MINAR International Journal of Applied Sciences and Technology
ISSN: 2717-8234
Article type: Research Article

Received: 05/10/2023 **Accepted:** 01/11/2023 **Published:** 01/12/2023

THE LANDSCAPE OF AUTHENTICATION SYSTEMS: A COMPREHENSIVE SURVEY

Ehab Younis MOSTAFA [1]

University of Mosul, Iraq

Saja J. MOHAMMED[2]

University of Mosul, Iraq

Abstract

Nowadays, authentication systems are extremely important in many aspects of digital life. They help to protect personal and confidential data from unauthorized access. authentication systems are effective ways to prevent hacking and fraud attacks. Also, They are crucial in ensuring digital security and protecting sensitive data in our connected world. The authentication can be done in multiple ways, one of which is using a password, such system is called a password-based authentication system. Password is the basic and most common method of authentication. This paper overviews the authentication systems, types, and objectives and mentions each type's disadvantages, advantages, and problems. The paper then highlights the text password authentication system, its weak points, and attacks they are exposed to, in addition to developing means and methods to increase the strength of passwords so that they can overcome the attacks they face. The paper provides a good background for anyone who wants to start in this field, as it gives a detailed idea of the systems used, making it easier for the reader to choose the authentication system to desire.

Keywords: *Information Security, Authentication System, Authentication Mechanisms, Authentication Factors, Password-Based Authentication.*

http://dx.doi.org/10.47832/2717-8234.17.1

[1] ehab.22csp27@student.uomosul.edu.iq

[2] sj_alkado@uomosul.edu.iq

Introduction

In the present time, the use of the Internet for communication and getting information has permeated every aspect of our everyday lives. Customers are extremely concerned about their user authentication and data security as a result of the enormous growth in sensitive and personal information being collected and stored digitally [1][2][3][4]. Companies must be transparent about how they gather customer data and give customers a choice to manage their data [5]. Users are also concerned about data cracks. Sensitive information is accessed or stolen by unauthorized people, which results in data cracks. These cracks can severely affect customers, including financial loss and identity theft [6],[7]. As a result, organizations must implement strong security controls to safeguard user data, including access limits and encryption, and notify clients immediately in the event of a crack [8][9].

Sensitive information is protected online using various techniques like encryption, authentication, and regular data backups. A password is a combination of letters, numbers, and symbols used to authenticate a user, grant access to a resource, or establish a user's identity [8]. Poor password habits might make it easier for fraudsters and criminals to undermine the privacy of your personal information online [11]. Users frequently utilize poor password security procedures; as a result, their accounts may be open to attack [12].

Through the utilization of diverse authentication methods, individuals can be identified. During the authentication process of a security system, the database information provided by the user is subjected to verification. The user is granted access to the security system if the provided information corresponds with the data stored in the database [13],[14].

This paper aims to study most authentication techniques, focusing on password-based authentication, and discuss password strength vulnerabilities with possible solutions to make it more secure. Section 2 of the paper included the authentication mechanisms. The authentication factors are listed in section 3. The password-based authentication (strength of password-based authentication, vulnerabilities of used password-based authentication with solution, attacks on password-based authentication, and benefits and drawbacks of password-based authentication) are discussed in section 4, where the final section is the conclusion of this paper.

2. AUTHENTICATION MECHANISMS:

There are three various authentication mechanisms [15][16]:

2.1 Password Based Authentication:

The password-based authentication system is a method used to verify the identity of a user by requiring them to provide a password. It is one of the most common and widely used approaches for authentication in the digital world. There are two distinct approaches to password-based authentication: graphical passwords and alphanumeric passwords [17][18][19][20][21].

In any server-client relationship, the server maintains a record of alphanumeric passwords consisting of names and corresponding passwords. The server grants access when a particular name is found in the list, and the user provides the correct password. Our cognitive faculties are adept at efficiently processing and retaining vast visual information. The recollection of familiar faces visited locations, and witnessed events tends to be more effortless for individuals than memorizing a sequence of fifty characters, which might pose considerable challenges [22],[23].

Below is the list of the advantages, disadvantages, and issues of the password-based authentication method [24][25]:

Advantages

- There is no requirement for peripheral hardware because it can be implemented fully within software.
- It is possible to carry an ID/password via SSL encryption.

Disadvantages

- Passwords and IDs moving over networks are more vulnerable to "eavesdropping."
- Password guessing and replay assaults are possible.
- Inadequate password management and restrictions (such as re-issuing and unlocking).
- Insufficient user awareness and training.
- Trojan horses can obtain user names and passwords through deceptive means.
- It may be observed or stolen.

Issues

- Lifetime: To stop password guessing, passwords should be changed regularly.
- Ownership: Passwords must be used and owned by a single person, not shared by several people.
- Distribution: The distribution method, whether electronic or hard copy, should include safeguards against disclosure.
- Storage: Passwords can be kept in a physically isolated location accessible only by approved system components or stored encrypted.
- Entry: When users enter their password, the computer terminal should not show it.
- Transmission: When sending passwords over a network, encryption should be considered.
- Cost: It is inexpensive and simple to use. The number of users drives up costs when

issuing/registering users becomes a substantial administrative task and when specialized software is needed to manage the authentication process effectively.

- User operability: The user does not have to worry about additional hardware devices because the complete solution is implemented in software.
- Social acceptance: People are accustomed to using passwords and feel at ease with the authentication process.

2.2 Token-based Authentication:

Token-based authentication is a security mechanism that validates the identity of a user who wishes to gain access to a server, network, or other secure system. This validation process involves the utilization of a security token provided by the server. In addition to facilitating user queries, the service has the task of verifying the security token. Electronic devices commonly used for identification and authentication include smart cards, USB keys, mobile devices, and Radio Frequency Identification (RFID) cards. Each instance of device usage results in the generation of a novel password, enabling the utilization of a security token for establishing a connection with a computer or virtual private network. This is accomplished by inputting the password generated by the device into the corresponding prompt [15].

Token-based authentication systems have advantages, disadvantages, and issues, which can be summarized as follows [24][25]:

Advantages

- Users may easily access the token since they only need to memorize one PIN.
- Simplicity in administration since a single token replaces several passwords.
- Enhanced security since it takes the attacker's token and PIN to impersonate the user.
- Increased responsibility because tokens are observable.
- They are more portable than digital signatures.
- Well-developed solutions that have been widely adopted and deployed in the market
- Compliant with the thin client methodology, without any client-side software.
- Portability and mobility: Users may access the Internet using any browser-based connection since security is not dependent on a particular system.
- Independent of browsers.

Disadvantages

- In order to access Internet banking services, the client must always have a token card on them.
- It is necessary to change tokens every four years.
- The expense of ongoing operations for managing token cards.
- Since the client can only utilize the service once he receives the token card, there may be a barrier to customer acquisition.
- It takes longer to validate the user's identity since more steps are involved in the client authentication process.

Issues

- Vendor dependence: Reliance on a vendor to provide tangible token cards raises the possibility of losing hardware support in the future.
- Scalability: After 100,000 users, this method does not scale effectively.
- Distribution: It is important to consider how tokens are distributed to clients.
- Cost: One must consider the cost of developing a token system. The token itself is one of the extra expenses of adopting token authentication solutions.
- Accuracy: Tokens have a high degree of accuracy since the reasoning and approach used in this method have produced very reliable user authentication.
- User operability: For token authentication to be user-operable, the end user has to keep up with certain hardware. This extra hardware required may grow to be a hassle.
- Social acceptance: A drawback of the token is that some people will only accept it as a form of identification if they fear misplacing the gadget. The acceptability of such a gadget will be reduced if replacement is expensive and requires payment from the user.
- Product lifetime: Two aspects must be considered to evaluate the token authentication lifecycle. First off, tokens are often portable. Because of this, the expense of replacing lost, stolen, or misplaced tokens tends to shorten their lifespan. Secondly, technologies for token authentication are still developing.
- Ease of installation: Implementing a token authentication system into the existing computer environment can be time-consuming.
- Non-repudiation: The token scheme possesses a medium level of non-repudiation.

2.3 Biometric-based Authentication:

Biometric-based authentication is a security procedure that is dependent on the distinct biometric attributes of an individual, as seen in Fig. (1). This form of authentication

is employed for the purpose of regulating entry to both physical and digital resources, including but not limited to buildings, rooms, and computer equipment [15][26].

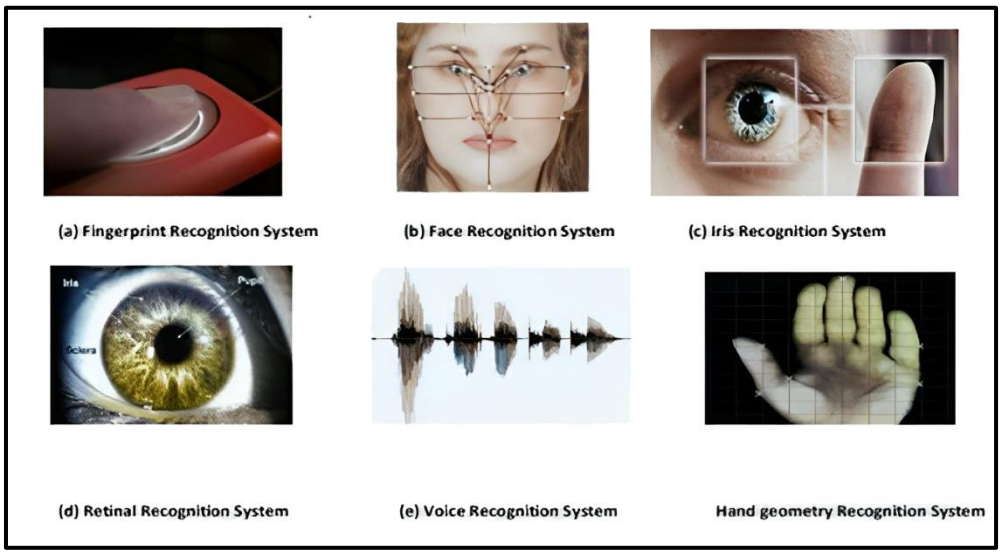

Figure 1. Types of biometrics [17]

Like any system, biometrics-based authentication systems have an advantages, disadvantages, and issues [24][25]:

Advantages

- Provides the highest level of security for user authentication because it is hard for someone to impersonate someone else physically.
- It is simple to use since it requires the user to show up in person and does not require them to carry tokens or know data.

Disadvantages

- Most systems need specific hardware input devices at every workstation.
- The individual can be impersonated if the physical reader is circumvented and biometrics information obtained from the scanning is input.
- Biometric devices are unreliable under abnormal circumstances (i.e., dirty fingers may bar biometrics authentication based on fingerprints).

Issues

• Physical variance: The relatively changeable nature of physical qualities and technical challenges in measuring and characterizing them might lead to certain issues when employing biometric sensors.

• Vendor interoperability: Most of the hardware and software sold today are incompatible with products from several suppliers.

• Costs Biometric: Gadgets are often pricey. Although biometrics systems are quite pricey initially, they only require a little upkeep or replacements throughout their lifetime.

• Accuracy: Since biometrics technology relies on a particular physical characteristic of each individual, it is optional to identify authorized system users while rejecting illegitimate users reliably.

• Operability: The biometrics method offers great convenience as it eliminates the user's requirement always to remember to carry a token. The lesser range of authentication speed counterbalances this high level of ease.

• Social acceptability: It is believed that biometrics have little social acceptance. This criterion varies depending on the kind of biometric device being used, as certain biometrics are thought to be invasive.

• Product life cycle: Regular upgrades to the host server are necessary to ensure appropriate levels of authentication are reached since some of an individual's physical attributes might change over time.

• Ease of installation: To use these devices, users must enroll in the system using a biometrics authentication technique.

• Non-repudiation: There is a high degree of non-repudiation with biometrics equipment. Since these gadgets are based on the distinct qualities of each individual, a user, for example, cannot deny that their fingerprint initiated a transaction.

3. UTHENTICATION FACTORS:

Three categories of authentication factors can be identified [27]:

3.1. Something you know:

Something the user is aware of includes passwords, passphrases, and Personal Identification Numbers (PINs). The most common type of authentication is passwords. The term "password" is a general term that might apply to passcode, passkey, or PIN. A string of characters called a password is used to verify a user's identity. It will be simpler for cyber-criminals to guess a user's password if this string of characters can be traced back to them (for example, if it contains their name, birth date, or address) [15][20][28].

3.2. What You Have:

Users may have items such as smart cards and security key fobs. As illustrated in Fig.

(2)، a smart card is a tiny plastic card roughly the same size as a credit card and has a tiny chip inserted inside it. The chip is an intelligent data carrier that processes, stores and protects data. Digital signatures, bank account numbers, personal identifying information, and other private data are all stored on smart cards. Smart cards include authentication and encryption to protect data [27].

Figure 2. A Credit card

3.3. Who You Are:

The term "biometric" pertains to a unique physical characteristic identifying a certain individual, such as a fingerprint, retina, or voice. In order to verify users, biometrics security checks physical traits against saved profiles. A profile is a data file that contains information about a person's known traits. If a user's traits fit preset criteria, the system authorizes access. A typical biometric device is a fingerprint reader. There are two distinct categories of biometrics identifiers [26][27]:

- Physiological characteristics - cover a range of biometrics identifiers, including fingerprints, Deoxyribonucleic Acid (DNA), facial attributes, hand anatomy, retinal patterns, and ear characteristics.

- Behavioral characteristics encompass various patterns of behavior exhibited by individuals, such as gestures, vocal attributes, typing rhythm, or even how a person walks.

The utilization of biometrics in consumer electronics, point-of-sale systems, and public security systems is experiencing a notable expansion. Implementing biometrics necessitates utilizing many components, namely a reader or scanning device, software for converting the scanned data into a digital format, and a database to store biometrics data for comparison [30].

4. Multi-factor Authentication:

Multi-factor authentication employs a minimum of two distinct verification procedures. A secure key fob serves as a prominent exemplification. The two elements encompass a tangible possession, such as a security key fob, and a cognitive component, such as a password. To enhance the level of security, it is recommended to use a fingerprint scan or any other form of biometrics authentication, hence augmenting the multi-factor authentication process [19][31].

Implementing multi-factor authentication can effectively reduce the incidence of online identity theft since it prevents cyber-criminals from gaining unauthorized access to user information solely through knowledge of the password. When accessing certain online platforms, such as an online banking website, users may be obligated to furnish a password and PIN obtained from their smartphone [32].

A security key fob is a compact gadget that can be conveniently affixed to a key ring, As illustrated in Fig. (3). A mechanism known as two-factor authentication is employed, which offers a higher level of security compared to the conventional method of relying just on a combination of username and password. Initially, the user provides a Personal Identification Number (PIN). Upon proper input, the security key fob will exhibit a numerical value. The second component is a need for the user to input to gain access to the device or network [27]. Table (1) explains the differences between the previous authentication factors.

Figure 3. Security key fob

Table 1. The differences between the previous authentication factors.

Differences	Single Factor Authentication	Two Factor Authentication	Multi-Factor Authentication
Verify the resources	There is only one way to verify the identity	There are two ways to verify the resources of the identity	More than two factors to verify the resources of the identity
Actions in Authentication	It is one action only, so it is simple and fast to access	There are two actions to complete the process. Simple and fast to access	It performs many actions to complete the authentication, So it is complex.
Security Level	Less security level	Mid security level	High-security level
User Performance	Less user performance	High user performance	High user performance
Access process	Very easy	Easy	Complex

5. Text Password-based authentication:

This mechanism has two components. The applicant must first enter their account and then their password. The password is the secret mixture of letters, numbers, and symbols the applicant knows [20][33].

A password should have at least eight characters [34],[35]. Users should only use a password that is shorter to remember or, on the other hand, too short to make it susceptible to password cracking. Upper- and lowercase letters, digits, and special characters should all be in your password. Users must employ distinct passwords for different systems, as compromising a user's password by a malicious actor would grant unauthorized access to all user accounts. The utilization of a password manager can facilitate the creation and recollection of robust passwords [36].

Service providers frequently need to improve their practices regarding securely storing user credentials. For instance, passwords are commonly saved in plain text or with insufficient protection [37].

The level of clarity about the confidentiality of user passwords by service providers is generally still being determined. Furthermore, there is a risk that a service provider, acting maliciously, could exploit a user's password to assume that user's identity across other service providers. For example, an online service provider can extract user credentials directly from the login page by capturing keystrokes [38], thereby acquiring access to all passwords supplied by the user. In addition to serving as a means of identification, passwords are employed to encrypt data, which can afterward be stored in contexts lacking trustworthiness [39]. It is crucial to note that password-based authentication mechanisms must not disclose passwords to prevent storage providers from accessing encrypted data [40].

5.1. Strength of Text Password-Based Authentication:

Longer passwords are extremely difficult to crack, which is one of their strengths. It is crucial to use strong passwords whenever using passwords. A strong secret key combines capital letters, lowercase letters, digits, and distinctive characters. Security experts now advise using passwords with 12 characters or more [1].

5.2. Vulnerabilities of Text Password-Based Authentication:

Since the user enters the password, as illustrated in Fig. (4), password sniffing is the largest issue. An attacker can sniff the password at many points in the communication process. Even if the password is secure, the attacker can still readily figure it out [32]. The human factor, a significant issue with user names and passwords, is [14]:

- Passwords are easy to guess or search if easy to remember.
- Passwords are easily stolen if written down.

- Users may share passwords.
- Passwords can be forgotten if they are difficult to remember.

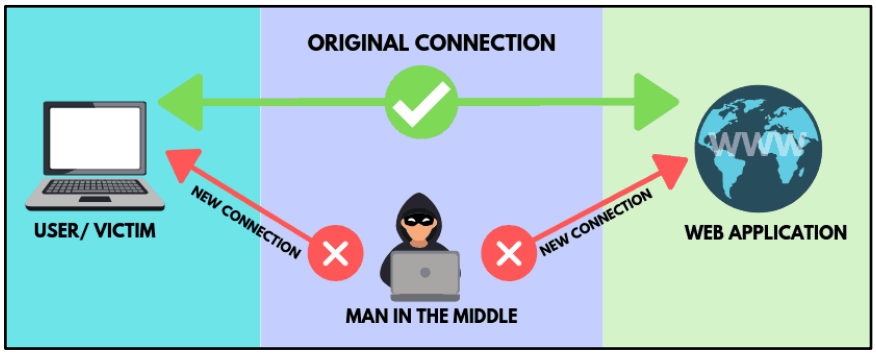

Figure 4. Password Sniffing

By applying the brute force technique with a less robust password, unauthorized individuals can effortlessly gain entry into the system. Most access control systems typically permit using passwords consisting of eight characters. The strength of a password is influenced by three variables: length, cardinality, and entropy. A password with a cardinality of 94 was generated utilizing a collection of 94 characters, encompassing a variety of capital letters, lowercase letters, digits, and special characters, allowing for any possible combination. The concept of entropy is utilized to quantify the computed bit strength of a password. For example, a password consisting of eight characters, each chosen from a set of 94 possible characters, has an entropy value of 52.4 bits. A normal personal computer can employ a brute force attack to crack a password consisting of 94 potential combinations within 20 minutes. With the assistance of supercomputers, the cracking process is estimated to require 0.07 seconds. An 8-character password possessing 52.4 bits of entropy can be considered inadequate. One additional outcome of social engineering involves the manipulation of users, leading them to access an alternative website. After that, the perpetrators illicitly acquire their usernames, passwords, and other sensitive personal data [41].

5.3. Recommended Solution of Text Password-Based Authentication:

The most valuable recommendation is to utilize more robust passwords. In order to enhance security measures, users must adhere to a more stringent password policy, necessitating the submission of passwords with a minimum length of 12 characters and a total number of possible combinations (cardinalities) up to 94. Individuals should be cautious while refraining from including personal information or commonly used words in their online communications.

To provide privacy and prevent visual access to your documents or keyboard, it is advisable to employ physical barriers such as using your body or cupping your hand to obstruct the line of sight while attending to olfactory stimuli on your shoulder. To mitigate the risk of social engineering, it is advisable to take measures to deter and counteract suspicious unwanted phone calls and emails. It is imperative to exercise vigilance when

encountering URLs that appear anomalous. Implementing firewalls and antivirus software to enhance cyber-security measures is recommended. Another alternative is the utilization of graphical passwords, which offer enhanced security compared to traditional text-based passwords. The user demonstrates a conscious endeavor to commit a password composed of text to memory. The graphic password authentication procedure entails the selection of images from a predetermined list, specifically images numbered. Implementing restrictions on the number of attempts allowed for password entering is expected to enhance security [14],[42].

5.4. Attacks of Text Password-Based Authentication:

The utilization of passwords can give rise to several security issues. There are multiple concerns about the security of passwords. These security concerns can be outlined in the following manner [43][44]:

- **A surfing attack** - is a malicious activity in which perpetrators covertly observe a user's online activities to acquire sensitive account information. The theft can be perpetrated by utilizing several tools, such as a webcam, monitoring a user's keystrokes, or surreptitiously observing the user's surroundings. One method employed by malicious actors is a dictionary attack, wherein the perpetrator attempts to get unauthorized access by systematically inputting many words, often sourced from a dictionary or similar word list.
- **Guessing attack** - With the user's data, such as name, date of birth, pet name, etc., hackers would attempt to guess the user's password.
- **Phishing** is the fraudulent practice in which an individual assumes a false identity to deceive a user into engaging in potentially hazardous activities. An example occurs when a user is presented with an email soliciting personal information purportedly from an authoritative representative of Apple, even though an official did not dispatch the communication from Apple. The message was sent by another entity known as "authorized Apple."
- **Eavesdropping**- refers to the unauthorized interception and surveillance of personal information by a perpetrator who covertly listens in on a user's conversation.

6. Conclusion:

Authentication systems are at the heart of modern digital security, serving as the bedrock for protecting data, verifying identities, and ensuring safe online interactions in an increasingly interconnected world. Authentication-based password systems remain a crucial component of authentication systems due to their familiarity, accessibility, and cost-effectiveness. However, user behavior and the implementation of best practices greatly influence their security effectiveness. Text password-based authentication systems hold particular importance in today's digital landscape for many reasons, such as User Control, cost-effectiveness, Initial Security Layer, User Familiarity, etc. For these reasons, the researcher advises using a strong text password to ensure data authentication, at least as the first level of security.

7. References

[1] . Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. *International journal of scientific & technology research*, *5*(11), 246-249.

[2] . Mohammed, S. J., & Taha, D. B. (2021). From cloud computing security towards homomorphic encryption: A comprehensive review. *TELKOMNIKA (Telecommunication et al.)*, *19*(4), 1152-1161.

[3] . Shantha, R., Mahender, K., Jenifer, A., & Prasanth, A. (2022, May). Security analysis of hybrid one-time password generation algorithm for IoT data. In AIP Conference Proceedings (Vol. 2418, No. 1). AIP Publishing.

[4] . Al-kateeb, Z. N., & Mohammed, S. J. (2020). A novel approach for audio file encryption using hand geometry. Multimedia Tools and Applications, 79(27-28), 19615-19628.

[5] . Tuan, T. N. (2023). Corporate Social Responsibility in Protecting the Right to a Private Life. In-Laws on Corporate Social Responsibility and the Developmental Trend in Vietnam (pp. 205–219). Singapore: Springer Nature Singapore.

[6] . Zulfahmi, M., Elsandi, A., Apriliansyah, A., Anggreainy, M. S., Iskandar, K., & Karim, S. (2023). Privacy protection strategies on social media. Procedia Computer Science, 216, 471-478.

[7] . Karale, A. (2021). The challenges of IoT address security, ethics, privacy, and laws. Internet of Things, p. 15, 100420.

[8] . Sharma, V., Saharan, R., Wilson, K., Sharma, D., Beniwal, S., & Dora, C. P. (2023). Privacy and Security Challenges in the Era of the COVID-19 Pandemic. In Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services (pp. 287–308). IGI Global.

[9] . Ravi, S., David, A., & Imaduddin, M. (2018). Controlling calibrating vehicle-related issues using RFID technology. International Journal of Mechanical and Production Engineering Research and Development, 8(2), 1125-1132.

[10] . Liu, Z., Hong, Y., and D. Pi, D. “A Large-Scale Study of Web Password Habits of Chinese Network Users.” JSW, vol 9, no 2, pp. 293-297, 2014.

[11] . E.H., Spafford, "Preventing Weak Password Choices," Computers & Security, vol.11, no 3, pp. 273-278, 1992

[12] . R.Wash, E, Rader, R. Berman, R., and Z . Wellmer, "Understanding password choices: How frequently entered passwords are re-used across websites," Twelfth Symposium on Usable Privacy and Security, SOUPS, pp. 175–188, 2016.

[13] . Webopedia, "Authentication," 2016. [Online]. Available: http://www.webopedia.com/TERM/A/authentication.html. [Accessed 1 October 2016].

[14] . H. Abie, "semanticscholar," 12 12 2006. [Online]. Available: https://pdfs.semanticscholar.org/3733/2607f7a7ac8284c514845957fd00583e5614.pdf. [Accessed 1 October 2016].

[15] . S.Rajarajeswari, Ms.A.Maria Stella, " A review of authentication and authorization methods, "International Journal of Computer Science and Information Technology Research

ISSN 2348-120X (online) Vol. 7, Issue 3, pp: (78-83), Month: July - September 2019, Available at: www.researchpublish.com.

[16] . Singla, D., & Verma, N. (2023). Performance Analysis of Authentication System: A Systematic Literature Review.

[17] . Masri, I. H., Siswantyo, S., & Mardhiyah, S. (2022, December). Formal Analysis and Improvement of Zero-Knowledge Password Authentication Protocol. In 2022, the 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI) (pp. 14-18). IEEE.

[18] . Dias, N. I., Kumaresan, M. S., & Rajakumari, R. S. (2023). Deep learning-based graphical password authentication approach against shoulder-surfing attacks. Multiagent and Grid Systems, 19(1), 99-115.

[19] . Iyanda, A. R., & Fasasi, M. E. (2022). Development of Two-factor Authentication Login System Using Dynamic Password with SMS Verification. International Journal of Education and Management Engineering, 12(3), 13.

[20] . Singh, M., Nedungadi, V., & Radhika, R. (2023, April). A Hybrid Textual-Graphical Password Authentication System with Enhanced Security. In 2023 International Conference on Networking and Communications (ICNWC) (pp. 1-7). IEEE.

[21] . Jadhao, P., & Dole, L. (2013). Survey on authentication password techniques. International journal of soft computing and Engineering (IJSCE), 3(2), 67-68.

[22] . L.Sobrado and J.C. Birget, "Graphical Passwords," The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002,

[23] . G. E. Blonder. Graphical passwords. United States Patent5559961, 1996.

[24] . Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review of authentication methods. Australian Journal of Basic and Applied Sciences, 7(5), 95-107.

[25] . Marily n Chun, Global Information Assurance Certification Paper, SANS Institute (2002), https://www.giac.org/paper/gsec/594/authentication-mechanisms-best/101431

[26] . Mohammed, S. J. (2017). Using biometric watermarking for video file protection based on chaotic principle. International Journal of Computer Science and Information Security (IJCSIS), 15(12), 201–206.

[27] . Dastane, D. O. (2020). The effect of bad password habits on personal data breach. International Journal of Emerging Trends in Engineering Research, 8(10)

[28] . Desale, H., Korde, S., Mahadik, D., & Aryan, V. TEXT–GRAPHICAL PASSWORD AUTHENTICATION SYSTEM.

[29] . Ghosh, P., & Dutta, R. (2012). A new approach towards biometric authentication system in palm vein domain. Copyrights© 2012 Votrix Publication (team. ijaiti@ Gmail. com).

[30] . Belhadj, F. (2017). *Biometric system for identification and authentication* (Doctoral

dissertation, Ecole nationale Supérieure en Informatique Alger).

[31] . Cybersecurity Essentials v1.1 https://btu.edu.eg/wp-content/uploads/2020/03/Chapter-4-The-Art-of-Protecting-Secrets.pdf

[32] . Awasthi, A. (2015). Reducing Identity Theft Using One-Time Passwords and SMS. EDPACS, 52(5), 9–19.

[33] . Pandey, K., Singh, A., Anand, A., Kaushik, A., & Gupta, S. N. (2023, January). Enhancement of Password Authentication System Using Vector (Graphical) Images. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 255–260). IEEE.

[34] . Jadhao, P., & Dole, L. (2013). Survey on authentication password techniques. International journal of soft computing and Engineering (IJSCE), 3(2), 67-68.

[35] . Marquardson, J. (2012). Password policy effects on entropy and recall: Research in progress.

[36] . Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J. H. (2017, December). Analysis of the security and use of password managers. In 2017, the 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT) (pp. 17-24). IEEE.

[37] . E. Bauman, Y. Lu, and Z. Lin, “Half a century of practice: Who is still storing plaintext passwords?” in ISPEC, 2015, pp. 253–267.

[38] . Zeidler, C., & Asghar, M. R. (2018, August). AuthStore: Password-based authentication and encrypted data storage in untrusted environments. In 2018, the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 996-1001). IEEE.

[39] . C. Zeidler and M. R. Asghar, Towards a Framework for PrivacyPreserving Data Sharing in Portable Clouds, Cham, 2017, pp. 273–293

[40] . G. Van Laer, R. Dasgupta, A. Patil, and M. Green, “Harden zero knowledge password proofs against offline dictionary attacks,” 2016.

[41] . Wikipedia, "Social engineering (security)," [Online]. Available: https://en.wikipedia.org/wiki/Social_engineering_(security). [Accessed 1 October 2016].

[42] . M. Farik, "Algorithm to Ensure and enforce Brutce force attack resilient password in routers," Algorithm to Ensure and enforce Brutce force attack resilient password in routers, vol. 4, no. 10, p. 5, 2015.

[43] . Scaria, B. A., & Megalingam, R. K. (2018, June). Enhanced E-commerce application security using three-factor authentication. In 2018, the Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1588-1591), IEEE.

[44] . Malau, h., & yovira, v. (2022). Review of text-based password and other authentication methods for e-commerce data protection. Journal of Theoretical and Applied Information Technology, 100(6).