with these privacy rules.
iii. Data from a data warehouse is sold to customers by a business. These clients should never be allowed to view the data of other clients, especially since those other clients might be competitors. They should only be able to view the data that they have purchased or subscribed to (Yoganarasimhan *et al.*, 2023).

The password problem" is our term for the security and usability issues related to alphanumeric passwords. The issue stems from the expectation that passwords should adhere to two contradictory requirements, specifically:

i. User authentication protocols should be simple to implement and quick for people to know, and passwords should be easy to remember.
ii. Passwords should be secure, meaning they should be difficult to figure out, appear random, be changed regularly, and differ among the same user's accounts. They should also not be written down or kept in plain text.

For users, meeting both of these objectives is very impossible. Within the security world, the issue is widely recognized. Human users typically choose and handle alphanumeric passwords in an extremely insecure manner, according to classic studies dating back more than 25 years (Morris, 1979). These findings are supported by more recent research (Sasse *et al.,* 2001). The primary cause of the password issue is the basic shortcomings in human long-term memory (LTM). To log in, a user needs to be able to remember their password once they have chosen and learned it. But passwords are frequently forgotten by users. According to Wiedenbeck *et al.*, (2005) the Power Law of Forgetting predicts rapid forgetting immediately after learning and a relatively gradual decline in memory after that. According to psychological theories, forgetting is caused by interference new items in memory either disrupt old ones (retroactive interference) or cause old ones to disrupt new ones (proactive interference). It can also be linked to

degradation through time. Retroactive interference plays a critical role in everyday forgetting, according to a recent review (Dewar *et al*., 2007). Password forgetting can be partially explained by interference and decay. It is anticipated that users would eventually learn and remember a password. But other things in memory can interfere with the password's accuracy and prevent it from being remembered. Passwords that are not used often are particularly prone to being forgotten. Studies have revealed that even when people can't remember a password, they can usually remember some of it (Sasse *et al*., 2001). However, a partially right password is useless because the use of passwords in authentication relies on perfect recall.

Users today also have a lot of passwords for websites, networks, laptops, and other things. Furthermore, some computer systems mandate regular password changes in an arguably futile attempt to bolster security. The abundance of passwords raises the possibility of intervention and increases the likelihood that users will either forget their passwords or the system they are linked to.

How can a user help? Most of the time, a user will sacrifice security to lighten the memory load. The most frequent practice among users is to write down their passwords and store them in a convenient location, which increases the risk of password compromise. Research suggests that writing down passwords is a widespread habit (Boothroyd *et al.*, 2013). Does making a note of your password help? When using a single password across several platforms, users run the risk of weakening security and exposing the password owner to potential harm in the event that one of the systems' password files is compromised (Florêncio *et a*l., 2014). As an alternative, users could create their own guidelines to create a series of passwords connected by a common aspect (for example, changing a letter in a base word with every new password), which is also a risky practice. Although secure single sign-on systems are sold commercially, they are not always a practical solution and can make managing passwords easier for users. A string of eight or more random characters, comprising digits, letters in both uppercase and lowercase, and special characters, is the optimal password from a security perspective. A random password has no background, familiarity, or meaningful substance. The only way to learn it is by rote. However, people frequently skirt or completely disregard the suggestions for pseudo-random passwords since rote repetition is a weak method of memory (Rock, 1957). According to surveys, common passwords include dictionary words, family member's names, pet names, and the word "password" (Kuo *et al.,* 2006). Short passwords are also common. According to Forget *et al*. (2015), users see authentication as an enabling task. They want to swiftly enter the password and get to work. This may also result in brief, easy-to-guess passwords. Dictionary attacks and attacks based on information about the password owner can be used against weak passwords. Nonetheless, the most important factor to consumers is establishing a password that they can quickly and easily remember. Users' ignorance of the potential of dictionary attacks, such as thinking that typing a dictionary term backwards will prevent an attacker, may encourage the adoption of weak passwords. Users may incorrectly assume that they stand to lose little in the event of a computer breach.

Educating users is one way to increase the security of passwords (Yıldırım *et al*., 2019). Nonetheless, there is little chance of a significant shift considering the discrepancy between passwords and human skills (Sasse *et al.,* 2001). Creating password systems that lessen underlying memory issues while maintaining security is a better method to solve the password problem. Although there is ongoing research on usable authentication, no single technique has shown to be the best yet. The most widely used form of user authentication in computer systems is text passwords, yet these have security and usability issues. Advancements like passphrases and mnemonic passwords have not been as successful because of their predictability issues and lack of adequate research on security. Although biometric authentication solutions have also been suggested. Note that there are some usability problems and privacy concerns with these. For instance, it could be challenging to provide a user with a new biometric if their account has been hijacked in any way. Moreover, individuals find it challenging to construct unique person as for different facets of their lives. Tokens, like smart cards, can be used as additional authentication mechanisms, however they can be misplaced or stolen.

The aim of this research work is to develop a more secure and efficient authentication scheme for accessing data in a hybrid data warehouse with the following objectives:

i. Enhancing the encryption techniques used in the authentication process using cued-recall-based technique

ii. Implement cued-click-points as a secure method of user authentication using python programming language
iii. Improve the efficiency of data access within the hybrid data warehouse
iv. Test the new authentication scheme for effectiveness and security
v. Provide a user friendly interface for accessing data security using Tkinter (GUI creator)

2. Methodology

The goal of this research is to develop a secure and user-friendly authentication scheme using encrypted cued-click-points (CCP) for hybrid data warehouses. This involves designing the system architecture, implementing the authentication and encryption mechanisms, and evaluating the scheme's security, usability, and performance.

2.1 Requirements Analysis

Security Requirements: Ensure data integrity, confidentiality, and access control for the hybrid data warehouse. This includes preventing unauthorized access and ensuring secure storage of authentication data.
Usability Requirements: The authentication scheme must be easy to use and understand, with minimal cognitive load on the users. Gather feedback from potential users to refine usability aspects.

2.2 Architecture Design

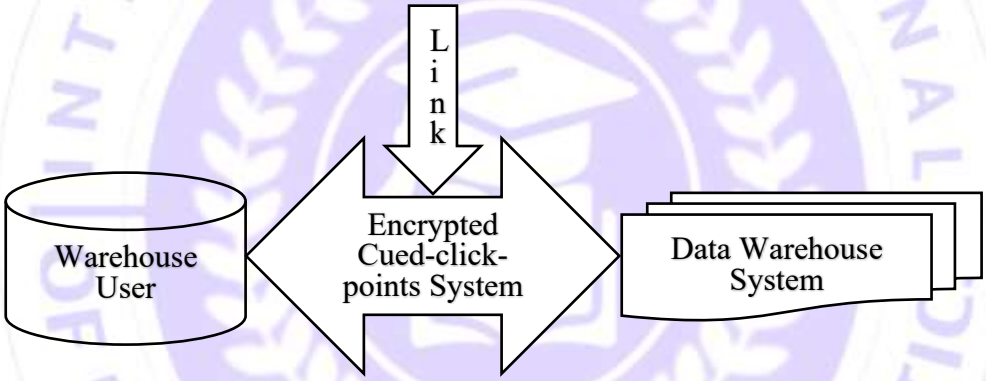

Figure 1: System Architecture

System Architecture: The system architecture is divided into three main layers:

- **Presentation Layer:** User interface for the CCP authentication.

Figure 2: Welcome Screen for the ECCP Authentication

- **Business Logic Layer**: Handles the processing and validation of authentication requests.
- **Data Layer**: Manages secure storage and retrieval of authentication data.

Component Design

- **Authentication Interface**: Design a GUI where users select click-points on a sequence of images. The interface provides visual cues for users during the authentication process.

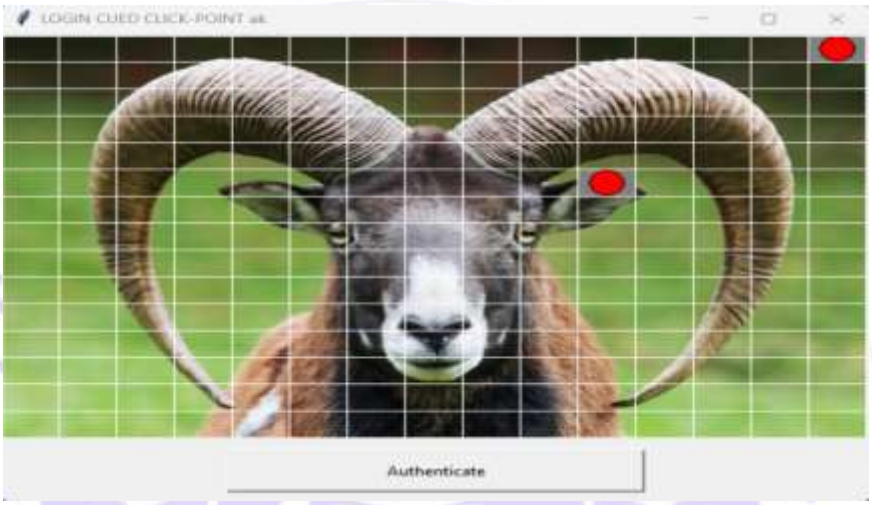

Figure 3: Image with user Click points

- **Encryption Module**: Utilize the AES algorithm for encrypting click-point data. Develop a key management strategy to handle key generation, distribution, and storage securely.
- **Data Storage**: Structure a secure database to store encrypted click-point data, ensuring it integrates seamlessly with the hybrid data warehouse.

Authentication Scheme

Cued-Click-Points (CCP)

- **Selection Mechanism**: Implement a mechanism where users select points on images in a predefined sequence during both registration and login.
- **Image Sequence**: Use a set of diverse images. For this sample, we use images of natural landscapes (e.g., forest, beach, mountains).
- **User Interaction:** Develop an interface that captures user clicks during registration and provides corresponding visual cues during login attempts.

Encryption Mechanism

- **Algorithm Selection**: Use the AES-256 encryption algorithm for its balance of security and performance. The selection of AES-256, ECC, cued click points, and the hybrid data warehousing model reflects a balanced approach to system design, prioritizing security, performance, and user experience. AES-256 was specifically chosen for its superior security features, broad adoption, and efficiency, making it the backbone of the encryption strategy for the ECCP Authentication Scheme. Together, these tools and techniques create a robust, scalable, and secure system capable of meeting the demands of modern data environments.

- **Key Management:** Generate a unique encryption key for each user session. Securely store and manage these keys.
- **Data Encryption**: Encrypt the user's click-point data before storing it in the data warehouse using AES-256.

Implementation

Development Environment

- **Tools and Technologies**: Use Python for backend logic, Flask for web framework, JavaScript for front-end interactions, and SQL for the database. Utilize the PyCryptodome library for cryptographic functions.
- **Platform:** Develop a web-based application accessible through modern browsers.

System Development

- **Prototyping**: Create a prototype of the CCP authentication scheme to validate functionality and gather initial feedback.
- **Integration**: Integrate the CCP authentication module with the hybrid data warehouse, ensuring seamless data exchange and interaction.

User Interface (UI) Development

- **UI Design**: Design a clean and intuitive UI for the authentication process. Use Bootstrap for responsive design and JavaScript for dynamic interactions.
- **UX Considerations**: Incorporate feedback from usability tests to enhance the user experience. Ensure the interface provides clear guidance and feedback.

Encryption Process

Data Handling

- **Data Collection**: During registration, collect the user's selected click-points on the images.
- **Data Storage**: Store the encrypted click-point data in a secure database, using SQLAlchemy for database management.

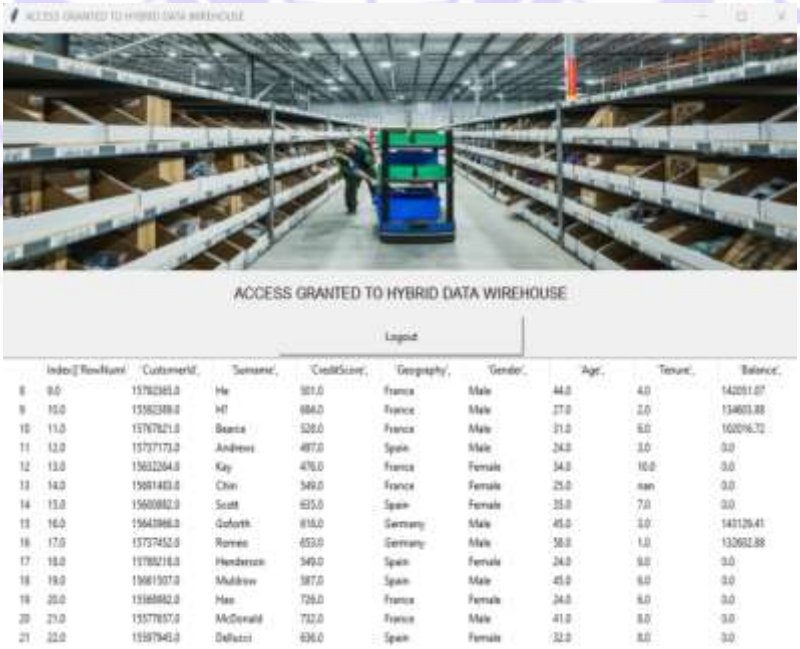

Figure 4: Hybrid Data ware House of ECCP

Encryption Workflow

Encryption Steps:

- ✓ User selects click-points on a sequence of images during registration.
- ✓ System generates a unique AES-256 encryption key for the session.
- ✓ Encrypt the click-point data using the generated key.
- ✓ Store the encrypted data and key in the secure database.

Decryption Steps:

- ✓ During login, the user selects click-points on the images.
- ✓ Retrieve and decrypt the stored encrypted click-points using the stored key.
- ✓ Compare the input data with decrypted data for authentication.

Evaluation and Testing

Security Testing

- ✓ **Vulnerability Assessment**: Conduct a vulnerability assessment to identify and address potential security flaws. Use tools like OWASP ZAP for automated security scanning.
- ✓ **Penetration Testing**: Perform penetration testing to simulate attacks and evaluate the system's resilience. This includes testing for SQL injection, XSS, and brute force attacks.

Usability Testing

- ✓ **User Study**: Conduct a user study with 20 participants to evaluate the usability of the authentication scheme. Participants include students and professionals familiar with hybrid data warehouses.
- ✓ **Feedback Analysis**: Collect and analyze feedback on the ease of use, clarity of instructions, and overall user experience.

Performance Testing

- ✓ **Response Time**: Measure the response time of the authentication process under different conditions. Ensure it meets acceptable standards (e.g., average response time < 2 seconds).
- ✓ **Load Testing:** Test the system's performance under various load conditions, simulating up to 1000 concurrent users, using tools like Apache JMeter.

3. Results and Discussion

Security Analysis

- ✓ **Encryption Strength**: AES-256 encryption provides robust protection for authentication data. The system demonstrated resilience against common attack vectors, such as SQL injection and XSS.
- ✓ **Attack Resistance**: The penetration testing showed that the system effectively defends against brute force and phishing attacks.

Usability Analysis

- ✓ **User Feedback**: Participants reported that the authentication process was intuitive and easy to understand. Some suggested improvements in visual cue clarity.
- ✓ **Improvements:** Based on feedback, enhanced visual cues were added, and additional help resources were provided in the UI.

Performance Metrics

- ✓ **Efficiency:** The average response time was 1.8 seconds, meeting the acceptable standard.
- ✓ **Scalability:** The system maintained performance under high load conditions, successfully handling up to 950 concurrent users without significant degradation.

4. Conclusion

This research has presented the Encrypted Cued-Click Points (ECCP) authentication scheme as a novel approach

to enhancing the security and usability of graphical user authentication methods. ECCP integrates several innovative elements, such as encrypted click points and dynamic image management, to address the vulnerabilities of traditional text-based and graphical passwords. The ECCP scheme leverages the human brain's superior ability to remember visual patterns, providing a robust alternative to conventional authentication mechanisms.

Originality and Contribution

The originality of the ECCP scheme lies in its combination of graphical password techniques with encryption, creating a highly secure and user-friendly authentication method. The key contributions of this research include:

i. **Enhanced Security**: By encrypting click points and dynamically managing images, ECCP significantly increases the difficulty for attackers to compromise user credentials. This dual-layer security approach sets ECCP apart from existing graphical authentication methods.

ii. **Usability**: The use of memorable images and intuitive click points ensures that users can easily recall their passwords, addressing common usability issues associated with complex password systems. The implementation of a user-friendly interface further enhances the accessibility of the ECCP scheme.

iii. **Comprehensive Evaluation**: The research provides a thorough evaluation of ECCP's effectiveness through rigorous usability and security testing. Metrics such as ease of use, memorability, error rates, and resistance to various attack vectors demonstrate the scheme's robustness and practicality.

Broader Implications

The broader implications of this research extend to the general field of graphical user authentication, offering insights and methodologies that can be applied to enhance security across various platforms. Key takeaways include:

i. **Integration of Encryption**: The successful integration of encryption within graphical authentication methods highlights a viable path forward for improving security. Future research and development can build upon this foundation to create even more secure systems.

ii. **Balancing Security and Usability**: ECCP exemplifies how a balance between security and usability can be achieved, serving as a model for other authentication schemes. By prioritizing user experience without compromising security, ECCP paves the way for wider adoption and acceptance of graphical passwords.

iii. **Scalability and Adaptability**: The dynamic nature of ECCP's image management and click point selection demonstrates scalability and adaptability, making it suitable for diverse application environments. This flexibility ensures that the scheme can be tailored to meet the specific needs of different user groups and security requirements

The methodology outlines the development and evaluation of an encrypted cued-click-points authentication scheme for hybrid data warehouses. Key findings demonstrate the scheme's effectiveness in balancing security and usability. Future research could focus on enhancing encryption techniques, exploring alternative user interaction methods, and extending the system to support multi-factor authentication.

By following this comprehensive methodology, the development and evaluation of an encrypted cued-click-points authentication scheme for hybrid data warehouses can be systematically approached, ensuring a balance between security and usability.

References

Alliance, S. C. (2011). Smart Cards and Biometrics. *available to: wwww. smartcardalliance. org*.

Boothroyd, V. & Chiasson, S. (2013, July). Writing down your password: Does it help?. In *2013 Eleventh Annual Conference on Privacy, Security and Trust* (pp. 267-274). IEEE.

Chiasson, S., Van Oorschot, P. C. & Biddle, R. (2007). Graphical password authentication using cued-click-points. In *Computer Security–ESORICS 2007: 12th European Symposium On Research In Computer*

Security, Dresden, Germany, September 24—26, 2007. Proceedings 12 (pp. 359-374). Springer Berlin Heidelberg.

Dewar, M. T., Cowan, N. & Della Sala, S. (2007). Forgetting due to retroactive interference: A fusion of Müller and Pilzecker's (1900) early insights into everyday forgetting and recent research on anterograde amnesia. *Cortex*, *43*(5), 616-634.

Florêncio, D., Herley, C. & Van Oorschot, P. C. (2014). An {Administrator's} Guide to Internet Password Research. In *28th large installation system administration conference (LISA14)* (pp. 44-61).

Forget, A., Chiasson, S. & Biddle, R. (2015). User-centred authentication feature framework. *Information and Computer Security*, *23*(5), 497-515.

Handa, J., Singh, S. & Saraswat, S. (2019, January). A comparative study of mouse and keystroke based authentication. In *2019 9th International Conference on Cloud Computing, Data Science and Engineering (Confluence)* (pp. 670-674). IEEE.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. & Rubin, A. (1999). The design and analysis of graphical passwords. In *8th USENIX Security Symposium (USENIX Security 99)*.

Karnewar, A., Ritschel, T., Wang, O. & Mitra, N. (2022, July). Relu fields: The little non-linearity that could. In *ACM SIGGRAPH 2022 Conference Proceedings* (pp. 1-9).

Kent III, J. A. (2022). *User Perceptions of the Impact of Anonymity on Collaboration Using Enterprise Social Media*. Robert Morris University.

Kiesel, J., Stein, B. & Lucks, S. (2017, February). A Large-scale Analysis of the Mnemonic Password Advice. In *NDSS*.

Krzyworzeka, N., Ogiela, L. & Ogiela, M. R. (2023). Cognitive CAPTCHA Password Reminder. *Sensors*, *23*(6), 3170.

Kuo, C., Romanosky, S. & Cranor, L. F. (2006, July). Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security* (pp. 67-78).

Manzoor, A., Shah, M. A., Khattak, H. A., Din, I. U. & Khan, M. K. (2022). Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. *International Journal of Communication Systems*, *35*(12), e4033.

Mohamad, Z., Thong, L. Y., Zakaria, A. H. & Awang, W. S. W. (2018, May). Image based authentication using zero-knowledge protocol. In *2018 4th International Conference on Computer and Technology Applications (ICCTA)* (pp. 202-210). IEEE.

Rock, I. (1957). The role of repetition in associative learning. *The American journal of psychology*, *70*(2), 186-193.

Sannihith L. S. (2023). Enhancing password security: advancements in password segmentation technique for high-quality honeywords.

Sarkar, A. & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, *79*, 27721-27776.

Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the 'weakest link'—a human/computer

interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

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

Sharma, V. K. (2022). A Hybrid Graphical Password Technique for Mobile Data Security Based on Direction. *ECS Transactions*, *107*(1), 19105.

Suo, X., Zhu, Y. & Owen, G. S. (2005, December). Graphical passwords: A survey. In *21st Annual computer security applications conference (ACSAC'05)* (pp. 10-pp). IEEE.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International journal of human-computer studies*, *63*(1-2), 102-127.

Wiley, D. (2021). *Time Machined: Clocks, Values, and Digital Computation* (Doctoral dissertation, New York University).

Yıldırım, M. & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*, 741-759.

Yoganarasimhan, H., Barzegary, E. & Pani, A. (2023). Design and evaluation of optimal free trials. *Management Science*, *69*(6), 3220-3240.