Exploring Authentication Techniques: A Comprehensive Review

Dalal N. Hammod [1]
Dalal.naeem@nahrainuniv.edu.Iq
daL-scin81@yahoo.com

Reem Hussain Ali [2]
reem.msco23@ced.nahrainuniv.edu.iq

Abstract: E-commerce represented one of various new technologies that triggered with development of the internet. This causes the security aspect of e-commerce to be one of important factors, especially to prevent unwanted things such as data leaks and financial losses. Authentication is a critical aspect of securing digital systems and protecting user data. This paper reviews and compared three primary authentication methods: single factor authentication (SFA), two-factor authentication(2FA), and multi-factor authentication (MFA). SFA, the simplest method, relies on a single layer of security, such as passwords or PINs, but is highly vulnerable to modern cyber threats. 2FA enhanced security by combining two distinct factors, such as a password and One-time password (OTP), reducing the risks of credential theft. MFA further strengthens authentication by incorporating multiple layers, including biometric and contextual elements, making it the most secure approach but also the most complex and resource intensive. The discussion highlights the trade-offs between these methods in terms of security, usability, scalability, cost, and risk mitigation. While SFA may suffice for low-risk applications, MFA is essential for environments requiring robust security. The study conclude that the choice of authentication method should depend on a specific use case, balancing security needs with user convenience and organization resources.

Keywords: Authentication, single factor authentication, two-factor authentication, multi-factor authentication, One-time password**.**

[1]Assist. Prof., Computer Science Department, College of Science, Nahrain University, Baghdad, Iraq
[2]M.Sc. Student, Computer Science Department, College of Science, Nahrain University, Baghdad, Iraq

1. Introduction

In today's digitally thriving world, organizations and businesses use advanced security systems to keep information safe from external threats by relying on authentication methods, and organizational data is vulnerable to cyberattacks such as unauthorized access and execution of malicious tasks within the system that can be harmful and break the chain of trust between the client and the service provider. This is managed using password policies, authentication, user-defined roles, and user account management. The first part, identity management, deals with the identity of the user while access management deals with providing and revoking user access [1][2] while the second part, authentication can be defined as the process of confirming the identity of the user to determine his/her authority to enter. If the user is trusted, the server allows access to its assets. Many authentication techniques and protocols are available for the purpose of protecting the server assets from unauthorized access. So, in this research paper, the problem of identity theft will be addressed, so we need to verify the identity before allowing the person by showing the most popular methods used in identity verification. [3] There is another definition of authentication, is an essential method for protecting against unauthorized access to a device, data or service, whether the implementation in two ways online or offline.[4]. Research in authentication has shown that passwords are weak, insecure, and not widely trusted. Despite efforts to find alternatives and reduce their complexity, there is still a lack of optimal solutions. To progress, intelligent technologies should be used to combine multiple authentication mechanisms and adapt their use to various situations. Several methods of authentication have emerged to choose from [5]. These are:

- Traditional username and password. This is usually the first factor for authentication.
- One-time password (OTP). This is a second factor in multi-factor authentication and is very common. It requires users to first enter a short code that is sent to them via email or text message, thus verifying their identity.
- Security questions are also used as a second factor with pre-defined answers.
- Document centralization. Users may be asked to upload a photo of themselves along with their passport or ID, confirming that they are the true owner of the identity. This method is commonly used in exams and job applications.
- Biometrics. This method is considered the most secure form of authentication because forging biometric data is not easy, if not very difficult. Forms of biometric authentication include: Facial recognition, Retina scanning, Fingerprint scanning, Voice recognition, Behavioral biometrics (speech and writing patterns, etc.) [6] [7] [8].

Finally, the aim of the research paper is to review the three methods of authentication, with reviews of the benefits and drawbacks of each method to clarify which of the methods is appropriate according to each user's opinion. This paper can be divided into six sections. Section two explains the types of authentications, section three presents related works, section four presents and discusses the results, section five presents conclusions and section six presents reference.

2.Authentication Types

There are many classifications for authentication types:

2.1 Authentication types based on information used

Authentication has three main types; each type depends on the different data or information that used to verify the identity of a user or system. The three important of authentication types are:

- Something you know: This is knowledge of a specific piece of information, such as a password.
- Something you are: This factor includes biological characteristics, such as fingerprints, face, and many other biometric data.
- Something you have: This factor includes owning a physical device or token, such as secure ID, a phone or cryptographic secret key. [3] [9] [10] [11]. The following Figure 1. shows the three common authentication type.

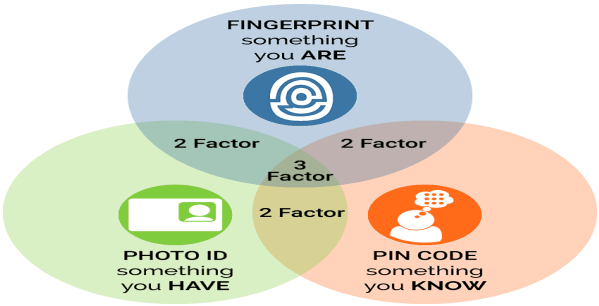

Figure 1: Authentication types based on information used [2] [3]

2.2 Authentication types based on number of Factors

In today's digitally connected world, user authentication is one of the key factors to ensure the security of transmitted data. Although the definition of authentication has not changed, the password is no longer the only factor. Two-factor authentication (FA) and multi-factor authentication (MFA) have been proposed to enhance security by adding additional layers, which are typically based on knowledge, biometric ownership, or user behavior. These factors will be explained below. [12]

2.2.1. One-factor authentication or (SFA) is the most widely used technique and is a combination of a username and a password (see Figure 2.). The password has been in use for a very long time and is considered the traditional method of one-factor authentication. One-factor authentication is very vulnerable to automated attacks, because people tend to reuse the same password in multiple places, or use default passwords. [13]

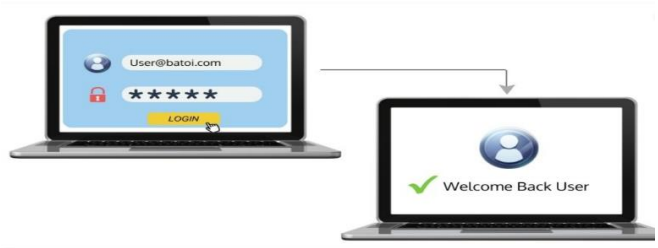

Figure2: Single factor authentication. [14]

2.2.2. Two-factor authentication (2FA) has been found to increases security by using a combining of representative data (username/password combination) with another form of identification such as a personal property factor that may include a secure token that uses a one-time password (OTP). Implementing this authentication method requires an additional mechanism that may include an electronic device such as a mobile phone, tablet, computer, or a physical component (see Figure 3). After completing the first stage of authentication, the second mechanism or an OTP sent via email, SMS, or another device is used. [4] [15]

Figure3: Two factor authentication [14]

2.3. Multi factor authentication (MFA) is becoming increasingly common due to the increasing threat of unauthorized access, particularly in banking and personal data platforms. MFA such as combines unique biological characteristics like fingerprints or iris scans to provide increased security. This approach helps protect computer equipment and other vital services from unauthorized access. For example, Automated

Teller Machine (ATM) can be made more secure by adding an additional biometric mechanism, such as a physical token for ownership and a PIN for knowledge. To address this, MFA is becoming increasingly more common (See figure 4). [4] [14].

Figure 4: Multifactor authentication [14]

Authentication in this figure, including passwords, smart cards, and biometrics, is crucial in information systems. While biometrics offer security, fingerprints have weaknesses. Combining multiple biometrics and digital certificates can enhance security, addressing future vulnerabilities. [4] [15]. Table (1) shows Advantages and Disadvantages for each type of the Authentication. [4] [17]**.**

Table 1: Advantages and Disadvantages for each type of the Authentication. [4] [16]

3. Related Works

Authentication Type	Advantages	Disadvantages
Single factor authentication (SFA)	• Simple and easy to use. • Widely utilized, especially passwords (Pins, Passwords can be a combination of letters, numbers, and symbols, which increases their strength. • Effortless, High acceptance.	• Can be passed on, easily forgotten
Two-factor authentication (2FA)	• improving security if the password is stolen, the attacker still needs access to the second authentication factor (e.g., smart device or token). • Cheap, Simple deployment • Enhances overall security without significantly complicating usability.	• Loss and theft • Requires extra hardware, adding to the cost. • If either authentication factor is unavailable (e.g., no device access), even authorized users cannot access their accounts. • Connectivity issues with smart devices can disrupt the process
Multi-factor authentication (MFA)	• Combines multiple factors, such as biometrics to improve identity verification, security, reliability, especially for user experience. • Scalable and suitable for various scenarios (e.g., Massive Open Online Courses (MOOCs), and medical records). • Unique unforgettable.	• Biometric authentication has issues, including ease of use and accuracy. • Variability in biometric data can cause issues with low-quality equipment. • Costly, additional hardware required and invasive.

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. [16] [17]. Many previous authors have studied the term authentication in its various forms, which are:

3.1 Related Works about Single Factor Authentication:

In [18] author focuses on used biometric fingerprint recognition for authentication. The system is designed for use in smart door access and can be installed in high-security areas such as defense offices, ICUs (Intensive Care Units), CCUs (Child Care Units), and research laboratories. The fingerprint recognition system uses the R305 fingerprint sensor, which captures and stores unique fingerprint images. However, it can be inferred that the system uses standard fingerprint matching techniques to authenticate users. The system relies on fingerprint biometrics as the main factor for authentication. In [19] author used is biometric fingerprint recognition for enrollment, verification, and identification. The system is proposed for use in government services such as bill payments (electricity, telephone), income tax returns, and other administrative tasks. It can also be applied in organizations to improve security and operational efficiency. The paper mentions the use of fingerprint recognition algorithms. The system primarily relies on fingerprint biometrics as the unique factor for authentication. In [20] author focuses on creating passwords that resist brute-force attacks, and the key factors mentioned for strong password creation are: Length, Cardinality, Entropy. These are the factors used to ensure passwords are resistant to brute-force attacks. Information Used It's Something You Know (Password-based Authentication): The authentication method is based on the password that a user knows. The password is derived using an algorithm that ensures resistance to brute-force attacks. In [21] author write about Reviewing authentication and authorization mechanisms and the paper explores how systems verify user identity and the process of authorization for granting access and it was mentioned Cybercriminals seek to illegally access other users' accounts to exploit the privileges and services that others have paid for. Therefore, strong and effective authentication methods are crucial for ensuring secure digital transactions. The username and password method, while simple, practical, scalable, and easy to implement, remains the most widely used and need to highlighting for enhanced security measures. In [22] author Focuses on passwords that are easy for humans to remember but might be vulnerable to attacks. Even with complex password creation rules, human-memorable passwords can still be vulnerable to "smart-dictionary" attacks. These are passwords designed to be easily remembered by users, often involving common word patterns and linguistic elements. algorithm enumerates the remaining password space efficiently, applying time-space tradeoff techniques to minimize memory accesses and speed up the attack.

3.2. Related Works about Two Factor Authentication:

In [23] author purposed Biometric Authentication: Utilizes first Knowledge Factor That refers to the traditional username and password combination and second Behavioral factor as unique biological characteristics to identify and authenticate users. In this case, the method is keystroking dynamics, which analyzes the timing patterns of keystrokes Keystroke Dynamics Algorithm: This algorithm captures the unique patterns in how a user types, including the timing of keystrokes and the duration of key presses. It is designed to work without additional hardware, relying on software to gather data during user interaction. The algorithm demonstrated an impressive accuracy rate of 99.5%. The authors suggest that expanding the training dataset could further improve accuracy. the algorithm was trained using the "BeiHang Keystroke Dynamics Database. "Testing was conducted on another
dataset, "Stonybrook Keystroke Patterns as Prosody in Digital Writings," to validate the algorithm's effectiveness. Simulation: A two-factor authentication simulation was developed, incorporating the keystroke dynamics method. In [24] author introduces DRAW-A-PIN, a user authentication system designed for touchscreen devices, where users authenticate themselves by drawing their PIN (Personal Identification Number) on the screen, instead of typing it. This approach aims to enhance security by incorporating behavioral biometrics—distinctive traits in how users draw their PIN—as an additional factor beyond just the secrecy of the PIN. The system is designed to be both secure and user-friendly, leveraging users' familiarity with PINs. The system uses the PIN itself as one factor and the behavioral traits (how the user draws the PIN) as a second factor. The system was tested on Android phones with 3203 legitimate finger-drawn PIN samples and 4655 forgery samples. The system achieved an EER of 4.84% in the shoulder surfing scenario, where an attacker already knows the PIN. And rejected attackers 85% of the time in the

case of an attack where the PIN was known, and the attacker had an exact animation of the PIN being drawn. The system of author uses an authentication algorithm based on the user's drawn PIN and the behavioral characteristics of how the PIN is drawn. In [25] author Used Two-factor authentication (2FA) [OTP (One-Time Password) generated dynamically and sent via SMS]. The system was tested using the OAU e-portal login system as a case study. The system generates dynamic passwords (OTPs) using an algorithm that ensures each password is unique and expires immediately after use. The system utilizes an SMS gateway service (EbulkSms) to deliver the OTP to users. The OTP generator ensures that the same password is never reused by removing it from the database after use and The system's effectiveness was evaluated by ensuring that OTPs were unique and never repeated. During testing, the OTP generator successfully produced unique OTPs for different users, and the overall process from request to OTP delivery took less than a second and was found to be operational, functional, and more secure than the traditional single-factor authentication. The system uses two factors for authentication Static factor: Username and password (traditional authentication) and Dynamic factor: OTP sent via SMS (second layer of security).In [26] author used Password manager (automatically handles and generates strong passwords) and Fingerprint recognition (biometric authentication) depend on Password Management Algorithm that Utilizes a secure algorithm to generate strong, unique passwords and stores them securely within the app and Fingerprint Recognition Algorithm that Leverages established biometric algorithms to authenticate users based on their fingerprint. Author Evaluate Fingerprint Accuracy by using the False Acceptance Rate (FAR) and False Rejection Rate (FRR). High-quality sensors are expected to exhibit low FAR and FRR, ensuring reliable authentication. The strength of the generated passwords is measured using entropy calculations to ensure the passwords are robust against common attacks. In [27] author uses Two-Factor Authentication (2FA) with Honeytokens. The system combines traditional 2FA (Google Authenticator) with honeytokens to increase security by confusing attackers with decoy data. Honeytokens (or honeywords) are generated as decoy passwords that look real but are fake. If an attacker tries to use these honeywords, the system detects the intrusion. The system uses the Google Authenticator app to generate time-based one-time passwords (OTPs), providing the second factor of authentication. The system improves security by making it more difficult for attackers to succeed, particularly against SIM swapping attacks. The system's effectiveness will be tested by integrating the 2FHA mechanism into environments like banking and healthcare organizations, which are common targets for cyberattacks. These organizations already use OTP systems, so the 2FHA mechanism will be evaluated to assess its added value in enhancing security. [28] This paper addresses the issue of user authentication on the internet, where traditional methods like static passwords are commonly used but have limitations. Biometric methods are a promising alternative, but the sensitivity of biometric data requires effective protection. The paper proposes an original method for generating one-time biometric templates, mitigating replay attacks (where attackers retransmit intercepted user identity data). The method utilizes deep learning for feature extraction from biometric data (e.g., faces and fingerprints), followed by biohacking (a cancelable biometric technique). Additionally, cryptographic hashing and symmetric encryption are used to ensure that the generated template is non-repayable. The proposed solution is flexible and can be applied to any biometric modality. The authors tested the scheme on face and fingerprint databases, achieving good performance in both identification and authentication contexts. This method provides enhanced security and privacy by design, ensuring protection against replay attacks while allowing service providers to perform the identity verification.

3.3. Related Works about multi-Factor Authentication:

In [29] The study uses a convolutional neural network (CNN) architecture for multi-factor authentication, incorporating three input factors: a face image, a password image, and a user-specified auxiliary image. The CNN learns from all factors simultaneously using feature-level concatenation. The proposed CNN-based multi-modal MFA system achieved an accuracy of 99.6% during experiments, indicating high reliability in the authentication process. Testing criteria focused on measuring the system's accuracy in correctly authenticating users. In [30] The study presents a two-layer security framework for online financial transactions, integrating multi-factor authentication that include Layer 1 (username–password, OTP, face recognition and fingerprint) were deployed in the MFA model to authenticate users and machine

learning, while Layer 2 uses machine learning to detect potential fraud. Classifiers tested include Logistic Regression, Decision Trees, Random Forest, and Naive Bayes. The study achieved accuracies of 97.938%, 97.881%, 96.717%, and 92.354% for each classifier. In [31] The author produces in this study a lightweight multi-factor authentication (MFA) protocol for securing smart homes based on Physical Unclonable Functions (PUFs). The method includes (ProVerif Tool was used for formal security analysis of the protocol and used it for verifying security properties of cryptographic protocols and PUF-Based Authentication it used in the protocol is based on Physical Unclonable Functions (PUFs), which provide unique identifiers for devices and are resistant to counterfeiting and ProVerif was used for formal analysis of the security of the protocol. In [32] The paper include study about design science methodology to develop and prototype the enhanced multi-factor authentication (MFA) scheme. Different development environments were utilized to prototype three schemes and evaluate them against established schemes using AppDynamics and Datadog Application Measurement (APM) tools for effectiveness evaluation. The algorithms for these modalities are typically those found in biometric authentication systems and OTP generators and this study include discusses the integration of multiple modalities of authentication, which suggests that various algorithms related to fingerprint or facial recognition, location triangulation, and possibly time-based OTP generation are employed such as Image capturing in MFA systems typically involves the use of computer vision algorithms and image recognition techniques. include (Facial Recognition algorithms (e.g. Local Binary Patterns, Histograms) and Optical Character Recognition for extracting information from images (e.g., ID cards), Geolocation Algorithms may be used for geo-fencing and location verification. In [33] This paper discusses a novel authentication method combining fingerprint hash codes, passwords, and OTP (One-Time Password) for improved security. It addresses the vulnerability of fingerprint biometrics, which are static and difficult to change once compromised. The method uses a fingerprint hash code generated by applying the MD5 hash function and Euclidean distance for security. The system employs Gabor filtering for fingerprint feature extraction and integrates it with password and OTP for multifactor authentication. This approach enhances security by combining multiple authentication factors. The model is implemented in MATLAB2015a and is not based on a client-server architecture but as a client-side process where fingerprint images are processed locally before being sent to the server for further verification. The paper also mentions the use of ABCD analysis to evaluate the proposed system's performance. In [34] author used method of a three-factor authentication protocol for securing mobile devices This method is designed to meet the requirements set forth by the European Commission regulations, which emphasize the use of at least two authentication factors from different categories for strong user authentication. The protocol combines three factors of authentication—Knowledge, Possession, and Inherence—to provide secure user authentication. the first factor of authentication is user provides a password or PIN. In second factor The system checks whether the user possesses the required device, such as a smartphone, or an authentication token and third factor The user provides a biometric input such as fingerprint recognition, facial recognition. The following Table .2 summarizes related work.

Table 2: summarizes related work depend on their references.

Ref.	No. of Factor	Method used &Algorithm used	objective of research	Pros of research	Negatives of research
[18]	Single Factor Authentication	The system relies on fingerprint biometrics as the main factor for authentication. system uses the R305 fingerprint sensor	This confirms its preference over the traditional method of identifying what you have such as, the use of password, a smartcard etc.	It helps to make troubleshooting easier. An alarm circuitry is provided to warn about an unauthorized use. This increase security of this system.	Not mentioned
[19]	Single Factor Authentication	The system primarily relies on fingerprint biometrics as the unique factor for authentication, based on the features of the fingerprint patterns.is biometric fingerprint recognition for enrollment, verification, and identification.	make automated system based on biometric fingerprint authentication.	help to achieve this objectives like security, efficiency, reliability	The system is exposed to fraud and forgery, and requires reliance on devices, and there are privacy concerns.
[20]	Single Factor Authentication	Enforcing strong password conditions (length, cardinality, entropy). A custom algorithm designed to enforce the above conditions for strong, brute-force resistant password.	develop and test an algorithm to ensure and enforce passwords in routers that are resistant to brute-force attack	enhanced functionality to enforce entry of only strong passwords.	Not mentioned
[21]	Single Factor Authentication	• Password Storage: Hashing is used as the method for storing passwords securely. • Password Cracking: Various methods, such as dictionary attacks and brute force attacks, are utilized to break passwords. • Network Defense: Multiple defenses are explored to guard against attacks, with analysis on their ease of implementation and effectiveness. • Distributed Security Testing: The Witch-DOCtoR framework is used for cooperative distributed testing of network security.	Study and analysis of password-based authentication techniques, focusing on the effectiveness of the methods by evaluating protection methods against brute-force attacks.	Using strong passwords with a combination of defenses (such as Using strong passwords with a combination of defenses (such as delays, limiting the number of attempts, and whitelists) has proven to be more effective than simpler methods.	Not mentioned
[22]	Single Factor Authentication	Markov modeling and efficient enumeration for password search.	Analyzing and studying the methods of creating passwords by human users to design passwords that are both easy and memorable.	Balancing ease of remembering and security	Passwords are vulnerable to guessing because they rely on known human patterns. The attack is easier if the attacker knows the password policy, which reduces the effectiveness of the password in terms of randomness. There are no field studies on actual users to confirm their ability to remember the suggested passwords according to the guidelines.

[23]	Two Factor Authentication	• Keystroke Dynamics (biometric factor based on typing patterns). • Username and Password (traditional authentication method).	Testing and analyzing biometric authentication algorithms in web applications, using keystroke dynamics (KD) as a method that is effective and does not require additional hardware, has also been demonstrated. Researchers have also implemented and simulated this method on real data to improve the accuracy of identity verification.	It doesn't require additional hardware such as a fingerprint, making it more suitable for large-scale web applications. Biometric features are invisible and stealable. It achieved very high authentication accuracy, reaching 99.5% in experiments	Natural variations in user behavior affect authentication accuracy, such as changes in typing due to fatigue or stress. Storing biometric data poses privacy concerns. Even if it is not visible, storing it opens the possibility of misuse.
[24]	Two Factor Authentication	• The PIN itself (traditional numeric PIN). • Behavioral Biometrics (unique drawing patterns, such as pressure, speed, and trajectory of drawing the PIN).	Using a new authentication system called DRAW-A-PIN, where users draw PIN numbers with their fingers on a touch screen instead of typing them, this is an additional biometric factor to enhance behavioral security (such as drawing style), especially against shoulder surfing and smudge attacks.	It remains difficult to imitate the user's drawing style, making it resistant to shoulder surfing attacks even if the attacker knows the PIN. Also, because the user draws over the same area multiple times, this reduces traceable fingerprints, making smudge attacks more difficult. As a result, security is enhanced through behavioral features, which add an additional layer of biometric verification. It delivers accurate results, achieving an Equivalent Error Rate (EER) of 4.84% even when the attacker knows the PIN, and it can be used as an additional option alongside traditional authentication.	The number recognition rate is not ideal because the system faces challenges in accurately recognizing drawn numbers and is sensitive to changing usage conditions, such as changing hand position, which can affect recognition performance, leading to poor performance in targeted attacks. Although 85% of accurate imitation attempts are rejected, there is still a possible success rate.
[25]	Two Factor Authentication	Two-factor authentication (2FA) using OTP (One-Time Password) generated dynamically and sent via SMS. • Static factor: Username and password (traditional authentication). • Dynamic factor: OTP sent via SMS (second layer of security).	A two-factor authentication (2FA) system based on a one-time password (OTP) has been evaluated and developed to secure logins, in order to protect user data from attacks such as brute-force.	Enhanced security and high rating in all performance criteria, including reliability: more than 95% of users rated it as excellent or good, effectiveness: 80% rated it as excellent or good, efficiency: 90% rated it as excellent or good, and usability: most participants rated it as easy to use and scalable.	The OTP data sent is not encrypted and the lack of support for smart devices such as fingerprint or face recognition may reduce integration with some modern authentication technologies.

[26]	Two Factor Authentication	• Two-factor authentication model in a smartphone environment. • Fingerprint authentication as one factor. •Application-managed password handling as the second factor.	Improve ease of use compared to existing solutions such as Google Authenticator by developing a two-factor authentication (2FA) model that combines a password and a fingerprint to maintain a high level of security against attacks such as: guessing, replay attacks, etc.	Improved user experience: Logging in requires only a fingerprint and strong passwords that are not managed by the user. Complex passwords are stored within the application itself, reducing the risk of using weak or duplicate passwords across sites. Using a fingerprint as a verification factor makes the authentication system more difficult to guess or crack than traditional passwords.	It is vulnerable to biometric cloning attacks, as a fingerprint can be cloned by attackers, although this is more difficult than stealing a password. Also, the proposed model relies on static passwords, making it more vulnerable to replay attacks than a temporary OTP.
[27]	Two Factor Authentication	The system combines traditional 2FA (Google Authenticator) with honey tokens Factor 1: Something the user knows (e.g., a password or OTP from Google Authenticator). Factor 2: Something the user has (e.g., a smartphone or SMS for additional authentication).	Proposing a new two-factor authentication (2FHA) mechanism that combines the traditional OTP used in applications such as Google Authenticator and Honeytokens (or Honeywords), to increase security and reduce the possibility of hacking even if the password is known. It can be used to repel advanced attacks such as targeted attacks, SIM card theft, and phishing.	High security: By integrating "Honeywords" into the two-factor authentication mechanism, the system not only asks for the password but also locates the correct one-time password (OTP) among several fake codes sent to another device. Attackers are unable to identify the real one, even if they have the password. It is compatible with a large number of systems currently used in companies.	It relies on smart devices because it requires Google Authenticator, which is not available to all users, especially in low-income countries. The login process becomes more complex, as the user must remember the location of the real code among the fake codes, which may be cumbersome for some.
[28]	Two Factor Authentication	Feature Extraction using Deep Learning and Cryptographic Hashing and Symmetric Encryption.	Proposing an authentication mechanism using single-use biometric templates that rely on the user's biometric characteristics (such as face or fingerprint) and protect them from replay attacks, while taking into account privacy protection.	The system generates a new biometric template each time, so previously recorded data cannot be reused. It uses techniques such as biohashing (a biometric data protection technique) and hashing and symmetric encryption, ensuring the protection of the biometric template. The method does not rely on a specific type of biometric feature; it can be used with any type of biometric data (fingerprint, face, behavior, etc.). Authentication accuracy is also enhanced and performance is improved by extracting biometric features using deep learning.	Increased computational and time complexity because the system requires multiple steps (feature extraction, biohashing, encryption, and temporary template generation). The system relies on deep learning algorithms, which require extensive data and intensive training, making it unsuitable for all environments.

[29]	multi-Factor Authentication	• Multi-Factor Authentication (MFA) using three factors:(Face image, Password image (converted from text password), Auxiliary image (user-designated image like pet, fruit, or possession)) • Parallel MFA approach: All factors processed simultaneously using Convolutional Neural Networks (CNN). • Lightweight CNN (MMCNN) for mobile devices, with reduced parameters for better efficiency and suitability on mobile platforms.	Developing a multi-factor authentication (MFA) system for mobile devices that uses convolutional neural networks (CNNs) to confirm user identity through multiple factors: facial image, password converted to image, in a secure manner.	It provides high security by using three different authentication factors, making it extremely difficult for any attacker to bypass the system. It provides intelligent combination of inputs, which enhances accuracy. High accuracy, reaching 99.6% in the lightweight model, demonstrates the system's effectiveness. It also securely converts the password to an image in a way that prevents the original password from being revealed. It doesn't require constant internet connection, which increases security.	Not intended for large-scale systems. Suitable for small groups (approximately 100 users), and may not be suitable for large enterprises yet. It relies primarily on the camera. If the camera malfunctions or the image quality is not sufficient, verification may fail. Also, it has limited compatibility with certain cultures or circumstances. Some users may not feel comfortable using their personal or private photos for verification purposes.
[30]	multi-Factor Authentication	• Username–password, Fingerprint, OTP (One-Time Password), Facial recognition for further authentication and fraud detection. • Machine Learning Layer: Facial recognition is used as an additional layer of security, activated upon detecting suspicious activity.	Increase security while maintaining ease of use by using two-factor authentication initially, and adding a machine learning-based intelligent layer in case of suspected fraud.	Striking a balance between security and ease of use. The models used demonstrated an accuracy of up to 97.938% in detecting illicit transactions, enhancing the system's effectiveness. The study addressed the problem of users feeling inconvenienced when using traditional MFA systems and sought to reduce this feeling.	The use of facial recognition may raise privacy concerns for some users. ML systems are not completely immune, and there is a potential for attacks such as adversarial attacks.
[31]	multi-Factor Authentication	Something the user has (Physical Unclonable Function) embedded in devices for authentication. And Something the user knows (The mutual authentication between gateway-users and gateway-devices, potentially involving PINs). the system could be extended with additional factors like biometrics, depending on the specific implementation.	Developing a lightweight multi-factor authentication protocol based on unclonable functions (PUFs) to ensure the security of smart homes powered by Internet of Things (IoT) technologies, ensuring mutual authentication between users and devices via the smart gateway, and reducing computational and storage complexity with a focus on resisting known attacks.	The protocol is suitable for devices with limited resources (in terms of power, memory, and processing power), and is practical and easy to use, which encourages its adoption in real-world smart home systems. It is also resistant to tampering and spoofing, and is difficult to physically replicate, increasing security against physical attacks due to the use of non-cloneable functions.	PUF technology may not be available or supported on all types of smart devices, which may limit the applicability of the protocol.
[32]	multi-Factor Authentication	uses five factors of authentication, which are: (Username,Password,Personal Identification Number (PIN),One-Time PIN (OTP),Biometric (Fingerprint or Facial scan), Registered smart device, and time-locked user location used These factors to strengthen the security of online banking platforms.	Developing an enhanced multi-factor authentication system consisting of five factors, incorporating the "track and trace" feature, to enhance response to suspicious activities, without negatively impacting the user experience, and to protect electronic banking platforms from increasing attacks.	The system's ability to respond to attacks in real time and offers significant performance improvements over existing systems (FNB and STD) in response speed (500 milliseconds versus 700 and 1000 milliseconds). The system is flexible and applicable to current banking environments, with intelligent tracking capabilities and immediate response.	Many factors may affect ease of use for some users, such as being cumbersome or complex for users with limited technical experience, having trouble reactivating when failed, and depending on smart devices and geographic location:
[33]	multi-Factor Authentication	Three factors are used in the authentication model: Fingerprint Hash Code (generated via MD5 and Euclidean distance), Password, One-Time Password (OTP).Feature Extraction: Gabor filtering is used to extract features from the fingerprint image.	Developing a multi-factor authentication (MFA) model that uses iris as a secure alternative to traditional passwords, and relies on the integration of iris image, one-time passcode (OTP), and fingerprint, to improve the level of security in authentication systems, especially in an environment based on the client-server architecture.	Using an iris print as a primary factor, it is unique to each person, cannot be easily forgotten or stolen, and remains stable throughout life. The model's results showed a low authentication error rate, enhancing verification accuracy. The integration of artificial intelligence (a neural network) into biometric data matching enhances accuracy and reliability.	This model cannot be used in systems such as biometric attendance systems that do not rely on smartphones. There is also the risk of biometric database breaches, and implementation complexity and cost are significant. The model requires advanced iris imaging and fingerprint sensor technologies, as well as complex techniques such as encryption, hashing, and fingerprint salting, which increases system complexity and requires additional computing resources.
[34]	multi-Factor Authentication	a three-factor authentication protocol for securing mobile devices, particularly in environments where confidential data is processed.	Analysis and design of a robust and secure authentication protocol in a mobile environment (specifically on Android), integrating three classes of factors (knowledge, biometric, ownership) in compliance with European standards (EU Regulation 2015/1502) and NIST standards, with resistance to known attacks	Full compliance with international standards and the use of three different factors reduces the possibility of account hacking and is suitable for the smartphone environment. The protocol has also been studied using formal analysis, which proves its validity and effectiveness from a theoretical perspective.	Combining three factors into a phone environment increases the complexity of the system. Some factors, such as OTP and server connections, require an internet connection, making the system ineffective in weak network environments. Using these factors is a burden on the user.

4. Discussion:

authentication methods can be broadly classified into single-factor, two factor, and multi-factor approaches, each with distinct advantages and limitations.

1- SFA depend on just one layer of security. while it remains the most common and straightforward method, it is also the most vulnerable weak or reused passwords, phishing attacks, and brute-force techniques make SFA highly susceptible to breaches. however, due to its simplicity, SFA is widely used in low-risk scenarios where ease of use takes precedence over security.

2- 2FA introduces an additional layer of security that improved security compared to SFA by requiring access to both factors.
3- MFA extends 2FA by combining two or more security factors, often incorporating behavioral or contextual elements. for instance, MFA might include a password, a biometric scan and a location-based verification. while this approach offers the highest level of security, it can be resource intensive and may impact user convenience. advanced MFA solutions often employ adaptive authentication where additional factors are required only in high-risk situations. Table (3) explain the Comparison between three authentication types.

Table 3: Comparison Between Three Authentication Types [36] [37] [38] [39].

Authentication Types	Security %	Ease of use %	Estimated implementation cost	Reduce risks%	Best use cases
SFA	30%	90%	Low	30%	Simple or non-sensitive systems.
2FA	70%	80%	medium	70%	Online banking, email.
MFA	90%	70%	high	90%	financial institutions, sensitive data.

The choice between single, two-factor, and multi-factor authentication depends on user convenience, the security requirements, and organization resources. For high-risk environments, MFA offers robust protection, while SFA may suffice for less critical applications where usability is prioritized. These ratios were determined based on market research and analysis related to each type of authentication, as well as the differences between password-based systems and more advanced authentication systems such as MFA. These ratios aim to provide a realistic estimate of performance in various areas, helping organizations or individuals make the most appropriate decision when choosing an authentication type. Note that, many sources consider two-factor authentication to be part of multi-factor authentication.

5. Conclusions

The evolution from single-factor authentication (SFA) to two-factor authentication (2FA) and multi-factor authentication (MFA) highlights the growing need for enhanced security in response to increasingly sophisticated cyber threats. While SFA offers simplicity and ease of use, its vulnerabilities make it unsuitable for high-risk scenarios. 2FA provides an additional layer of security by combining two elements, significantly reducing risks associated with credential theft. MFA by incorporating multiple factors-often including adaptive and contextual authentication –offers the highest level of protection but at the cost of increased complexity and implementation challenges.

Ultimately, the choice of authentication method reflects the ongoing need to balance security, usability, and technologies advancements. traditional approaches like passwords and PINs, while widely adopted, face increasing vulnerabilities due to evolving cyber security threats. In contrast, modern techniques such as biometrics authentication, multi-factor authentication (MFA), and emerging behavioral and Al-driven methods offer enhanced security but come with challenges related to cost, privacy, and implementation complexity. ultimately, the ideal authentication solution depends on a specific context, balancing user convenient with robust protection against unauthorized access. continuous innovation and integration of adaptive, user-friendly, and also There is no better method than the other, but it depends on the user's need and importance of the data. They are all used and effective, but with varying degrees of security and secure technologies will be essential to meet the dynamic demands of digital security in the future.\

6. Reference

[1] Adhav, S. (2023). *Enhancing cloud security through integration of three-factor authentication and role-based access control* (MSc Research Project). National College of Ireland. Supervisor: Joel Aleburu.

[2] Rajarajeswari, S., & Maria Stella, A. (2019). A review of authentication and authorization methods. *International Journal of Computer Science and Information Technology Research, 7*(3), 78–83. Retrieved from.

[3] Prakash, A., & Kumar, U. (2018). Authentication protocols and techniques: A survey. *International Journal of Computer Sciences and Engineering, 6*(6), 1014–1021. Retrieved from.

[4] Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern authentication methods: A comprehensive survey. *AI, Computer Science and Robotics Technology, 2022*(0), 1–24.

[5] Arias-Cabarcos, P., Krupitzer, C., & Becker, C. (2019). A survey on adaptive authentication. *ACM Computing Surveys, 1*(1), Article 1, 30 pages.

[6] Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health, 9*, 20552076231177144.

[7] Wiercioch, A., Teufel, S., & Teufel, B. (2018). The authentication dilemma. *Journal of Communications, 13*(8).

[8] Abdulkader, S. N., Atia, A., & Mostafa, M.-S. M. (2015). Authentication systems: Principles and threats. *Computer and Information Science, 8*(3).

[9] Cheung, S. H., Chen, W., & Ma, J. (2023, April 11). *Lecture Note 6: Authentication*.

[10] Net-Ctrl. (2020). *Comprehensive guide to authentication* [White paper].

[11] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five two-factor authentication methods. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* (SOUPS 2019), Santa Clara, CA, August 12–13.

[13] Alqahtani, A. A. S., El-Awadi, Z., & Min, M. (2021). A survey on user authentication factors. In *2021 IEEE IEMCON* (pp. 1–7).

[14] Batoi. (2022, 6 october). *Single-Factor vs Multi-Factor Authentication: Impact on Account Security*. Batoi. https://www.batoi.com/blogs/developers/single-factor-vs-multi-factor-authentication-impact-account-security-6331ac82f3dbc:contentReference[oaicite:4]{index=4}

[15] Tamm, E. (2024). *Implementation and comparison of two-factor authentication methods* (Bachelor's thesis, Tallinn University of Technology). Supervisor: Viljam Puusep.

[15] Mustafa, B. A., & Al-Qirimli, F. A. (2023). The impact of information security processes on providing secure digital systems. *Journal of Port Science Research, 6*(4).

[17] Sadikan, S. F. N., Ramli, A. A., & Fudzee, M. F. M. (2019). A survey paper on keystroke dynamics authentication for current applications. *AIP Conference Proceedings, 2173*(1), 020010.

[18] 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.

[19] Rajasingh, J., & Yaswanth, D. S. (2021). Fingerprint authentication. *International Journal of Engineering and Advanced Technology, 10*(5). ISSN: 2249–8958.

[20] Jadhav, V. V., Patil, R. R., Jadhav, R. C., & Magikar, A. N. (2016). Efficient biometric authentication technique using fingerprint. *International Journal of Computer Science and Information Technologies, 7*(3), 1132–1135.

[21] Farik, M., & Ali, A. B. M. S. (2015). Algorithm to ensure and enforce brute-force attack-resilient password in routers. *International Journal of Scientific & Technology Research, 4*(10), 2277–8616.

[22] Drašar. (2009). *Password based authentication* (Master's thesis). Masaryk University, Faculty of Informatics, Brno.

[23] Helkala, K., & Snekkenes, E. (2009). Password generation and search space reduction. *Journal of Computers, 4*(7).

[24] Liskin, V., Serdobolskiy, E., Sopilko, I., & Okhrimenko, T. (2020). Two-factor user authentication using biometrics. In *Proceedings of the International Workshop on Cybersecurity and Secure Communications* (Vol. 2654, pp. 263–268).

[25] Nguyen, T. V., Sae-Bae, N., & Memon, N. (2017). DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices. *Computers & Security, 67*, 70–86.

[26] Iyanda, A. R., & Fasasi, M. E. (2022). Development of two-factor authentication login system using dynamic password with SMS verification. *I.J. Education and Management Engineering, 12*(3), 13–21.

[27] Persson, O., & Wermelin, E. (2017). *A theoretical proposal of two-factor authentication in smartphones* (Bachelor's thesis, Blekinge Institute of Technology).

[28] Papaspirou, V., Papathanasaki, M., Maglaras, L., Kantzavelou, I., Douligeris, C., Ferrage, M. A., & Janicke, H. (2021). Cybersecurity revisited: Honeytokens meet Google Authenticator. *arXiv preprint arXiv:2112.08431*.

[29] Gernot, T., & Rosenberger, C. (2024). Robust biometric scheme against replay attacks using one-time biometric templates. *Computers & Security, 137*, 103586.

[30] Han, J. (2024). CNN-based multi-factor authentication system for mobile devices using faces and passwords. *Applied Sciences, 14*(12), 5019.

[31] Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning. *AI, 5*, 177–194.

[32] Sarbishaei, G., Aminian Modarres, A. M., Jowshan, F., Khakzad, F. Z., & Mokhtari, H. (2024). Smart home security: An efficient multi-factor authentication protocol. *IEEE Access, 12*, 12345–12356.

[33] Moepi, G. L., & Mathonsi, T. E. (2023). Implementation of an enhanced multi-factor authentication scheme with a track and trace capability for online banking platforms. *Preprints*.

[34] Prasad, K. K., & Aithal, P. S. (n.d.). A study on multifactor authentication model using fingerprint hash code and iris recognition. In *Impact of Ideas and Innovations on Management, IT, Education & Social Sciences* (Paper 19). ISBN: 978-93-5300-881-9.

[35] Bartłomiejczyk, M., Imed, E. F., & Kurkowski, M. (2019). Multifactor authentication protocol in a mobile environment. *IEEE Access, 7*, 141890–141904.

[36] The Business Research Company. (2025). Multi-factor authentication global market report.

[37] Straits Research. (2025). Passwordless authentication market.

[39] Microsoft. (2025). The impact of multi-factor authentication on account security.

مراجعة شاملة : لاستكشاف تقنيات المصادقة

دلال نعيم حمود[1]
Dalal.naeem@nahrainuniv.edu.Iq
daL-scin81@yahoo.com

ريم حسين علي[2]
reem.msco23@ced.nahrainuniv.edu.iq

المستخلص: تُعدّ التجارة الإلكترونية إحدى التقنيات الحديثة المتنوعة التي رافقت تطور الإنترنت. وقد جعل هذا من الأمن عاملاً أساسياً في التجارة الإلكترونية، إذ يمنع الحوادث غير المرغوب فيها مثل تسريب البيانات والخسائر المالية. تُعد المصادقة جانباً بالغ الأهمية في تأمين الأنظمة الرقمية وحماية بيانات المستخدم. تستعرض هذه الورقة البحثية وتُقارن ثلاث طرق مصادقة رئيسية: المصادقة أحادية العامل(SFA) ، والمصادقة ثنائية العامل (2FA)، والمصادقة متعددة العوامل .(MFA) تعتمد المصادقة أحادية العامل(SFA) ، وهي أبسط الطرق، على طبقة أمان واحدة، مثل كلمات المرور أو أرقام التعريف الشخصية(PIN) ، ولكنها شديدة التأثر بالتهديدات السيبرانية الحديثة. عززت تقنية المصادقة الثنائية (2FA) الأمان من خلال الجمع بين عاملين متميزين، مثل كلمة المرور وكلمة المرور لمرة واحدة(OTP) ، مما يقلل من مخاطر سرقة بيانات الاعتماد. كما تعزز تقنية المصادقة متعددة العوامل (MFA) المصادقة من خلال دمج طبقات متعددة، بما في ذلك العناصر البيومترية والسياقية، مما يجعلها النهج الأكثر أمانًا، ولكنها أيضًا الأكثر تعقيدًا واستهلاكًا للموارد. تُسلط المناقشة الضوء على أوجه التشابه بين هذه الطرق من حيث الأمان وسهولة الاستخدام وقابلية التوسع والتكلفة وتقليل المخاطر. في حين أن تقنية المصادقة أحادية العامل (SFA) قد تكون كافية للتطبيقات منخفضة المخاطر، فإن تقنية المصادقة متعددة العوامل (MFA) ضرورية للبيئات التي تتطلب أمانًا قويًا. خلصت الدراسة إلى أن اختيار طريقة المصادقة يجب أن يعتمد على حالة استخدام محددة، مع الموازنة بين احتياجات الأمان وراحة المستخدم وموارد المؤسسة.

الكلمات المفتاحية: المصادقة، المصادقة أحادية العامل، المصادقة ثنائية العوامل، المصادقة متعددة العوامل، كلمة مرور لمرة واحدة.

[1] استاذ مساعد دكتور؛ قسم علوم الحاسوب – جامعة النهرين - كلية العلوم – بغداد - العراق
[2] طالب ماجستير؛ قسم علوم الحاسوب – جامعة النهرين - كلية العلوم – بغداد - العراق