International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

Authentication and Securing the System: A Comprehensive Review Paper

Tejeswari Devi, Mohammad Jeelani, Sana Bee, Sweta Yadav, Mohini, Abhishek Saxena

Department of Computer Application, Future University, Bareilly, U.P., India.

tejeswaridevi4321@gmail.com, jeelani.0018@gmail.com, sanansari6395@gmail.com, swetayadavkckicbly@gmail.com, m82438303@gmail.com, abhisheksaxena@futureuniversity.in

Abstract:
This review paper provides a comprehensive analysis of authentication methods and their role in securing digital systems. Authentication is the process of verifying the identity of users, devices, or systems before granting access to protected resources. As cyber threats continue to evolve in complexity, implementing robust authentication mechanisms has become increasingly important for protecting sensitive information and maintaining system integrity. This paper examines various authentication techniques, from traditional password-based systems to modern multi-factor and biometric approaches, discussing their strengths, limitations, and implementation considerations. This study reviews existing literature and analyses current authentication technologies to highlight best practices for enhancing security while maintaining usability. The findings suggest that a layered approach to authentication, combining multiple factors and adaptive security measures, offers the most effective protection against unauthorised access in today's digital landscape.

Keywords: *Authentication, Security, Biometric authentication, MFA (Multi-factor Authentication), unauthorised access*

1. Introduction

Large-scale personal information leaks have been commonplace in recent years, leading to widespread concern about personal information and online shopping. Furthermore, the number of bank certificates compromised or released through phishing increased 100-fold over the past few years. Additionally, it's time to adopt innovative, user-friendly methods and systems that provide certification services and reduce anxiety. The Digital Signature Act and the Electronic Financial Transaction Act were modified in 2014, and evidence of hacking incidents involving financial firms and forced e-commerce articles employing certificates was removed. OTP roles are merely a backup; key passwords need to be entered during actual electronic finance transactions, and this remains the biggest issue [1].

Conventional authentication techniques, such as identity documents and passwords, are insufficient to prevent identity theft or ensure security. Such fictitious identities are easily shared, forgotten, misplaced, guessed, or stolen. Anatomical characteristics (fingerprint, face, palmprint, iris, voice) or behavioural characteristics (signature, gait) are used by biometric systems to identify people. Biometric recognition is a natural and more reliable way to ensure that only authorised or authentic users can enter a facility, as these characteristics are physically linked to the user. Biometric systems provide greater security when appropriately integrated into applications that require user authentication. The sole method to identify duplicate identities is biometric recognition, which also provides more reliable user authentication than identity documents and passwords. Although biometric technologies are not infallible, the scientific community has made great progress in identifying weaknesses and creating countermeasures [2]. Biometric authentication has been extensively researched and has attracted particular attention in both academia and industry as a means of addressing password management challenges and enhancing the usability of authentication systems. Numerous biometric identification solutions, particularly for mobile devices, have been studied and created. Nevertheless, there are still issues with the current biometric authentication technologies [3]. As hacking becomes more advanced, electronic financial fraud is expected to increase despite security measures like ARS (Automated Response System) and SMS (Short Message Service) authentication. QR codes are now used for authentication, but they are vulnerable to forgery and difficult for ordinary users to verify, raising concerns about their reliability [1].

This research paper explores the different aspects of authentication and how it helps secure computer systems. We will review the existing literature on authentication methods, examine how authentication works, discuss various types of authentication and biometric authentication systems, their advantages and vulnerabilities, and finally look at emerging trends in authentication technology. The goal is to provide a clear understanding of how authentication protects our digital lives and what methods work best for different situations.

2. Related Work

Park et al. [1] build on prior authentication methods such as password-based, OTP, and certificate-based systems, which had limitations in usability, security, or regulatory compliance. Unlike earlier works that focused on single-factor or isolated multi-factor solutions, their study proposes an integrated user authentication service to replace outdated digital certificate systems in financial and e-commerce applications. Jain et al. [2] emphasised the importance of balancing system security and user privacy in biometric authentication systems. Their work highlights challenges in protecting sensitive biometric data while ensuring accurate and reliable user verification. Rui et al. [3] reviewed existing biometric authentication techniques, highlighting advances in spoof detection, multimodal systems, and privacy-preserving methods.

They emphasised that while earlier systems focused on accuracy, emerging approaches must integrate both security and user data protection to address evolving threats. Kovalan et al. [4] conducted a systematic literature review on authentication safety practices among internet users. Their study sheds light on common behaviours and attitudes toward authentication methods, identifying significant gaps in user awareness and the need for improved education to enhance online security. Ezugwu et al. [5] examined password-based authentication among Nigerian users and found generally positive user experiences, with low reported incidents of compromise regardless of age or education level. Balaj [6] provides a comparative analysis of session-based authentication vs token-based authentication (e.g. using OAuth2 or JWT), highlighting that token-based schemes are more scalable, stateless, and better suited to RESTful APIs, while session-based methods maintain server-side state, which can lead to higher load and management complexity. Prakash et al. [7] presented a comprehensive survey of authentication protocols and techniques. Their work classifies various authentication mechanisms and highlights the strengths and weaknesses of each. This serves as a foundational reference for research in secure communication systems. Bhattacharyya et al. [8] conducted a detailed review of biometric authentication methods, discussing key techniques such as fingerprint, iris, and facial recognition. Their study highlights the advantages, limitations, and practical considerations of biometric systems in real-world applications. Progonov et al. [9] explored behaviour-based user authentication methods on mobile devices across different usage contexts. Their study emphasises the adaptability and accuracy of behavioural biometrics, such as touch dynamics and usage patterns, in enhancing mobile security. Mahadi et al. [10] conducted a comprehensive survey of machine learning techniques used in behaviour-based biometric user authentication. The study reviews various algorithms, highlighting their effectiveness in modelling user behaviour for secure access control. Kim and Hong [11] proposed a risk assessment method tailored for multifactor authentication systems. Their approach evaluates security risks based on the combination of authentication factors used, aiming to enhance decision-making in access control. Suleski et al. [12] reviewed multifactor authentication (MFA) approaches within the Internet of Healthcare Things (IoHT).

Their study highlights the unique security challenges in healthcare environments and evaluates MFA techniques for balancing usability and protection of sensitive data. Kolluri et al. [13] presented a comprehensive analysis of neural network architectures applied to multimodal biometric authentication systems. Their work emphasises how AI and machine learning enhance the accuracy and robustness of biometric security across multiple modalities. Hafeez et al. [14] developed a real-time human authentication system based on iris recognition technology. Their system focuses on accuracy and speed, demonstrating practical applications for secure access in various environments. Ross et al. [15] introduced a prototype verification system based on hand geometry as a biometric modality. Their work laid foundational insights into the use of geometric features for personal authentication. Tiwari et al. [16] presented a comprehensive review of voice recognition and authentication systems, highlighting recent advancements and challenges in voice biometrics for secure communication. Navaz et al. [17] explored biometric methods for signature authentication, analysing various techniques to improve accuracy and reliability in verifying handwritten signatures.

3. Authentication Factors

Identification occurs when a user declares their identity (e.g., by entering a login ID), while authentication verifies that identity (e.g., by providing the correct password). Once authenticated, the user is granted appropriate rights, privileges, and permissions [7].

Authentication methods are commonly categorised into three factors, as mentioned in Figure 1:[7]

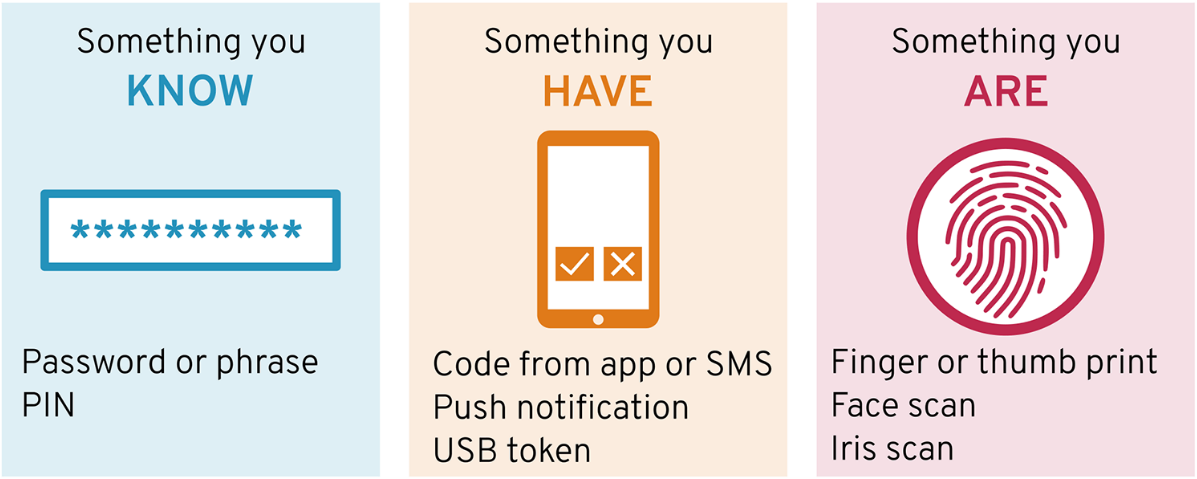

Fig.1: Authentication factors

3.1 **Something You Know**:

- Involves passwords or PINs.
- Common and requires no hardware or heavy processing.
- Drawbacks include being easy to guess, susceptible to eavesdropping, and often exposed in visible areas.
- Passwords are usually stored in encrypted form, not plain text.

3.2 **Something You Have**:

- Includes smart cards and tokens.
- Smart cards contain embedded certificates and require a reader.
- Tokens display a time-based code that must match the server's value during login.

3.3 **Something You Are**:

- Refers to biometrics like fingerprints, voice, and iris scans.
- Highly unique and reliable, even between twins.
- More expensive but offers the strongest security.

Multi-factor authentication (MFA), which combines two or more of these factors, is increasingly used to strengthen security, as shown in Table 1.

Table 1: Evolution of Authentication Methods

Era	Authentication Type	Examples
1960s–1980s	Knowledge-based	Passwords, PINs
1990s	Possession-based	Smart cards, hardware tokens
2000s	Biometrics	Fingerprints, facial recognition
2010s	Multi-Factor Authentication (MFA)	2FA with OTP, push notification

2020s	Passwordless, Adaptive, Behavioural	FIDO2, WebAuthn, AI-based auth

4. Types of Authentication Methods

This section addresses several forms of authentication identified in the study, including multifactor authentication, biometric authentication (fingerprint, face, retina, voice, and digital signature), and password authentication (textual and graphical). Authentication is one of the most crucial components of any system. Since they prevent kleptomaniacs from accessing user data illegally, authentication systems are often seen as the first and last line of defence. However, many programs and websites that are vulnerable to various kinds of attacks still use traditional text-based passwords.

4.1. Password-based authentication

Passwords are commonly used for end-user authentication in ICT (Information and Communication Technology) systems due to their simplicity. This authentication method is applied in network services, computers, and mobile devices [5]. Passwords have long been used for online security, but their reuse and lack of expiration make them vulnerable to cyberattacks. Strong passwords should be memorable yet difficult to hack. This review identifies two main types of password authentication: textual and graphical [4].

4.2. Token-based authentication

A token is a signed, unencrypted string containing user data for authentication. It can be a hardware device or a software-based component used in multi-factor authentication systems to verify identity and grant access [6]. An authentication token is a digital credential that securely verifies a user's identity without requiring repeated password input. Often in the form of JSON Web Tokens (JWTs), these tokens contain user data, expiration times, and integrity signatures, enhancing both security and convenience by allowing temporary session-based access [6].

According to RFCs (Request for Comments), there are different types of tokens:[6]

- **Perishable tokens** validate a single action.
- **Session tokens** are temporary and reusable within one session.
- **Access tokens** can be used repeatedly but are not renewable.
- **Refresh tokens** are single-use and must be invalidated after use.

4.3. Biometric authentication

Biometric systems provide access by comparing live scans of unique physical traits to stored data, offering a more secure and convenient alternative to traditional methods like passwords or tokens, which can be forgotten, stolen, or compromised. During enrolment, a biometric system captures a user's biometric data (e.g., a facial image) using a sensor and extracts key features (like fingerprint minutiae) to create a template, which is stored with identifiers such as a name or ID. For authentication, the user provides a new biometric sample, from which features are extracted and compared to the stored template using a matcher to verify the claimed identity [2].

Biometric traits are generally classified into two main types, as elaborated in Fig. 2:

- **Physiological** biometrics are based on physical characteristics like **f**ingerprints, facial features, hand geometry, and iris patterns.
- **Behavioural** biometrics are based on a person's actions, such as voice, signature, and keystroke dynamics. Voice can sometimes be considered physiological due to its physical components.

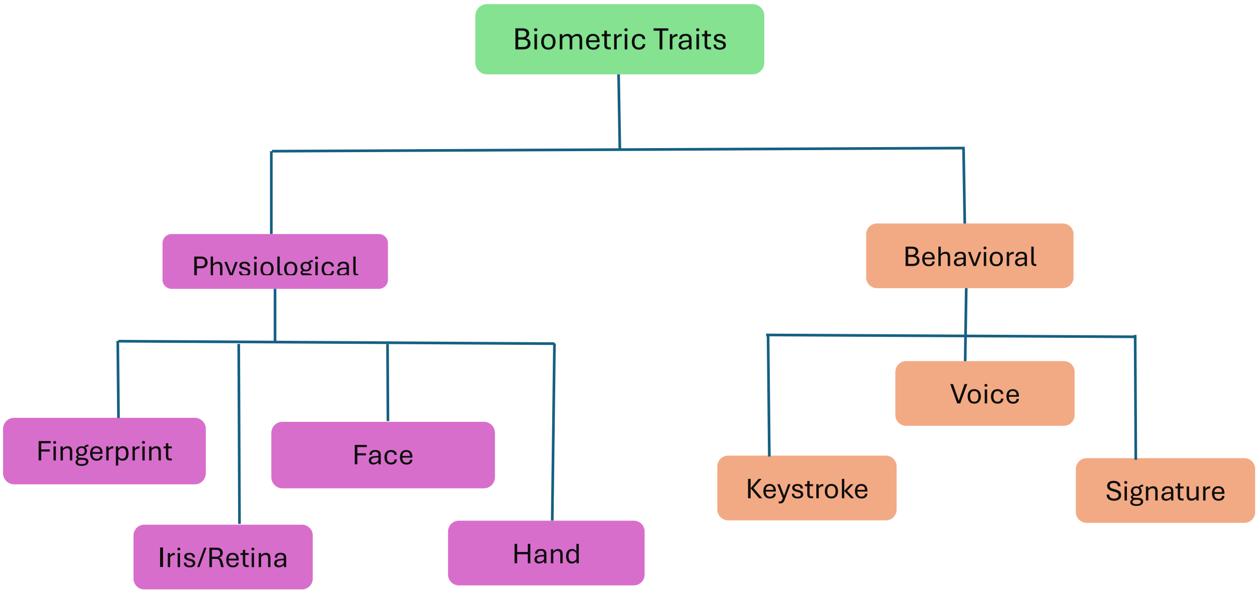

Fig. 2: Classification of biometric traits

A newer trend, known as cognitive biometrics, combines human perception with computer systems using brain-machine interfaces for authentication. The foundation of cognitive biometrics is how the brain reacts to specific stimuli, which can be utilised to initiate a computer database search.

4.3.1. Fingerprint Technology

Fingerprint recognition is the oldest and most widely used biometric method. A fingerprint is an impression of the friction ridges, raised skin patterns found on the fingers, palms, soles, and toes, also known as dermal ridges. Traditionally, fingerprints were captured using ink and paper, but modern systems use live fingerprint readers based on thermal, optical, silicon, or ultrasonic technologies. Among these, optical fingerprint readers are the most common. They detect changes in light reflection caused by contact between the finger's papillary lines and the sensor surface. These devices typically include a light source, a light sensor, and a pressure-sensitive reflective surface, with some models also featuring built-in processors and memory for data storage, as shown in Fig. 3 and Fig. 4.

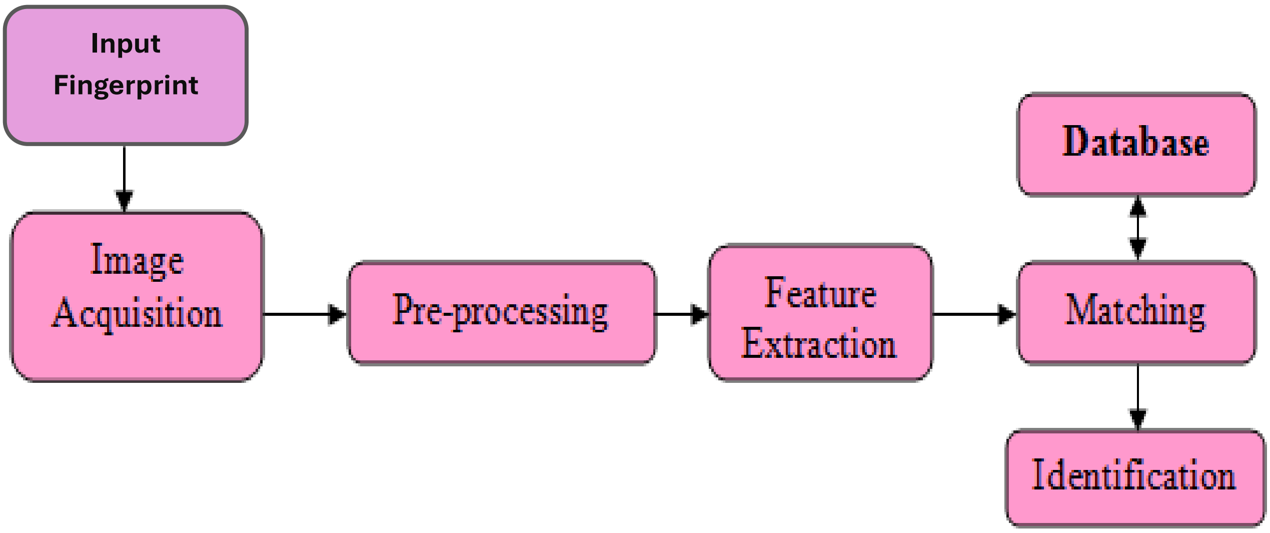

Fig. 3: Fingerprint authentication process

Fig. 4: Image of a fingerprint

4.3.2. Face recognition technology

A facial recognition approach is a computer program that uses a digital image or a video frame from a video source to automatically identify or validate a person. It is the most organic method of biometric recognition. Recently, two developments in facial recognition technologies have emerged: Eigenfaces and facial metrics [8]. Four processes are considered to create a robust facial recognition system: facial detection, feature extraction, feature classification, and feature matching, as shown in Fig. 5 [13].

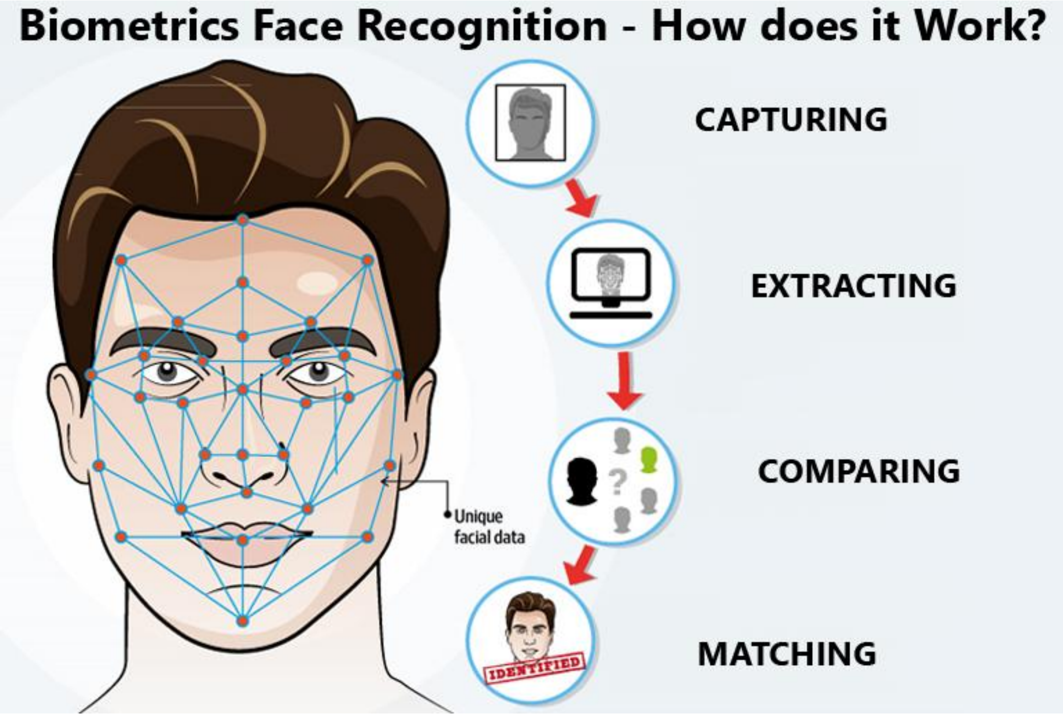

Fig. 5: Face recognition

4.3.3. Iris recognition

The distinctive, intricate, and consistent patterns of a person's iris, the colored portion of the eye, are used by iris authentication, a high-security biometric verification tool, to verify identity.

Four components make up the iris identification framework: iris segmentation, iris normalisation, iris feature extraction, and matching, as given in Fig. 4 [14].

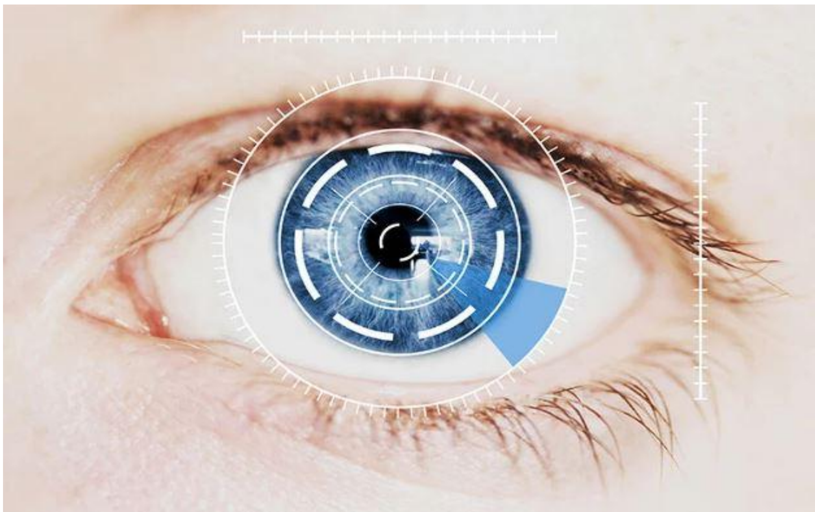

Fig. 6: Iris recognition

4.3.4. Hand geometry recognition

The hand's dexterity and the simplicity of the sensing process, which eliminates the need for complex optics, make hand geometry recognition a practical biometric technique. Hand geometry is more resilient and easier to record than fingerprint systems, which depend on healthy skin, or iris/retina systems, which require specific illumination. Additionally, it works well with other biometrics, particularly fingerprints. For instance, as mentioned in Fig. 7, a system may employ hand geometry for frequent verification and fingerprints for infrequent identification. Both biometric characteristics may be recorded simultaneously by a single sensor [15].

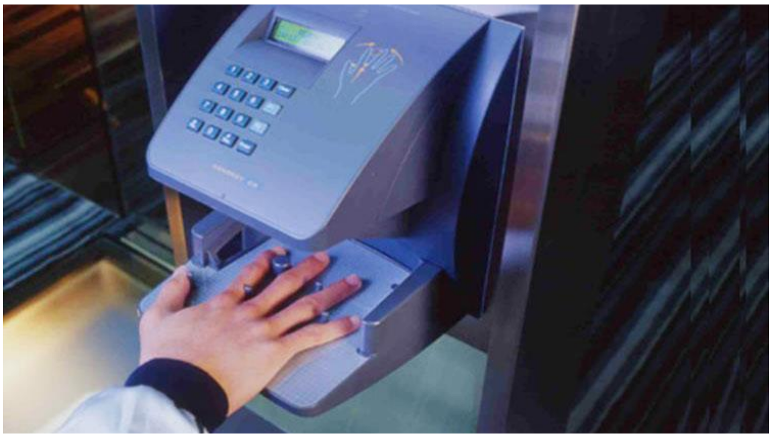

Fig.7: Hand geometry authentication

4.4. Behaviour-based authentication

BehaviorID is a context-aware, transparent, behaviour-based user authentication method. It leverages embedded sensors to track and update user behavioural templates based on varying usage contexts, and can quickly adapt to new, unseen scenarios. As mentioned in Fig. 8, evaluations across three scenarios, typing arbitrary text in a fixed context, typing fixed text in a fixed context, and typing arbitrary text in shifting contexts [9].

Keystroke dynamics is an automated method of verifying a user's identity based on their typing style and rhythm. In developing such a system, the authors used a Support Vector Machine (SVM) as the classification algorithm. Another kind of user verification that analyses handwriting style, specifically the signature, is signature recognition. The support vector machine (SVM) classifier was established for offline signature verification, and fuzzy modeling based on the Takagi-Sugeno (TS) model was suggested [10].

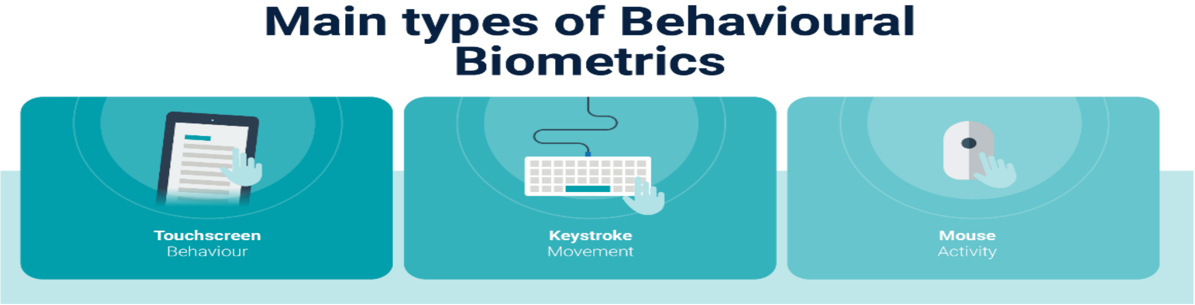

Fig. 8: Types of behavioural biometrics

4.4.1. Voice recognition technology

Using the distinctive qualities of a person's voice, voice recognition authentication, also known as voice biometrics, serves as a "voice password" to confirm identity. A user's speech is used to create a voiceprint, which is then compared to a stored template in subsequent voice samples.

Each person has a voice that is both unique and distinctive, influenced by both behavioural and physiological factors. While the behavioural component includes things like accent and tonal nuances, the physiological component is mostly linked to the vocal tract's structure. When these elements are combined, a single voice profile is produced that can be used for accurate identification [16].

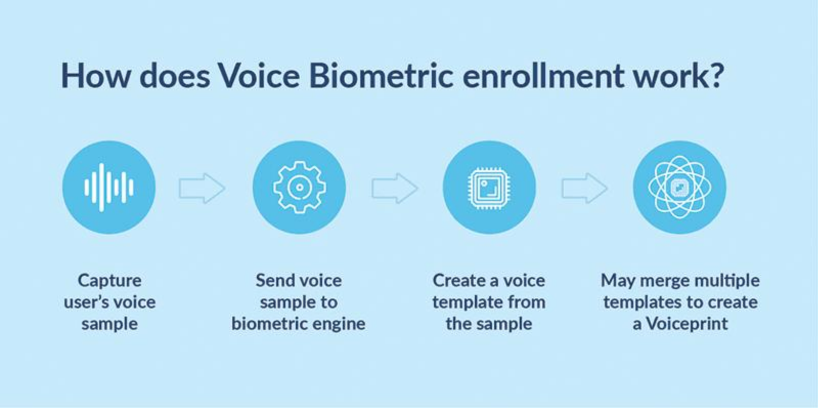
How does Voice Biometric enrollment work?
Capture user's voice sample
Send voice sample to biometric engine
Create a voice template from the sample
May merge multiple templates to create a Voiceprint

Fig. 9: Voice recognition method

4.4.2. Signature authentication

Using distinctive behavioural characteristics, such as pressure, speed, and stroke angle, captured during a handwritten signature on a digital device, biometric signature verification verifies an individual's identity. In contrast to conventional electronic signatures, this approach strengthens the connection between the signer and the document by adding behavioural data that is difficult to fabricate. Unlike current approaches that allow passwords to be cracked through trial-and-error, the signature identification cannot be replicated, as shown in Fig. 10 [17].

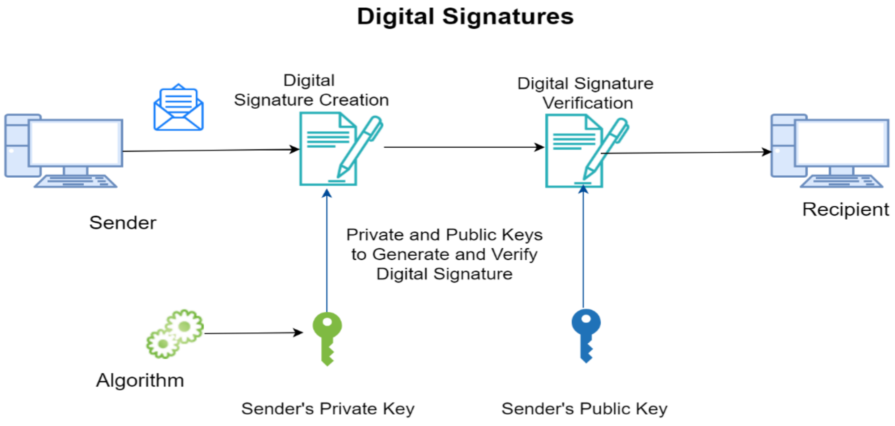
Digital Signatures
Digital Signature Creation
Digital Signature Verification
Sender
Recipient
Private and Public Keys to Generate and Verify Digital Signature
Algorithm
Sender's Private Key
Sender's Public Key

Fig. 10: Signature authentication

4.5. MFA (Multi-factor Authentication)

Multi-factor authentication (MFA) is a security process that requires a user to provide two or more distinct forms of verification to access an account or system, such as a password, a code from a trusted device, or a biometric scan, such as a fingerprint**.** It handles high-risk financial transactions and priority client information. An authentication mechanism's strength can be assessed by the number of factors it depends on [11]. By requiring multiple forms of verification to confirm a user's identity, Multi-Factor Authentication (MFA) improves system security. It gathers evidence from a variety of authentication principles, frequently spanning several devices, including knowledge-based, credential-based, and trust-based systems.

Passwords, PINs, biometric characteristics, and security tokens are common techniques used in MFA (Multi-Factor Authentication) or 2FA (Two-Factor Authentication) configurations. There are three primary types of authentication factors, as mentioned in Fig. 11:

- Knowledge (passwords, for example)
- Possession (such as security tokens or memory cards)
- Inherence (biometrics, for example)

MFA strengthens access control by requiring at least two factors from different categories, whereas Single-Factor Authentication (SFA) relies solely on knowledge-based credentials [12].

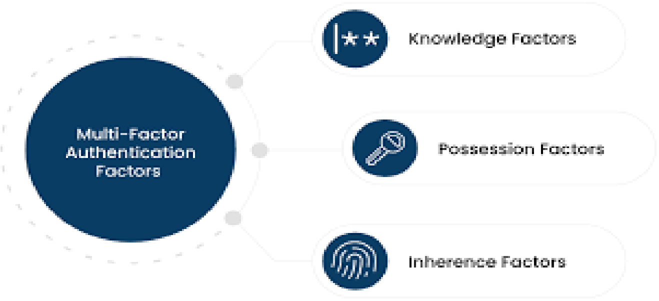

Fig. 11: Authentication Factor Categories

- **Knowledge:** Factors the user knows, typically in the form of alphanumeric information that must be kept private. The user must remember and correctly provide this information.
  Example: Passwords, Security question/answer pairs, PIN codes
- **Possession:** Factors the user has, physical objects or devices that store or transmit data, often using cryptographic techniques.
  Example: Physical keys, USB devices, Mobile phones, One-Time Passwords (OTPs), Smartcards
- **Inherence:** Factors that the user is, based on biometric or behavioural characteristics that are unique and difficult to replicate.
  Example: Fingerprint recognition, Face recognition, Voice recognition, Iris recognition, Signature recognition

5. Authentication Protocols and Standards

- Several standards and protocols have been developed to ensure secure authentication. Some common protocols include LDAP (Lightweight Directory Access Protocol), which is used in enterprise directories; Kerberos is widely used for secure authentication in Windows environments; RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) serve as vital protocols for remote network access, especially in VPNs and device-level security. Each protocol has different security characteristics and implementation requirements.
- Modern web applications increasingly rely on OAuth 2.0, a powerful authorisation framework that allows third-party applications to access user resources without exposing passwords.
- Emerging standards such as FIDO2 and WebAuthn promote passwordless authentication via biometrics or hardware keys, offering enhanced security and greater resistance to phishing. Supporting these systems are JWTs (JSON Web Tokens), which securely encode identity and session data, and PKI (Public Key Infrastructure), which uses digital certificates to authenticate users and encrypt data. Together, these protocols and standards form the backbone of modern digital security.

6. Security Considerations and Vulnerabilities

- Password-based authentication is highly vulnerable to phishing, brute-force attacks, and credential reuse, making it one of the weakest forms of security.
- Token-based methods, such as OTPs sent via SMS or email, are vulnerable to SIM swapping, interception, and phishing, while authenticator apps can be compromised if the device is lost or infected.
- Biometric authentication, although secure, can be spoofed with fake fingerprints or photos, and once biometric data is stolen, it cannot be changed.
- Behavioural authentication is susceptible to mimicry or behavioural drift and may produce false positives, especially under stress or when devices change.
- Multi-factor authentication (MFA) strengthens security, but methods like push notifications can be abused through “push fatigue” attacks, where users mistakenly approve fraudulent login attempts.
- Passwordless systems (e.g., FIDO2/passkeys) are highly secure, but device loss or lack of recovery options can lock users out.

Each method has its vulnerabilities, and layered security is essential to minimise risk. Even technically sound authentication systems are compromised by these actions. Thus, in addition to technical safeguards, user education and awareness initiatives are essential for effective authentication security.

6.1. Usability and User Experience

Authentication systems must balance security with usability. Traditional password-based systems often frustrate users due to forgotten credentials and frequent resets, leading to poor security practices like reuse. Biometric authentication (fingerprint, face ID) offers a fast and seamless experience, making it highly user-friendly. Token-based methods like OTPs or hardware keys can be secure but may add friction, especially if users lose access to their devices. Behavioural authentication operates passively, enhancing convenience without disrupting workflow. Passwordless authentication, using passkeys or biometrics, is emerging as the ideal balance providing both strong security and a smooth, frictionless user experience. Ultimately, systems that are easy to use are more likely to be adopted and followed correctly by users. As shown in Table 2.

Table 2: Comparison of Various Authentication Methods

Authentication Method	**Security strength**	**Usability**	**Implementation Complexity**	**Common use cases**
Password-based	Low to Medium	High	Low	Most online services
Token-based	Medium to High	Medium	Medium	Mobile devices, Physical access
Biometric	High	High	Medium	Enterprise systems, Banking
Behavioral-based	Medium	Very High	High	Government systems, Critical systems
Multi-factor	Very High	Medium to High	Medium to High	Critical systems

7. Emerging Trends and Future Directions

Authentication technology continues to evolve in response to emerging trends and changing user expectations. Adaptive or Risk-based authentication (RBA) is a dynamic security approach that evaluates the context of a login attempt, such as location, device, behaviour, or time, to assess risk. If a login is deemed suspicious, it triggers stronger authentication measures like OTPs or additional verification. RBA balances security and user convenience by adapting authentication requirements based on real-time risk.

- Behavioural authentication uses patterns like typing and mouse movements to verify identity continuously and detect unusual activity, improving security without disrupting users. Authentication systems use AI/ML to detect anomalies, continuously monitor sessions, and leverage behavioural biometrics to adapt authentication.
- Zero Trust Architecture is a security model based on the principle “never trust, always verify.” It requires continuous verification of every user and device before granting access, assuming no one is trusted by default. It enforces strict controls and monitoring to enhance security, especially in cloud and remote work setups.
- Passwordless authentication is rapidly becoming a key trend, replacing passwords with biometrics, security keys, and passkeys for stronger security and better user experience. Major companies and governments are driving their adoption to reduce phishing and credential theft. For example, Governments and large organisations are increasingly

replacing passwords with passkeys (FIDO2/WebAuthn-based) that pair public/private key cryptography. Germany, for instance, is moving toward using passkeys as a primary authentication method for many services.

8. Conclusion

Authentication is a critical component of cybersecurity, serving as the first line of defence against unauthorised access to systems and data. This research has examined various authentication methods, from traditional password-based systems to modern multi-factor and biometric approaches. Each method has strengths and weaknesses, but the evidence consistently shows that multi-factor authentication provides the best balance of security and usability for most applications. The evolution of authentication technology has been driven by the need to address vulnerabilities in existing methods while maintaining usability. Passwords, while still widely used, have significant security limitations due to human factors such as weak password choices and password reuse across multiple services. Biometric authentication offers greater security and convenience, but raises privacy concerns and cannot be changed if compromised. Multi-factor authentication addresses these limitations by requiring multiple independent factors, significantly reducing the risk of unauthorised access. Looking forward, the trend in authentication is moving toward passwordless systems that use biometric factors, possession factors, and behavioural analytics to verify identity without requiring users to remember complex passwords. Adaptive authentication approaches that adjust security requirements based on contextual risk factors offer promise for providing strong security without unnecessary user friction. These developments, combined with continued emphasis on user education and awareness, will help create more secure and usable authentication systems in the future.

References

[1] Park, J. K., Lee, H. S., Kim, S. J., & Park, J. P. (2015). A study on a secure authentication system using an integrated user authentication service. *Indian Journal of Science and Technology*, *8*(23), 1.

[2] Jain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. *Computer*, *45*(11), 87-92.

[3] Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access*, *7*, 5994-6009.

[4] Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A., & Pitchan, M. A. (2021). A systematic literature review of the types of authentication safety practices among internet users. *International Journal of Advanced Computer Science and Applications*, *12*(7).

[5] Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., ... & Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, *21*, e01743.

[6] Balaj, Y. (2017). Token-based vs session-based authentication: A survey. *no. September* 1-6.

[7] Prakash, A., & Kumar, U. (2018). Authentication protocols and techniques: a survey. *Int. J. Comput. Sci. Eng*, *6*(6), 1014-1020.

[8] Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, *2*(3), 13-28.

[9] Progonov, D., Cherniakova, V., Kolesnichenko, P., & Oliynyk, A. (2022). Behaviour-based user authentication on mobile devices in various usage contexts. *EURASIP Journal on Information Security*, *2022*(1), 6.

[10] Mahadi, N. A., Mohamed, M. A., Mohamad, A. I., Makhtar, M., Kadir, M. F. A., & Mamat, M. (2018). A survey of machine learning techniques for behaviour-based biometric user authentication. In *Recent Advances in Cryptography and Network Security*. IntechOpen.

[11] Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, *7*(1), 187-198.

[12] 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.

[13] Kolluri, V., Jain, S., Malaga, M., & Das, J. (2024). Advancing biometric security through AI and ML: a comprehensive analysis of neural network architectures for multimodal authentication systems. *International Journal of Communication Networks and Information Security*, *16*(5), 487-505.

[14] Hafeez, H., Zafar, M. N., Abbas, C. A., Elahi, H., & Ali, M. O. (2022). Real-time human authentication system based on iris recognition. *Eng*, *3*(4), 693-708.

[15] Ross, A., Jain, A., & Pankati, S. (1999, March). A prototype hand geometry-based verification system in *Proceedings of the 2nd conference on audio and video-based biometric person authentication* (pp. 166-171).

[16] Tiwari, M., & Verma, D. K. (2024). Real voice recognition and authentication system: a comprehensive review. *Int. J. Intell. Commun. Comput. Sci*.

[17] Navaz, A. S., & Durairaj, K. (2016). Signature Authentication Using Biometric Methods. *January 2016, International Journal of Science and Research, Vol. 5, Issue 1*, 1581-1584.