Int. J. Advanced Networking and Applications
Volume: 17, Issue: 03, Pages : 6922-6932 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17305

Evolving Security: A Comprehensive Analysis of Authentication Methods

Adnan Shaout
The University of Michigan Dearborn, The Electrical and Computer Engineering Department, Dearborn, MI
Email: shaout@umich.edu
Anik Hasmukhbhai Patel
The University of Michigan Dearborn, The Electrical and Computer Engineering Department, Dearborn, MI
Email: anikhp@umich.edu

----------ABSTRACT----------

This paper examines the classification and evolution of authentication methods, underscoring their pivotal role in cybersecurity. Early systems primarily employed knowledge-based techniques, such as passwords, but growing threats have driven a shift toward more secure methods, incorporating possession-based (e.g., smart devices) and inherence-based (e.g., biometrics) technologies. The study explores the development and adoption of two-factor (2FA) and multi-factor authentication (MFA), which combine multiple elements—knowledge, possession, and inherence—to provide stronger protection for sensitive digital assets. Further, emerging approaches such as location-based and behavior-based authentication are discussed, highlighting their potential to leverage contextual information and user habits for adaptive security solutions. Practical implementations, including automatic safe deposit lockers and intelligent smart cards, illustrate the integration of artificial intelligence (AI) and machine learning to dynamically assess risk, optimize memory management, and enhance user experience. These advances not only improve security but also add convenience for users. Through comprehensive analysis, the paper assesses the effectiveness and deployment of these authentication technologies, outlining future directions in digital security. By tracing the progression of authentication mechanisms, this research addresses the ongoing challenge of safeguarding digital identities and access in an increasingly interconnected and complex technology landscape.

Keywords – Artificial Intelligence, Authentication, Biometrics, Classification, Cybersecurity, Machine Learning, Multi-Factor Authentication

---

Date of Submission: August 10, 2025 Date of Acceptance: September 30, 2025

---

1. INTRODUCTION

Authentication is critical to securing digital systems [1], evolving from simple passwords to advanced methods in response to growing cyber threats. Traditional password systems proved insufficient as technology and cyber risks advanced, prompting the adoption of multi-factor authentication (MFA) and combining knowledge, possession, and inherence factors [2]. Modern approaches now encompass a diverse array of methods, including biometrics and adaptive systems powered by AI [3]. Looking ahead, innovations like blockchain and quantum computing are poised to further transform authentication methods, integrating with biometrics for enhanced security [3, 4]. Defense-in-Depth strategies apply multiple security layers for comprehensive protection [5, 6]. This research reviews the historical and current landscape of authentication, analyzes user experience, implementation challenges, and regulatory compliance, and anticipates future trends [4], [7], [8]. Additionally, practical implementations such as automatic safe deposit lockers and intelligent smart cards demonstrate advancements in security and user convenience [9], [10], [11], [12]. The goal is to inform researchers and practitioners on creating adaptable authentication frameworks for a connected world [13], guiding the design and deployment of next-generation solutions [14]. The paper reviews the literature (Section 2), classifies methods (Section 3), details technological applications (Section 4), proposes intelligent smart card solutions (Section 5), and concludes with findings (Section 6).

2. MATERIALS AND METHODS

This paper's literature review adopted a systematic approach to identify, screen, and include relevant studies. An initial pool of 7,367 records from databases such as Science Direct, IEEE, ResearchGate, ACM Digital Library, and others was consolidated for screening. Duplicates, unrelated topics, non-journal articles, and sources in unknown languages were excluded, reducing the dataset by 7,245 records. A full-text review was then conducted on the remaining studies, focusing on relevance to embedded systems and authentication, and peer-reviewed status, which led to the exclusion of 21 more records. The final review included 61 reports: 4 from Science Direct, 18 from IEEE, 14 from ResearchGate, 2 from ACM Digital Library, and 22 from other sources, ensuring high quality and relevance.

2.1 Classification of Authentication Methods

Table 1 categorizes authentication methods into three phases: Historical Authentication Methods, Emerging Authentication Technologies, and Future Directions in Authentication. This organization distinguishes past, present, and future approaches, providing a clear tem-

poral context for understanding the evolution and prominence of each technology. Each category will be examined in detail.

Table 1. Classification of Authentication Methods

Category	Methods	Period
Historical Authentication Methods	- Passwords and PINs-Based Authentication - Radio Frequency Identification (RFID)-Based Authentication - Question-Answer (Q&A)-Based Authentication	Up to 1990s
Emerging Authentication Technologies	- Geolocation-based Authentication - Single Sign-On (SSO)-Based Authentication - IP Address-Based Authentication - Proximity-Based Authentication - Two-Factor Authentication (2FA) - Multi-Factor Authentication (MFA) - Biometric Authentication - Behavioral-based Authentication - CAPTCHA	2000s to Present
Future Directions in Authentication	- Adaptive Authentication - Risk-Based Authentication - Blockchain-based Authentication - Artificial Intelligence (AI) and Machine Learning (ML)-Based Authentication - Zero Trust Architecture-based Authentication - Integration of AI and Quantum Technologies-based Authentication - Decentralized and Self-Sovereign Identity Systems-Based Authentication	Present to Future

2.1.1 Historical Authentication Methods

Authentication has been vital throughout history for ensuring trust and secure access. Early examples include seals, signatures, and secret passcodes. The introduction of PINs with ATMs in the 1960s and the widespread use of password-based authentication in the 1970s marked technological advancements [1], [2], [4]. Security questions were later implemented to reinforce authentication protocols.

Key historical methods include:

- Passwords and PINs: Used since ancient times and widely adopted in computer systems, but vulnerable to brute-force and phishing attacks [2], [7].
- User ID and Password: A fundamental mechanism utilizing a unique identifier and a confidential password, though susceptible to theft and brute-force attacks. Strong, unique passwords and multi-factor authentication are recommended [1], [4], [8].
- Customer ID and PIN: Essential in banking for user verification, with security depending on the confidentiality, complexity, and length of the PIN [1], [4], [8].
- RFID-based Authentication: Utilized for access management and transactions, employing verification protocols (including challenge-response and mutual authentication) and enhancing security through cryptographic measures

and PUFs [1], [8], [9], [13]. Future RFID authentication aims at lightweight, efficient protocols for IoT applications [14], [15].

- Question-Answer Based Authentication: Relies on personal information, providing an extra layer of security but remains vulnerable to social engineering and data breaches. Security can be increased with unpredictable, non-factual answers [16], [17].

These methods illustrate the origins of modern authentication and highlight the need for ongoing evolution in identity verification to maintain security in today's digital landscape.

2.1.2 Emerging Authentication Technologies

To address the evolving threat landscape and limitations of traditional methods, authentication technologies are adopting innovative approaches focused on user security and convenience. These methods utilize advances in biometrics, artificial intelligence, behavioral analytics, and cryptography to enhance authentication systems.

Key emerging technologies include:

- Geolocation-Based Authentication: Uses a user's physical location—gathered from GPS, Wi-Fi, IP address, or cellular towers—as an additional authentication factor, increasing security but raising privacy and accuracy concerns [18][19][20].
- Single Sign-On (SSO): Enables users to access multiple services with one set of credentials, simplifying user experience but introducing potential risks if the central provider is compromised.
- IP Address-Based Authentication: Controls access by verifying the user's IP address, providing a straightforward, scalable security option, especially when combined with VPN and multifactor authentication [18][19][21].
- Proximity-Based Authentication: Relies on Bluetooth or NFC to verify that a user is physically near a trusted device or location, improving usability and security for digital payments and IoT devices [22][23].
- Biometric Authentication: Leverages unique physiological traits—like fingerprints, facial recognition, iris and voice—for secure and convenient access. Combining biometrics with cryptography and MFA strengthens security, but raises privacy concerns [30]-[33].
- Two-Factor Authentication (2FA): Requires two forms of identification, increasing account security and encouraging the shift toward password-less solutions using biometrics and behavioral analysis [24][25][26].
- Multi-Factor Authentication (MFA): Expands on 2FA by layering multiple methods (e.g., biometrics, passwords, tokens), significantly reducing unauthorized access risk [27]-[30].
- Behavioral-Based Authentication: Analyzes unique patterns, such as keystroke dynamics, mouse movements, touchscreen gestures, and gait, for real-time, continuous user verification using machine learning [33]-[38].
- CAPTCHA: Differentiates humans from bots through visual, audio, or interactive challenges, and is evolving to adopt adaptive, behavior-based techniques using AI [39].

These emerging authentication technologies strengthen security, address privacy and adaptability challenges, and promise to improve the user experience as cyber threats become more complex.

2.1.3 Future Directions in Authentication

Authentication methods are rapidly evolving to respond to emerging cybersecurity threats and technological advancements. Key future directions include:

- Adaptive Authentication: Dynamically adjusts authentication requirements based on user activity and risk context, leveraging techniques such as adversarial training and anomaly detection to defend against evolving threats [40][41][42].
- Risk-Based Authentication: Assesses login risk using contextual data (location, device, behavior), adjusting security measures accordingly and providing stronger protection for suspicious access attempts [3][37][43][44][45].
- Blockchain-Based Authentication: Utilizes decentralized, tamper-proof ledgers for storing identity credentials, enhancing transparency and user control. Future developments enable cross-blockchain identity bridging, digital passports, and secure biometric storage via smart contracts [23][45][46][47][49][50].
- AI and Machine Learning-Based Authentication: Integrates pattern recognition and adaptive intelligence to detect anomalies, insider threats, and brute-force attacks, continuously optimizing security based on behavioral and contextual analytics [51]-[55].
- Zero Trust Architecture (ZTA): Moves beyond traditional perimeter security with continuous verification, granular access controls, micro-segmentation, and behavioral analytics, ensuring least privilege and MFA for all access [52][53][56][57].
- Integration of AI and Quantum Technologies: Combines AI's adaptive analysis with quantum-resistant cryptography and quantum key distribution for robust defenses against both current and future quantum computing threats, with applications in healthcare, IoT, and secure communications [14][52][53][58][59].
- Decentralized and Self-Sovereign Identity (SSI) Systems: Empowers users with control over identity data on decentralized networks, improving privacy and interoperability while reducing single points of failure [50][52]. Ap-

plications include smart contracts in decentralized finance (DeFi) and secure, traceable supply chains [60][61].

These future-focused methods aim to strengthen authentication resilience, privacy, and user control, addressing both present and emerging security challenges across various digital ecosystems.

3. INTEGRATION OF MULTIPLE AUTHENTICATION METHODS

Traditionally, safe deposit lockers relied on basic verification methods such as photograph matching and signature checks, limiting access to banking hours and requiring manual oversight. This system type transcends these limitations by incorporating a multilayered security framework that leverages RFID, card and PIN verification, OTP (One-Time Password), and future-ready biometric authentication methods, ensuring only authorized users are granted access at any time of day.

3.1. Multistep Authentication Process

The locker access workflow is designed for maximum security and convenience:

- Step 1: The customer presents their card and enters a confidential PIN, both of which are validated by the system.
- Step 2: Availability of the selected locker is verified in real time. If unavailable, users can select an alternative without restarting the process.
- Step 3: A time-sensitive OTP is generated and sent to the customer's registered device, adding an additional secure verification layer.
- Step 4: Upon successful multi-factor authentication, a robotic retrieval system brings the assigned locker to a private access cabin, preserving privacy.
- Step 5: The customer uses a physical key for the final stage of access, combining digital safeguards with tangible control.

  This process is meticulously logged, capturing access times, failed attempts, and system resets for a complete audit trail.

3.2. Distance-Based Biometric Authentication

Elevating security further, distance-based fingerprint sensors—utilizing both capacitive and ultrasonic technologies—allow for contactless biometric verification at the entrance to the locker vault:

- Initialization: The system activates on user proximity, reducing hold-ups and sensitivity issues from environmental conditions.
- Secure Matching: Captured fingerprint images undergo enhancement and are mathematically compared against Secure Element-stored templates, rejecting unauthorized users after multiple failed attempts with automatic security alerts.

3.3. Advanced Sensor Technology for Biometric Robustness

Capacitive and ultrasonic sensors create highly detailed 3D fingerprint profiles, capturing sub-surface data such as pores, sweat glands, and blood flow [50][52]. These features thwart spoofing, perform reliably even with dirt or moisture present, and offer liveness detection to differentiate between real and artificial fingerprints. Their durable, contactless design also minimizes wear, ensuring efficient, rapid authentication and maintenance-free operation.

3.4. Customer Information Console

A dedicated console situated in the vault corridor grants customers secure access to key account information—such as last access timestamp, yearly access history, locker deed expiration, and annual charges—via Customer ID and PIN. Stringent input validation, case sensitivity, and auto-logout after consecutive failed attempts add an extra shield against unauthorized data retrieval. All interactions are logged, maintaining data integrity and auditability.

3.5. Enhanced Security and User Experience Features

- Simultaneous Data Access: Customers can view multiple account or locker details in one session, streamlining the management of their valuables and related information.
- Built-In Error Recovery: The system's error handling enables users to correct mistakes without losing progress or being forced to restart complex authentication steps.
- Automatic Session Termination: The security model is proactive—users are signed out after three incorrect attempts, significantly reducing brute-force and unauthorized access risks.

Comprehensive Benefits and Impact:

The integration of these state-of-the-art authentication and access technologies not only transforms the safe deposit locker paradigm but also delivers tangible benefits, including:

- 24/7 Availability: Unrestricted access means increased convenience for customers.
- Reduced Operational Overhead: Automation cuts the need for constant staff supervision and lowers costs.
- Optimized Space Utilization: Automated systems allow for more lockers in the same physical area.
- Streamlined Audit and Compliance: Comprehensive record-keeping meets the regulatory demands of modern banking.
- Unparalleled Security and Privacy: Layered defenses, advanced biometrics, and robust audit mechanisms set a new benchmark for protecting high-value assets and personal data.

By adopting this advanced locker system, banks can offer customers unmatched convenience, transparency, and peace of mind, positioning themselves at the forefront of secure, customer-centric digital transformation in financial services.

3.6 Benefits of an Automatic Safe Deposit Locker with Integration of Advanced Authentication Technologies

An automatic safe deposit locker system equipped with state-of-the-art authentication technologies offers a

transformative upgrade over conventional banking solutions, delivering a multi-dimensional array of advantages that cater to both security and service excellence:

3.6.1 Enhanced Security: Such systems leverage breakthrough features—biometric authentication (including fingerprints and facial recognition), advanced multi-factor authentication (MFA), intelligent smart cards, and the adoption of Self-Sovereign Identity (SSI) protocols enabled by decentralized identifiers (DIDs). These robust layers significantly mitigate the risks posed by unauthorized access, insider threats, and fraudulent activities, setting new benchmarks for asset protection in banking [57].

3.6.2 Improved User Experience: User-centric design is a core tenet of these solutions. Intuitive interfaces, streamlined locker assignment, and easily navigable console systems empower customers to access their valuables with minimal friction. The integration of private access cabins not only maintains confidentiality but also elevates the overall sense of security and comfort during each transaction.

3.6.3 Convenience and Accessibility: One of the standout advantages is unrestricted 24/7 availability. Users can gain access to their locker at any time, independently of bank operating hours or staff schedules. This unparalleled accessibility enhances client satisfaction and broadens the user base to accommodate modern, fast-paced lifestyles.

3.6.4 Operational Efficiency: Automation replaces cumbersome manual processes, alleviating pressure on staff while minimizing human errors and delays. Smart systems manage locker assignment, monitor usage, and control access seamlessly, leading to faster turnarounds and elevated customer service.

3.6.5 Real-time Monitoring and Alerts: Advanced monitoring tools integrated into the system continuously track user activity. Automated real-time alerts and notifications are triggered in response to suspicious behaviors or failed authentication attempts, enabling banks to act swiftly and preemptively to safeguard assets and sensitive information.

3.6.6 Cost Savings: Although the initial deployment incurs capital expenditure, the system drives long-term cost optimization. The reduction in physical security personnel and paperwork, along with space-efficient designs that maximize vault capacity, translates into ongoing savings for financial institutions and customers alike.

3.6.7 Data Analytics and Insights: Automatic locker systems harness advanced data collection and analytics capabilities. By examining usage patterns and system interactions, banks can optimize locker allocation, personalize offerings, and spot emerging security trends for constant refinement of services.

3.6.8 Scalability: The modularity and flexibility of automated systems facilitate seamless scaling in line with institutional growth. Expansion or reconfiguration requires minimal structural change, ensuring the bank can meet fluctuating demand without disrupting operations.

3.6.9 Environmentally Friendly: Automation minimizes reliance on paper-based processes and manual record-keeping, promoting eco-friendly banking practices and aligning with sustainability initiatives.

With these transformative features and strategic benefits, automatic safe deposit locker systems represent the future of secure, efficient, and customer-focused banking. They not only fortify institutions against evolving security threats but also unlock new levels of convenience, accessibility, and operational agility—meeting the evolving expectations of both modern customers and forward-thinking financial organizations.

4. THE INTELLIGENT SMART CARD OF THE FUTURE FOR TRANSACTION APPROVAL

In today's increasingly digital financial landscape, ensuring secure, flexible, and user-centric authentication for financial transactions is paramount. RFID cards are already ubiquitous for access control and basic authentication, but their security remains susceptible to cloning, skimming, and unauthorized physical access. To address these limitations and prepare for the future of secure financial services, an intelligent multi-authentication smart card, or “3-in-1” card, that integrates RFID, PIN, and biometric fingerprint modalities, collaboration with advanced memory management, power solutions, data protection, and Self-Sovereign Identity (SSI) frameworks is needed.

The future intelligent smart card should allow the following three flexible and interconnected forms of authentication:

A. RFID Access:
Standard wireless authentication for routine entries or contactless approvals in common banking, workplace, or high-security settings. RFID still enjoys global infrastructure support, maximizing backward compatibility.

B. Card and PIN Authentication:
Conventional debit/credit card functionality with PIN entry, enabling secure access to banking terminals, retail checkouts, or ATM withdrawals.

C. Transaction Authentication through Fingerprint:
The integration of a capacitive fingerprint sensor embedded within the card’s structure marks a paradigm shift. No transaction is approved unless the registered cardholder’s unique fingerprint is presented on the sensor—providing an unforgeable physical verification step. Not only

does this reduce the card's vulnerability to theft and fraud, but it also minimizes the need for users to memorize or disclose sensitive PINs.

5. HARDWARE AND SECURITY ARCHITECTURE

The advancement in authentication and security in hardware are as follows:

A. Advanced Biometric Integration

- A miniaturized, high-resolution capacitive fingerprint sensor is embedded in the card, powered by an integrated ultra-thin battery.
- The card securely stores fingerprint data inside a Secure Element (SE or eSE), using powerful cryptographic techniques for storage and comparison.
- All captured templates and fingerprints never leave the device unencrypted. Match-on-card verification ensures biometric privacy.

B. Power Management Solutions

- DC charger port for conventional recharging of the battery.
- Motion-powered generation transforms card movement (e.g., swiping or inserting) into electrical energy, ensuring the card remains charged during regular use with no user intervention.
- Solar paper technology harvests both natural and indoor light to supplement the card's battery, providing eco-friendly, renewable power. These innovations guarantee the multi-functional card remains consistently operational.

C. Robust Data and Memory Protection

- Electromagnetic and electrostatic shielding (using ferrite beads) to divert disruptive energy safely, counter electromagnetic attacks, and prevent data corruption or unauthorized memory access.
- Multi-layered encryption guards all stored credentials (RFID IDs, PINs, biometric data) and ensures secure wireless and contact-based communication with payment terminals, card readers, or access-point controllers.

D. Memory Management and System Optimization

A unified memory architecture enables rapid, seamless interaction between authentication modes:

- Integrated Memory Handling:
  All credential data is dynamically managed via secure, partitioned memory pools. RFID tags, PINs, transaction logs, and fingerprint templates coexist within a protected, efficiently organized storage system.
- Advanced Encryption & Secure Storage:
  Memory is protected using modern cryptographic standards, with confidential data encrypted at rest and in transit.
- Intelligent Allocation:
  The system uses dynamic, adaptive allocation algorithms to minimize latency and maximize performance during simultaneous or rapid authentication requests, supporting high-frequency financial environments.

E. Optimized Access Control and Real-Time Verification

- Rapid Data Processing:
  Authentication algorithms prioritize speed and accuracy, delivering fast transaction approvals without compromising security. Matching and validation for all three modalities occur in real time, enhancing customer satisfaction and trust.
- Continuous Monitoring:
  Embedded software continuously monitors for anomalies or irregular access attempts, logging actions for compliance and providing early warnings to issuers about possible security risks.
- User Experience:
  Customers benefit from immediate feedback, minimized wait times, and frictionless interoperability across systems—contributing to a positive, secure experience.

F. Fraud Mitigation, Compliance and Autonomy

- Enhanced Security and Fraud Prevention:
  The tri-modal system nearly eliminates risks from card skimming, "tap-on" tech fraud, PIN theft (via shoulder surfing, phishing, or malware), and unauthorized duplication. Since biometric information cannot be guessed or shared, even if the card is stolen, transactions will not process without the rightful user's finger.
- Regulatory Compliance:
  Embedded privacy and security architectures facilitate compliance with mandates such as the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS).
- Self-Sovereign Identity (SSI) Compatibility:
  By supporting DIDs and verifiable credentials, the card not only allows secure, decentralized credential management but also fosters user sovereignty over identity, removes reliance on central authorities, and reduces single points of failure [50].

G. SSI (Self-Sovereign Identity) Framework: Framework and Implementation

- Requirements and Tech Stack: Development is built on blockchain technology for registering and managing DIDs, compliant with W3C and major industry standards.
- SSI Application Integration: The card embeds all required logic for RFID, biometric, and

payment operations, and stores/updates DIDs and VCs for multi-platform compatibility.
- Middleware and User Interface: Supporting mobile and web control, users can view, manage, and revoke credentials, transactions, and security settings in real time.
- Testing & Compliance: Rigorous physical and digital testing ensures operational integrity, compliance, and robustness of both hardware and software.
- Deployment, Onboarding, & Monitoring: Easy onboarding, proactive system monitoring, and instant support infrastructure guarantee a secure and smooth user transition.

6. REAL-WORLD IMPACT AND STRATEGIC ADVANTAGES

Some of the real word impact and strategic advantages of the authentication methods are as follows:

A. User and Institutional Benefits:
- Sets a new standard in secure, seamless banking, blending convenience and the highest security for both in-person and remote transactions.
- Providers can deploy fewer human resources for manual verification, decreasing operational costs.

B. Interoperability and Scalability:
- The unified design and standards compliance make it easy to integrate with new terminals, banking applications, and third-party authentication platforms both now and as the ecosystem evolves.
- Supports future-proof expansion with minimal infrastructure investment.

C. Sustainability:
- Eco-friendly charging reduces electronic waste and paperless, digital record-keeping promotes green banking practices.

D. Societal and Global Impact:
- Empowers users globally to control their identity, enhancing privacy, reducing identity theft, and facilitating secure cross-border payments and access.
- The decentralized identity model is especially valuable in developing regions where central authority reliability is limited.

The future intelligent smart card, through its multifaceted authentication options and robust SSI framework, brings security, autonomy, efficiency, and user convenience into the next era of digital transactions. Its holistic integration of hardware, encryption, identity protocols, and green power solutions addresses the multifarious needs of banks, users, and regulators. It should offer not just a secure transaction medium but a platform for the digital identity ecosystem of the future.

8. CONCLUSION

The evolution of authentication methods has been pivotal in advancing digital security, leveraging technological innovations to combat ever-evolving cyber threats. The journey from basic password protection to sophisticated, multi-layered approaches demonstrates how authentication continues to adapt to the complex requirements of modern digital environments, balancing the dual imperatives of security and user convenience.

Comparative Analysis and Insights: Table 2 offers a thorough comparison of diverse authentication techniques—from traditional passwords and PINs to state-of-the-art methods such as biometrics, blockchain, and AI-powered systems. This analysis evaluates each method's user experience, integration complexity, regulatory compliance, security strength, cost-effectiveness, and scalability. Such insights are invaluable for researchers and practitioners aiming to select or develop authentication solutions best suited for their specific contexts.

Innovations and Emerging Technologies: Recent advancements, including biometric modalities (e.g., fingerprints, facial recognition), adaptive authentication, and Self-Sovereign Identity (SSI), have introduced novel ways to enhance both the security and user-friendliness of digital identity management. The integration of artificial intelligence, machine learning, and quantum-safe cryptography is driving the next generation of authentication, enabling systems that are more accurate, robust, and resistant to emerging threats.

Call for Continued Research and Development: Despite these strides, several unresolved issues present avenues for future investigation and innovation:

A. Securing Biometric Data in Decentralized Systems:
   a. Exploring advanced encryption and secure sharing protocols to safeguard biometric information against breaches and misuse in decentralized networks.

B. Developing Quantum-Resistant Algorithms:
   a. As quantum computing matures, cryptographic methods must evolve to withstand quantum attacks, ensuring the continued protection of sensitive data.

C. Ensuring Privacy-Preserving AI Models:
   a. Future AI-driven authentication must be designed to minimize user data exposure, championing privacy rights even as these models process personal information.

D. Interoperability Among Authentication Systems:
   a. Seamless integration and standardization across diverse authentication protocols are essential to enhance both security and the user experience.

E. User Adoption and Usability Challenges:
   a. Understanding and addressing barriers to adoption through improved accessibility and user-friendly design is critical to the widespread success of advanced authentication technologies.

By engaging with these ongoing challenges and research directions, scholars and professionals can ensure that authentication systems remain robust, adaptive, and user-centric. This ongoing evolution is essential to safeguarding digital interactions and identities in a perpetually interconnected world. The insights provided—especially those highlighted in Table 2—serve as a foundation for future research and practical applications, supporting the advancement of secure and resilient authentication frameworks against both current and future cyber risks.

Table 2. Authentication Methods Comparison

Aspect	1. Passwords/PINs	2. Smart Cards	3. Q&A	4. Geolocation	5. SSO	6. IP Address	7. Proximity
User Experience	Forgettable	Convenient	User-dependent	Mobile seamless	Streamlined	Transparent	Physical access
Deployment & Integration	Easy, low cost	Card readers	With Q&A	With Geo services	With SSO	With network	With proximity
Regulatory Compliance	Data breach concerns	Compliance	Compliance	Location laws	Data protection	IP laws	Access control
Security	M	M	H	M	H	M	H
Cost-effectiveness	High	Medium	Medium	Medium	High	High	Medium

Aspect	8. 2FA (Password + OTP)	9. MFA	10. Biometrics	11. Facial	12. Iris	13. Voice	14. Behavioral
User Experience	Secure, slower	Enhanced	Privacy issues	Privacy issues	Accurate	Environmental	Continuous
Integration with Infrastructure	High	High	Medium	Medium	Medium	Medium	Medium
Scalability	High	High	Medium	High	High	Medium	High

Aspect	15. CAP-TCHA	16. Adaptive	17. Risk-Based	18. Blockchain	19. AI/ML	20. Zero Trust	21. AI/Quantum	22. SSI
User Experience	Disruptive	Dynamic	Adaptive	Decentralized	Predictive	Zero trust	Futuristic	Privacy-enhanced
Security	Low	High	High	High	High	High	High	High
Implementation Complexity	Low	Medium	High	High	High	High	High	High

Note that the ratings M, H, and L stand for medium, high, and low, respectively.

REFERENCES

[1]. Barkadehi M, Nilashi M, Ibrahim O, Fardi A, Samad S. Authentication Systems: A Literature Review and Classification. Telemat Inform. 2018 Mar;35. doi: 10.1016/j.tele.2018.03.018.

[2]. Bonneau J, Herley C, van Oorschot PC, Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: 2012 IEEE Symposium on Security and Privacy. San Francisco, CA, USA: IEEE; 2012 May. p. 553-67. doi: 10.1109/SP.2012.44.

[3]. Bhargav-Spantzel A, Squicciarini A, Bertino E. Privacy preserving multi-factor authentication with biometrics. In: Proceedings of the second ACM workshop on Digital identity management. New York, NY, USA: Association for Computing Machinery; 2006 Nov. p. 63-72. doi: 10.1145/1179529.1179540.

[4]. Chenchev I, Aleksieva-Petrova A, Petrov M. Authentication Mechanisms and Classification: A Literature Survey. In: Intelligent Computing. Cham: Springer International Publishing; 2021. p. 1051-70. doi: 10.1007/978-3-030-80129-8_69.

[5]. Xu Y, Guo Y, Kou W, Yang J, Zhou Z, Li F. D3IR: Securing Multi-Domain Networks via Extending Depth-in-Defense Strategies Across Nested Management Domains. In: 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Sanya, China; 2024. p. 1320-5. doi: 10.1109/TrustCom63139.2024.00185.

[6]. Godakanda ML, Cook DM. Honey in Depth: A Multi-Layered Deception Framework for Internet of Things Security. In: 2024 7th International Conference on Information and Communications Technology (ICOIACT). Ishikawa, Japan; 2024. p. 119-24. doi: 10.1109/ICOIACT64819.2024.10913376.

[7]. Herley C, van Oorschot P. A Research Agenda Acknowledging the Persistence of Passwords. IEEE Secur Priv. 2012 Jan;10(1):28-36. doi: 10.1109/MSP.2011.150.

[8]. Karim NA, Khashan OA, Kanaker H, Abdulraheem WK, Alshinwan M, Al-Banna AE. Online Banking User Authentication Methods: A Systematic Literature Review. IEEE Access. 2024; 12:741-57. doi: 10.1109/ACCESS.2023.3346045.

[9]. Juels A. RFID security and privacy: A research survey. Sel Areas Commun IEEE J. 2006 Mar; 24:381-94. doi: 10.1109/JSAC.2005.861395.

[10]. Tan C, Sheng B, Li Q. Secure and Serverless RFID Authentication and Search Protocols. IEEE Trans Wirel Commun. 2008 Apr;7(4):1400-7. doi: 10.1109/TWC.2008.061012.

[11]. Piramuthu S. Protocols for RFID tag/reader authentication. Decis Support Syst. 2007 Apr;43(3):897-914. doi: 10.1016/j.dss.2007.01.003.

[12]. Maes R, Verbauwhede I. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In: Towards Hardware-Intrinsic Security. 2010. p. 3-37. doi: 10.1007/978-3-642-14452-3_1.

[13]. Katzenbeisser S, Kocabaş Ü, Rožić V, Sadeghi A-R, Verbauwhede I, Wachsmann C. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon. In: Cryptographic Hardware and Embedded Systems – CHES 2012. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. p. 283-301. doi: 10.1007/978-3-642-33027-8_17.

[14]. El-hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A Survey of Internet of Things (IoT) Authentication Schemes. Sensors. 2019 Mar;19(5):1141. doi: 10.3390/s19051141.

[15]. Moschetta E, Antunes RS, Barcellos MP. Flexible and secure service discovery in ubiquitous computing. J Netw Comput Appl. 2010 Mar;33(2):128-40. doi: 10.1016/j.jnca.2009.11.001.

[16]. Rabkin A. Personal knowledge questions for fallback authentication: security questions in the era of Facebook. In: Proceedings of the 4th symposium on Usable privacy and security. New York, NY, USA: ACM; 2008 Jul. p. 13-23. doi: 10.1145/1408664.1408667.

[17]. Florencio D, Herley C, van Oorschot PC. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts.

[18]. Lu J-Z, Zhou J. On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks. In: WiCOM 2010: 6th International Conference on Wireless Communications Networking and Mobile Computing. 2010 Oct. p. 1-3. doi: 10.1109/WICOM.2010.5601341.

[19]. Kamil I, Olakanmi O, Ogundoyin S. A secure and privacy-preserving lightweight authentication protocol for wireless communications. Inf Secur J Glob Perspect. 2017 Nov; 26:287-304. doi: 10.1080/19393555.2017.1385116.

[20]. Shweta M, Tanvi P, Poonam S, Nilashree M. Multipurpose Smart Bag. Procedia Comput Sci. 2016; 79:77-84. doi: 10.1016/j.procs.2016.03.011.

[21]. Tourani R, Misra S, Mick T, Panwar G. Security, Privacy, and Access Control in Information-Centric Networking: A Survey. IEEE Commun Surv Tutor. 2018;20(1):566-600. doi: 10.1109/COMST.2017.2749508.

[22]. Li L, Zhao X, Xue G. A Proximity Authentication System for Smartphones. IEEE Trans Dependable Secure Comput. 2016 Nov;13(6):605-16. doi: 10.1109/TDSC.2015.2427848.

[23]. Velamakanni RS, Patwal DPS. Enhancing IoT Security Through Experimental Methods and Blockchain Integration. Educ Adm Theory Pract. 2024 May. doi: 10.53555/kuey. v30i5.4468.

[24]. Aloul F, Zahidi S, El-Hajj W. Two factor authentication using mobile phones. In: 2009 IEEE/ACS International Conference on Computer Systems and Applications. 2009 May. p. 641-4. doi: 10.1109/AICCSA.2009.5069395.

[25]. Sucasas V, et al. A privacy-enhanced OAuth 2.0 based protocol for Smart City mobile applications. Comput Secur. 2018 May; 74:258-74. doi: 10.1016/j.cose.2018.01.014.

[26]. Hu B, Tang W, Xie Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments. Neurocomputing. 2022 Aug; 500:741-9. doi: 10.1016/j.neucom.2022.05.099.

[27]. Das A, Bonneau J, Caesar M, Borisov N, Wang X. The Tangled Web of Password Reuse. In: Proceedings of NDSS 2014. 2014 Jan. doi: 10.14722/ndss.2014.23357.

[28]. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. Digit Health. 2023 May; 9:20552076231177144. doi: 10.1177/20552076231177144.

[29]. Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-Factor Authentication: A Survey. Cryptography. 2018 Jan;2(1). doi: 10.3390/cryptography2010001.

[30]. An introduction to biometric recognition | IEEE Journals & Magazine | IEEE Xplore. [Internet]. Available from: https://ieeexplore.ieee.org/abstract/document/1262027

[31]. Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J. 2001;40(3):614-34. doi: 10.1147/sj.403.0614.

[32]. Jain A, Ross A, Pankanti S. Biometrics: a tool for information security. IEEE Trans Inform Forensics Secur. 2006 Jul; 1:125-43. doi: 10.1109/TIFS.2006.873653.

[33]. Pereira TMC, Conceição RC, Sencadas V, Sebastião R. Biometric Recognition: A Systematic Review on Electrocardiogram Data Acquisition Methods. Sensors. 2023 Jan;23(3):1507. doi: 10.3390/s23031507.

[34]. Farid F, Elkhodr M, Sabrina F, Ahamed F, Gide E. A Smart Biometric Identity Management Framework for Personalized IoT and Cloud Computing-Based Healthcare Services. Sensors. 2021 Jan;21(2):552. doi: 10.3390/s21020552.

[35]. Mondal S, Bours P. A study on continuous authentication using a combination of keystroke and mouse biometrics. Neurocomputing. 2017 Mar; 230:1-22. doi: 10.1016/j.neucom.2016.11.031.

[36]. Mondal S, Bours P. Continuous authentication using mouse dynamics. In: Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI). 2013 Sep.

[37]. Teh PS, Teoh ABJ, Yue S. A Survey of Keystroke Dynamics Biometrics. Sci World J. 2013 Nov; 2013:408280. doi: 10.1155/2013/408280.

[38]. Bursztein E, Bethard S, Fabry C, Mitchell JC, Jurafsky D. How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation. In: 2010 IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE; 2010. p. 399-413. doi: 10.1109/SP.2010.31.

[39]. Freeman D, Jain S, Duermuth M, Biggio B, Giacinto G. Who Are You? A Statistical Approach to Measuring User Authenticity. In: Proceedings 2016 Network and Distributed System Security Symposium. San Diego, CA: Internet Society; 2016. doi: 10.14722/ndss.2016.23240.

[40]. Stobert E, Biddle R. The Password Life Cycle: User Behavior in Managing Passwords.

[41]. Macas M, Wu C, Fu W. Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. Expert Syst Appl. 2023 Oct; 238:122223. doi: 10.1016/j.eswa.2023.122223.

[42]. Kontaxis G, Polychronakis M, Keromytis AD, Markatos EP. Privacy-Preserving Social Plugins.

[43]. Bhargav-Spantzel A, Squicciarini A, Modi S, Young M, Bertino E, Elliott S. Privacy preserving multi-factor authentication with biometrics. J Comput Secur. 2007 Jul; 15:529-60. doi: 10.3233/JCS-2007-15503.

[44]. Rubavathy BA. Blockchain Based Secure Digital Identity Verification System for Robust Documents. Tuijin JishuJournal Propuls Technol. 2024 Apr;45(02). doi: 10.52783/tjjpt. v45.i02.6809.

[45]. Zyskind G, Nathan O, Pentland AS. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: 2015 IEEE Security and Privacy Workshops. 2015 May. p. 180-4. doi: 10.1109/SPW.2015.27.

[46]. Han Y, Wang C, Wang H, Yang Y, Wang X. A study of blockchain-based liquidity cross-chain model. PLOS ONE. 2024 Jun;19(6): e0302145. doi: 10.1371/journal.pone.0302145.

[47]. Yang Y, Wu L, Yin G, Li L, Zhao H. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet Things J. 2017 Apr; PP:1-1. doi: 10.1109/JIOT.2017.2694844.

[48]. Bernal Bernabe J, Canovas Sanchez JL, Hernández-Ramos J, Torres Moreno R, Skarmeta A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access. 2019 Nov; PP:1-1. doi: 10.1109/ACCESS.2019.2950872.

[49]. Li J. A review of identity authentication based on blockchain technology. Appl Comput Eng. 2024 Jan; 30:173-8. doi: 10.54254/2755-2721/30/20230094.

[50]. Yu D, Foster H, Fitzpatrick T. A Survey of Machine Learning Applications in Functional Verification.

[51]. Chaudhary R, Aujla G, Kumar N, Zeadally S. Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions. IEEE Internet Things J. 2018 Oct; PP:1-1. doi: 10.1109/JIOT.2018.2878707.

[52]. Ozkan Okay M, et al. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. 2024 Jan; PP:1-1. doi: 10.1109/ACCESS.2024.3355547.

[53]. Kayan Fadlelmula F, Qadhi S. A systematic review of research on artificial intelligence in higher education: Practice, gaps, and future directions in the GCC Citation. J Univ Teach Learn Pract. 2024 Apr;21. doi: 10.53761/pswgbw82.

[54]. Zhu G, Al-Qaraghuli Y. AI-Assisted Authentication: State of the Art, Taxonomy and Future Roadmap. 2022.

[55]. Kang H, Liu G, Quan W, Meng L, Liu J. Theory and Application of Zero Trust Security: A Brief Survey. Entropy. 2023 Nov; 25:1595. doi: 10.3390/e25121595.

[56]. Liu C, et al. Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity. 2024 May;7(1):20. doi: 10.1186/s42400-024-00212-0.

[57]. Zbinden H, Bechmann-Pasquinucci H, Gisin N, Ribordy G. Quantum cryptography. Appl Phys B. 1998 Dec;67. doi: 10.1007/s003400050574.

[58]. Li F. Application and challenges of artificial intelligence in cybersecurity. Appl Comput Eng. 2024 Mar; 47:262-8. doi: 10.54254/2755-2721/47/20241480.

[59]. Schueffel P. DeFi: Decentralized Finance - An Introduction and Overview. J Innov Manag. 2021 Dec;9: i. doi: 10.24840/2183-0606_009.003_0001.

[60]. Chang A, El-Rayes N, Shi J. Blockchain Technology for Supply Chain Management: A Comprehensive Review. FinTech. 2022 Jun; 1:191-205. doi: 10.3390/fintech1020015.

[61]. Gangopadhyay A, Chatterjee O, Chatterjee A. Hand shape based biometric authentication system using radon transform and collaborative representation based classification. In: 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013). 2013 Dec. p. 635-9. doi: 10.1109/ICIIP.2013.6707672.

[62]. Raina V. Integration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices. Int J Law Inf Technol. 2011 Dec; 1:15-25. doi: 10.5121/ijitcs.2011.1602.