Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 2, No. 2, 2025, pp. 333~341 DOI: 10.26740/vubeta.v2i2.38218
ISSN: 3064-0768

Password Authentication Using Modify Multi-Connect Architecture Associative Memory

Rusul Hussein Hasan[1]*, Inaam Salman Aboud[2], Rasha Majid Hassoon[3]
[1,3] University of Baghdad, Baghdad, Iraq
[2] College of Education Al-Mustansiriya University, Baghdad, Iraq

Article Info

Article history:

Received January 11, 2025
Revised March 23, 2025
Accepted April 3, 2025

Keywords:

Associative Memory
MMCA
Authentication
Password
Traditional password

ABSTRACT

Traditional password authentication systems often face challenges related to security vulnerabilities, slow authentication speeds, and susceptibility to noise interference. While previous methods such as Multi-Bias Associative Memory (MBAM) have made progress in improving authentication performance, they still suffer from inefficiencies in training time, accuracy, and robustness to noisy input data. To address these limitations, this research introduces an Enhanced Password Authentication System leveraging Modified Multi-Connect Architecture (MMCA) associative memory, supporting both graphical and textual passwords. MMCA enhances pattern recognition, enabling faster and more accurate authentication while ensuring robustness against noise interference. Compared to traditional methods, MMCA reduces computational overhead, improves resistance to adversarial inputs, and accelerates the authentication process. Experimental validation on 100 trials demonstrates 100% authentication accuracy for both graphical and textual password-based methods. The system achieves authentication times of 0.5 seconds for textual passwords and 1 second for graphical passwords, significantly outperforming existing solutions. Additionally, MMCA maintains reliable authentication even in the presence of up to 15% noise in graphical passwords. Comparative analysis shows that MMCA surpasses MBAM and other approaches in training efficiency and authentication speed, making it a promising solution for secure, fast, and noise-resistant user authentication.

1. INTRODUCTION

Access authentication is essential for computer security and is a critical procedure for granting users access to resources [1]. As computer security plays an increasingly vital role in daily life, existing authentication methods face certain limitations [2][3]. One drawback of the MMCA approach is that multiple usernames may share the same password, leading to potential security risks. A proposed solution involves combining a password with a unique key to identify the username; however, this method remains ineffective [4]-[6]. To address this limitation, this research introduces a novel technique—password authentication using the Modified Multi-Connect Architecture (MMCA)—which enhances security and efficiency.

Password authentication is one of the most widely used methods for verifying a user's identity in digital systems [7][8]. It involves a user providing a secret string of characters, known as a password, to gain access to a system, application, or network [9][10]. This method serves as the first line of defense against unauthorized access, ensuring that only legitimate users can interact with a service.

Despite its simplicity and widespread use, password authentication comes with several challenges, including vulnerabilities to brute-force attacks, phishing, credential stuffing, and password leaks. Security best

*Corresponding Author
Email: russl@colaw.uobaghdad.edu.iq

practices recommend strong password policies, hashing techniques, multi-factor authentication (MFA), and password managers to mitigate these risks[1].

Modern systems often integrate hashed and salted password storage, ensuring they remain challenging to crack even if stored passwords are leaked. Technologies like bcrypt, Argon2, and PBKDF2 help enhance security by making password hashing computationally expensive for attackers. Additionally, organizations are increasingly adopting passwordless authentication methods—such as biometrics and hardware security keys—to address password-related security flaws.

As cyber threats evolve, password authentication remains a critical yet imperfect security measure, necessitating continuous improvements and complementary security mechanisms to safeguard user credentials effectively[11][12].

How Password Authentication Works When a user creates an account, they typically go through the following process:

1. Account Creation: The user selects a password stored in a hashed and sometimes salted format.
2. Login Attempt: The user enters their password, which is processed and compared to the stored credentials.
3. Verification: If the password matches, access is granted; if not, the attempt is rejected.

Security Risks in Password Authentication Despite its widespread use, password authentication has several vulnerabilities:

- Brute-force attacks: Automated tools try multiple password combinations until the correct one is found [13][14].
- Credential stuffing: Attackers use previously leaked username-password pairs to gain access to multiple accounts [15]-[17].
- Phishing: Malicious actors trick users into revealing their passwords [18].
- Keylogging: Malware records keystrokes to steal passwords [19][20].
- Password leaks: If a stored password database is exposed, users' credentials become vulnerable [21][22].

Best Practices for Secure Password Authentication. To improve password security, organizations and users should follow these best practices:

(a) Use Strong Passwords

- At least 12–16 characters long
- Includes a mix of uppercase and lowercase letters, numbers, and special characters
- Avoids common words and predictable patterns

(b) Hash and Salt Passwords

Instead of storing plaintext passwords, websites and applications use hashing algorithms to protect user credentials. Hashing converts passwords into irreversible strings. Common hashing techniques include:

- BCrypt (recommended for its built-in salting and computational cost control) [23][24]
- Argon2 (a modern algorithm resistant to brute-force attacks) [25]
- PBKDF2 (used in many security applications) [23]

Salting is the process of adding a random value (salt) to passwords before hashing to prevent rainbow table attacks.

(c) Implement Multi-Factor Authentication (MFA) [26]-[28]

MFA enhances security by requiring additional verification beyond the password, such as:

- One-time passwords (OTP) sent via SMS, email, or authenticator apps
- Biometric authentication (fingerprint, facial recognition)
- Hardware security keys (e.g., YubiKey, FIDO2)

(d) Use Password Managers

Password managers generate and store complex passwords, reducing the need for users to remember multiple credentials. Popular options include Bitwarden, LastPass, and 1Password [29][31].

(e) Monitor for Credential Leaks

Services like Have I Been Pwned allow users to check if their passwords have been exposed in data breaches. Organizations can use password blacklists to prevent the use of compromised passwords.

(f) Modern Alternatives to Password Authentication

Due to the weaknesses of passwords, alternative authentication methods are gaining popularity:

- Passwordless Authentication: Users authenticate using biometrics, security keys, or device-based authentication (e.g., Windows Hello, Apple Face ID) [32][33].
- Single Sign-On (SSO): Users log in once to access multiple applications securely [34][35].
- Behavioral Authentication: Systems verify identity by analyzing typing patterns, mouse movements, or other behavioral factors [36]-[38].

While password authentication remains the most common method for securing online accounts, its security limitations require continuous improvements. Organizations and users can significantly enhance account security by following best practices, such as using strong passwords, implementing MFA, and adopting modern authentication methods.

RELATED WORK

ASN Chakravarthy et al (2011). This paper described Password authentication using the Hopfield Neural Network, which explains the Hopfield Neural Network Scheme for graphical and textual passwords, converting the input Password into probabilistic values. Compared to existing layered neural network techniques, the proposed method provides better accuracy and quicker response time to registration [39].

ASN Chakravarthy and P S Avadhani (2011) described a method using the Bidirectional Associative Memory (BAM) algorithm for graphical password and alphanumeric (Text) password in this paper. Then, the amount of security provided for the user can be enhanced. This paper, along with test results, illustrates that user password input is converted into probabilistic values and given to BAM, which improves the system's security [40].

Rusul Hussein Hasan et al (2016). This paper describes a password authentication method by using the Modified Bidirectional Associative Memory (MBAM) algorithm for both graphical and textual passwords for faster speed and accuracy. The accuracy result for 100 tests is 100% for graphical and textual passwords [41].

2. METHOD

2.1. Modify Multi-Connect Architecture Associative Memory

Associative memory involves storing data as a memory or weight matrix, which generates outputs based on given inputs. This type of memory can be categorized as either auto-associative or hetero-associative. The Hopfield neural network is a widely used model for auto-association and optimization tasks. Still, it has several limitations, such as a restricted number of patterns it can store, susceptibility to local minima, low tolerance to noise, the retrieval of inverted patterns, and issues with shifting and scaling.

The Modified Multi-Connect Architecture (MMCA) was introduced to address these challenges. MMCA enhances the Multi-Connect Architecture (MCA) by reducing the size of the network and weights, improving noise robustness, and speeding up both the learning and convergence processes. It modifies both the network structure and the algorithms for learning and convergence.

These improvements are achieved by introducing new algorithms for both learning and convergence. During the learning phase, the pattern (a sequence of 1's and -1's) is divided into pairs of elements, which are treated as vectors. Each vector either generates a learning weight matrix during the learning phase or helps identify the convergence pattern during the convergence phase (see Figure 1).

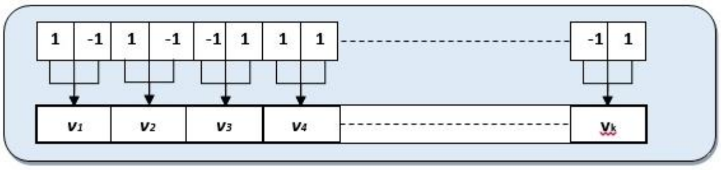

Figure 1. The data (pattern) is divided into several vectors of size two, which are needed to create its learning weight matrix.

As a result of this process, MMCA can handle patterns of any size, providing unlimited associative memory capacity and enabling it to recall even correlated patterns. Furthermore, since the vector size is two, there are no more than four possible vectors (see Table 1), meaning that only two weight matrices (W) will be created during the learning process. This is because each pair of orthogonal vectors shares the same weight. These matrices are symmetric, have no zero diagonal elements, and are of size 2x2.

Table 1. Illustrated: The Four Possibilities Of The Bipolar Vector With Length Two.

-1	-1
-1	1
1	-1
1	1

The architecture of MMCA is illustrated in Figure 2. It shows each path represents one learning weight matrix (1< m <2); thus, all the vectors in the pattern will be replaced with a number, which means the number of the path in the net. By this number, we can call the path again.

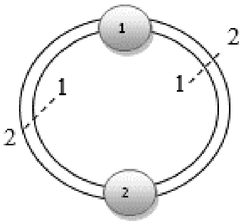

Figure 2. The Architecture of MMCA Associative Memory.

2.2. Proposed Method Using Modified Multi-Connect Architecture

The password authentication flow using the Modify Multi-Connect Architecture (MMCA) is illustrated in Figure 3. The input to this module can either be a graphical or textual password. The initial step in the process is to combine the user's username and password, as shown in Figure 4. However, this approach is limited, as merging the username and password can lead to identical outputs in certain cases, as depicted in Figure 5.

An additional character, acting as a delimiter between the username and password, is introduced to address this issue, as shown in Figure 6. Following this, the username and password are converted into binary values using bipolar representation. These binary values are then used as training samples, following the procedure outlined in Figure 7.

Once the training phase is completed, the network is stored on each server. When a user wishes to access an application hosted on a server, they connect to the server and input their username and password into the application. The server loads the MMCA, processes the username as input, and generates an output. If the output matches the password provided by the user, the server grants access to the application.

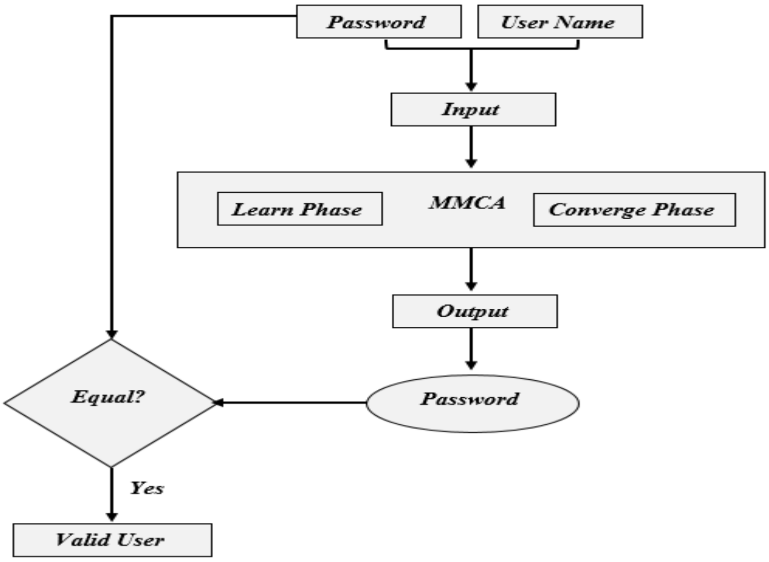

Figure 3. Password Authentication Flowchart Using MMCA.

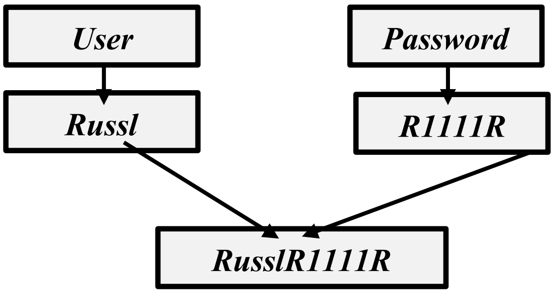

Figure 4. Merge Input User Name And Password.

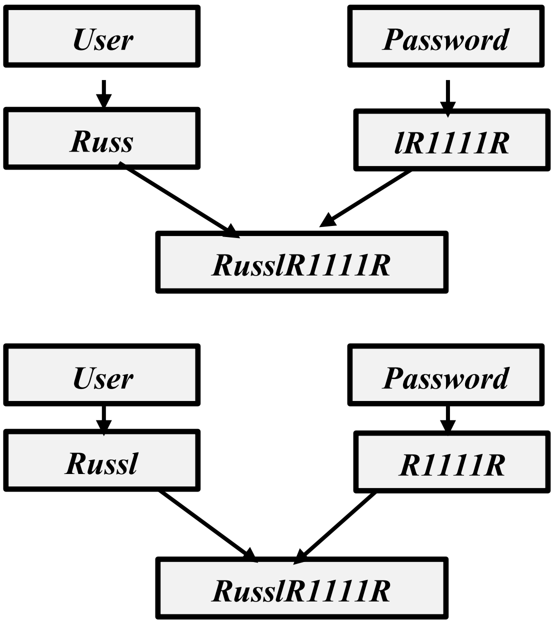

Figure 5. Problem with merging.

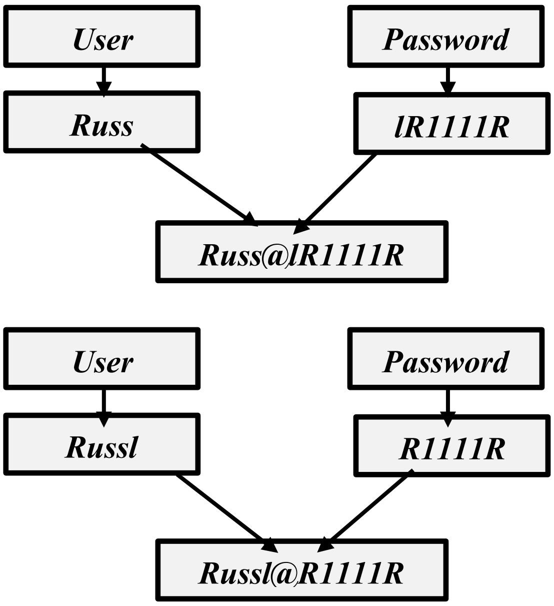

Figure 6. Adding Delimiter for Merging Process

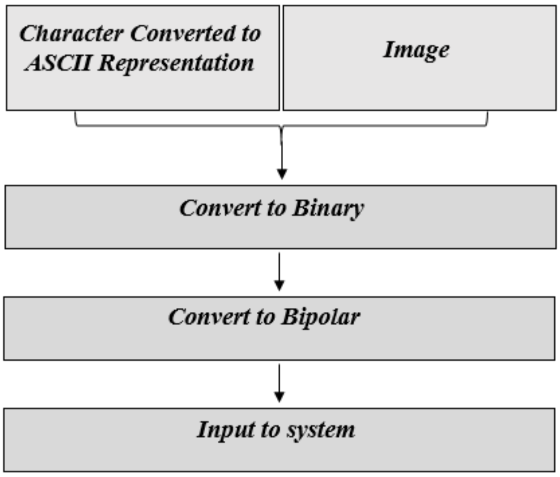

Figure 7. Steps in the Authentication Process.

Once the training is completed, the network is quickly stored on each server. When a user wants to access an application on the server, they connect to the server and input their username and password into the application. The server loads the MMCA, processes the username as input, and generates an output. If the output matches the password provided by the user, the server grants access to the application.

3. RESULT AND DISCUSSION

The system demonstrates 100% accuracy in authenticating 100 users using textual passwords. For graphical password authentication, the accuracy remains 100% when the image is noise-free. However, if the image contains noise (below a 15% noise threshold caused by format changes or transformations), the server will send an authentication code to the user's email. The authentication times are 0.5 seconds for textual passwords and 1 second for graphical passwords.

In addition, it is essential to compare the proposed method with other similar approaches. This comparison evaluates training time and the neural network's capacity, measured by the number of stored patterns, using identical training sets across methods. Authentication times are also compared with the MBAM technique.

Figure 7 shows the training times for different networks (see Table 2). Figure 8 presents the percentage of patterns stored by various training sets. This capacity differs from the number of patterns used in training, as neural networks often cannot store all the patterns from the training set (see Table 3).

As shown in Figure 8, the MMCA outperforms other networks by requiring less training time. Figure 9 highlights the network's capacity, showing that MMCA and MBAM can store all the patterns. Regarding authentication times, MMCA significantly outperforms MBAM, taking just 0.5 seconds for textual passwords and 1 second for graphical passwords, whereas MBAM requires 2.3 seconds for textual passwords and 15 seconds for graphical passwords.

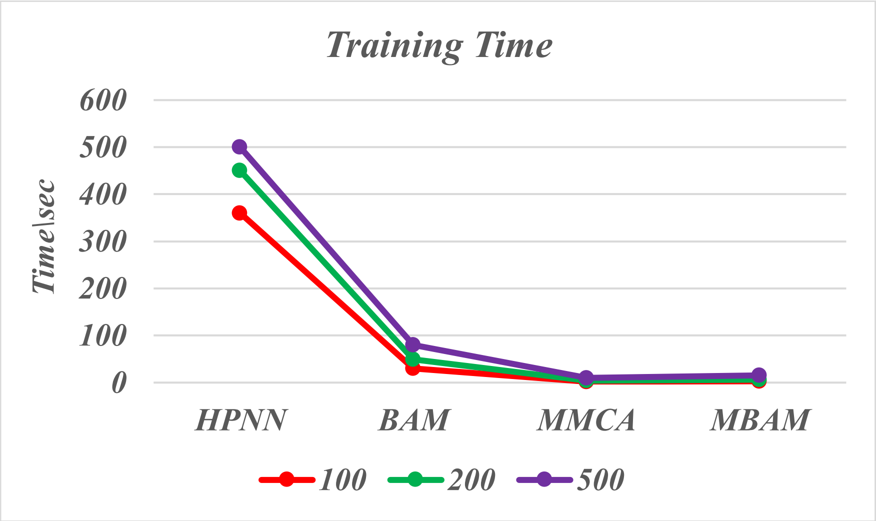

Figure 8. Training Time.

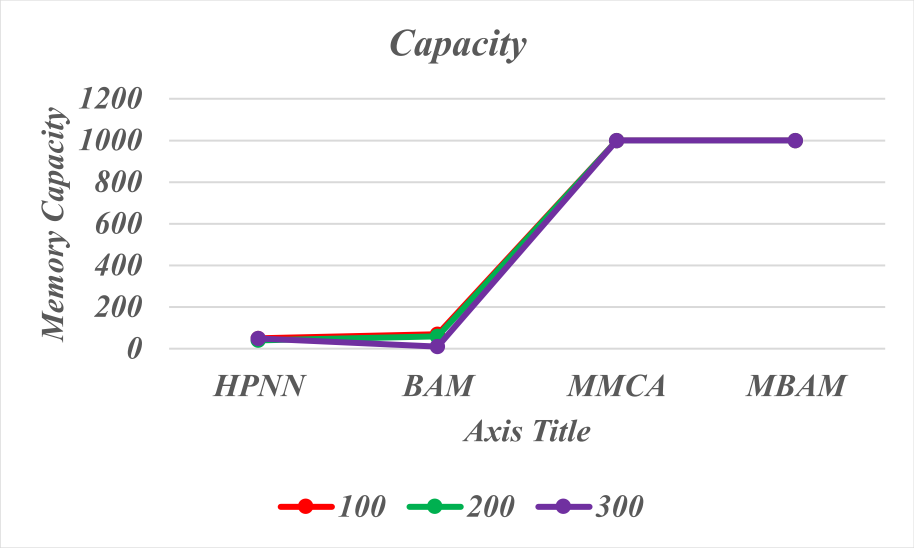

Figure 9. Capacity Result.

Table 2. Training Time

Training Time			
Training set	100	200	500
HPNN	360	450	500
BAM	30	49	80
MMCA	2	4	10
MBAM	3	6	15

Table 3. Accuracy Result

Accuracy			
Memory Capacity in term (No. of pattern)			
	100	200	500
HPNN	50	40	50
BAM	70	60	50
MMCA	Return all stored pattern		
MBAM	Return all stored pattern		

4. CONCLUSION AND LIMITATION

This research proposes a password authentication system using the Modified Multi-Connect Architecture (MMCA), achieving 100% accuracy for graphical and textual passwords. The system is designed to enhance the speed and accuracy of password authentication.

The process takes 0.5 seconds for textual password authentication, while for graphical passwords, it takes 1 second. The system performs effectively even when graphical images contain noise (less than 15%), sending an authentication code to the user's email in such cases. The network's performance was evaluated by comparing it with other similar methods, including MBAM. MMCA was found to require less training time, store all patterns effectively, and offer faster authentication, with times of 0.5 seconds for textual and 1 second for graphical passwords, compared to 2.3 seconds and 15 seconds for MBAM, respectively.

The system's ability to recall correlated patterns and handle large pattern sizes is an added advantage. Overall, the proposed MMCA method improves the efficiency and robustness of password authentication systems regarding speed, accuracy, and capacity.

REFERENCES

[1] A. Mostafa, M. Ezz, M. Elbashir, M. Alruily, E. Hamouda, M. Alsarhani et al., "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication", *Applied Sciences*, vol. 13, no. 19, pp. 10871, 2023. https://doi.org/10.3390/app131910871

[2] D. Gupta, N. Mazumdar, A. Nag, & J. Singh, "Secure Data Authentication and Access Control Protocol for Industrial Healthcare System", *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 4853-4864, 2023. https://doi.org/10.1007/s12652-022-04370-2

[3] N. Karim, O. Khashan, H. Kanaker, W. Abdulraheem, M. Alshinwan, & A. Al-Banna, “Online Banking User Authentication Methods: A Systematic Literature Review", *IEEE Access*, vol. 12, pp. 741-757, 2024. https://doi.org/10.1109/access.2023.3346045

[4] E. Hamouda, M. Ezz, A. Mostafa, M. Elbashir, M. Alruily, & M. Tarek, "Innovative Hetero-Associative Memory Encoder (HAMTE) for Palmprint Template Protection", *Computer Systems Science and Engineering*, vol. 46, no. 1, pp. 619-636, 2023. https://doi.org/10.32604/csse.2023.035830

[5] T. Kang, N. Woo, & J. Ryu, "Enhanced Lightweight Medical Sensor Networks Authentication Scheme Based on Blockchain", *IEEE Access*, vol. 12, pp. 35612-35629, 2024. https://doi.org/10.1109/access.2024.3373879

[6] S. Kaur, G. Kaur, & M. Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing", *Security and Communication Networks*, vol. 2022, pp. 1-9, 2022. https://doi.org/10.1155/2022/7540891

[7] M. Ahmad, G. Tripathi, F. Siddiqui, M. Alam, M. Ahad, M. Akhtar et al., "BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities", *Sensors*, vol. 23, no. 5, pp. 2757, 2023. https://doi.org/10.3390/s23052757

[8] T. Suleski, M. Ahmed, W. Yang, & E. Wang, "A Review of Multi-Factor Authentication in the Internet of Healthcare Things", *Digital Health*, vol. 9, 2023. https://doi.org/10.1177/20552076231177144

[9] M. Almaiah, F. Hajjej, A. Ali, M. Pasha, & O. Almomani, "A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS", *Sensors*, vol. 22, no. 4, pp. 1448, 2022. https://doi.org/10.3390/s22041448

[10] H. Seksak, K. Amin, & S. Zarif, "Choice-Based Graphical Password (CGP) Scheme for Web Applications", *IJCI. International Journal of Computers and Information*, vol. 10, no. 3, pp. 104-112, 2023. https://doi.org/10.21608/ijci.2023.236026.1127

[11] C. Fidas and D. Lyras, "A Review of EEG-Based User Authentication: Trends and Future Research Directions", *IEEE Access*, vol. 11, pp. 22917-22934, 2023. https://doi.org/10.1109/access.2023.3253026

[12] J. Rivera, M. Afaq, & W. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication", *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2792-2814, 2024. https://doi.org/10.1109/ojcoms.2024.3391728

[13] I. Alkhwaja, M. Albugami, A. Alkhwaja, M. Alghamdi, H. Abahussain, F. Alfawaz et al., "Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming", *Applied Sciences*, vol. 13, no. 10, pp. 5979, 2023. https://doi.org/10.3390/app13105979

[14] G. Andreianu, "Protecting Your E-Commerce Business. Analysis on Cyber Security Threats", *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*, 2023. https://doi.org/10.19107/cybercon.2023.17

[15] K. Jyothi, S. Borra, K. Srilakshmi, P. Balachandran, G. Reddy, I. Colak et al., "A Novel Optimized Neural Network Model for Cyber Attack Detection using Enhanced Whale Optimization Algorithm", *Scientific Reports*, vol. 14, no. 1, 2024. https://doi.org/10.1038/s41598-024-55098-2

[16] K. Wang and M. Reiter, "Using Amnesia to Detect Credential Database Breaches", *Advances in Information Security*, pp. 183-215, 2022. https://doi.org/10.1007/978-3-031-16613-6_9

[17] H. El-Taj, D. Hamedah, & R. Saeed, "Artificial Intelligence and Advanced Cybersecurity to Mitigate Credential-Stuffing Attacks in the Banking Industry", *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 1, 2025. https://doi.org/10.22399/ijcesen.754

[18] G. Misra, B. Hazela, & B. Chaurasia, "Privacy Preserving Authentication of IoMT in Cloud Computing", *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024. https://doi.org/10.4108/eetiot.6235

[19] S. Shinde, "A Study for an Ideal Password Management System", *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, no. 1, pp. 976-980, 2022. https://doi.org/10.22214/ijraset.2022.39970

[20] W. Yu, Q. Yin, H. Yin, W. Xiao, T. Chang, L. He et al., "A Systematic Review on Password Guessing Tasks", *Entropy*, vol. 25, no. 9, pp. 1303, 2023. https://doi.org/10.3390/e25091303

[21] A. Juozapavičius, A. Brilingaitė, B. Linas, & R. Lugo, "Age and Gender Impact on Password Hygiene", *Applied Sciences*, vol. 12, no. 2, pp. 894, 2022. https://doi.org/10.3390/app12020894

[22] X. Guo, K. Tan, Y. Liu, M. Jin, & H. Lu, "LPG–PCFG: An Improved Probabilistic Context- Free Grammar to Hit Low-Probability Passwords", *Sensors*, vol. 22, no. 12, pp. 4604, 2022. https://doi.org/10.3390/s22124604

[23] J. Blocki, B. Harsha, & S. Zhou, "On the Economics of Offline Password Cracking", *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 853-871, 2018. https://doi.org/10.1109/sp.2018.00009

[24] T. Batubara, S. Efendi, & E. Nababan, "Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force", *Journal of Physics: Conference Series*, vol. 1811, no. 1, pp. 012129, 2021. https://doi.org/10.1088/1742-6596/1811/1/012129

[25] S. Eum, H. Kim, M. Song, & H. Seo, "Optimized Implementation of Argon2 Utilizing the Graphics Processing Unit", *Applied Sciences*, vol. 13, no. 16, pp. 9295, 2023. https://doi.org/10.3390/app13169295

[26] A. Obiki-Osafiele, E. Agu, & N. Chiekezie, "Protecting Digital Assets in Fintech: Essential Cybersecurity Measures and Best Practices", *Computer Science & IT Research Journal*, vol. 5, no. 8, pp. 1884-1896, 2024. https://doi.org/10.51594/csitrj.v5i8.1449

[27] M. Roopesh, "Cybersecurity Solutions and Practices: Firewalls, Intrusion Detection/Prevention, Encryption, Multi-Factor Authentication", *Academic Journal on Business Administration, Innovation Sustainability*, vol. 4, no. 3, pp. 37-52, 2024. https://doi.org/10.69593/ajbais.v4i3.90

.

[28] M. Hasan, F. Rozony, M. Kamruzzaman, & M. Uddin, "Common Cybersecurity Vulnerabilities: Software Bugs, Weak Passwords, Misconfigurations, Social Engineering", *Global Mainstream Journal*, vol. 3, no. 4, pp. 42-57, 2024. https://doi.org/10.62304/jieet.v3i04.193

[29] M. Grilo, J. Campos, J. Ferreira, J. Almeida, & A. Mendes, "Verified Password Generation from Password Composition Policies", *Lecture Notes in Computer Science*, pp. 271-288, 2022. https://doi.org/10.1007/978-3-031-07727-2_15

[30] G. Balayogi and K. Kuppusamy, "An Approach for Mitigating Cognitive Load in Password Management by Integrating QR Codes and Steganography", *Security and Privacy*, vol. 7, no. 6, 2024. https://doi.org/10.1002/spy2.447

[31] P. Gallus, D. Stanek, & I. Klaban, "Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions", *International Conference on Cyber Warfare and Security*, vol. 20, no. 1, pp. 105-113, 2025. https://doi.org/10.34190/iccws.20.1.3330

[32] A. Prasad, "Breaking Barriers: Passwordless Authentication as the Future of Security", *International Journal of Computer Applications*, vol. 186, no. 60, pp. 29-35, 2025. https://doi.org/10.5120/ijca2025924353

[33] T. Oduguwa and A. Arabo, "Passwordless Authentication Using a Combination of Cryptography, Steganography, and Biometrics", *Journal of Cybersecure Privacy*, vol.4, pp. 278-297, 2024. https://doi.org/10.20944/preprints202401.1466.v1

[34] D. Krishna, R. Ramaguru, K. Praveen, M. Sethumadhavan, K. Ravichandran, R. Krishankumar et al., "SSH-Dauth: Secret Sharing Based Decentralized OAuth using Decentralized Identifier", *Scientific Reports*, vol. 13, no. 1, 2023. https://doi.org/10.1038/s41598-023-44586-6

[35] A. Pratama, F. Firmansyah, & F. Rahma, "Security Awareness of Single Sign-on Account in the Academic Community: The Roles of Demographics, Privacy Concerns, and Big-Five Personality", *PeerJ Computer Science*, vol. 8, pp. e918, 2022. https://doi.org/10.7717/peerj-cs.918

[36] M. Παπαϊωάννου, F. Pelekoudas-Oikonomou, Γ. Μαντάς, E. Serrelis, J. Rodríguez, & M. Fengou, "A Survey on Quantitative Risk Estimation Approaches for Secure and Usable User Authentication on Smartphones", *Sensors*, vol. 23, no. 6, pp. 2979, 2023. https://doi.org/10.3390/s23062979

[37] A. Wong, Z. Huang, X. Chen, & K. Wu, "ArtiLock: Smartphone User Identification Based on Physiological and Behavioral Features of Monosyllable Articulation", *Sensors*, vol. 23, no. 3, pp. 1667, 2023. https://doi.org/10.3390/s23031667

[38] M. Παπαϊωάννου, G. Zachos, Γ. Μαντάς, I. Essop, F. Saghezchi, & J. Rodríguez, "Outlier Detection for Risk-Based User Authentication on Mobile Devices", *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, pp. 2778-2783, 2023. https://doi.org/10.1109/globecom54140.2023.10437467

[39] A. Chakravarthy, P. Avadhani, P. Prasad, N. Rajeev, & D. Reddy, "A Novel Approach for Authenticating Textual or Graphical Passwords Using Hopfield Neural Network", *Advanced Computing: An International Journal*, vol. 2, no. 4, pp. 33-42, 2011. https://doi.org/10.5121/acij.2011.2404

[40] A. Chakravarthy, P. Raja, & P. Avadhani, "A Novel Approach for Pass Word Authentication Using Bidirectional Associative Memory", *Advanced Computing: An International Journal*, vol. 2, no. 6, pp. 123-135, 2011. https://doi.org/10.5121/acij.2011.2404

[41] R. Hasan, N. Jabr, & E. Kareem, “Password Authentication Based on Modify Bidirectional Associative Memory (MBAM)”, *International Journal of Recent Trends in Engineering & Research*, vol. 2, no. 2, pp. 261-267, 2016.