Journal of Systems Architecture 162 (2025) 103402

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis

Phat T. Tran-Truong [a,b,*,1], Minh Q. Pham [a,b], Ha X. Son [c,*], Dat L.T. Nguyen [d], Minh B. Nguyen [d], Khiem L. Tran [e], Loc C.P. Van [f], Kiet T. Le [f], Khanh H. Vo [f], Ngan N.T. Kim [g], Triet M. Nguyen [f], Anh T. Nguyen [f]

[a] Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Viet Nam
[b] Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Viet Nam
[c] RMIT University, Ho Chi Minh City, Viet Nam
[d] Cantho University of Technology, Can Tho, Viet Nam
[e] Imutably Oy, Helsinki, Finland
[f] FPT University, Can Tho, Viet Nam
[g] FPT Polytechnic, Can Tho city, Viet Nam

ARTICLE INFO

Keywords:
Multi-factor authentication (MFA)
Digital payments
Biometric verification
Identity assurance
Security compliance
Authentication tools

ABSTRACT

This survey presents a systematic evaluation of Multi-Factor Authentication (MFA) practices in digital payment systems, analyzing their alignment with NIST Special Publications 800-63 guidelines. Through a comprehensive review of 70 academic papers published between 2017–2024 and 13 industry-based authentication tools, we examine how current implementations measure against Identity Assurance Level (IAL) and Authentication Assurance Level (AAL) standards. Our analysis reveals a significant gap between theoretical capabilities proposed in academic research and actual industry implementations, with 33% of tools relying primarily on OTP-based authentication despite more advanced methods being available. The survey identifies emerging trends like biometric authentication adoption (60% of analyzed papers) and varying regulatory compliance across sectors, with payment systems demonstrating 77% alignment with standards while IoT and E-Service domains show fragmented approaches. We propose a framework for developing adaptive authentication systems that balance security requirements with user experience through context-aware risk assessment. This work provides valuable insights for researchers, practitioners, and policymakers working to enhance the security and usability of digital payment authentication systems.

Contents

* Corresponding authors.
E-mail addresses: phatttt@hcmut.edu.vn (P.T. Tran-Truong), ha.son@rmit.edu.vn (H.X. Son).
[1] First author.

https://doi.org/10.1016/j.sysarc.2025.103402
Received 21 January 2025; Received in revised form 8 March 2025; Accepted 16 March 2025
Available online 26 March 2025

1. Introduction

Authentication, a fundamental component of most systems in the digital world, is the process of verifying the identity of a user, device, or system. It serves as the first line of defense in ensuring that access to resources and information is granted only to those who are authorized. The concept of authentication is not new; it has been a part of human society for thousands of years. In a long time ago, documents or the transactions were authenticated or authorized primarily by physical presence, i.e., for example, by applying the wax seal [1] or signet rings. By that time, Single-Factor Authentication (SFA) was mostly adopted by the community due to its simplicity and user friendliness [2,3]. For example, the use of a password (or a PIN) to confirm the ownership of the user ID could be considered. Apparently, this is the weakest level of authentication [4,5]. With the advent of the digital age, the need for setting up and upgrading reliable authentication mechanisms has become increasingly critical. Therefore, the concept of multi-factor authentication (MFA) was born (Fig. 1). MFA, a significant evolution in the field of digital security, is a method of verifying a user's identity by requiring them to present two or more separate pieces of evidence, or 'factors'.

These factors typically fall into one of three categories (Fig. 2): something the user knows (like a password), something the user has (like a physical token or a smartphone), or something the user is (like a fingerprint or other biometric trait). The primary purpose of MFA is to create a layered defense system. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. This makes MFA an effective tool in preventing unauthorized access to systems [6–8], data, and applications, thereby significantly enhancing the overall security posture of an organization. MFA is particularly important in protecting sensitive data and high-value transactions. Industries such as banking, healthcare, and government often employ MFA to protect customer data, comply with regulatory requirements, and maintain public trust. In the era of digital transformation, where data breaches and cyberattacks are increasingly common, MFA plays a pivotal role in safeguarding digital identities and assets. By requiring multiple forms of verification, MFA significantly reduces the risk of unauthorized access, providing a more secure and reliable authentication mechanism.

Problem: Despite the widespread adoption of MFA across industries, including digital payment systems, assessing its security remains a complex challenge. Our review of 70 academic papers (2017–2024) acknowledges that several studies have proposed systematic frameworks for evaluating MFA, such as authentication mechanisms for real-time data access in industrial wireless sensor networks [9], enhanced security bounds for two-factor authentication [10], and anonymity constraints in distributed systems [11]. Additionally, recent frameworks include Enhancing Online Transaction Security with Multi-Factor Authentication and Machine Learning [12], security analysis of MFA protocols, particularly in cloud-based systems [13], and a framework utilizing reversed Lagrange polynomial in Shamir's Secret Sharing (SSS) for secure authentication [14]. Another notable approach integrates MFA with multi-layer security mechanisms, incorporating access control, intrusion detection, and automated authentication method selection [15]. While these frameworks provide valuable insights, they primarily rely on generalized security metrics such as attack resistance, computational efficiency, or user experience. However, they often lack a structured approach to identity proofing rigor and authenticator

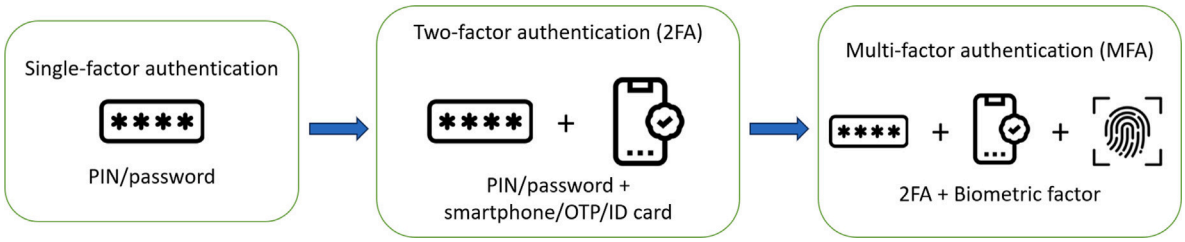


Fig. 1. The evolution of the authentication factor.

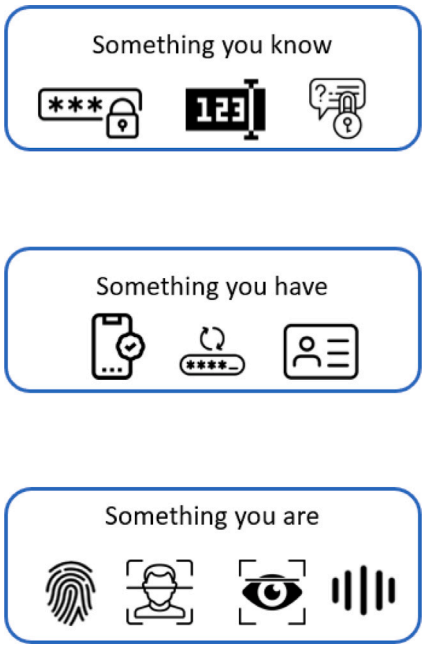


Fig. 2. Conceptual authentication examples.

assurance, aspects that the National Institute of Standards and Technology (NIST) addresses through its Identity Assurance Levels (IALs) and Authenticator Assurance Levels (AALs), and some frameworks such as [9–11,14], do not systematically incorporate NIST's structured approach to identity proofing (IAL) and phishing-resistant authenticators (AAL). Moreover, there remains a significant gap in academic research concerning a systematic evaluation of these solutions based on the National Institute of Standards and Technology (NIST) guidelines, such as Ali et al. (2020) [16] primarily analyzes threat models in two-factor authentication (2FA) schemes and proposes countermeasures, or Sinigaglia et al. [17] focuses on evaluating MFA solutions in the banking sector based on their resistance to specific attacker models. This gap underscores the need for a thorough investigation into how well current MFA solutions align with NIST standards, identifying potential shortcomings and areas for improvement.

The primary objective of this survey is to critically assess the existing body of literature on MFA from the years 2017 to 2024, using the guidelines established by the National Institute of Standards and Technology (NIST). The NIST guidelines, specifically SP 800-63 A [18], SP 800-63B [19], and SP 800-63C [20], correspond to Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL), respectively, and will be elaborated upon in the Background section of our survey. While numerous articles propose solutions to enhance the security of authentication systems, they have not been systematically evaluated against these NIST standards. Through our survey, we aim to bridge this gap by scrutinizing the extent to which current MFA practices align with these standards, thereby uncovering trends, identifying areas of improvement, and highlighting opportunities for future research. Furthermore, we will extend our evaluation to MFA-related tools, focusing on their analysis capabilities, support services, and the feedback they provide to developers in the design of authentication models pertinent to payment systems.

Architectural Considerations: The design of MFA systems presents complex architectural challenges that span multiple system levels. From microarchitecture design of authentication modules to system-wide software integration, these architectural choices critically influence the overall security, performance, and scalability of authentication mechanisms. Our research delves into these architectural dimensions, exploring how different design choices impact the effectiveness of authentication systems across various domains.

Our contribution: This survey makes several significant contributions to the field of MFA. *Firstly*, it provides a systematic and comprehensive review of the MFA literature from 2017 to 2024, offering a consolidated resource for researchers and practitioners alike. *Secondly*, it introduces a novel evaluation framework based on the National Institute of Standards and Technology (NIST) guidelines, specifically SP 800-63 A [18] and SP 800-63B [19], which correspond to IAL and AAL, respectively. This framework allows for a standardized assessment of MFA practices, facilitating comparison and benchmarking. *Thirdly*, our survey identifies gaps and trends in the current MFA practices, providing valuable insights for future research and development. It highlights areas where MFA practices align with NIST standards and where they fall short, offering a clear direction for improvement. *Lastly*, we extend our evaluation to tools related to MFA, providing a critical analysis of their capabilities, support services, and feedback they offer developers. This analysis can guide developers in designing more effective and secure authentication models for payment systems.

The rest of the paper is organized as follows: Section 2 provides a comprehensive evaluation of the existing literature and studies related to MFA in Payment Systems, Edge and Cloud Communication, E-Commerce, and Online Retail. Section 3 delves into the background information necessary to understand the complexities of MFA, including a detailed explanation of NIST's IALs and AALs. The section outlines our research methodology, detailing how we selected and analyzed the academic papers we collected. Section 4 presents a comprehensive analysis of the academic papers, discussing their alignment with the NIST standards, the trends observed, and the gaps identified. Section 5 provides an evaluation of industry tools, assessing their adherence to the NIST guidelines and their effectiveness in implementing MFA in payment systems. Section 6 presents a detailed discussion of our findings, synthesizing insights from academic literature and industry implementations, highlighting key trends, challenges, and opportunities in MFA practices. The prior work and conclusion are presented in Sections 7 and 8, respectively.

2. Background

2.1. Authentication system

Authentication system plays an important role in proving the security and integrity of various digital platforms, networks, and applications.

They serve as a primary means of verifying the identity of individuals or organizations before granting access to sensitive information, resources, or services. Authentication is a fundamental component of cyber Security and is deployed in many contexts, from user authentication on a website to an access control system in an enterprise. In [21], authentication systems are defined and classified on many different platforms.

Authentication systems are not merely a collection of security mechanisms, but intricate architectural constructs that require careful design considerations. The architectural design must balance multiple competing requirements: security robustness, system performance, user experience, and adaptability to evolving threat landscapes. This architectural complexity involves strategic decisions at multiple system levels, including module design, communication protocols, and integration strategies.

The primary goal of authentication systems is to establish trust and confidence in the identity of users or entities attempting to access a system. This process involves the presentation of credentials, such as usernames, passwords, tokens, or biometric information, which are then verified against stored records or communicate to a trusted authority for validation.

Passwords have long been the most commonly used form of authentication [22]. They require users to provide a unique combination of characters known only to them, serving as a secret key to access their accounts. However, passwords have several limitations, including vulnerability to brute-force attacks [23], weak user practices (e.g., using easily guessable passwords) [21], and the risk of being stolen or intercepted from man-in-the-middle (MiTM) attack or malware attack [21, 24].

For added security, *MFA* has become popular. MFA combines two or more authentication factors to provide an extra layer of protection. These elements fall into three main categories: *something you knows* (e.g. a password or personal identifier), *something you owns* (e.g. a smart card or hardware token) and *something you are* (e.g. biometric features like fingerprints or facial recognition). We will analyze MFA in more detail in Section 2.2.

2.2. Multi-factor authentication system

MFA is an advanced security mechanism that greatly enhances the authentication process by requiring users to provide multiple forms of verification. Unlike traditional one-factor authentication systems that rely solely on usernames and passwords, MFA systems introduce additional layers of security (Fig. 2. These layers typically include a combination of something you know 2.2.1 (such as a password or PIN), something you own 2.2.2 (such as a physical token or mobile device), and something you are 2.2.3 (such as biometric data including fingerprints or facial recognition). By combining these factors, MFA systems strengthen the security posture of computer systems and networks. Even if one element is compromised, an attacker still needs to overcome the other factors to gain unauthorized access. This multi-layered approach greatly reduces the risk of unauthorized access and provides strong protection for sensitive information.

MFA systems have been widely adopted in various industries, including finance [25–27], healthcare [28,29] and electronic services [30, 31], as they provide an effective means of protecting user accounts and important data from access attempts With the growing prevalence of cyber Security threats, the deployment of MFA systems has become imperative for organizations to ensure a high level of security for their assets. Their digital identity and user identity.

2.2.1. Something you know

Something you know is fundamental in multi-factor authentication and is often represented by a password or personal identification number (PIN). This knowledge-based element relies on user recall and provides a unique combination of characters or numbers associated with their account or system.

Passwords are the most common form known to users. They require the user to create a secret string of characters that only they know. Strong passwords are typically long, complex, and include a combination of upper and lower case letters, numbers, and special characters. The purpose of a password is to act as a “secret handshake” between the user and the system, verifying their identity and granting access.

However, there are some considerations and challenges associated with passwords. First, users tend to choose weak, easy-to-guess passwords, such as birthdays, names, or frequently used words [21,32]. This makes it easier for attackers to crack or crack passwords, especially if they have access to the user’s personal information. Second, users often reuse passwords across multiple accounts (in Fernando et al. (2023) [33], 45.7% of users keep the same password or the same password set for multiple web services), which increases the risk of a single password being compromised leading to unauthorized access to multiple systems.

To mitigate these problems, password management best practices include enforcing password complexity requirements, implementing a password expiration policy, and encouraging users to use a password manager to create and store strong, unique passwords for each account.

Following modern password security guidelines, such as avoiding common patterns and easy-to-guess information, using unique passwords for different accounts, and not sharing passwords with others are important steps in maintaining security. As noted by the National Cyber Security Centre (NCSC), forcing regular password changes can be counterproductive as it often leads users to choose weaker passwords or make minimal changes to existing ones [34,35].

2.2.2. Something you own

Something the user owns is another factor in multi-factor authentication that adds an additional layer of security to the authentication process. This factor typically involves the possession of a physical token or device that is unique to the user and is required to complete the authentication.

Physical tokens are commonly used as ownership factors. These can be hardware devices or smart cards that are issued to the user and are used as a means of authentication. The token is usually synchronized with the system or service being accessed and generates a unique one-time password (OTP) or a digital signature that is required for authentication. The user must physically possess the token and enter the OTP or use the digital signature to validate their identity.

Another form of ownership factor is the use of mobile devices. Many services offer the option of using a mobile application or a registered phone number as a means of authentication. In this case, the user links their mobile device to their account and receives OTPs or authorization prompts on their device. The user must have access to their mobile device to receive and respond to the authentication request.

When combined with knowledge factors like passwords, ownership factors contribute to a multi-layered security approach. The requirement for both physical possession of a token/device and knowledge of authentication credentials creates a more robust security system than either factor alone. This combination is fundamental to the principle of multi-factor authentication, where the strength lies in the integration of multiple independent factors rather than individual components [35].

However, it is important to consider the potential risks associated with ownership factors. Physical tokens can be lost, stolen, or damaged, which may lead to inconvenience or potential security. Mobile devices can also be compromised if they fall into the wrong hands or if the user does not adequately secure their device with strong passcodes or biometric authentication.

To mitigate these risks, users should keep their physical tokens secure and report any loss or theft immediately. They should also enable additional security features on their mobile devices, such as

Table 1
Entropy comparison of authentication methods [38].

Authentication method	Entropy (bits)	Reference
4-digit PINs	8.41	Wang et al. [36]
6-digit PINs	13.21	Wang et al. [36]
Fingerprint	18.6	Feng et al. [39]
Human-chosen passwords	20–22	Wang et al. [40]
Speech biometrics	15–20	Inthavisas et al. [41]

passcodes, fingerprint or facial recognition, and remote wipe capabilities. Organizations can implement measures to ensure the integrity and validity of the ownership factors, such as periodically refreshing or reissuing tokens and employing secure communication protocols with mobile devices.

2.2.3. Something you are

Something you are referring to the use of biometric data as a factor in multi-factor authentication. Biometrics involve unique physical or behavioral characteristics of an individual that can be used to verify their identity. Common examples include fingerprints, facial recognition, iris scans, voice recognition, and even behavioral biometrics like typing patterns or gait analysis.

While biometric data provides unique physical characteristics for identification, its security level needs careful consideration. Research has shown that the entropy of biometric authentication (e.g., fingerprints at 18.6 bits) can actually be lower than well-chosen passwords (20–22 bits) [36]. The security of biometric authentication depends not only on uniqueness but also on the information entropy of the biometric features, the quality of capture devices, and the robustness of the matching algorithms [37]. Additionally, unlike passwords or PINs which can be changed if compromised, the permanent nature of biometric traits presents unique security challenges [38].

The security strength of authentication factors is most accurately measured through entropy — the quantifiable level of unpredictability in an authentication system. When analyzing entropy values across different authentication methods, research reveals important security considerations. Wang et al. [36] demonstrated that human-chosen 4-digit PINs provide only approximately 8.41 bits of entropy, while 6-digit PINs offer slightly better protection at 13.21 bits. Fingerprint authentication, despite its biological uniqueness, offers approximately 18.6 bits of entropy as shown by Feng et al. [39], which is notably less than well-chosen passwords that typically contain 20–22 bits of entropy [40]. This quantitative comparison challenges the common assumption that biometric authentication inherently provides superior security based solely on physical uniqueness.

Additionally, Inthavisas et al. [41] highlight that speech biometric templates have similar entropy limitations. The entropy gap becomes particularly significant in high-security environments where the mathematical probability of authentication bypass through brute force or sophisticated attacks must be minimized. Furthermore, the static nature of biometric data means that once compromised, users cannot simply "change" their biometric identifiers, creating a fundamental security vulnerability not present with knowledge-based factors [38]. These entropy-based assessments provide a more objective framework for evaluating the actual security strength of different authentication factors beyond subjective assumptions about their resistance to attack.

Table 1 summarizes the entropy values across different authentication methods, clearly illustrating that biometric factors do not inherently provide higher security levels than well-designed knowledge-based factors when measured quantitatively.

When using biometrics as a factor in multi-factor authentication, there are several important considerations to take into account. First, the storage and protection of biometric data are critical. Since biometric traits are unique identifiers, they need to be securely stored to prevent unauthorized access. Biometric data should be encrypted and stored in a manner that prevents reverse engineering or reconstruction of the original biometric traits.

Another consideration is the possibility of false negatives or false positives. False negatives occur when a valid user is wrongly denied access, while false positives happen when an unauthorized individual is incorrectly granted access. These errors can be caused by factors such as poor-quality biometric samples, changes in biometric traits due to aging or injuries, or limitations in the biometric recognition algorithm being used.

Organizations must adopt robust security practices when implementing biometric authentication to address these concerns. These include secure storage and transmission of biometric data, strong encryption methods, liveness detection techniques to detect spoofing attempts, and regularly updating and refining recognition algorithms to enhance accuracy.

2.2.4. Overall rating

Mutual compensation can be achieved by leveraging the strengths of each factor while minimizing their respective weaknesses in multi-factor authentication (Table 2). Combining something the user knows, something the user owns, and something the user creates a robust authentication system that addresses different attack vectors and overall security.

The knowledge element offers familiarity and ease of use, but it can be vulnerable to password-related attacks. By combining it with the ownership element, which requires physical ownership of the token or device, the risk of unauthorized access is greatly reduced even if the password is compromised. However, the element of ownership can involve costs and potential risks if tokens or devices are lost or stolen. To further enhance security, the biometric element, which belongs to the user, adds an extra layer of uniqueness and convenience. It minimizes the risk of password-related attacks and involves the need for physical tokens, but it requires strong protection of biometric data and can lead to positive results. or negative. false negative.

Overall, the combination of these three factors in multi-factor authentication provides a balanced approach to security. It combines the familiarity and user-friendliness of knowledge, physical ownership, the uniqueness and convenience of biometrics. By carefully considering the strengths and weaknesses of each and implementing appropriate security measures, organizations can establish a strong authentication system that provides a higher level of trust, minimizes risks and protection from unauthorized access.

2.3. NIST SP 800-63B: Authentication and lifecycle management

2.3.1. Related information about NIST

The *National Institute of Standards and Technology* (NIST), an agency of the U.S. Department of Commerce, is recognized globally for its contribution to the creation and propagation of standards in multiple sectors, including information technology and cyber Security. Established originally as the National Bureau of Standards in 1901, it has been pivotal in establishing robust, reliable, and up-to-date standards that help to ensure the integrity, confidentiality, and availability of information systems worldwide.

NIST has been particularly influential in the development of authentication standards, a critical aspect of information security. This includes the NIST Special Publication 800-63 series, which encompasses SP 800-63 A [18], 800-63B [19], and 800-63C [20], each focusing on different aspects of the digital identity lifecycle. SP 800-63 A [18] ("Digital Identity Guidelines: Enrollment and Identity Proofing") establishes guidelines for the process of identity proofing. SP 800-63B [19] ("Digital Identity Guidelines: Authentication and Lifecycle Management") provides recommendations for the authentication process, including the selection and management of authenticators. Lastly, SP 800-63C [20] ("Digital Identity Guidelines: Federation and Assertions")

Table 2
Comparison of factors in multi-factor authentication.

Factors	Advantages	Disadvantages
Some-thing You Know	Widely familiar and established method of authentication.	Susceptible to password guessing, cracking, or phishing attacks.
	User-friendly and easy to use.	Users tend to choose weak passwords or reuse them across multiple accounts.
	Can be easily changed or reset if compromised.	Vulnerable to interception or theft through data breaches.
Some-thing You Own	Requires physical possession of the token or device.	Tokens or devices can be lost, stolen, or damaged, leading to inconvenience or security breaches.
	Adds an extra layer of security, even if the password is compromised.	Cost involved in issuing and maintaining physical tokens or devices.
	Provides flexibility with various types of tokens or mobile devices.	Tokens or devices may need to be replaced or reissued periodically.
Some-thing You Are	Biometric traits are unique and difficult to forge or replicate.	Biometric data storage requires strong security measures to protect against unauthorized access.
	Offers convenience and ease of use for users.	False negatives and false positives can occur due to variations in biometric traits.
	Eliminates the need for passwords or physical tokens.	Tokens or devices Biometric data cannot be changed if compromised, raising privacy concerns.

offers guidelines for the use of federated identity architectures and assertion technologies in the authentication process.

The contribution of NIST to authentication processes and protocols cannot be overstated. The Special Publication 800-63 series, in particular, serves as the gold standard for digital authentication, laying the groundwork for a comprehensive approach to identity management, from enrollment and proofing to authentication and federation. These guidelines play a crucial role in ensuring the security and privacy of individuals and organizations in the digital space, reducing the risk of unauthorized access and potential data breaches. As technology evolves and digital threats become more sophisticated, the role of NIST in providing these robust and adaptable guidelines is likely to become even more important.

2.3.2. The NIST special publication 800-63 series and research direction

The *NIST Special Publication 800-63* series lays out a comprehensive framework for digital authentication and identity lifecycle management. The series is divided into three parts (see Fig. 3): SP 800-63 A [18], SP 800-63B [19], and SP 800-63C [20], each addressing a distinct component of the digital identity and authentication process.

- SP 800-63 A [18], titled "Digital Identity Guidelines: Enrollment and Identity Proofing", delineates the procedures for identity proofing. This document provides a detailed roadmap for validating an individual's association with their real-world identity at the time of the digital identity enrollment. The document defines the Identity Assurance Level (IAL), which is a measure of the confidence in the claimed identity's validity. The IALs range from 1 (lowest confidence) to 3 (highest confidence) and depend on the rigor of the identity proofing process.
- SP 800-63B [19], "Digital Identity Guidelines: Authentication and Lifecycle Management", focuses on the authentication of the established digital identity over time, detailing the selection, management, and use of authenticators. It introduces the concept of Authenticator Assurance Level (AAL), which is a measure of the confidence in the authentication process. Like IAL, AAL also has three levels, from 1 (least assurance) to 3 (most assurance), based on the strength and verification of the authenticator(s).
- SP 800-63C [20], "Digital Identity Guidelines: Federation and Assertions", discusses how federated identity architectures and assertion technologies can be used to authenticate an individual across different systems or networks. It emphasizes the importance of managing and validating identity-related assertions in the digital space, ensuring interoperability across different systems while maintaining security and privacy.

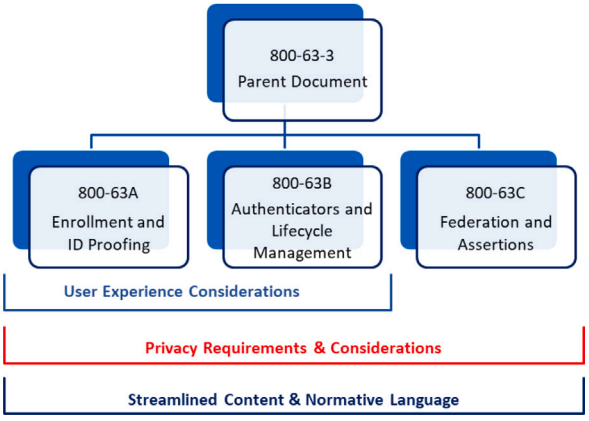


Fig. 3. The NIST special publication 800-63 series.

In our survey, we focus on the *Identity Assurance Levels (IALs)* and *Authenticator Assurance Levels (AALs)*, as defined in NIST's SP 800-63 A [18] and SP 800-63B [19] respectively, do not consider the*Federation Assurance Levels (FALs)* as outlined in SP 800-63C [20]. This decision is informed by our primary interest in the identity proofing and authentication processes, which are the heart of digital identity systems. While FALs are integral to a comprehensive understanding of digital identity architectures, they pertain specifically to federated identity systems and the trustworthiness of assertions in such setups. FALs become critical when considering single sign-on and similar scenarios where identity information is shared across different systems or networks. However, since our focus is more aligned with understanding the underlying identity proofing and authentication mechanisms, a detailed exploration of FALs is beyond the scope of this survey.

Moreover, our survey is not limited to examining academic papers on authentication methods alone. We believe that a comprehensive analysis should also include a consideration of the practical implementation of these concepts, as well as the challenges faced therein. Therefore, we extend our investigation to cover industry authentication tools as well. By doing so, we aim to bridge the gap between theoretical advancements and real-world applications, offering a more balanced and pragmatic perspective on the state of digital authentication methods and their alignment with NIST's guidelines.

By narrowing our focus to IAL and AAL, we aim to provide a comprehensive and detailed review of both the theory and practice

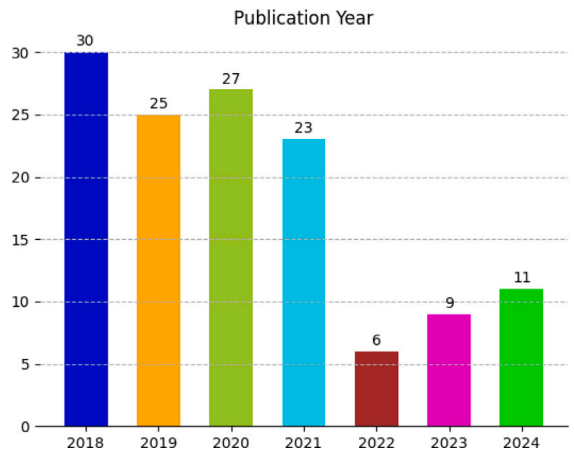


Fig. 4. Publication year of studied papers.

of identity proofing and authentication, thereby making a meaningful contribution to the literature on digital identity management. Through this work, we hope to facilitate a deeper understanding of the nuances of these processes, and the ways in which they can be effectively and securely implemented in both academic and industrial contexts.

3. Methodology

3.1. Search strategy

To achieve the objective of this survey, we collected academic papers that focus on MFA OR analyze security issues within MFA systems OR papers that mention some terms in NIST standard such as: *"identify proofing"* (or *"identify verification/evidence/service"*), *"biometric authentication"* (or *"biometric verification"*).

We selected the timeframe from January 1, 2018, to September 1, 2024, because the revision of NIST Special Publication 800-63 (Digital Identity Guidelines) introduced significant updates to the IAL and AAL frameworks, signaling a shift in authentication standards and practices. This period allows us to analyze the evolution of MFA implementation following the NIST revision, assess industry adoption of the updated standards, and evaluate contemporary authentication practices.

The selected papers were sourced from multiple English-language databases, including Springer, Elsevier, the IEEE Digital Library, MDPI, and other digital repositories. To ensure a comprehensive and relevant selection, we employed a systematic search strategy. This strategy involved using multiple databases and identifying a broad set of search terms pertinent to our research focus. We used the following list of keyword phrases, combining terms to increase specificity and relevance in our automated searches:

- "two-factor authentication" AND ("payment service" OR "mobile evaluation")
- "authentication" AND ("service design" OR "payment service")
- ("authentication" AND "threat model" AND "countermeasure") OR ("authentication" AND "payment service")
- "Multi-factor authentication" AND ("mobile payment" OR "evaluation")
- "Multi-factor authentication" AND "mobile payment" AND "usability"

Fig. 4 shows the breakdown of the number of relevant papers published each year from 2018 to 2024.

3.2. Inclusion and exclusion criteria

While our initial screening excluded papers that did not explicitly mention IAL and AAL, we recognize this may have limited our analysis. We have expanded our review to include papers that:

- Propose or evaluate authentication frameworks aligned with NIST principles, even if not explicitly referencing IAL/AAL.
- Present authentication schemes that can be mapped to IAL/AAL requirements.
- Discuss security levels or assurance requirements similar to NIST framework.

This broader inclusion allows us to:

1. Capture relevant works that may predate widespread NIST adoption.
2. Evaluate implicit alignment with NIST standards.
3. Provide more comprehensive coverage of authentication schemes.

To maintain the relevance and quality of the selected papers (focused on MFA practices and related security concerns), the additional inclusion criteria were as follows:

- Papers published after 2017.
- Keywords aligned with those used in our search strategy, ensuring a strong correlation with our research objectives.
- Papers explicitly discussing the development or analysis of MFA systems in payment services or digitalized environments.
- Papers accessible either via open access or through institutional subscriptions.

The exclusion criteria were:

- Patents, to focus on academic research rather than legal documentation.
- Duplicate papers from the same study, with only the most recent publication included.
- Papers published before or during 2017, to ensure the review is up to date.
- Inaccessible papers due to paywalls or subscription barriers.
- Grey literature or papers without a clear connection to authentication or security issues.

3.3. Data analysis methodology

Once the relevant papers were collected, we categorized them into five key domains: Mobile Payment, Authentication Technology, Internet of Things (IoT), Digital Finance, and Electronic Services. These categories represent significant areas of identification and authentication, helping to focus the review. The categorization was based on the primary focus of each paper, derived from its title and content.

The categorization process followed this methodology:

- **Mobile Payment:** Papers proposing MFA models for mobile payment systems, securing user data in such systems, or analyzing security threats to mobile payment transactions.
- **IoT:** Papers discussing MFA models for IoT devices or networks, or evaluating security solutions for IoT environments.
- **Electronic Services:** Papers that propose or evaluate MFA models or services for digital platforms like e-commerce and mobile payment, focusing on security issues in these services.
- **Digital Finance:** Papers discussing MFA-related challenges, models, or applications in securing digital finance services like banking and e-wallets, as well as analyzing security threats in these systems.

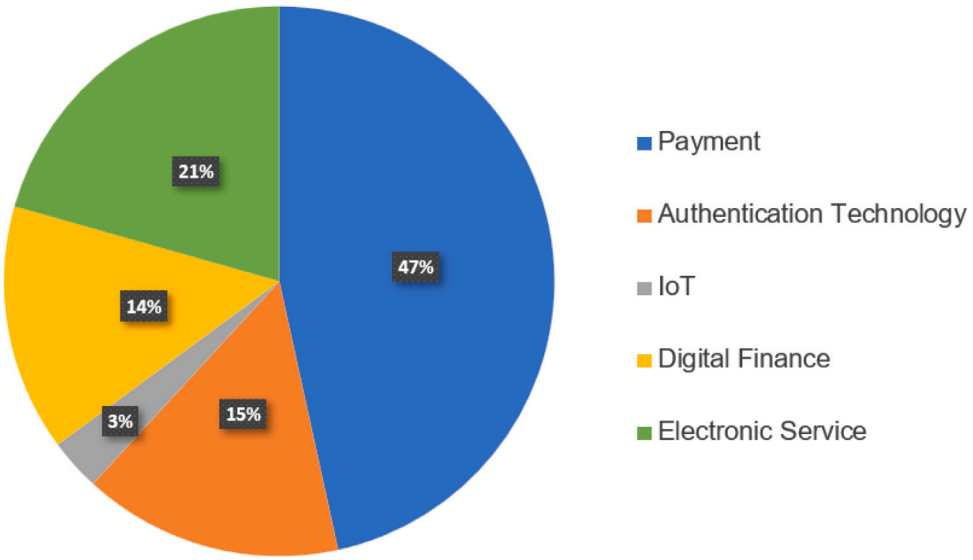


Fig. 5. Topics of research papers.

- **Authentication Technology:** Papers that explore the use of technologies such as blockchain or biometrics in MFA systems or analyze threats to these technologies.

From this categorization process, we collected a total of 131 papers: 61 papers on Mobile Payment, 20 on Authentication Technology, 4 on IoT, 19 on Digital Finance, and 27 on Electronic Services. A pie chart illustrating the distribution of these papers by category is shown in Fig. 5.

After 2017, NIST SP 800-63-3 and its related documents introduced a more structured and risk-based approach to digital identity guidelines. The standard clearly separates Identity Assurance Level (IAL), Authentication Assurance Level (AAL), and Federation Assurance Level (FAL), allowing organizations to implement authentication and identity verification methods that align with their specific risk profiles. It also emphasizes a risk-based approach, enabling organizations to evaluate and apply security measures according to the actual risk level of their applications. Furthermore, NIST encourages the adoption of advanced technologies such as multi-factor authentication, hardware-based security, and enhanced protection against phishing attacks. Alongside strengthening security, the updated standards also consider user experience, ensuring a balance between security and usability in authentication processes.

Due to this revision, we decided to use this update standard as defined in NIST Special Publications (SP) 800-63 A and 800-63B to analyze the security levels (IALs and AALs). We assessed the strengths and weaknesses of each MFA practice (after categorization) based on the context and risk factors associated with its domain. Additionally, we reviewed 45 industry-based tools that assist developers in designing authentication models, particularly in the payment process.

4. Systematic review of MFA papers

4.1. MFA paper collection process

We read and analyzed those 131 articles and removed those that we thought were surveys, in order to remove material that did not match the research objectives. As a result, 85 articles were re-selected. We then proceed to delete articles that did not explicitly mention IAL (Identity Assurance Level) and AAL (Authentication Assurance Level) to generate sample data more reliable. As a result we have obtained 70 remarkable articles for further research. Out of these 70 articles, we have categorized them by key themes to better understand and differences in uniformity and authenticity. This list includes 39 articles related to payment topic, 8 articles related to financial research, 15 articles about authentication technology, 1 research paper on IoT and 7 articles on e-services. The main aim of this study is to develop a comprehensive view of the performance and safety of current security systems. By comparing and contrasting different systems, we hope to spot differences in meeting requirements and demonstrate information security. The results of this study will help us better understand the challenges and opportunities in the field of security and authentication, and contribute to the development of better security systems in the future.

4.2. MFA research paper analysis

Following our overview of the studies mentioned in the list of 70, we have undertaken an in-depth review to provide our personal opinions and insights. It is crucial to note that these reviews are the result of rigorous analysis and critical assessment of each study's methodologies, findings, and implications.

Throughout the review process, we considered the research designs, sample sizes, data collection methods, and statistical analyses employed in each study. We also paid close attention to the clarity and coherence of the research objectives and how well they aligned with the reported outcomes. Our aim in conducting these reviews is to offer an objective evaluation while acknowledging that our analysis may be influenced by our own experiences, expertise, and perspective. By recognizing the subjective nature of our opinions, we hope to foster a transparent and open discourse around the findings presented in these studies. In addition to the scientific aspects, we also explored the broader significance and potential applications of the research within the respective fields. Our reviews aim to uncover the practical implications of the studies and their potential contributions to advancing knowledge in relevant areas. While we strive to maintain objectivity, it is important to acknowledge that no review process is entirely free from bias. Therefore, we encourage readers to consider multiple perspectives and consult the original studies to form their own informed judgments.

In conclusion, our reviews offer a comprehensive evaluation of the selected studies, with the intention of shedding light on their strengths and limitations. It is our hope that these insights will not only serve as a valuable resource for researchers and academics but also contribute to the broader dissemination of knowledge and the pursuit of further research in the field.

4.2.1. Payment

Konoth et al. [42] present a research paper that addresses the weaknesses in existing two-factor authentication (2FA) schemes used for secure online transactions. The authors propose SecurePay, a solution that provides isolation, integrity, and authenticity guarantees for mobile-based 2FA. The key findings of the study include the successful implementation of SecurePay on commodity mobile phones, even in the presence of a compromised operating system. By leveraging ARM TrustZone technology, the authors achieve the desired security properties. Moreover, SecurePay can be seamlessly integrated into existing applications with minimal modifications, offering a secure alternative to insecure SMS-based 2FA solutions. The methodology employed by Konoth et al. [42] involves a thorough analysis of the requirements for securing mobile-based 2FA transactions. The authors discuss the design and implementation challenges of SecurePay and highlight the significance of formal verification, making their solution the first formally-verified one in this domain. A notable strength of the paper lies in its practicality. SecurePay can be easily integrated into various applications, providing improved security without extensive code modifications. Additionally, the authors' emphasis on formal verification enhances the credibility and reliability of SecurePay, bolstering its overall effectiveness. In conclusion, Konoth et al. [42] present a significant contribution with SecurePay, a solution that strengthens the security of mobile-based 2FA. Their findings demonstrate the successful implementation and practicality of SecurePay, while the emphasis on formal verification ensures its robustness and reliability.

Ibrahim and Hashim [43] propose a secure model for M-payment transactions that incorporates Two-factor authentication and Tokenization techniques. The study focuses on enhancing transaction authentication and confidentiality, which are crucial factors in mobile payment security. The authors highlight the importance of authentication and confidentiality in mobile payment systems as money transitions from traditional forms to electronic formats. The proposed model aims to address security concerns by implementing Two-factor authentication and Tokenization. The authors modify the Tokenization technique algorithm to generate spatial x509 certificates for mobile wallets, adding an additional security layer to each transaction. The strengths of the thesis lie in its emphasis on security in M-payment transactions. The proposed model offers enhanced transaction authentication and confidentiality, providing a practical solution for mobile payment security. The implementation on the Android platform demonstrates the feasibility and applicability of the proposed model. In summary, Ibrahim and Hashim [43] contribute to the field of M-payment security by proposing a secure model that incorporates Two-factor authentication and Tokenization. The study emphasizes the importance of authentication and confidentiality and provides a practical approach for addressing security concerns in mobile payment transactions.

Wolters and Jacobs [44] on "The security of access to accounts under the PSD2" Wolters and Jacobs [44] examine the security implications of the revised Payment Services Directive (PSD2) in their research paper. The PSD2 aims to promote the development of an integrated market for payment services while ensuring consumer protection, secure payment transactions, and protection against fraud. Wolters and Jacobs [44] address the question of how the access granted to payment initiation service providers and account information service providers balances the development of the market for payment services with the security of the payment account and the privacy of the user. An analysis of the PSD2 shows that the development of the market for payment services has a higher priority, with security and privacy being ultimately subordinate. First, Wolters and Jacobs [44] find that the PSD2 does not adequately protect the personal data of the users. The definition of 'account information service' is broad and covers a wide range of services, allowing payment service providers to circumvent the limitations of the access to accounts. Next, Wolters and Jacobs [44] highlight that the payment service providers have a 'fallback option' that allows 'screen scraping' if the dedicated interface is not functioning properly. Although this access is constrained by several safeguards, the fallback option gives the payment service providers unlimited access to the account of the user. Finally, Wolters and Jacobs [44] point out that the payment service providers have considerable freedom to arrange their authentication process as they see fit, and the banks are required to trust this process. The PSD2 and regulatory technical standards do not demand that a bank is able to verify the authentication or the integrity of the payment order. A notable strength of the paper by Wolters and Jacobs [44] lies in their critical analysis of the security implications of the PSD2. By identifying the shortcomings and potential risks, they contribute to the ongoing discussion about balancing market development with user security. Their paper serves as a valuable resource for policymakers, regulators, and industry stakeholders seeking to enhance the security and privacy aspects of the PSD2. In conclusion, Wolters and Jacobs [44] shed light on the security of access to accounts under the PSD2. Their findings underscore the need to address the inadequacies in protecting user data, limiting fallback options, and ensuring robust authentication processes. Their insights provide valuable guidance for future improvements to the PSD2 framework.

Tran [45] examines the security implications of mobile payment by conducting a case study on MOMO, the most popular digital wallet in Vietnam. The objective of the study is to assess the effectiveness of the security technologies implemented by MOMO. To investigate the problem, Tran [45] conducts theoretical research and studies based on the working and security principles of mobile payment and e-wallets. The study aims to expand knowledge and provide a deep understanding of mobile payment. It explores different types of mobile payment technologies, their advantages and disadvantages, and compares the benefits and drawbacks of mobile payment in comparison to traditional payment methods. Additionally, the study addresses the threat model associated with all stakeholders involved in mobile payment and proposes security measures for each stakeholder. The security testing of MOMO e-wallet is carried out using the OWASP Top 10 as the primary guideline. Quantitative research methods and experiments are employed by Tran [45] to identify security threats that can be considered as vulnerabilities in mobile payment. Primary data is collected to gain familiarity with MOMO and perform practical security evaluations. The analysis is conducted for each security risk using a separate framework. Based on the summary of the security test results, the identified factors are considered as valuable lessons to enhance m-commerce in the future. The research findings highlight the continuous and diverse development of mobile payment. Tran [45] examines the security mechanism of MOMO and verifies its security system. The thesis contributes to a better understanding of mobile payment and digital wallet security. It serves as a reference for further studies on mobile payment security and MOMO security enhancement. In conclusion, Tran [45] presents a significant contribution through the case study on mobile payment security, specifically focusing on the popular digital wallet, MOMO. The research provides insights into the security technologies employed by MOMO and the broader landscape of mobile payment security. The study enhances knowledge in the field and offers valuable guidance for future research and security enhancements in the realm of mobile payments.

Bhargava et al. [46] delve into the Unified Payment Interface (UPI), a modern payment system introduced in India by the National Payment Corporation of India (NPCI). The research paper highlights the significant growth of UPI since its inception in 2016, driven by the strong push from the Indian government and the increasing popularity of smartphone-based payment systems, which now facilitate over two billion transactions per month. However, the authors point out the lack of comprehensive safety and security testing for this sensitive technology that enables money transfers between users. The paper thoroughly examines the introduction of digital payments in India and provides a detailed analysis of the Unified Payment Interface's technology, focusing on its architecture and security systems through a comprehensive review of dynamic and theoretical literature. Bhargava

et al. [46] highlight that UPI represents a significant improvement over existing payment systems in terms of cost-effectiveness, ease of use for consumers, transaction speed, and security, leading to widespread user adoption. The automated API-based design of UPI paves the way for the development of innovative solutions for both consumers and businesses. The authors emphasize that UPI has reached a high level of maturity, and the continued development of vendor UPI solutions will further enhance user acceptance. They argue that UPI has the potential to bring a large segment of the population into the digital economy and can serve as a valuable investment tool for India's economic growth. In conclusion, Bhargava et al. [46] present a comprehensive analysis of the expansion of the Unified Payment Interface in India. Their research sheds light on the transformative impact of UPI in revolutionizing digital payments and driving financial inclusion. The paper highlights the strengths of UPI, such as its cost-effectiveness, user-friendly design, and enhanced security measures. It also underscores the importance of continued investment in UPI solutions to improve user acceptance and maximize its potential as a catalyst for India's digital economy.

Bartoszczyk-Brzoskowski [47] conducts a comprehensive evaluation of the second payment service directive (PSD2) and its impact on the cyber security of payment service users. The research paper employs a multi-faceted approach, encompassing academic theory, regulatory acts, and qualitative studies, to assess the purpose and specific cyber security measures associated with the directive. The study begins by analyzing 27 academic papers to identify the underlying purpose of the PSD2. By synthesizing the findings from these literature sources, Bartoszczyk-Brzoskowski [47] elucidates the primary objectives of the directive. Subsequently, the research delves into evaluating three key regulatory acts – 2015/2366 (PSD2), EBA/GL/2017/17, and EBA/RTS/2017/02 – that form the foundation of the PSD2. This evaluation aims to identify the specific cyber security measures outlined in these acts, which directly influence the safety of payment service users. Moreover, the paper presents a qualitative study involving three key stakeholders: a traditional bank, a third-party service provider, and a legislator. Through this empirical analysis, Bartoszczyk-Brzoskowski [47] assesses the real-world impact of the second payment service directive on these institutions and explores additional implications that emerged as a result of the policy's introduction to the payment market. Overall, Bartoszczyk-Brzoskowski [47] provides a comprehensive examination of the purpose and impact of the second payment service directive on the cyber security of payment service users. By synthesizing academic theory, evaluating regulatory acts, and conducting qualitative studies, the paper sheds light on the measures implemented to enhance cyber security and safeguard users' payment transactions. The research serves as a valuable resource for policymakers, regulators, and industry stakeholders seeking to understand the implications of the PSD2 and develop effective cyber security strategies in the payment services landscape.

Jamil et al. [48] present a groundbreaking research paper that introduces "PetroBlock", a blockchain-based payment mechanism designed specifically for fueling smart vehicles. With the rapid advancements in information technology and the growing adoption of smart cities, technology-oriented companies, particularly car manufacturers, have introduced various features to enhance user privacy and comfort. The emergence of smart vehicle technology has paved the way for the widespread use of machine-to-machine (M2M) communication, including third-party financial services that support M2M transactions. While these monetary systems primarily focus on reliability and security, they often overlook aspects such as user behavior and needs. The paper highlights the potential privacy and security issues associated with conventional practices, such as sharing bank cards or credentials for money withdrawal on behalf of others. To address these concerns, Jamil et al. [48] propose a novel blockchain-based strategy that enables seamless and secure payment for fueling smart cars without human intervention. The proposed system ensures transparency, privacy, and trust by leveraging blockchain technology to facilitate data sharing among system users while safeguarding sensitive information. Furthermore, the research paper introduces a blockchain-based secure privacy-preserving strategy for fueling payment between the fuel seller and the buyer, eliminating the need for human intervention. The authors also conduct analytical evaluations and experiments to assess the usability and efficiency of the proposed blockchain platform. The performance of the system is evaluated using Hyperledger Caliper, considering factors such as transaction latency, transactions per second, and resource consumption. The introduction of PetroBlock by Jamil et al. [48] offers a promising solution for secure and automated payment in the context of fueling smart vehicles. By harnessing the potential of blockchain technology, the proposed mechanism ensures transparency, privacy, and trust while eliminating the risks associated with traditional payment practices. The research contributes to the advancement of payment systems in the automotive industry, addressing the evolving needs of users in an increasingly connected and technologically driven world. Overall, the paper by Jamil et al. [48] provides valuable insights into the development of blockchain-based payment mechanisms for smart vehicles, showcasing the potential of this technology to enhance privacy, security, and efficiency. The research findings and analytical evaluations contribute to the understanding and implementation of secure and automated payment systems, serving as a valuable reference for researchers, industry professionals, and policymakers in the field of smart transportation.

Omotubora and Basu [49] delve into the regulation of e-payment systems, focusing on the analytical approaches that extend beyond private ordering. With the rise of technology-driven payment instruments and services, e-commerce has experienced significant growth. However, the implementation of these systems faces security concerns, particularly in developing countries. This article takes a closer look at the limitations of private ordering in regulating e-payment systems, using Nigeria as an example of a developing country that is actively advocating for a regulatory framework based on private ordering. The authors argue that while technical standards and self-regulation by the financial industry are important, the role of law as a regulatory mechanism is largely overlooked. Omotubora and Basu [49] propose that the law should be utilized as a means to establish and enforce compliance with technical and industry standards. By doing so, trust can be built, public interest concerns can be addressed, and the regulatory process can be legitimized. The article highlights the significance of incorporating legal frameworks into the regulation of e-payment systems, particularly in developing countries where the adoption and implementation of such systems are on the rise. By integrating legal mechanisms, regulations can provide a robust foundation for ensuring the security and reliability of e-payment systems. This approach goes beyond private ordering and recognizes the necessity of a legal framework to safeguard the interests of users and stakeholders. The authors utilize Nigeria as a case study to exemplify the need for a regulatory framework based on legal mechanisms. They emphasize that technical standards and self-regulation alone are insufficient to address the complexities and challenges associated with e-payment systems. The law plays a vital role in setting and enforcing compliance with industry standards, thereby enhancing trust, safeguarding public interests, and legitimizing the regulatory process. In conclusion, Omotubora and Basu [49] shed light on the importance of regulatory approaches that go beyond private ordering in the realm of e-payment systems. Their analysis emphasizes the need for legal frameworks to complement technical standards and self-regulation. By proposing the utilization of law as a means to establish compliance and address public interest concerns, the authors provide valuable insights for policymakers, regulators, and stakeholders involved in shaping the regulatory landscape of e-payment systems. Their work contributes to the ongoing discourse on enhancing the security and legitimacy of e-payment systems through effective regulation.

Abraham [50] explores the Unified Payment Interface (UPI) in the context of India's digital transformation and its pursuit of greater cyber sovereignty. The article commemorates the 5-year anniversary of

Digital India and highlights the significance of UPI as an indigenous innovation that has played a pivotal role in preparing India for the challenges posed by the COVID-19 pandemic and reducing reliance on foreign technologies, such as the ban on China-made apps. The author emphasizes that India's experience with UPI offers valuable lessons that can be emulated by other countries aspiring to provide affordable, ubiquitous, and high-quality digital payment services to their citizens. While many countries are still awaiting market-driven solutions, the Indian government's interventionist approach and the fostering of private–public partnerships have yielded positive outcomes. However, Abraham [50] acknowledges the need for course corrections to safeguard the UPI ecosystem. The article underlines the importance of cyber sovereignty, which refers to a country's ability to exercise control over its cyberspace and digital infrastructure. By developing and promoting UPI, India has demonstrated its commitment to enhancing its cyber sovereignty, reducing dependence on foreign payment systems, and nurturing its own digital ecosystem. The UPI's success has been attributed to the collaborative efforts between the government, financial institutions, and technology providers. Abraham [50] suggests that other countries can learn from India's UPI model by adopting an interventionist approach and fostering public–private partnerships. This approach enables governments to play an active role in shaping their digital payment ecosystems and ensures the availability of affordable and reliable services to the public. The author also highlights the need for continuous efforts to protect the UPI from emerging risks and vulnerabilities. In conclusion, Abraham [50] sheds light on the achievements and lessons from India's UPI experience, emphasizing the importance of cyber sovereignty and indigenous digital payment systems. The article offers valuable insights for policymakers and stakeholders in other countries who seek to enhance their digital payment infrastructure. By examining India's interventionist approach and public–private partnerships, the author advocates for a proactive role of governments in shaping the digital payment landscape and ensuring affordable and secure services for their citizens.

Petry and Moormann [51] present a research paper titled "Mobile Payment in the Connected Car: Developing Services Based on Process Thinking" in the Business Systems Research journal. Petry and Moormann's paper explores the transformation of the automotive world into suppliers of mobility services. The authors emphasize the significance of customer processes and connectivity driven by the Internet of Things. Mobile payment plays a crucial role as an enabler for these services. The objectives of Petry and Moormann [51] are to demonstrate promising ways of designing payment-enabled services for connected cars based on process thinking and to validate their approach using the methodology of use cases. The authors conduct semi-structured interviews with industry experts to validate their use case study. The results of Petry and Moormann's [51] study suggest that the core characteristics and challenges of payment-enabled services in connected cars can be predicted in advance using the theoretical framework presented in the paper. Specifically, the paper outlines the necessary steps for a driver's request for on-demand horsepower for a specific time span, along with mobile payment for this service. The conclusions drawn by Petry and Moormann [51] highlight that the connectivity paradigm, complemented by mobile payment options, enables consistent implementation of customer centricity in terms of process thinking. Petry and Moormann's [51] research paper makes a significant contribution by demonstrating how payment-enabled services in connected cars can be designed based on process thinking. The practical approach and validation through industry expert interviews enhance the credibility of their findings. The paper provides valuable insights for stakeholders in the automotive industry looking to leverage mobile payment and process thinking to develop innovative services for connected cars.

Antonio Martinez Villegas et al. [52] focuses on investigating the factors that influence small business owners' decisions to use electronic payment services, specifically within the context of the national awareness campaign initiated by the Central Bank of Egypt. The researchers employed a mixed-methods approach to gather data for their study. They conducted a self-administered questionnaire to collect primary data and conducted interviews with three bank managers to gain additional insights. The questionnaire, available in both English and Arabic, was distributed among 150 participants. Secondary data from the literature review and past research were also utilized. The statistical package for the social sciences (SPSS) was employed to analyze the collected data. The findings of the study reveal several important insights. The researchers found a moderate positive relationship between the perceived usefulness of electronic payment services and small business owners' decision to use them. Additionally, a positive relationship was observed between the perceived ease of use and the adoption of e-payment services. Conversely, there was a negative relationship between the perceived risk associated with electronic payment and small business owners' decision to use it. The implications of this research are significant, particularly in understanding the factors influencing small business owners' decisions to adopt electronic payment services. It provides valuable insights into how to enhance the success of electronic payment systems and promote their usage among individuals in Egypt. By considering the perceived usefulness, ease of use, and addressing potential risks, policymakers and stakeholders can work towards improving electronic payment services to meet the needs and expectations of small business owners. Overall, the study by Antonio Martinez Villegas et al. [52] sheds light on the factors influencing the adoption of electronic payment services by small businesses. The findings contribute to the existing knowledge in this area and can guide future initiatives aimed at promoting the benefits of electronic payment in Egypt.

Ramesh et al. [53] present a research paper titled "NPCI: chartering a payment freeway" that focuses on the National Payment Corporation of India (NPCI). The authors highlight the significant growth of NPCI over the past decade, with the organization aiming to achieve 100 million transactions per day. Initially established as a collaborative effort between the Reserve Bank of India and the Indian Bank's Association, NPCI aspires to become the leading global payments network and aims to provide payment services to every Indian. The paper emphasizes NPCI's presence across various segments, including B2B, B2C, B2G, P2P, B2B, and G2P, and highlights its pivotal role as the backbone of India's payment system. NPCI has successfully developed universally acclaimed products and services such as UPI, BHIM, NACH, and more. Notably, NPCI operates in the FinTech World on a not-for-profit basis, which showcases its commendable achievements. The authors also discuss how NPCI's resilience was put to the test during the COVID-19 lockdown. NPCI responded swiftly to the challenges posed by the lockdown and social distancing measures, utilizing the opportunity to introduce rapid technological changes. Overall, Ramesh et al. [53] shed light on the remarkable growth and accomplishments of NPCI in the Indian payment landscape. The organization's vision, extensive reach, and successful products and services position it as a key player in the financial technology sector. The paper highlights NPCI's adaptability and responsiveness in times of crisis, emphasizing its commitment to leveraging technology for the benefit of the Indian population.

D'souza [54] presents a research paper titled "Cashless India: getting incentives right" that delves into the debate surrounding digital transactions and the concept of a "cashless" economy in India. The paper aims to outline a suitable strategy that can propel the Indian economy towards a cashless state. The author begins by introducing a theoretical model of the digitalization process, which identifies key structural parameters that determine a nation's readiness to transition from a cash-based economy to a cashless one. D'souza [54] evaluates India's performance on these parameters and identifies areas of deficiency. Additionally, the paper draws insights from the experiences of Sweden, a country that has made significant strides towards becoming cashless, as well as the rapidly transitioning economy of China. By studying these cases, D'souza [54] explores the lessons India can learn and apply to its own cashless journey. The paper contributes to the

ongoing discourse on cashless economies and provides valuable insights into the challenges and opportunities India faces in its pursuit of a cashless society. By emphasizing the importance of appropriate incentives and strategies, D'souza [54] encourages a more nuanced understanding of the factors that can drive India's digital transformation.

Geewax [55] presents a research paper titled "Design Principles for Third-party Initiation in Real-time Payment Systems". The paper focuses on the increasing recognition of Real-Time Payment (RTP) systems as essential infrastructure for facilitating peer-to-peer and commercial payments in various countries. The author highlights the successful implementation of Unified Payments Interface (UPI) in India, emphasizing the significance of third-party initiation of payments in driving adoption and functionality. The objective of the paper is to establish guidelines and best practices for incorporating third-party participants in RTP systems, particularly as payment initiators. The guidelines proposed in the paper are categorized into three key areas: security, privacy, and user experience. These guidelines are derived from a comprehensive analysis of the consequences associated with different alternatives, real-world integration experiences with diverse systems, and the development of a reference implementation of Third-party Payment Initiation (3PPI) using an open-source RTP system called Mojaloop. By drawing on this research, Geewax [55] provides implementation guidelines for incorporating support for 3PPI in an RTP system. The paper contributes to the understanding of how third-party participation can be effectively integrated into real-time payment systems while addressing security, privacy, and user experience considerations. Overall, Geewax's work highlights the importance of designing robust and user-friendly systems that accommodate third-party initiation in real-time payment environments. The research aims to facilitate the development and adoption of efficient payment systems that meet the evolving needs of users and promote wider financial inclusion.

Basin et al. [56] present a research paper titled "Card Brand Mixup Attack: Bypassing the PIN in non-Visa Cards by Using Them for Visa Transactions". The paper explores a vulnerability in EMV transactions that involves inducing a mismatch between the card brand and the payment network. Typically, an authorization request is sent from a merchant's payment terminal to the card issuer over a payment network operated by the card brand, such as Visa or Mastercard. The authors demonstrate that it is possible to manipulate the terminal's perception of the card brand, leading to a card brand mixup attack with significant security implications. This attack allows criminals to use a victim's Mastercard contactless card for making high-value purchases without knowledge of the card's PIN. The paper describes how the attacker tricks the terminal into perceiving the card as a Visa card and subsequently applies a PIN bypass attack previously reported on Visa. The authors have developed an Android application and successfully carried out this attack on transactions involving both Mastercard debit and credit cards. Notably, they conducted a transaction exceeding 400 USD using a Maestro debit card. Furthermore, the authors extend their formal model of the EMV contactless protocol to identify and verify fixes for the discovered vulnerabilities, ensuring the development of effective countermeasures. The research conducted by Basin et al. [56] sheds light on the potential security risks associated with card brand mixup attacks in EMV transactions. By exposing this vulnerability and providing concrete examples of successful attacks, the paper underscores the need for robust security measures in payment systems to safeguard against such exploits. The findings contribute to the ongoing efforts to enhance the security of card-based payment protocols and mitigate the risk of unauthorized transactions.

Kumar et al. [57] present a research paper titled "Security Analysis of Unified Payments Interface and Payment Apps in India". The paper focuses on the security analysis of the Unified Payments Interface (UPI) protocol and payment apps used in India. Since 2016, smartphone-based payment apps have gained significant popularity in India, with billions of dollars transacted through these apps. The UPI protocol, introduced by the Indian government, serves as the underlying infrastructure for many of these apps. However, there has been a lack of comprehensive security analysis of this critical infrastructure supporting money transfers. The authors employ a principled methodology to conduct a detailed security analysis of the UPI protocol. They reverse-engineer the design of the protocol by studying seven popular UPI apps. Through their analysis, they uncover previously unreported design-level flaws in the UPI 1.0 specification related to multi-factor authentication. When combined with an attacker-controlled application, these flaws can lead to significant attacks. In some extreme cases, these vulnerabilities can allow an attacker to link and empty a victim's bank account, even if the victim has never used a UPI app. The potential attacks are scalable and can be carried out remotely. The paper discusses the methodology employed by the authors and addresses the challenges they encountered in reverse-engineering the unpublished application layer protocol of UPI. Notably, all UPI apps in India undergo a rigorous security review and are designed to resist analysis, making the task more challenging. The research resulted in the discovery of several Common Vulnerabilities and Exposures (CVEs), and one of the reported attack vectors was subsequently addressed in the UPI 2.0 version. The findings presented by Kumar et al. [57] emphasize the importance of conducting thorough security assessments of payment protocols and applications. By exposing the vulnerabilities in the UPI protocol, the research contributes to the ongoing efforts to enhance the security and resilience of India's mobile payment ecosystem. The identified flaws and reported CVEs serve as valuable insights for improving the design and implementation of future versions of the UPI protocol, ultimately ensuring safer and more secure transactions for users.

Tommasi et al. [58] investigate the security risks in micropayment systems, specifically focusing on operator centric micropayments (OCM). With the widespread adoption of micropayment systems, there is an increased interest from computer criminals and dishonest entities to exploit vulnerabilities for unauthorized access to personal data and financial theft. The authors introduce a new attack technique called mobile session fixation, which targets an OCM system used by millions of users. The mobile session fixation attack allows a criminal to obtain the payer's phone number and potentially orchestrate the theft of funds. The paper not only describes this attack technique but also proposes countermeasures and provides insights into potential threats that require further analysis. The study sheds light on the security risks associated with micropayment systems and offers recommendations to mitigate those risks. By highlighting the vulnerabilities in OCM systems and suggesting countermeasures, the authors contribute to the ongoing efforts to enhance the security of micropayment systems. In summary, Tommasi et al. [58] examine the mobile session fixation attack in micropayment systems, emphasizing the importance of addressing security concerns in these systems. The paper provides valuable insights into the risks associated with OCM and proposes countermeasures to mitigate those risks.

Mega [27] presents a doctoral thesis focused on improving the security of mobile money applications (MMS) in Tanzania. The study addresses the security flaws associated with the usage of personal identification numbers (PINs) as the sole authentication method for accessing MMS, which can be easily forged, shared, or observed during entry, leading to unauthorized access. The thesis proposes a framework for enhanced security in MMS through the implementation of a two-factor authentication (2FA) system combining PIN and iris biometric authentication. The aim is to provide secured access to MMS in Tanzania. The research utilizes a mixed research approach, combining observation, literature review, and user perceptions obtained through questionnaires. To develop the mobile money application based on the proposed framework, a rapid application development (RAD) approach is employed. Use-case and flow chart diagrams depict the information flow between mobile money users (MMU) and mobile network operators (MNO). Various tools and programming languages, including Microsoft Visio, MySQL database, Android Studio, PHP, JSON, and

Java, are utilized in the development process. The evaluation of the developed mobile money application demonstrates positive results. A significant percentage of customers and agents strongly agree that implementing the proposed framework would eliminate unauthorized access to MMS. Additionally, a majority of customers and agents express acceptance and willingness to use the developed mobile money application based on the proposed framework. The implementation of the 2FA system incorporating PIN and iris biometric authentication proves effective in mitigating unauthorized access to MMS. The study recommends mobile network operators and other stakeholders to consider the findings as a roadmap for improving the security of accessing MMS. In summary, Mega [27] contributes to the field of mobile money security by proposing a framework that combines 2FA and iris biometric authentication to enhance the security of mobile money applications in Tanzania. The thesis emphasizes the limitations of PIN-based authentication and provides practical solutions for securing access to MMS.

Ciccarello [59] presents a PhD thesis focused on the design and development of a mobile payment application, with a secondary objective of comparing its performance with the Lightning Network, a payment system for the Bitcoin cryptocurrency. The thesis acknowledges the increased use of digital payments in the wake of the global pandemic and the evolving regulations surrounding digital finance, particularly the European Payment Service Directive (PSD). The thesis specifically addresses two important aspects influenced by PSD regulations: stronger security requirements through multi-factor authentication and the implementation of an architecture enabling banks and financial institutions to share customer account information with third-party payment service providers. The primary goal of the thesis is to examine the design and development process of a digital payment mobile application, which was achieved in collaboration with a Turin-based IT company specializing in digital payment solutions. The author's contribution to the project involved drafting the Security Analysis document and implementing Android modules for user registration within the mobile application. The thesis discusses various factors considered during the software development process, including architectural patterns, actors involved, and security requirements. The application allows users to link payment instruments from different bank accounts and perform banking operations. Its release was scheduled for the summer of 2021 after six months of development. Additionally, the thesis compares the performance of the mobile payment application with the Lightning Network, a payment system for Bitcoin. Performance measures for Lightning Network payments were obtained through simulations using the CLoTH Lightning Network simulator, based on a snapshot captured on December 17, 2020. Performance measures for the mobile payment application were computed from an IT audit conducted in September 2020. The results indicate that the traditional payment methods used in the application have a higher success rate compared to the Lightning Network (99.97% vs. 82.73%, respectively). However, the Lightning Network is still in the early stages of development, and efforts are being made to improve its performance. The thesis highlights the strong evolution of the digital payments landscape, particularly in the European context, driven by regulations promoting efficiency and openness. Financial institutions are encouraged to adopt more community-oriented networks, moving away from closed banking applications. Concurrently, cryptocurrency-based solutions are gaining interest in the social scenario, with their potential adoption driving the development of increasingly reliable and effective payment solutions. In summary, Ciccarello [59] contributes to the field of mobile payment systems by presenting a detailed examination of the design and development process of a mobile payment application. The thesis also provides insights into the performance comparison between the developed application and the Lightning Network. The research emphasizes the evolving landscape of digital payments and the importance of security, efficiency, and openness in the development of payment solutions.

Sturgess et al. [60] present a research paper titled "Watch-Auth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch". The paper introduces a system that utilizes the tap gesture performed on a smartwatch when making a payment as a biometric for user authentication and intent recognition. The proposed system is designed to operate purely in software on the smartwatch, without requiring updates to payment terminals. It is compatible with various types and positions of terminals, and the intent recognition component does not rely on any training data from the user. To validate the system, the authors conduct a user study involving 16 participants. Wrist motion data is collected from users as they interact with payment terminals, including long-term data from a subset of 9 participants during their daily activities. Based on the collected data, the authors identify optimal gesture parameters and develop authentication and intent recognition models. The Equal Error Rates (EERs) achieved for authentication and intent recognition are 0.08 and 0.04, respectively. In summary, Sturgess et al. [60] propose a system called WatchAuth that leverages the tap gesture on a smartwatch for user authentication and intent recognition in mobile payments. The research demonstrates the feasibility of using the tap gesture as a biometric without requiring changes to payment terminals. The authentication and intent recognition models achieve promising results, indicating the potential of this approach for enhancing the security and user experience of mobile payments.

Ali et al. [61] present a research article titled "A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications". The article addresses the security vulnerabilities of mobile money schemes that rely solely on two-factor authentication (2FA) using a personal identification number (PIN) and subscriber identity module (SIM). The study aims to develop a more secure and efficient authentication algorithm for mobile money applications by combining PIN, a one-time password (OTP), and a biometric fingerprint. The algorithm enhances the security of mobile money authentication by using secure hashing algorithm-256 (SHA-256) for PIN and OTP, Fast IDentity Online (FIDO) biometric fingerprint with RSA-based public key cryptography, and Fernet encryption for QR code and database records. The researchers adopt the evolutionary prototyping model to develop native mobile money application prototypes and demonstrate the feasibility and security of the proposed algorithm. The developed applications are tested, and a comprehensive security analysis is conducted. The results show that the proposed multi-factor authentication algorithm is secure, efficient, and effective against various threat models. It provides enhanced authentication, data confidentiality, integrity, non-repudiation, user anonymity, and privacy. Furthermore, the performance analysis indicates that the proposed algorithm outperforms existing mobile money systems. In summary, Ali et al. [61] propose a secure and efficient multi-factor authentication algorithm for mobile money applications. The algorithm combines PIN, OTP, and biometric fingerprint to enhance the security of mobile money authentication. The research demonstrates the feasibility of the algorithm through native mobile application prototypes and provides a detailed security analysis. The proposed algorithm offers improved security and performance compared to existing mobile money systems.

Vincent et al. [62] present a research article titled "An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security". The study addresses security breaches and violations of user privacy in mobile payment systems and proposes an improved security scheme using elliptic curve cryptography (ECC) over a binary field with International Mobile Equipment Identity (IMEI) for enhanced security. The scheme incorporates a payment gateway for user registration and maps input text to elliptic curve points using ASCII values. Payment details are encrypted and stored on the gateway, and decryption can only be performed using the merchant's decryption key. The proposed scheme is evaluated based on key size, security strength, computational power, memory capacity, encryption and decryption time, and mobile phone battery usage. The results of the evaluation demonstrate that

the proposed scheme provides integrity, confidentiality, and privacy for mobile payment transactions. The scheme is also shown to be time-efficient and computationally inexpensive, making it suitable for resource-constrained environments like mobile payment systems. In summary, Vincent et al. [62] propose an identity-based elliptic curve cryptography scheme for mobile payment security. The scheme utilizes IMEI and ECC to enhance the security of mobile payment transactions. The research shows that the proposed scheme provides integrity, confidentiality, and privacy while being efficient in terms of computational resources and time.

Oladapo [63] is titled "Development of a Multi-Level Security Model for Mobile Payment System". The thesis addresses the authentication challenges in mobile payment systems and proposes a multi-level security model using Support Vector Machine (SVM) for enhanced security. The traditional authentication methods in mobile payments rely on passwords or PINs ("what you know") and tokens ("what you have"). However, these methods have weaknesses, such as password management difficulties and the risk of token loss or theft. Furthermore, they cannot ensure that the presenter of the password or token is the genuine user. To overcome these challenges, the thesis presents a multi-level security model that incorporates different techniques. The model involves user enrollment, authentication, and payment processing. Face detection is performed using the Viola and Jones algorithm, and face recognition is carried out using SVM. Additionally, user data is encrypted using the Rivest–Shamir–Adleman (RSA) algorithm. The results of the evaluation demonstrate the effectiveness of the proposed model. The combination of Viola Jones + SVM + RSA achieves an accuracy of 0.90, recall of 0.923, and F1-Score of 0.1. When compared with other facial recognition algorithms, the model shows a significant impact on the security of the mobile payment system. In summary, Oladapo [63] presents a PhD thesis that develops a multi-level security model for mobile payment systems. The model incorporates face detection, face recognition using SVM, and data encryption using RSA. The evaluation results indicate the model's effectiveness and its potential to enhance the security of mobile payment systems.

Hassan and Shukur [64] is titled "Device Identity-Based User Authentication on Electronic Payment System for Secure E-wallet Apps". The article addresses the need for secure authentication methods in e-wallet applications and proposes a design that focuses on device identity as an extension security element. E-wallets have gained popularity as a convenient and efficient electronic payment system. However, the existing authentication methods used in e-wallets, such as knowledge-based (password), ownership-based (one-time password), and biometric-based (fingerprint) authentication, are susceptible to security threats like account takeover, sim swapping, app cloning, or know your customer verification attacks. To enhance the security of e-wallet apps, this study proposes a design that incorporates device identity as an authentication factor. The design includes four fundamental categories of authentication: password, one-time password, fingerprints, and International Mobile Equipment Identifier (IMEI). By using IMEI, the e-wallet is bound to a specific device, aligning it with the personal and unique nature of a physical wallet. This design aims to address the mentioned security threats and create a more reliable user experience. The proposed authentication design consists of two phases: the registration phase and the authentication phase. The design has been implemented using Android Studio, Firebase real-time database management, and PayPal. Functional requirement testing has been conducted to evaluate the design's performance and adherence to functionality requirements. The results of the testing show that the proposed method meets the functionality requirements and prevents the use of the same account on multiple devices, thereby enhancing security. The proposed method also exhibits better security parameters compared to existing methods. In summary, Hassan and Shukur [64] propose a design for e-wallet apps that incorporates device identity as an authentication factor. The design covers password, one-time password, fingerprint, and IMEI-based authentication. The evaluation results indicate that the proposed method meets functionality requirements, enhances security, and outperforms existing methods in terms of security parameters.

Centeno [65] is titled "Applying Machine Learning to Enhance Payments Systems Security". The thesis focuses on enhancing the security of payment systems, particularly in the context of card payments and mobile payment systems. The thesis starts by addressing the increasing economic losses due to fraudulent card payment transactions, particularly in e-commerce. With the growing popularity of mobile devices for electronic purchases, this trend is expected to continue in the future. While big financial institutions can model processed transactions to predict fraud, merchants have access to valuable information collected from the users' devices during transactions. In the thesis, a series of measures are proposed to enhance the security of both scenarios based on past transactional data and information collected from users' devices. Unlike previous approaches that primarily used supervised machine learning techniques to model processed transactions, the thesis proposes a fraud detection system for card payments based on unsupervised machine learning. This allows the system to recognize new patterns of fraud. Additionally, the thesis looks ahead and focuses on enhancing the security of mobile payment systems. It proposes user identification and verification systems specifically designed for smartphones. These systems are based on motion data, eliminating the need for explicit user actions during the identification and verification processes. In summary, Centeno's thesis [65] presents measures to enhance the security of payment systems. It proposes an unsupervised machine learning-based fraud detection system for card payments and user identification and verification systems for smartphones based on motion data. The thesis aims to improve security in both card payments and mobile payment systems.

4.2.2. Finance

Massoth and Ahier [66] address the need for fast, automated, and secure online authentication methods in the era of digitization. The authors highlight that previous solutions for online authentication, such as postal authentication, video identification, or eID cards, have limitations. These solutions can be time-consuming, rely on human interaction, or require additional hardware that may be expensive. Therefore, there is a need for a simple yet efficient process for authenticating individuals online. To address this need, the startup company SEIN has conceptualized a new approach called fast electronic identification (SEIN). The SEIN method leverages tokenization and pre-authenticated data sets collected by financial institutions as a result of the German Money Laundering Act (GwG). These data sets are made accessible through the Payment Service Directive (PSD2) using established technologies such as OAuth 2.0, OpenID Connect, and Transport Layer Security (TLS) 1.3. The main goal of SEIN is to provide fast authentication at a substantial trust level without collecting user data or transferring data between the bank and the entity requesting authentication. The process ensures that the bank does not know the identity of the party requesting authentication, and the requesting party does not know which bank has provided the user data. The paper provides more detailed information on how SEIN plans to deliver this new and innovative approach to online authentication. In summary, the paper by Massoth and Ahier [66] introduces SEIN, a fast electronic identification method that leverages pre-authenticated data sets collected by financial institutions. The goal is to provide secure and automated online authentication without data collection or data transfer between banks and the inquiring party. The paper outlines the technology and principles behind SEIN's approach to authentication.

N'Gumah [67] addresses the increasing interest in cryptocurrency trading and the need for users to understand how to protect themselves and use wallets with high security. The objective of the paper is to propose a framework that allows users to evaluate the security and privacy features of cryptocurrency wallets. The framework aims to provide users with a set of attributes that define the level of user

protection provided by cryptocurrency wallets. By using this framework, users will be able to assess the security and privacy features of different cryptocurrency wallet options. This evaluation process will help users make informed decisions about which wallets to use and how to interact safely with these platforms. The main goal of the article is to improve security and privacy in cryptocurrency wallets and empower users to engage with these platforms securely. In summary, the article by N'Gumah [67] introduces a framework for evaluating the security and privacy of cryptocurrency wallets. The framework aims to assist users in assessing the level of user protection provided by different wallets and enabling them to interact with cryptocurrency platforms safely.

Thuy et al. [68] investigates the satisfaction of students at Ho Chi Minh City University of Technology and Education (HCMUTE) for e-wallet services. The study analyzes the factors that affect students' satisfaction with e-wallet services based on survey data collected from 289 students at HCMUTE between February and May 2021. The results of the study indicate that the students at HCMUTE widely use e-wallet services and express a high level of satisfaction. The research identifies several factors that influence students' satisfaction with e-wallet services, including convenience, safety and security, reliability, policy to approach customers/employees, and frequency of use. The study highlights the importance of these factors in shaping students' satisfaction with e-wallet services. Factors such as convenience, safety and security, and reliability play a significant role in determining the level of satisfaction among students. Additionally, the study emphasizes the significance of policies related to customer and employee interaction, as well as the frequency of e-wallet usage, in influencing students' satisfaction with these services. In summary, the article by Thuy et al. [68] examines the satisfaction of HCMUTE students with e-wallet services. The study identifies various factors that impact students' satisfaction and emphasizes the importance of convenience, safety and security, reliability, policy approach, and frequency of use in shaping their satisfaction levels.

Harkácsi and Szegfü [26] explores the role of the compliance function in the financial sector in the context of digitalization, artificial intelligence, and robotization. The study addresses the challenges faced by the compliance function in adapting to the changing landscape of financial services and examines the responses and strategies employed to maintain a delicate balance between legislative requirements and ethical frameworks. The authors highlight the significant impact of digitalization on the financial services industry, with the emergence of FinTech enterprises reshaping business and risk models. This transformation has had implications for the regulatory environment and has necessitated a reassessment of trust, reliability, and ethical behavior. As new technologies continue to emerge, regulators face the challenge of keeping up with their functioning and associated risks to establish appropriate regulations. The study emphasizes the need for the compliance function to adapt and find its place in this evolving landscape. Efficient support from the compliance function is essential for financial sector participants in ensuring compliance with regulations and promoting fair and ethical conduct. The authors stress the importance of striking a balance between the quality of legislative environments, both at the international and national levels, and the implementation of ethical and due diligence frameworks. Overall, the article sheds light on the role of the compliance function in the financial sector amidst digitalization, artificial intelligence, and robotization. It underscores the challenges posed by these technological advancements and emphasizes the need for effective compliance strategies to uphold regulatory requirements and promote ethical behavior in the financial industry.

Shipalana [69] explores the role of digital financial services in promoting financial inclusion in South Africa. The paper begins by discussing the significance of financial inclusion in addressing poverty, promoting inclusive development, and achieving the Sustainable Development Goals. It highlights the potential benefits and risks associated with digital financial services in the context of financial inclusion. The article then focuses on South Africa as a case study to examine the country's efforts in promoting financial inclusion. It provides an overview of the progress made in enhancing financial inclusion, identifies the challenges faced in deepening financial inclusion, and discusses ongoing reforms aimed at achieving greater inclusion. The South African case study offers insights into the current state of financial inclusion and the strategies employed to expand access to the financial sector. Furthermore, the paper explores the opportunities that exist to improve digital financial inclusion in Africa as a whole. It discusses the potential leverage points and initiatives that can enhance access to digital financial services and contribute to broader financial inclusion efforts across the continent. In conclusion, the article presents recommendations for strengthening the financial inclusion strategy in South Africa and suggests potential takeaways that can be applied to other African countries pursuing financial inclusion. By examining the South African experience and discussing the opportunities and challenges associated with digital financial services, the paper contributes to the understanding of how digitization can facilitate financial inclusion and advance inclusive development.

Morakinyo [70] presents a secure bank login system that utilizes a multi-factor authentication approach. The paper acknowledges the importance of user authentication in ensuring system security, especially in the context of the rapid expansion of wireless communication technology. The traditional authentication process typically involves sending the user's password to the authentication server, which can pose security risks if intercepted by attackers. To address this concern, the article proposes the use of one-time passwords (OTP) and two-factor authentication (2FA) as a solution. Additionally, the system incorporates QR codes to enhance reliability and efficiency. The main objective of the system is to improve the existing login authentication method. It achieves this by implementing a MFA system that combines QR codes, OTP, and the user account number for authentication. By leveraging multiple factors, the system aims to enhance security and mitigate the risks associated with password-based authentication. Overall, the article presents a novel approach to secure bank login systems by incorporating multi-factor authentication and QR codes. The proposed system offers an alternative and more secure method for user authentication, contributing to the overall goal of ensuring system security in the context of wireless communication technology.

Avdić [71] explores the use of biometrics in mobile banking security, specifically focusing on a case study of Croatian banks. The author highlights the increasing integration of mobile phones into business processes and how financial institutions, particularly banks, utilize mobile applications as a means of direct communication with customers, streamlining processes and generating cost savings. Considering the advancements in technology, the paper raises the question of whether the security of mobile applications has kept pace with these developments. The article provides a brief overview of the impact of biometrics on modern business, with a particular emphasis on mobile technology. It aims to investigate whether banks in EU Member States employ advanced authentication methods that incorporate biometric user identifiers. The study includes a survey conducted among Croatian banks to gather information on the use of biometric authentication methods in mobile banking. The research findings are analyzed, and conclusions are drawn based on the results of the study. Overall, the article explores the application of biometrics in enhancing mobile banking security within the context of Croatian banks. It discusses the potential benefits and challenges associated with the integration of biometric authentication methods in mobile applications. By presenting the case study and research findings, the article contributes to the understanding of the use of biometrics in mobile banking and its implications for security in the banking sector.

Iqbal et al. [72] introduces a novel mobile wallet model specifically designed for the elderly population, utilizing fingerprint authentication as the primary factor for user verification. The authors recognize that

the elderly often face challenges in operating digital payment applications and may perceive them as insecure. To address these concerns, the study leverages the availability of fingerprint verification technology on mobile devices to create a user-friendly and secure digital wallet payment system. The proposed model incorporates Bluetooth technology for billing purposes at the point of sale, while fingerprint verification serves as the authentication mechanism for users. The authors conducted a proof-of-concept study to validate the effectiveness of the proposed model. Usability questionnaires and attributes were employed to assess user satisfaction and ease of use among the target group, namely the elderly. The research findings indicate that the proposed methodology successfully provides a satisfactory user experience and is perceived as easy to use by the elderly population. By utilizing fingerprint authentication and simplifying the digital payment process, the model aims to enhance accessibility and security for the elderly, enabling them to leverage mobile wallet services more effectively. Overall, the article presents a promising approach to address the usability and security concerns of elderly users in the context of mobile wallet services. The study highlights the potential benefits of utilizing biometric authentication, such as fingerprint verification, to create inclusive and user-friendly financial technology solutions.

4.2.3. Authentication technology

Kim et al. [73] presents a multi-factor authentication approach that employs randomly selected authentication methods, along with decentralized identifiers (DID), on a random terminal. With the increasing emphasis on security in the context of information and communication technology, the authors recognize the vulnerabilities associated with traditional methods of user authentication, such as ID and password entry, which can lead to the leakage of sensitive information in the event of server attacks or keylogging. To address these security concerns, the study proposes the use of biometric authentication technology, which is commonly available on smartphones. However, the challenge lies in the management of biometric data in cases where the device is lost, as the central server does not typically store this information. To overcome this limitation, the authors suggest encrypting transactions using blockchain technology, which offers enhanced data security through its distributed nature and absence of a primary target for hackers. The proposed method aims to create an authentication system that ensures both security and integrity by leveraging the synergistic use of biometric and blockchain technologies. Importantly, the user's sensitive biometric data is not stored in the service provider's system but is only used for verification purposes within the blockchain transaction, ensuring anonymity and reducing privacy concerns. Overall, Kim et al. [73] introduces a novel approach to multi-factor authentication that combines randomly selected authentication methods, biometric technology, and blockchain-based data encryption. By integrating these technologies, the proposed method offers improved security and privacy for users, instilling confidence and safety in the provision of services.

Jayasinghe et al. [74] explores the application of blockchain technology in the philanthropic sector. The authors investigate how the blockchain can be utilized to facilitate charitable donations in fiat currency or Bitcoin through a web-based donor platform. The paper presents a case study focused on providing humanitarian aid to a community facing challenges in a geographically constrained environment with limited internet access. To address this limitation, the authors propose an SMS-based mobile payment system that leverages the existing GSM network and basic mobile phones. Additionally, the system incorporates One Time Password (OTP) security tokens to enhance security. The proposed scheme is evaluated in terms of its security implications and its impact on charities and donors. By leveraging blockchain technology and mobile-based payment systems, the paper suggests that philanthropic initiatives can be streamlined, enabling secure and efficient donation processes. This has the potential to make a significant impact in areas where internet connectivity is limited or unreliable. Jayasinghe et al. [74] highlights the potential of blockchain technology in transforming philanthropy by providing secure and transparent donation mechanisms, even in challenging environments.

Guerar et al. [75] addresses the challenges of user authentication in smartwatches. While smartwatches offer convenient features and services like mobile payment, ticketing, and access control, they also become attractive targets for attackers. Traditional authentication methods such as PINs and Pattern Locks are not robust against various cyber Security attacks, posing risks to user security and privacy. To address these issues, the authors propose a new authentication framework called 2GesturePIN. This framework leverages the rotating bezel or crown, which are intuitive ways to interact with a smartwatch, as dedicated hardware for authentication. With 2GesturePIN, users can securely authenticate themselves to their smartwatches and related sensitive services using just two gestures. The goal of 2GesturePIN is to improve the resilience of PIN-based authentication methods against state-of-the-art cyber Security attacks while maintaining a high level of usability. By utilizing the dedicated hardware components of smartwatches, this approach offers a more secure authentication mechanism compared to traditional methods. Guerar et al. [75] highlights the importance of strong authentication schemes in smartwatches and presents 2GesturePIN as a solution to enhance security while ensuring usability. By addressing the limitations of existing authentication methods, this framework contributes to the overall security of smartwatches and protects user information from potential attacks.

Dey and Jain [76] discusses an innovative approach to point-of-sale (POS) systems. POS systems have evolved over time, incorporating hardware and software components to enable transactions. Traditional cash-based POS systems have been supplemented by credit card and debit card payment options, often utilizing barcode readers. In this paper, the authors propose an AI-based POS system that combines face recognition technology with a password-based authentication method. This novel approach aims to eliminate the need for physical cards during payment transactions. Instead, customers can make payments by having their faces recognized and entering a password. The integration of face recognition technology into the POS system offers several advantages. It provides convenience to customers as they no longer need to carry physical cards, and it can enhance the overall security of the transaction process by leveraging biometric authentication. The password serves as an additional layer of security, ensuring authorized access to the system. Dey and Jain [76] presents this proposed method as a modern alternative to traditional POS systems. By leveraging face recognition and password authentication, the authors aim to create a more streamlined and secure payment experience. The paper provides insights into the development and potential benefits of this AI-based POS system, which offers a cards-free payment solution.

Nguyen, Dao, and Do [77] introduces a blockchain-based authentication system designed to address the issue of fake certificates in Vietnam. The authors recognize the potential of blockchain technology in enhancing data transparency and user trust, and they aim to leverage these advantages to develop a solution for certificate management. The system proposed in the study is called the Vietnamese Educational Certification blockchain (VECefblock). The authors outline the development principles and steps involved in building VECefblock, including designing the overall architecture, defining business processes, and implementing a decentralized application. They also discuss the specific requirements for the Vietnamese context. To test the functionality of VECefblock, the authors utilize Hyperledger Fabric as the blockchain platform, deployed on the Amazon EC2 cloud. Through performance evaluations, the study demonstrates the operability of VECefblock in a practical deployment environment. The results of the experiment support the feasibility of the proposed blockchain-based authentication system. The authors argue that the application of blockchain technology, as exemplified by VECefblock, has the potential to address not only certificate management issues in Vietnam but also other social problems by leveraging the functionalities of blockchain,

such as anti-forgery information, transaction verification, and smart contracts. Nguyen, Dao, and Do [77] presents an approach to utilize blockchain technology for the authentication and management of educational certificates in Vietnam. By applying blockchain principles and leveraging Hyperledger Fabric, the authors demonstrate the potential of blockchain-based solutions in enhancing trust and combating the problem of fake certificates in the Vietnamese context.

Okokpujie et al. [78] introduces a point of sale (POS) terminal that incorporates fingerprint biometric authentication as an additional layer of security. The authors recognize the importance of secure payment transactions in retail businesses and propose the use of fingerprint recognition to enhance the authentication process. The proposed POS terminal aims to strengthen the existing authentication process, which typically relies on PINs and passwords. By incorporating fingerprint biometric recognition, the authors argue that the system can achieve a zero false match and false non-match rate, thereby reducing the risk of fraud. This added layer of security aims to enhance user trust and confidence in POS devices. The study emphasizes the significance of retail businesses that still rely on in-person transactions rather than online platforms. To address security concerns in these transactions, the authors propose the use of fingerprint biometric authentication as a more secure and reliable method. Overall, the article presents a proposal for a fingerprint biometric authentication-based POS terminal. By integrating fingerprint recognition technology into the authentication process, the authors aim to enhance security and build trust in retail transactions conducted through POS devices.

Türk [79] discusses the use of Near Field Communication (NFC) technology for mobile payment and identification. The author highlights the increasing adoption of mobile devices for electronic payments and the potential of NFC technology to transform smartphones into mobile wallets. The article points out that current mobile wallet solutions mainly focus on credit card enrollment and usage, while other aspects such as identification, loyalty cards, and public transport cards are not well integrated. The author explores the reasons behind this limitation and proposes a new method for utilizing the Secure Element (SE) within NFC-enabled phones. The proposed method enables standard enrollment and usage for proprietary payment and identification schemes. It introduces a model that leverages the SE to support various payment scenarios, including public transport payment. The author emphasizes that this approach contributes to NFC technology by enabling proprietary transaction flows in parallel with NFC credit card payment solutions. Furthermore, the article presents an open protocol that can serve as a standard for executing NFC payment and identification transactions. By providing an open and independent solution, the author aims to facilitate the development and adoption of NFC-based mobile payment and identification methods. In summary, the article explores the limitations of current mobile wallet solutions and proposes an NFC enabler independent method for mobile payment and identification. The proposed approach leverages the Secure Element within NFC phones and introduces an open protocol to support various payment scenarios beyond credit card usage.

Kumar et al. [80] introduces a security system for mobile phones that aims to protect users' data from theft or deletion. With the rapid increase in mobile phone usage, there is a growing need for improved security measures. The paper addresses the vulnerabilities of device-in-built security mechanisms, which can be easily compromised through techniques like shoulder surfing, random guessing, or brute force attacks. To enhance security, the proposed system utilizes image-based authentication with a pattern-based approach and incorporates Image CAPTCHA. In this system, users set a graphical password by selecting and arranging images in a matrix according to a specific pattern. The users are provided with a variety of images and are required to choose three different images. Then, they draw a password associated with the selected images. This process adds a high level of security to mobile/web applications, reducing the risk of data loss. Additionally, the system implements a two-factor authentication mechanism. When a user wants to access their mobile phone or web application, they need to enter one of the passwords they selected during the registration phase. After entering the password, the user is required to click on the screen at a specific location chosen during registration. Overall, Türk [79] a two-factor image-based authentication system that leverages graphical passwords and Image CAPTCHA to enhance security on mobile devices and web applications. The proposed system provides an additional layer of protection against common security vulnerabilities and aims to mitigate the risk of data loss.

Zheng et al. [81] focuses on iris recognition as a high-security authentication technology in the fields of mobile payment, mobile security, and privacy protection. The authors address the limitations of conventional Convolutional Neural Networks (CNNs) for iris recognition, such as weak anti-noise ability and high memory requirements. To overcome these limitations, the authors propose an improved architecture based on Mask R-CNN and fine-tuning neural network architectures using mobile Inception V4. The proposed framework integrates iris detection, extraction, and recognition functions into a comprehensive iris recognition system. It is designed to be scalable and highly available, capable of learning scale-variant features through zero-padding normalization. The framework aims to enhance the overall robustness of the learning process. Importantly, the custom architectures developed in this work can be trained using different spectra of samples, including Visible Wavelength (VW) and Near Infrared (NIR) iris biometric image data. The authors achieve a recognition average accuracy of 99.10% when executing the framework on the mobile edge calculation device Nvidia Jetson Nano. Overall, the article presents a deep learning-based ensemble framework for robust iris authentication. The proposed framework addresses the limitations of traditional CNN approaches and demonstrates promising results in terms of accuracy and efficiency, making it suitable for applications in mobile payment, security, and privacy protection.

Lucy Jepkemboi Chetalam [25] focuses on improving the authentication process of MPesa, a mobile money transfer service, through the incorporation of voice biometrics. The objective is to enhance efficiency, accuracy, and authentication levels of MPesa accounts for subscribers. The thesis highlights voice biometrics as a state-of-the-art technology that offers better usability and aims to combat fraud, empower self-service, and save costs for companies through time efficiency and reduced administration costs. The research study investigates authentication schemes used by mobile money services and major MPesa fraud techniques in Kenya. Using a design science research approach, the study develops and implements a voice biometric MPesa model to address the problem of fraudulent MPesa transactions, particularly those involving SIM-swap methods. The population of study includes MPesa subscribers around the Mirema-USIU area, and data collection is done through an online Google Forms questionnaire survey. The findings reveal that respondents perceive the current security measure of a 4-digit PIN as insufficient, with a significant percentage believing their PINs can be easily guessed. The study identifies a gap in the security of mobile money transactions and suggests that adding biometrics can improve MPesa security. Regarding MPesa fraud techniques, the study uncovers various methods employed by fraudsters, including transaction reversals, unauthorized SIM-swap, identity theft, erroneous transactions, scam messages, and insider theft. Subscribers are found to be aware of these fraud techniques, particularly unauthorized SIM-swap and identity theft. These issues, the study develops the VMPESA model on the Android platform, which implements a secure mobile-based multi-factor authentication scheme using device-specific ID, voice biometrics, and a PIN. The research concludes that a PIN alone is not sufficient for securing mobile transactions, and voice biometrics can significantly enhance security in mobile financial systems like MPesa. The study recommends that mobile money service providers focus on implementing multi-factor authentication schemes and identify weaknesses in single-factor authentication measures like PINs. Continuous

upgrading of security features is essential due to the evolving techniques used by fraudsters. Safeguarding subscriber information and accounts is a top priority for these organizations. The thesis suggests further research on alternative multi-factor authentication schemes with enhanced functionalities to improve the overall process's seamlessness, convenience, and intelligence. Additionally, researchers should explore advanced techniques used by fraudsters to acquire subscribers' personal information. Overall, the thesis emphasizes the importance of incorporating voice biometrics to enhance the security and integrity of MPesa transactions, providing valuable insights and recommendations for mobile money service providers and future research directions in the field.

4.2.4. IoT

Paribesh Ranabhat [82] focuses on the design and development of a secure IoT-driven fast DC charging infrastructure for electric vehicles (EVs). The objective is to address the challenges associated with traditional AC charging stations, such as time consumption and the requirement of an onboard charger, by utilizing DC charging stations. The article highlights the significance of electric vehicles in reducing carbon emissions and transitioning away from traditional fossil-fuel cars. To encourage widespread adoption of EVs, it is crucial to have a corresponding infrastructure of EV charging stations. The IoT-driven infrastructure can enhance the efficiency and safety of charging processes by enabling control through user devices like smartphones. However, the rapid development of IoT-driven EV charging stations has raised concerns about cyber Security threats and vulnerabilities. The article emphasizes the need for secure design considerations to mitigate these risks. It evaluates the potential security risks associated with IoT components, including EVs and EV charging infrastructure, and presents detailed secure design recommendations for implementing IoT-enabled charging infrastructure. The research includes an assessment of asset and threat taxonomy specific to the IoT infrastructure. It is important to note that the public version of the thesis does not disclose specific implementation details and sensitive information due to the inclusion of enterprise-level secrets and business-sensitive material. Overall, Paribesh Ranabhat [82] highlights the importance of developing a secure IoT-driven charging infrastructure for electric vehicles. It provides insights into the potential security risks and offers recommendations for implementing secure design considerations in IoT-enabled charging stations. By addressing cyber Security concerns, this research contributes to the development of a reliable and secure infrastructure for electric vehicle charging.

4.2.5. Electronic service

Joanna Mehtälä et al. [30] focuses on the design and implementation of citizen-centric e-government services in Namibia, with a particular emphasis on mobile platforms. The aim is to bridge the digital divide and provide equal opportunities for citizens to access government services, considering the prevalent digital divide and income inequality in the country. The article highlights the low level of e-government implementation in Africa and the need for socially inclusive and accessible services. It suggests that offering government services on mobile platforms and employing user-centered design approaches can contribute to addressing these challenges in Namibia. The research explores the opportunities that mobile platforms offer for delivering citizen-centric e-government services and how a combination of design science and user-centered design can support the creation of such services. To demonstrate the practical application of these concepts, the article presents the design challenge of creating prototypes for two mobile services related to identification: an online ID application service and a digital authentication service for individuals. The results indicate that mobile platforms can enhance the efficiency and accessibility of existing government services. The study highlights the proficiency of young, urban Namibians in mobile use and their positive perceptions regarding offering identification services on mobile platforms. For rural communities, m-government services have the potential to reduce travel associated with government interactions, although internet coverage remains an issue in these areas. Furthermore, the article suggests that the use of prototypes facilitates cross-cultural co-creation of knowledge by establishing a mutual understanding of concepts between different parties involved in the design process. Overall, the research emphasizes the opportunities presented by mobile platforms for delivering citizen-centric e-government services in Namibia. By adopting user-centered design principles and employing prototypes, it is possible to create intuitive and inclusive mobile services that address the needs of diverse user groups and contribute to reducing the digital divide in the country.

Mattia Santoro et al. [83] explores the role of Application Programming Interfaces (APIs) in the digital transformation of governments and public administration units. It focuses on the adoption of APIs in the context of digital government services and highlights the importance of utilizing stable APIs that conform to existing standards and technical specifications. The report begins by discussing the impact of digital technologies on society, particularly in the private and public sectors. It emphasizes the shift from traditional workflow-based public service provisions to more innovative, user-centric approaches facilitated by digital technologies. APIs are identified as key enablers of this digital transformation, both in the private sector and in government operations. The European Commission initiated the APIs4DGov study to explore the API technological landscape and provide guidance for the adoption of stable APIs in digital government services. The report presents an analysis of the API technological landscape, including relevant standards and technical specifications for general-purpose use. The goal is to avoid the development of ad hoc solutions with limited scalability and reuse potential, and instead, promote the adoption of existing standards and specifications. The report provides definitions of basic concepts related to APIs and discusses various standards and technical specifications. It classifies these documents based on resource representation, security, usability, testing, performance, and license. Additionally, it proposes a shortlist of selected documents based on their utilization, maintenance, and stability. The European Commission's initiatives related to APIs are also presented in the report. To support API stakeholders in identifying and selecting appropriate solutions, the report includes a glossary with definitions of relevant terms collected during the APIs4DGov study. Overall, the report aims to provide a comprehensive overview of general-purpose API standards and technical specifications, with the goal of promoting the adoption of stable APIs in digital government services. It serves as a valuable resource for governments and public administration units seeking to leverage APIs in their digital transformation efforts.

Mahsa H. Sadi and Eric Yu [84] introduces RAPID (Rational API Designer), an open-source assistant designed to aid software developers in addressing non-functional requirements during the design of web APIs. As the development of web APIs becomes increasingly common, ensuring the security, performance, and privacy of back-end systems and data becomes crucial. RAPID is equipped with a comprehensive set of expert knowledge about API design, which has been systematically collected and extracted from literature. This knowledge is encoded as a set of 156 rules using the Non-Functional Requirements (NFR) multi-valued logic, a formal framework commonly used to describe non-functional and functional requirements in software systems. The assistant utilizes the encoded knowledge through a stepwise inference procedure. Given a requirement, RAPID provides a set of design alternatives and ultimately arrives at a final recommendation for a given API design specification. The article presents the evaluation of RAPID's consultations by seven experienced software engineers. The evaluations cover seven different cases of web API design and include thirty design questions. The results indicate that RAPID's recommendations met acceptable standards for the majority of evaluators in 73.3% of cases. The article also discusses the feedback provided by the evaluators, noting that some of the unacceptable ratings were due to valid but

incomplete design guidelines. The authors anticipate that the accuracy of RAPID's consultations will improve as the knowledge of API design is expanded and refined. Overall, the article introduces RAPID as a knowledge-based assistant that offers guidance in addressing non-functional requirements during web API design. It demonstrates the potential of using encoded knowledge and inference procedures to provide recommendations for API design specifications.

Tiantian Zhu et al. [31] presents a system called RiskCog that enables unobtrusive and real-time user authentication on mobile devices. With the widespread use of mobile devices and the need to protect user privacy, various user authentication mechanisms have been proposed. However, many of these mechanisms require expensive sensors and explicit user input, as well as an internet connection for authentication. RiskCog takes a different approach by leveraging the motion sensors available on mobile devices, such as smartphones and smartwatches, to capture data related to users' daily device usage. This learning-based system uses the captured data to authenticate the ownership of mobile devices in a real-time manner. It does not rely on explicit user input, motion state, or specific device placement, making it unobtrusive and privacy-sensitive. One of the key advantages of RiskCog is its cross-platform deployment capability, allowing it to be used on different types of devices. Additionally, it can perform offline user identity verification, making it usable even in environments without internet access. The article presents comprehensive experiments conducted on smartphones and smartwatches to evaluate the performance of RiskCog. The results demonstrate that RiskCog achieves rapid and accurate authentication of device users. Tiantian Zhu et al. [31] offers a novel approach to unobtrusive and real-time user authentication on mobile devices by utilizing motion sensor data. It provides an alternative authentication mechanism that is privacy-sensitive, does not require costly sensors, and can operate offline.

Onyechere Patricia Onyinyechi et al. [85] discusses the potential benefits of using Quick Response (QR) code technology in business marketing, particularly for small and medium-scale enterprises (SMEs). The article highlights the need to bridge the gap between digital and paper-based communication media in business marketing. By incorporating QR code technology into their marketing plans, businesses can provide instant accessibility to both online and offline content through a single platform, thereby reaching a larger audience of potential customers. QR code technology, although introduced in 1994, is perceived as cutting-edge and can greatly improve marketing efforts, especially considering the widespread use of mobile devices by potential customers. By scanning and decoding QR codes using smartphones, customers can quickly access business information that may not be available on traditional paper-based media, such as business cards. The article emphasizes that QR code technology serves as the missing link for achieving breakthroughs in business marketing for SMEs globally. It enables the tracking of product information in supply chains and facilitates marketing and advertising campaigns. By connecting consumers of paper-based content to online resources, smartphone users can access product information, company websites, and social media pages. The authors propose a suitable model of QR code technology based on Roger's Innovation Decision Process Theory and the CIPP Evaluation Model. This model aims to enhance marketing efforts for small-scale enterprises that may have limited budgets for traditional marketing strategies or affiliate marketing agencies. Overall, Onyechere Patricia Onyinyechi et al. [85] highlights the potential benefits of QR code technology in enhancing business marketing, particularly for SMEs. The technology provides a cost-effective and efficient way to connect offline and online content, enabling businesses to reach a wider audience and improve their marketing efforts.

Ziyi Han et al. [86] presents a novel authentication scheme for mobile cloud computing environments that addresses the security and privacy concerns associated with the storage of biometric information on servers. The article starts by highlighting the limitations of traditional username-password authentication methods, such as vulnerability to disclosure and low reliability. To overcome these limitations, multifactor biometrics-based authentication has gained popularity due to its simplicity, convenience, and high reliability. Biometrics, particularly fingerprint information, is widely used in mobile payment scenarios. However, storing biometric information on servers introduces a significant security risk. If the server is compromised, it can lead to the leakage of sensitive fingerprint information, posing a severe threat to user privacy. To address this security issue, the authors propose a novel multifactor two-server authenticated scheme under mobile cloud computing (MTSAS). In the MTSAS scheme, the authentication method and means are separated, and the user's biometric characteristics, such as fingerprint information, remain on the user device. This design choice ensures that biometric information is not stored on the server, thereby protecting user privacy and enhancing data security. The scheme also considers different authentication factors based on the privacy level required for authentication, catering to the diverse needs of users. The authors provide a security analysis of MTSAS, demonstrating that it achieves the authentication goals and satisfies security requirements based on the BAN logic. Furthermore, a comparison with other schemes reveals that MTSAS offers reasonable computational efficiency while maintaining superior communication costs. In summary, Ziyi Han et al. [86] presents an efficient and secure authentication scheme, MTSAS, that separates the storage of biometric information from servers in mobile cloud computing environments. By addressing the privacy concerns associated with biometric data, the scheme provides enhanced security and protects user privacy in mobile payment scenarios.

4.3. IAL and AAL classification

To improve upon the given paragraph, let us provide a revised version: IAL (Identity Assurance Level) and AAL (Authentication Assurance Level) are determined based on a set of distinct standards for each level. These standards play a vital role in ensuring secure and reliable identity verification and authentication processes. The IAL establishes the level of confidence in verifying an individual's identity. It considers factors such as the strength of the authentication methods used, the reliability of the identity proofing process, and the assurance level of the credentials provided. These criteria help determine the level of trust and assurance placed on an individual's claimed identity. Similarly, the AAL focuses on the level of assurance in the authentication process itself. It takes into account factors like the strength of the authentication protocols, the resistance to fraudulent attempts, and the robustness of the security measures in place. These standards help assess the reliability and security of the authentication systems used. By adhering to these separate standards, organizations and systems can establish appropriate levels of identity assurance and authentication assurance. This enables them to maintain the necessary security and trust required for various applications, such as online transactions, access to sensitive information, and protection against identity theft. Overall, the use of these distinct standards for IAL and AAL ensures a comprehensive approach to identity verification and authentication, enhancing security and reducing the risk of unauthorized access or fraudulent activities. The paper categorization protocol was as follows:

- Identity Assurance Level (IAL)
  IAL1: Basic Identity Authentication. Requires users to provide basic personal information and does not require physical evidence.
  IAL2: Intermediate level identity authentication. Request personal information verification through physical evidence such as passport, driver's license or citizen identification card.
  IAL3: Advanced Identity Authentication. Requires accurate verification of identity and personal information through physical evidence and a more rigorous vetting process.

- Authentication Assurance Level (AAL)
  AAL1: Basic Authentication. Requires simple authentication like username and password.
  AAL2: Intermediate level authentication. Requires additional authentication measures such as OTP (One Time Password) or phone verification code.
  AAL3: Premium Authentication. Require stronger authentication measures such as the use of physical security devices such as smart cards, USB tokens, or biometric identification technology.

Having performed an objective and meticulous assessment of the studies presented in Section 4.2, we now turn our attention to conducting a comprehensive analysis of the level of identity and authentication within each study. The primary goal of this analysis is to provide a concise overview of the approaches utilized by researchers to establish the identity and verify the authenticity of participants or subjects involved in their investigations.

Throughout this analysis, we carefully examine the identity and authentication methods employed by researchers, paying close attention to the sophistication and robustness of these approaches. Furthermore, we consider the level of security and reliability associated with the chosen methods based on the concepts outlined in 4.3, as this directly impacts the trustworthiness of the collected data and, consequently, the validity of the study's conclusions.

In addition to evaluating the individual studies, we also identify any emerging patterns or trends in the adoption of identification and authentication practices across the research landscape. This broader perspective allows us to draw meaningful comparisons and contrasts between different methodologies, providing valuable insights into the evolution and current state of identification and authentication practices in relevant fields.

By presenting this analysis (In Table 3, 4, 5, 6, Tables 7 and 8), we aim to offer a comprehensive understanding of the significance and challenges related to identification and authentication in the context of the reviewed studies. Furthermore, we hope that our insights will foster discussions and improvements in research practices, ultimately contributing to the advancement of knowledge in these domains. As with any analysis, we acknowledge that our evaluation is subject to the available information within the research papers and may not encompass all possible nuances. Nonetheless, we have endeavored to conduct a thorough and impartial assessment, ensuring the accuracy and reliability of the presented overview.

Across all five domains, a clear trend towards MFA emerges. However, the implementation of MFA varies significantly between sectors. In payment systems, there is a strong emphasis on combining traditional methods like PINs with more advanced techniques such as biometrics. For instance, Ibrahim and Hashim [43] propose a model combining PIN and fingerprint biometrics for mobile payments. Similarly, in the finance sector, Harkácsi and Szegfü [26] discuss systems utilizing biometric data alongside PINs for high-level assurance.

The authentication domain, as expected, showcases the most diverse range of methods. Kim et al. [73] explore the integration of blockchain technology with traditional ID and password systems, while Chetalam [25] investigates the use of voice biometrics in combination with device-specific IDs and PINs. This diversity reflects the sector's role in pioneering new authentication technologies.

Interestingly, the IoT and E-Service domains show a more conservative approach. Ranabhat [82] discusses the use of strong passwords or PINs for IoT devices, with biometrics for higher assurance levels. In E-Services, there is a notable reliance on established protocols like OAuth and OpenID, as seen in the work of Santoro et al. [83] and Sadi and Yu [84].

Biometric integration — a common thread. Biometric authentication emerges as a common thread across all domains, albeit with varying degrees of sophistication. In payment and finance sectors, biometrics are often used as a high-assurance factor, frequently combined with other methods. The authentication domain pushes the boundaries of biometric usage, exploring novel approaches like behavioral biometrics [31] and voice recognition [25].

E-Services and IoT domains, while adopting biometrics, show a more cautious approach. This could be attributed to the diverse range of devices and services in these sectors, some of which may have limited biometric capabilities.

Regulatory influence and standardization. The influence of regulatory requirements is most evident in the payment and finance sectors. Wolters and Jacobs [44] explicitly discuss the impact of PSD2 on authentication practices in payment services. In the finance sector, adherence to standards like PCI DSS is noted [68]. This regulatory influence is less pronounced in the other domains, suggesting a potential area for future development, especially in IoT and E-Services where standardization could enhance interoperability and security.

Innovation and emerging technologies. While all domains show some level of innovation, the payment and authentication sectors appear to be at the forefront. Jamil et al. [48] explore blockchain-based authentication for vehicle payments, while Geewax [55] discusses the use of public-key cryptography in real-time payment systems. In the authentication domain, the exploration of decentralized identity solutions [73] stands out as a potentially transformative approach.

The IoT and E-Service sectors, while less adventurous, show innovation in adapting existing technologies to their unique challenges. For instance, Zhu et al. [31] propose using behavioral biometrics for unobtrusive authentication in mobile devices, an approach particularly relevant to IoT and E-Services.

Balancing security and usability. A common challenge across all domains is balancing high security with user-friendly authentication. This is particularly evident in the payment and finance sectors, where the need for robust security must be balanced against the demand for frictionless transactions. Sturgess et al. [60] exemplify this balance with their innovative use of smartwatch gestures for payment authentication.

In the E-Service domain, the focus appears to be more on usability, with a preference for familiar authentication methods. This is seen in the widespread use of OAuth and OpenID [83], which provide a balance of security and user convenience.

Domain-specific considerations. Each domain presents unique considerations in authentication:

- **Payment:** Emphasis on transaction speed and security, with a trend towards invisible authentication.
- **Finance:** High focus on regulatory compliance and fraud prevention.
- **Authentication:** Exploration of cutting-edge technologies and methods.
- **IoT:** Challenges of authenticating diverse devices with varying capabilities.
- **E-Services:** Focus on scalable, user-friendly authentication across different platforms.

Future directions. Based on this cross-domain analysis, several future research directions emerge:

1. Development of adaptive authentication systems that can adjust security levels based on context and risk across all domains.
2. Further exploration of decentralized and blockchain-based authentication, particularly in finance and E-Services.
3. Investigation of privacy-preserving authentication methods, especially relevant for IoT and E-Services.

Table 3
Evaluate the IAL and AAL factors of 70 articles - 1.

Topic	Article	IAL Level	AAL Level
Payment	[42]	IAL2: TEE (Trusted Execution Environment)	AAL2: OTP
	[43]	IAL2: PIN, Fingerprint	AAL2: OTP
	[44]	IAL3: Password, OTP and Biometrics	AAL3: Password, OTP and Biometrics
	[45]	IAL3: PIN, Face ID or Fingerprint	AAL3: Password, PIN, OTP, Grid Card
	[46]	IAL1: MPIN	AAL1: MPIN
	[47]	IAL2: Physical card or a smartphone and PIN or Password	AAL3: PIN code and Fingerprint or Iris scan
	[48]	IAL3: Mutual Authentication (elliptic curve encryption and Diffie–Hellman key exchange)	AAL3:Smart contracts, Access control
	[49]	IAL2: ATM cards and PIN	AAL3: Biometrics and ATM Card
	[50]	IAL2: MPIN and Secret Code	AAL2: MPIN and Secret Code
	[51]	Not mentioned	AAL2: Strong password and PIN
	[52]	IAL3: Gesture patterns, Biometric data, Encryption techniques	AAL3: Gesture patterns, Biometric data
	[53]	IAL2: Mobile number or Virtual address	AAL2: Mobile number or Virtual address, QR Code
	[60]	IAL2: Biometrics	AAL2: NFC, Biometrics
	[63]	IAL2: Face Recognition	AAL2: Face Recognition
	[55]	IAL3: Public-key cryptography, digital signatures	AAL3: Public-key cLryptography, digital signatures

Table 4
Evaluate the IAL and AAL factors of 70 articles - 2.

Payment	[54]	IAL2: Virtual ID, M-PIN, OTP	AAL2: Virtual ID, M-PIN
	[57]	IAL3: Number phone, government-issued IDs, biometrics	AAL2: Number phone, PIN, OTP
	[56]	IAL3: PIN, Biometrics and Signature	AAL3: Biometrics, PIN
	[58]	IAL2: Session ID (TR-ID), Code SMS	AAL2: TCP/IP data and Mobile phone number
	[27]	IAL3: Citizenship ID, PIN, Iris biometric	AAL3: PIN and Iris biometric
	[59]	IAL2: Mobile number, OTP, Biometrics	AAL2: Password, Biometrics
	[61]	IAL3: PIN, OTP, Fingerprint Biometric	AAL3: PIN, OTP, Fingerprint Biometric
	[62]	IAL1: International Mobile Equipment Identity (IMEI)	AAL2: Elliptic curve cryptography over a binary field
	[64]	IAL2: International Mobile Equipment Identifier (IMEI), OTP	AAL2: Password, fingerprint
	[65]	IAL3: Card Payment (Chip and PIN), Motion-based Identification on Smartphones, biometrics	AAL3: Card Payment (Chip and PIN), biometrics
Finance	[66]	IAL2: Third-Party (eIDAS, ISMS)	AAL2: Identification Number (PIN) and a Transaction Authorization Number (TAN)
	[67]	IAL2: Email Verification, 2FA	AAL2: Backup security phrase
	[68]	IAL2: PCI DSS (unique ID, strong Password)	AAL2: Password, OTP
	[69]	IAL3: Location-based identification, biometrics	AAL2: Password, biometrics

4. Integration of AI and machine learning for fraud detection and continuous authentication.
5. Standardization efforts in IoT authentication to address the challenge of device diversity.

Generally, while each domain has its unique authentication landscape, there are significant opportunities for cross-pollination of ideas and technologies. The ongoing challenge will be to develop authentication systems that are secure, user-friendly, and adaptable to the specific needs of each domain while keeping pace with evolving threats and technological advancements.

5. MFA tool review

5.1. MFA tool selection process

The rapid evolution of digital payment systems has necessitated the development of robust and secure authentication mechanisms to safeguard users and their financial transactions. MFA has emerged as a pivotal solution, providing layered security by requiring users to present multiple forms of verification, or factors, to authenticate their identity. While academic research offers theoretical foundations and innovative methodologies, industry tools often bridge the gap between theory and practical implementation. These tools, designed to assist developers in building authentication frameworks, play a crucial role in shaping the real-world application of MFA in payment systems. Our tool selection was guided by four primary criteria:

Table 5
Evaluate the IAL and AAL factors of 70 articles - 3.

Finance	[26]	IAL3: Biometric data and audited electronic communications equipment	AAL3: PIN and fingerprint
	[70]	IAL2: OTP, QR code, user account number	AAL2: QR code, user account number
	[71]	IAL2: Number phone, biometrics	AAL2: Number phone, biometrics
	[72]	IAL2: Fingerprint	AAL2: Fingerprint
Authentication	[73]	IAL3: ID, Password, DID Blockchain	AAL3: ID, Password, Face ID
	[74]	IAL2: OTP, PIN, multi-signatures	AAL2: OTP, PIN
	[75]	IAL1: PIN	AAL1: PIN
	[77]	IAL3: IDs, Unique Identification (Identification key in the blockchain network, supports password-based authentication.)	AAL3: Encrypted Private Keys
	[78]	IAL2: Fingerprint	AAL2: Fingerprint
	[79]	IAL3: Secure Element (SE), biometrics	AAL3: Biometrics, PIN
	[81]	IAL2: Iris biometric	AAL2: Iris biometric
	[25]	IAL3: Device-specific ID, voice biometrics, and a PIN	AAL3: Device-specific ID, voice biometrics, and a PIN
	[76]	IAL3: Password and Face Recognition	AAL3: Password, AMSR Hardware Dongle
	[80]	IAL2: Password and Images with pattern-based	AAL2: Passwords and perform a specific action on the screen (clicking)
IoT	[82]	IAL2: Strong passwords or personal identification numbers (PINs)	AAL2: Biometrics

Table 6
Evaluate the IAL and AAL factors of 70 articles - 4.

E-Service	[30]	IAL2: Mobile SIM, ID	AAL2: Mobile SIM and bank credentials
	[83]	IAL2: OAuth 2.0 Access Token, OpenID	AAL2: API keys, Security Assertion Markup Language (SAML) 2.0
	[84]	IAL2: Username, password and OpenID	AAL2: OpenID, OAuth 2.0
	[31]	IAL2: Behavioral biometrics and usage patterns	AAL2: Behavioral biometrics and usage patterns
	[85]	IAL1: QR Code	AAL1: QR Code
	[86]	IAL2: Fingerprint biometric remain stored only on the user's device	AAL2: Fingerprint biometric remain stored only on the user's device
Authentication	[87]	IAL3: PIN and biometric data, or combination of QR codes and public key cryptography (PKI)	AAL3: OTP, fingerprint, and facial recognition.
E-service	[88]	IAL2: Biometrics (facial recognition, fingerprint), OTP and QR codes	AAL3: Combination of biometric and OTP or device-based authentication (e.g., FaceID).
Payment	[89]	IAL2: OTP, PIN, biometric authentication (fingerprint, iris scan), and robot verification (CAPTCHA).	AAL2: Biometric (e.g., fingerprint, facial recognition) and OTP.
	[90]	IAL2: Cloud-based payment systems (CBPS) and 2FA mechanisms: PINs, passwords, and biometrics (e.g., facial recognition, fingerprint).	AAL2: The paper discusses the use of 2FA for securing payment systems.

1. **Market Presence and Adoption**: We prioritized tools with significant market share and widespread adoption in enterprise environments, as indicated by industry reports from Gartner, Forrester, and IDC. This included consideration of both user base size and deployment across different sectors.
2. **Technological Diversity**: We ensured representation across different technological approaches to MFA, including hardware security keys, software authenticators, biometric solutions, and enterprise identity management platforms. This diversity allows for a more comprehensive assessment of the current state of MFA implementation.
3. **Payment System Relevance**: Given our focus on payment systems, we selected tools that have documented implementations in financial services or are commonly recommended for securing payment processes. This includes tools with PCI-DSS compliance features or specific payment security capabilities.
4. **Documentation Availability**: We prioritized tools with sufficient public documentation to enable thorough analysis of their security features, authentication mechanisms, and compliance with standards.

In practices, we evaluate 45 industry-based tools that support developers in designing authentication models tailored specifically for payment systems.[2] To ensure a comprehensive assessment of the tools, we adopted a multi-pronged approach that integrates both academic insights and industry solutions. The tools were evaluated through several prominent sources and frameworks:

1. **Open-source Authentication Frameworks:** We began by examining authentication frameworks from popular open-source platforms such as Graylog, GitLab, and ArgoCD. These platforms offer a diverse range of tools and libraries that have been

[2] A summary of the initial analysis based on the evaluation of 45 industry-based tools is available at: https://bitly.li/a2sq

Table 7
Evaluate the IAL and AAL factors of 70 articles - 5.

Authentication	[91]	IAL2: Biometric authentication (Touch ID and Face ID).	AAL3: Combining biometrics (fingerprint or facial recognition) with tokenization and cryptographic security.
	[92]	IAL3: The paper categorizes MFA into two primary approaches: biometric and non-biometric mechanisms.	AAL3: The inclusion of multiple authentication factors and strong cryptographic protection.
	[93]	IAL3: Biometric (fingerprints, iris, face recognition, and voice)	AAL3: Multimodal biometrics, cryptographic methods and PIN.
	[94]	IAL3: Biometric authentication, behavioral analytics, and AI-driven recognition systems.	AAL3: Biometric factors (fingerprints, facial recognition), real-time behavioral analytics.
Payment	[95]	IAL2: Geolocation-based MFA system and PIN.	AAL2: User's mobile device.
	[96]	IAL2: SMS-based authentication	AAL2: 2 factors: a password or PIN, and a one-time code sent via SMS.
	[97]	IAL2: OTP or biometric (can often fall back to KBA)	AAL2: OTP or biometric.
	[98]	IAL3: Biometric, passwords, and tokenization (MFA mechanisms in Alipay).	AAL3: Biometrics (facial recognition) and device-based authentication (involving cryptographic tokens and tokenization).
	[99]	IAL3: public-key cryptography, biometrics, and certificates (x509)	AAL3: Biometrics, public-key cryptography, and certificates.

Table 8
Evaluate the IAL and AAL factors of 70 articles - 6.

Payment	[100]	IAL3: Biometric (fingerprint and facial recognition) and blockchain technology.	AAL3: Biometric authentication, cryptographic tokenization
	[101]	IAL2: Encryption techniques such as symmetric encryption (AES), asymmetric encryption (RSA), and hybrid encryption.	AAL3: end-to-end encryption (E2EE), blockchain-based encryption.
	[102]	IAL2: Continuous Authentication with Sequential Sampling (CASS)	AAL3: Multimodal biometrics, cryptographic methods and PIN.
	[103]	IAL3: Biometrics (fingerprint, facial recognition), location, and fund verification.	AAL3: Biometric authentication, location-based verification, and cryptographic tokenization.
	[104]	IAL3: Discusses MFA methods, role of biometric data.	AAL3: Blockchain technology and intrusion detection systems (IDS) combining with the use of biometric authentication and cryptographic techniques.
	[105]	IAL2: PINs, passwords, and user IDs.)	AAL2: cryptographic methods, TLS/SSL, and 2FA.
	[106]	IAL2: Biometric authentication (Touch ID and Face ID) and cryptographic mechanisms (tokenization).	AAL3: Biometric and cryptographic verification (through tokenization and dynamic cryptograms).

widely adopted by the industry, providing a rich resource for authentication solutions.

2. **Alternative Software Platforms:** Websites like AlternativeTo and G2 offer free services that assist users in finding software and applications based on their needs. Searching for MFA-related tools on these platforms also reveals similar tools, broadening the scope of potential solutions. Specifically, we explored categories such as "Authentication & Identity Service" and "Authentication in Backend".
3. **Cloud Native Computing Foundation (CNCF):** The CNCF, an organization that archives cloud-native services, provided another important resource. We evaluated tools based on CNCF's criteria for cloud compatibility. Tools that met these criteria were registered with CNCF and subsequently included in their approved services.
4. **Other Open-source Platforms:** We also explored platforms such as Apache, utilizing keywords like "authentication" and "identity" to filter tools related to MFA. This method resulted in a refined list of MFA tools pertinent to the search criteria.
5. **GitHub Approach:** Finally, we leveraged GitHub to identify curated collections of MFA tools compiled by developers. We focused on repositories labeled as "awesome lists", which consist of recommended tools and resources for MFA solutions, further expanding our database of industry tools.

After gathering a comprehensive list of tools through the aforementioned approaches, we classified the tools into five distinct categories:

- **Big Cloud:** Cloud services that support MFA solutions.
- **Apache Open-source:** Tools found within the Apache platform.
- **CNCF Authentication and Identity Projects:** Tools listed within CNCF's directory of approved services.
- **Authentication and Identity Service:** Tools discovered through alternative platforms using the search term "Authentication & Identity Service".
- **Authentication in Backend:** Tools identified on alternative platforms using the search term "Authentication in Backend".

Following this classification, we will provide a detailed analysis of each tool, including its features, adherence to NIST guidelines, and its implications for developers and payment systems. While our initial analysis encompassed 45 tools, we chose to focus on the 13 most suitable with MFA-supported tools based on their widespread industry adoption, advanced security features, and compliance with evolving regulatory standards. This selective approach allows for a more in-depth evaluation, ensuring that only the most robust and scalable

solutions are examined, which are better suited to meet the critical demands of modern payment systems. The focused review of these 13 tools is presented in Table 9.

5.2. Acronym and technical term explanation for MFA tools

This section outlines the key acronyms and technical terms frequently referenced in the context of authentication tools — i.e., MFA. These terms encompass the technical standards, protocols, and authentication mechanisms employed in modern security systems. Understanding these definitions is essential for evaluating the performance and utility of the tools listed in Table 9.

- **SSO (Single Sign-On):** Single Sign-On is an authentication scheme that allows a user to log in once and access multiple systems without re-entering credentials. This approach is critical in enterprise environments where users frequently access multiple applications throughout the day. SSO reduces password fatigue, strengthens security by centralizing authentication management, and enhances productivity by simplifying the login process. SSO implementations often rely on protocols such as OAuth2, SAML (Security Assertion Markup Language), or OpenID Connect.
- **OAuth2:** OAuth 2.0 is a widely adopted open standard used to grant third-party applications access to resources without directly sharing the user's credentials. It supports a token-based approach to authentication and authorization, particularly useful in enabling SSO capabilities. OAuth2 streamlines user experience by delegating authentication to trusted third-party providers (such as Google or Facebook), facilitating access to multiple applications with a single login. Its architecture separates the resource owner, client, and authorization server, improving security by minimizing the exposure of user credentials.
- **MFA (Multi-Factor Authentication):** Multi-Factor Authentication is a security process that requires users to provide multiple forms of verification to confirm their identity. Typically, MFA combines two or more of the following: something the user knows (e.g., a password), something the user has (e.g., a hardware token or OTP), or something the user is (e.g., biometric data like fingerprints or facial recognition). MFA significantly strengthens security by making it more difficult for unauthorized users to gain access to sensitive systems or data, even if they have compromised the user's password.
- **OTP (One-Time Password):** A One-Time Password is a dynamically generated code that is valid for a single login session or transaction. OTPs are commonly used as a second factor in MFA, offering an additional layer of security beyond static passwords. Generated by specialized authentication applications (e.g., Google Authenticator, Duo Security) or sent via SMS/email, OTPs are either time-based or event-based, reducing the risk of password reuse or interception.
- **JWT (JSON Web Token):** JSON Web Tokens are an open standard used to transmit information securely between parties as a JSON object. These tokens are signed using a secret or public/private key pair to ensure data integrity and authenticity. JWTs are extensively used in stateless authentication systems, allowing servers to verify a user's identity without storing session data. This makes JWTs an ideal solution for modern web applications that require scalable authentication mechanisms.
- **LDAP (Lightweight Directory Access Protocol):** LDAP is a protocol designed for accessing and managing distributed directory information services over an Internet Protocol (IP) network. LDAP serves as the backbone for user authentication and directory management in many enterprise systems, especially in environments that rely on centralized control, such as Microsoft Active Directory. Through LDAP, applications can query and authenticate user credentials from a directory, facilitating seamless user management across various systems.
- **FIDO U2F (Universal Second Factor):** FIDO U2F is an open authentication standard that enables users to securely authenticate using hardware-based tokens (e.g., YubiKey). Unlike traditional MFA methods that rely on passwords or OTPs, U2F provides strong phishing-resistant authentication by requiring both the physical presence of a security token and a user's password. The hardware token generates unique, per-transaction cryptographic signatures, ensuring that an attacker cannot replay a previously captured token.
- **BASIC Authentication:** BASIC Authentication is a simple and widely-used authentication mechanism where the client sends its username and password in the HTTP request headers encoded in Base64. While easy to implement, it is not secure on its own, as credentials can be easily intercepted if not paired with encryption protocols like HTTPS. BASIC authentication remains common in legacy systems, particularly for internal applications, where security demands are lower or network access is tightly controlled.
- **AD (Active Directory):** Active Directory (AD) is a directory service developed by Microsoft that provides centralized authentication and authorization services for Windows domain networks. It stores information about users, devices, and resources, allowing administrators to manage access control, user permissions, and security policies across a network. AD integrates protocols such as LDAP and Kerberos to facilitate secure user authentication, playing a critical role in enterprise identity management.
- **Self-hosted:** The term *self-hosted* refers to software or services that are hosted and operated by an organization on its own infrastructure, rather than relying on third-party hosting providers. Self-hosted solutions offer greater control and customization over the application environment, data storage, and security protocols. However, they also require a higher level of technical expertise to ensure proper installation, maintenance, and security.
- **SaaS (Software as a Service):** Software as a Service (SaaS) is a cloud-based service delivery model in which applications are hosted by a third-party provider and accessed by users via the internet. SaaS solutions eliminate the need for organizations to manage hardware or install software locally, as the service provider is responsible for maintaining infrastructure, performing updates, and ensuring security. SaaS models are widely favored for their scalability, ease of access, and lower upfront costs, especially in small to medium-sized enterprises (SMEs).

These technical terms and acronyms are integral to understanding the underlying architecture, protocols, and authentication mechanisms employed by the industry-based tools assessed in this article. They form the basis for evaluating each tool's security, usability, and overall applicability in real-world scenarios.

5.3. MFA tool analysis

We conducted a comprehensive evaluation of 13 MFA-supported tools. This assessment focused on the overall security capabilities, especially the MFA support of 13 tools widely used in designing payment systems. Our analysis revealed that the majority of these tools implement One-Time Passwords (OTP) as the second authentication factor, reflecting the widespread reliance on OTP for enhancing security. However, only a limited number of tools, such as Authentik, support more advanced authentication factors like biometrics. This evaluation provides valuable insights into the current state of MFA support in industry tools, highlighting areas where improvements are needed to meet higher security standards. The summary of this evaluation is represented in Table 9.

ArgoCD: ArgoCD uses JSON Web Tokens (JWTs) exclusively for authentication to its API server, avoiding traditional username/password bearer tokens. For the local admin user, a JWT is obtained by

Table 9
Evaluation of 13 industry-based tools.

No.	Name	Type	MFA supported	Cost
1	ArgoCD	Authentication in Backend	OAuth2 login flow for SSO users	Open Source
2	Shiro	Apache Opensource	Verify user by username & password. After users submit their identity include principals and credentials, the token for user is created and used when user request something in the application.	Open Source
3	Kerby	Apache Opensource	Supports Token Preauth mechanism to allow clients to request tickets using JWT tokens and supports OTP mechanism to allow clients to request tickets for internal users.	Open Source
4	Knox	Apache Opensource	This tool provides authentication and access for Apache Hadoop services which are used by internal user. The current release of Knox ships with an authentication provider based on the Apache Shiro project and is initially configured for BASIC authentication against an LDAP store	Open Source
5	Fortress	Apache Opensource	Employ an LDAP backend for authentication	Open Source
6	Syncope	Apache Opensource	The Web Access is supported via the Apereo CAS and provided some MFA modules like Duo Security/Google Authenticator (not supported out of the box)	Open Source
7	Deployd	Authentication and Identity Service	Verify by username & password	Open Source, Self-hosted
8	SuperTokens	Authentication and Identity Service	If users sign in by email & password, then SuperTokens will ask the users to do email verification, followed by Time-based OTP/email OTP/SMS OTP.	SaaS, Self-hosted
9	TOTPRadius	Authentication and Identity Service	LDAP Proxy mode is an authentication mode in TOTPRadius that supports 2FA (AD/LDAP password and OTP).	Self-hosted
10	FusionAuth	Authentication and Identity Service	After users login by thier password, users is prompted to choose one of 2 methods (TOTP/an SMS or Email-based one time use code).	Open Source, SaaS, Self-hosted
11	Authentik	Authentication and Identity Service	Authentik is an open-source IdP with an integrated user directory that supports OAuth2 Provider (OIDC) as well as LDAP. Authentik supports configuring 2FA login flow (password and OTP) for SSO users.	Open Source, Self-hosted
12	Gluu server	Authentication and Identity Service	A number of interception scripts which are used to implement MFA are included out-of-the-box, including scripts to support FIDO U2F tokens, Super Gluu (Gluu's free Android and iOS 2FA application), Duo Security, OTP.	Open Source, SaaS, Self-hosted
13	Zitadel	Authentication and Identity Service	Users can setup MFA in their account by choosing TOTP, SMS OTP, Email OTP or U2F to be the second factor in login flow.	Open Source, Self-hosted

exchanging a username and password via the /api/v1/session endpoint. This token is issued and signed by the ArgoCD server, expiring after 24 h, with immediate revocation upon password change. Single Sign-On (SSO) users authenticate through an OAuth2 flow with an OIDC provider, and the JWTs are managed and issued by the provider. For automation, project-specific JWTs are generated with limited privileges and configurable expiration, and can be revoked by deleting the reference ID.

Shiro: Apache Shiro provides a flexible and comprehensive authentication mechanism, using a variety of methods such as username/password, tokens, and cryptographic techniques. At its core, Shiro uses the concept of "realms" to authenticate users. A realm acts as a data source for obtaining user credentials, and it can connect to databases, LDAP, or other external systems. When a user attempts to authenticate, their credentials are compared against the data in the configured realm. Shiro also supports session management and can integrate with single sign-on (SSO) solutions. Additionally, it provides features like remember-me functionality, role-based access control (RBAC), and flexible encryption for protecting user data and passwords. Shiro's modular design allows developers to implement custom authentication strategies as needed.

Kerby: Apache Kerby provides a Kerberos-based authentication mechanism that is secure and widely used for authenticating users in distributed systems. Kerby simplifies the traditional Kerberos protocol by offering an easy-to-use, lightweight, and Java-based implementation. In this mechanism, authentication is based on ticket-granting tickets (TGTs) and service tickets. Users authenticate by initially obtaining a TGT from the Kerby Key Distribution Center (KDC) using their credentials (typically username and password). This TGT can then be used to request service tickets for accessing other network services securely. Kerby supports various encryption methods and can work with both traditional and modern identity providers, offering flexibility for enterprise environments. Its key feature is secure, mutual authentication, ensuring both the user and service can verify each other's identity.

Knox: Apache Knox provides a gateway that secures access to Hadoop clusters and other big data services by centralizing authentication and enforcing access control. Knox supports multiple authentication mechanisms, including Kerberos, LDAP, Active Directory, SAML, and OAuth. When a user or system requests access to a Hadoop service, Knox acts as a reverse proxy, handling authentication on behalf

of the user. Depending on the configured method, Knox either validates credentials directly (e.g., through LDAP) or integrates with external identity providers for Single Sign-On (SSO). Once authenticated, Knox generates a token for the user, which is used to manage session state and authorize subsequent requests without re-authentication. This architecture ensures consistent and secure access across all Hadoop services while abstracting the complexity of handling authentication mechanisms from individual services.

Fortress: Apache Fortress employs an LDAP backend to provide Java APIs and web components for authentication, authorization, administration, and review, with strict adherence to ANSI RBAC and IETF LDAPv3 standards. In terms of Java EE security, Apache Fortress uses the Fortress Realm to handle authentication and coarse-grained authorization by mapping users and roles to an LDAP server. User authentication is performed using standard HTTP Basic Auth tokens for userid and password credentials. These credentials are verified by the Apache Fortress Realm through a bind operation to the Directory Server, ensuring secure authentication.

Syncope: Apache Syncope provides a flexible authentication mechanism through various Authentication Modules, which define how credentials are verified based on the configured Authentication Policy. Syncope supports multiple principal authentication methods, including databases, JAAS, LDAP, SPNEGO, X509, OpenID Connect, OAuth2, SAML, Apple Sign-In, Azure Active Directory, Google OpenID, and Keycloak, enabling integration with a wide range of identity providers. Additionally, it supports MFA via Duo Security, Fido U2F, and Google Authenticator for enhanced security. Each authentication module allows Syncope to securely authenticate users against specific technologies or repositories, offering versatile identity management across different environments and use cases.

Deployd: Deployd provides a simple and customizable authentication mechanism for building APIs. It includes built-in user authentication using a resource called Users, which handles registration, login, and session management. Users can create accounts by submitting their credentials (e.g., username and password), and Deployd stores this information securely, typically in a database. For login, Deployd validates user credentials and creates a session for authenticated users, storing session data in cookies or tokens.

SuperTokens: SuperTokens provides a robust MFA mechanism that enhances security by requiring users to provide multiple forms of verification during login. Typically, MFA in SuperTokens involves a primary factor, like a password or OAuth-based login, followed by a second factor, such as an OTP (one-time password) delivered via email or SMS. SuperTokens supports customizable MFA workflows, allowing developers to define when and how the second authentication step is triggered.

TOTPRadius: TOTPRadius offers a MFA mechanism based on the Time-Based One-Time Password (TOTP) algorithm, which adds an extra layer of security to user logins. In this system, after entering their primary credentials, users must provide a time-sensitive OTP generated by an authenticator app, such as Google Authenticator or Authy, which is synced with TOTPRadius. The OTP is typically valid for a short duration (e.g., 30 s), ensuring that each login attempt requires a fresh code. TOTPRadius integrates with various VPNs, network devices, and remote access systems to enforce TOTP-based MFA across environments. It supports LDAP and Active Directory for user management and can be easily configured to enhance security without disrupting the user experience. This combination of primary credentials and TOTP ensures that even if a password is compromised, unauthorized access is prevented without the correct time-sensitive OTP.

FusionAuth: FusionAuth provides a flexible and secure MFA mechanism, allowing developers to enhance user account protection by requiring additional verification methods beyond just a password. Typically, FusionAuth implements MFA using Time-Based One-Time Passwords (TOTP), where users link their accounts with an authenticator app like Google Authenticator or Authy. After a successful initial login with their username and password, users are prompted to enter a TOTP generated by their authenticator app, ensuring an additional layer of security. FusionAuth also supports other MFA methods like SMS-based codes or email verification.

Authentik: Authentik offers a comprehensive MFA mechanism to enhance security for user logins. It supports various MFA methods, including TOTP, WebAuthn for hardware tokens or biometric verification, and SMS or email-based one-time codes. After a user provides their primary credentials, Authentik prompts for a second verification step, such as entering a TOTP from an authenticator app like Google Authenticator or verifying through WebAuthn.

Gluu Server: Gluu Server utilizes interception scripts to implement its robust MFA mechanism, providing a versatile and secure authentication experience. The platform comes with a variety of pre-configured scripts that support various authentication methods, including FIDO U2F tokens, Gluu's own Super Gluu mobile app for two-factor authentication, certificate authentication, Duo Security, and One-Time Passwords. For organizations with unique MFA requirements, Gluu Server allows the creation of custom interception scripts, enabling the enforcement of specific policies like prompting only certain user groups for two-factor authentication or requiring additional authentication steps for access from unknown IP addresses.

Zitadel: Zitadel's MFA mechanism enhances security by requiring additional authentication layers beyond a password. For instances without custom login settings, Zitadel supports both second factors (2FA) and multi factors (MFA). The second factor, such as an authentication app, fingerprint, or Windows Hello, is used after a password to provide extra security. Multi-factor (MFA), often referred to as passwordless or passkey authentication, can be used as both the first and second layer, eliminating the need for a password.

5.4. Review of hardware security keys

5.4.1. Selection criteria

Our tool selection was guided by four primary criteria:

1. **Market Presence and Adoption**: We prioritized tools with significant market share and widespread adoption in enterprise environments, as indicated by industry reports from Gartner, Forrester, and IDC. This included consideration of both user base size and deployment across different sectors.
2. **Technological Diversity**: We ensured representation across different technological approaches to MFA, including hardware security keys, software authenticators, biometric solutions, and enterprise identity management platforms. This diversity allows for a more comprehensive assessment of the current state of MFA implementation.
3. **Payment System Relevance**: Given our focus on payment systems, we selected tools that have documented implementations in financial services or are commonly recommended for securing payment processes. This includes tools with PCI-DSS compliance features or specific payment security capabilities.
4. **Documentation Availability**: We prioritized tools with sufficient public documentation to enable thorough analysis of their security features, authentication mechanisms, and compliance with standards.

5.4.2. Tool categories

Based on these criteria, we classified the selected tools into five distinct categories:

1. **Hardware Security Keys**: Physical authentication devices that provide cryptographically secure verification, including FIDO U2F and FIDO2/WebAuthn compatible devices such as Google Titan Security Keys and YubiKey.

2. **Software Authenticators**: Mobile or desktop applications that generate time-based one-time passwords (TOTP) or provide push-based verification, including Google Authenticator, Microsoft Authenticator, and Duo Mobile.
3. **Biometric Authentication Platforms**: Systems that leverage fingerprint, facial recognition, or other biometric factors, often integrated with device hardware like Touch ID, Face ID, or Windows Hello.
4. **Enterprise MFA Solutions**: Comprehensive identity and access management platforms with MFA capabilities designed for organizational deployment, such as Okta, Auth0, and ForgeRock.
5. **Open-Source MFA Frameworks**: Community-maintained authentication frameworks that provide MFA capabilities, including FusionAuth, Gluu Server, and PrivacyIDEA.

5.4.3. Data collection process

For each selected tool, we gathered information from the following sources:

1. Official product documentation and technical specifications
2. Security whitepapers and compliance certifications
3. API documentation and developer resources
4. Independent security assessments and penetration testing reports
5. Academic literature analyzing the security properties of these tools

This systematic approach ensured that our analysis captured a representative sample of the MFA tool landscape, with particular emphasis on solutions relevant to payment systems security.

5.4.4. Hardware security keys analysis

Hardware security keys represent one of the strongest forms of authentication factors in MFA implementations. Our analysis includes two prominent solutions in this category:

1 — Google Titan Security Key Google Titan Security Keys implement the FIDO U2F and FIDO2 standards, providing phishing-resistant authentication through cryptographic operations.[3] In our assessment against NIST standards:

- **IAL Support**: The Titan Security Key supports IAL2 by providing a high-confidence association between the authenticator and the claimed identity, especially when paired with initial identity verification.
- **AAL Support**: The key achieves AAL3 compliance by implementing FIDO2 protocols with hardware-based key protection and cryptographic authentication, making it suitable for high-security payment applications.
- **Key Features**: Tamper-resistant hardware security module, protection against physical attacks, FIDO certification, NFC capabilities (in selected models), and resistance to phishing attacks through origin validation.

2 — YubiKey (Yubico) YubiKeys represent another leading hardware security key solution with broader protocol support:[4]

- **IAL Support**: Similar to Titan, YubiKeys support IAL2 implementation when properly integrated with identity proofing processes.
- **AAL Support**: YubiKeys achieve AAL3 through FIDO2/WebAuthn implementation, hardware-protected cryptographic keys, and multi-protocol support. Their versatility makes them particularly valuable in heterogeneous authentication environments.
- **Key Features**: Support for multiple authentication protocols (FIDO2, FIDO U2F, PIV, OpenPGP, OATH-TOTP), physical durability, no battery or connectivity requirements, and availability in various form factors including USB-A, USB-C, and NFC.

3 — Microsoft Authenticator Microsoft Authenticator provides MFA through TOTP, push notifications, and passwordless sign-in, enhancing security across various platforms.[5] In our assessment against NIST standards:

- **IAL Support**: Microsoft Authenticator can support IAL2 when used in conjunction with identity verification mechanisms, ensuring a moderate level of confidence in the asserted identity.
- **AAL Support**: The application can achieve AAL2 compliance by leveraging multi-factor authentication, such as biometric authentication or device binding. However, it does not meet AAL3 requirements due to the absence of hardware-based cryptographic protections.
- **Key Features**: Supports passwordless authentication, biometric verification, app-based MFA, device binding for enhanced security, and push notification approval for user convenience.

4 — Authy Authy, developed by Twilio, provides multi-factor authentication through TOTP and push notifications, ensuring secure access across multiple devices.[6] Support in Authy include:

- **IAL Support**: Authy can support IAL2 by enabling multi-device authentication with encrypted backups, which helps establish a trusted identity.
- **AAL Support**: Authy achieves AAL2 compliance through multi-factor authentication, offline OTPs, and encrypted backups. However, it does not reach AAL3 as it lacks hardware-based cryptographic security measures.
- **Key Features**: Multi-device support, encrypted backups for enhanced security, offline OTP generation for authentication without internet access, and app-based MFA for user convenience.

5 — Duo Security Duo Security, a Cisco solution, offers adaptive multi-factor authentication through push notifications, SMS, phone calls, and hardware tokens, providing flexible security options and also support security that satisfied NIST standard.[7]

- **IAL Support**: Duo Security can support IAL2 by leveraging risk-based access controls and adaptive authentication to verify user identity with a moderate level of confidence.
- **AAL Support**: Duo Security achieves AAL2 compliance by utilizing multi-factor authentication, including hardware tokens and risk-based access. However, it does not meet AAL3 requirements as it lacks a dedicated hardware security module for cryptographic authentication.
- **Key Features**: Adaptive authentication, risk-based access control, endpoint security integration, app-based and hardware token authentication, and support for various verification methods including SMS and phone calls.

6 — RSA SecurID (RSA Security) RSA SecurID is a widely used hardware security solution that provides multi-factor authentication through various methods.[8]

- **IAL Support**: RSA SecurID can support IAL2 when integrated with identity proofing mechanisms, ensuring strong identity verification in enterprise environments.

[3] Titan Security Key https://cloud.google.com/security/products/titan-security-key

[4] YubiKey https://www.yubico.com/

[5] Microsoft Authenticator https://www.microsoft.com/en-us/security/mobile-authenticator-app

[6] Authy https://authy.com/

[7] Duo Security https://duo.com/

[8] RSA SecurID https://www.rsa.com/en-us/products/rsa-securid-suite

- **AAL Support**: RSA SecurID achieves AAL2 or AAL3 depending on the deployment. Hardware tokens and time-based OTP provide AAL2, while push notifications and additional cryptographic protections can enhance security to AAL3 in compliant implementations.
- **Key Features**: Time-based OTP generation, support for hardware tokens and mobile app-based authentication, on-premises or cloud deployment, and seamless enterprise integration with Windows, macOS, Linux, iOS, and Android platforms.

7 — Feitian ePass Security Key (Feitian) Feitian ePass Security Key is a hardware-based authentication solution designed for strong phishing-resistant security.[9]

- **IAL Support**: Feitian ePass Security Key can support IAL2 when combined with appropriate identity proofing mechanisms, ensuring a higher level of identity assurance in secure environments.
- **AAL Support**: The security key achieves AAL3 through FIDO2/WebAuthn implementation, hardware-protected cryptographic authentication, and resistance to phishing attacks. These capabilities make it suitable for high-security applications.
- **Key Features**: FIDO2 and U2F support for passwordless authentication, hardware-based protection against phishing attacks, FIDO certification, and multiple connectivity options, including USB-A, USB-C, NFC, and Bluetooth, ensuring broad platform compatibility.

8 — OnlyKey (CryptoTrust) OnlyKey is a multi-functional hardware security key that provides secure authentication with built-in encryption and PIN protection.[10]

- **IAL Support**: OnlyKey can support IAL2 when integrated with identity proofing processes, ensuring strong identity verification through PIN protection and secure key storage.
- **AAL Support**: OnlyKey achieves AAL3 by implementing FIDO2/WebAuthn, hardware-based encryption, and multi-factor authentication with PIN entry. Its robust security features make it suitable for high-assurance authentication needs.
- **Key Features**: Multi-protocol support (FIDO2, U2F, OTP, Smart Card), hardware-based security with encrypted storage, PIN protection for enhanced security, and broad platform compatibility via USB-A and USB-C connections.

9 — SoloKey (SoloKeys) SoloKey is an open-source hardware security key designed to provide strong, phishing-resistant authentication with transparent security practices.[11]

- **IAL Support**: SoloKey can support IAL2 when combined with identity proofing processes, ensuring a strong level of identity assurance in secure authentication scenarios.
- **AAL Support**: SoloKey achieves AAL3 through FIDO2/WebAuthn implementation, hardware-backed cryptographic security, and phishing-resistant authentication. Its open-source firmware enhances transparency and security auditability.
- **Key Features**: Support for FIDO2 and U2F authentication protocols, open-source firmware for enhanced security transparency, secure hardware for cryptographic key protection, and multiple connectivity options including USB-A, USB-C, and NFC for broad platform compatibility.

10 — Google Authenticator (Google) Google Authenticator is a widely used app-based authentication solution that generates time-based one-time passwords (TOTP) for two-factor authentication.[12]

- **IAL Support**: Google Authenticator can support IAL1 as it does not include built-in identity proofing mechanisms. However, when integrated with an identity verification system, it may contribute to an IAL2-compliant authentication process.
- **AAL Support**: Google Authenticator achieves AAL2 by generating time-based OTPs (TOTP) for authentication. However, it does not reach AAL3 since it lacks hardware-backed security and resistance to phishing attacks.
- **Key Features**: Offline OTP generation without internet connectivity, simple setup via QR codes, app-based authentication for iOS and Android platforms, and broad compatibility with various online services.

11 — Google Passkeys (Google) Google Passkeys offer a modern, passwordless authentication solution leveraging FIDO2 and WebAuthn standards.[13]

- **IAL Support**: Google Passkeys can support IAL2 when combined with an identity-proofing process. Since passkeys are tied to a user's device and identity, they can enhance identity assurance levels in federated authentication models.
- **AAL Support**: Google Passkeys achieve AAL3 by utilizing device-based authentication, FIDO2/WebAuthn cryptographic mechanisms, and phishing-resistant security measures. The cloud-sync capability ensures strong authentication across multiple devices.
- **Key Features**: Passwordless authentication, phishing resistance, multi-device synchronization, secure cloud-based key storage, and compatibility with major platforms including Windows, macOS, Android, and iOS.

12 — Apple Passkeys (Apple) Apple Passkeys provide a secure, passwordless authentication solution leveraging FIDO2 and WebAuthn standards.[14]

- **IAL Support**: Apple Passkeys can support IAL2 when integrated with identity verification mechanisms. By leveraging biometric authentication (Face ID, Touch ID) and secure enclave technology, they enhance identity assurance.
- **AAL Support**: Apple Passkeys achieve AAL3 by utilizing hardware-backed cryptographic credentials, biometric authentication, and cloud-based key synchronization via iCloud Keychain. These factors provide strong authentication with phishing resistance.
- **Key Features**: Passwordless authentication, biometric-based security, secure enclave protection, automatic multi-device synchronization via iCloud Keychain, and cross-platform support for Windows, macOS, Android, and iOS.

13 — Microsoft Passkeys (Microsoft) Microsoft Passkeys provide a secure and passwordless authentication mechanism utilizing FIDO2 and WebAuthn standards.[15]

- **IAL Support**: Microsoft Passkeys can support IAL2 when integrated with identity proofing processes. By leveraging biometric authentication through Windows Hello and hardware security, they strengthen identity assurance.
- **AAL Support**: Microsoft Passkeys achieve AAL3 by employing hardware-backed cryptographic credentials, biometric authentication, and secure key storage mechanisms. These ensure phishing-resistant and strong authentication.

[9] Feitian ePass Security Key https://www.ftsafe.com/Products/FIDO
[10] OnlyKey https://onlykey.io/
[11] SoloKey https://solokeys.com/
[12] Google Authenticator https://support.google.com/accounts/answer/1066447?hl=en
[13] Google Passkeys https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password/
[14] Apple Passkeys https://support.apple.com/en-us/HT213305
[15] Microsoft Passkeys https://www.microsoft.com/en-us/security/blog/2022/05/05/the-passwordless-future-with-passkeys/

- **Key Features**: Passwordless login, biometric-based authentication via Windows Hello, secure hardware-backed credentials, seamless cloud-based synchronization, and support for Windows 10, Windows 11, Edge, and Android.

14 — YubiKey (Passkey Support) (Yubico) YubiKey with Passkey Support provides a robust hardware-based authentication solution, integrating multiple security protocols for enhanced protection.[16]

- **IAL Support**: YubiKey supports IAL2 when combined with appropriate identity proofing measures. The integration of FIDO2/WebAuthn and hardware-based security ensures strong identity assurance.
- **AAL Support**: YubiKey achieves AAL3 through its hardware-protected cryptographic credentials, phishing-resistant authentication mechanisms, and support for multiple authentication protocols, including FIDO2, U2F, and OTP.
- **Key Features**: Hardware-based authentication, support for multiple protocols (FIDO2, U2F, OTP), phishing-resistant security, no battery or internet dependency, and compatibility with various platforms (Windows, macOS, Linux, iOS, Android) through USB-A, USB-C, and NFC connectivity.

15 — Dashlane Passkeys Dashlane Passkeys offer a convenient and secure passwordless authentication solution, integrating with Dashlane's password manager for seamless user experience.[17]

- **IAL Support**: Dashlane Passkeys support IAL2 when integrated with identity proofing systems, offering a high level of identity assurance through FIDO2 and WebAuthn protocols.
- **AAL Support**: Dashlane achieves AAL3 through its cloud-based authentication process, leveraging password manager integration, phishing-resistant security, and support for multiple platforms, ensuring strong authentication at all levels.
- **Key Features**: Password manager integration, phishing-resistant security, multi-device access, cloud-based authentication, browser extension support, and compatibility across Windows, macOS, iOS, Android, and web platforms.

Both hardware security keys provide strong protection against sophisticated attacks including phishing, man-in-the-middle attacks, and credential theft. Their implementation in payment systems offers significantly enhanced security compared to traditional OTP-based solutions. We also classified the 10 selected tools into five distinct categories (see Table 10):

6. Discussion

The comprehensive analysis of MFA implementations across various domains and tools reveals significant insights into the current state and future directions of digital payment security. This discussion synthesizes our findings and explores their broader implications for the field, highlighting key trends, challenges, and opportunities for advancement.

6.1. Evolution of authentication mechanisms

The landscape of authentication mechanisms has undergone substantial transformation, evolving from traditional password-based systems to sophisticated multi-factor solutions. Our analysis reveals a marked increase in the adoption of biometric authentication, particularly within payment and financial sectors, where approximately 60% of analyzed papers incorporate biometric verification components. This trend reflects a growing recognition of the limitations inherent in conventional authentication methods and the need for more robust security measures.

Payment systems demonstrate the highest level of innovation in authentication mechanisms, frequently implementing hybrid approaches that combine traditional methods with advanced biometric and behavioral analysis. This evolution is particularly evident in mobile payment platforms, where facial recognition and fingerprint authentication have become increasingly prevalent. Financial services, while equally focused on security, show a more measured approach, carefully balancing innovation with regulatory compliance and operational stability.

Interestingly, IoT and E-Service domains exhibit more conservative authentication strategies, primarily due to technical constraints and the need for broad compatibility across diverse platforms. This observation suggests that the evolution of authentication mechanisms is not uniform across sectors but rather is shaped by specific domain requirements and technological capabilities.

6.2. Industry implementation and academic research gap

A significant finding from our analysis is the substantial gap between theoretical capabilities proposed in academic research and actual implementations in industry tools. While academic literature explores numerous innovative authentication methods, industry implementations tend to favor more established, proven approaches. This disparity is most evident in the implementation of second-factor authentication, where approximately 33% of evaluated tools rely primarily on OTP mechanisms, despite research suggesting the potential benefits of more sophisticated approaches.

The limited adoption of advanced authentication methods in industry tools can be attributed to several factors. First, the complexity of implementing and maintaining sophisticated authentication systems often presents practical challenges for organizations. Second, concerns about user acceptance and adaptation to new authentication methods may discourage the adoption of more innovative solutions. Third, the need for backward compatibility and integration with existing systems often constrains the implementation of cutting-edge authentication technologies.

6.3. Security and usability considerations

Our analysis reveals a persistent tension between security requirements and user experience, particularly in payment systems where transaction speed and convenience are crucial. High-security implementations achieving IAL3/AAL3 levels typically introduce additional user friction, potentially impacting adoption rates and user satisfaction. Conversely, simplified authentication methods may compromise security in favor of usability, creating potential vulnerabilities in the system.

Context-aware authentication emerges as a promising approach to balancing these competing demands. By dynamically adjusting security requirements based on transaction risk levels, user behavior patterns, and environmental factors, such systems can provide appropriate security measures while minimizing unnecessary user friction. However, the implementation of context-aware authentication requires sophisticated risk assessment capabilities and careful consideration of privacy implications.

6.4. Regulatory landscape and standardization

The influence of regulatory frameworks varies significantly across domains, with payment and financial sectors showing the strongest alignment with regulations such as PSD2. Our analysis indicates that approximately 77% of analyzed payment systems demonstrate high regulatory compliance, reflecting the critical role of these systems in

[16] YubiKey Passkeys https://www.yubico.com/solutions/passkeys/

[17] Dashlane Passkeys https://www.dashlane.com/blog/introducing-passkeys-the-future-of-passwordless-authentication

Table 10
Comprehensive comparison of MFA tools for payment systems.

Tool	Category	IAL support	AAL support	Auth methods	Payment-specific features
Google Titan	Hardware Security Key	IAL2	AAL3	FIDO2, U2F	Phishing resistance, Origin validation
YubiKey	Hardware Security Key	IAL2	AAL3	FIDO2, U2F, OATH, PIV	Biometric authentication, Multi-protocol, PCI-DSS compatible
Microsoft Authenticator	Hardware Security Key	IAL2	AAL2	TOTP, Push Notifications, Passwordless	Passwordless sign-in, Device binding
Authy	Hardware Security Key	IAL2	AAL2	TOTP, Push Notifications	Multi-device support, Encrypted backups
Duo Security	Hardware Security Key	IAL2	AAL2	Push Notifications, SMS, Phone call, Hardware tokens	Risk-based access, Endpoint security
RSA SecurID	Hardware Security Key	IAL2	AAL2/ AAL3	OTP, Hardware Token, Push Notifications	On-premises or cloud deployment, Enterprise integration
Feitian ePass Security Key	Hardware Security Key	IAL2	AAL3	FIDO2, U2F	Phishing-resistant
OnlyKey	Hardware Security Key	IAL2	AAL3	FIDO2, U2F, OTP, Smart Card	Encrypted storage, PIN protection
SoloKey	Hardware Security Key	IAL2	AAL3	FIDO2, U2F	Phishing-resistant
Google Authenticator	Hardware Security Key	IAL1	AAL2	FIDO2, U2F	Offline OTPs, Simple setup
Google Passkeys	Hardware Security Key	IAL2	AAL3	FIDO2, WebAuthn	Phishing-resistant, Passwordless, Multi-device sync
Apple Passkeys	Hardware Security Key	IAL2	AAL3	FIDO2, WebAuthn	Secure enclave, Auto-sync
Microsoft Passkeys	Hardware Security Key	IAL2	AAL3	FIDO2, WebAuthn	Passwordless login
Dashlane Passkeys	Hardware Security Key	IAL2	AAL3	FIDO2, WebAuthn	Phishing-resistant, Multi-device access
ArgoCD	Backend	IAL1–2	AAL1	OAuth2	Limited payment relevance
Shiro	Apache	IAL1–2	AAL1	Username/Password	Basic security for payment backends
Kerby	Apache	IAL2	AAL2	Kerberos, JWT, OTP	Token-based authorization
Knox	Apache	IAL2	AAL1–2	LDAP, Basic Auth	API security for data services
Fortress	Apache	IAL2	AAL1	LDAP	Role-based access control
Syncope	Apache	IAL2	AAL2	OAuth2, CAS	Extensible for payment workflows
Deployd	Identity	IAL1	AAL1	Username/Password	API backend for payment apps
SuperTokens	Identity	IAL2	AAL2	Email/Password, TOTP, SMS/Email OTP	Customizable payment flows
TOTPRadius	Identity	IAL2	AAL2	AD/LDAP, OTP	Enterprise payment systems
FusionAuth	Identity	IAL2	AAL2	TOTP, Email/SMS	Customizable for payment workflows
Authentik	Identity	IAL2	AAL2	OAuth2, OTP	SSO for payment services
Gluu Server	IAM	IAL2–3	AAL2–3	FIDO, OTP, Mobile	Financial compliance support
Zitadel	IAM	IAL2	AAL2–3	TOTP, SMS/Email OTP, U2F	Modern payment platform support

financial infrastructure. However, the regulatory landscape for authentication in IoT and E-Service sectors remains less defined, leading to fragmented approaches and varying security standards.

The lack of comprehensive standardization across domains presents challenges for interoperability and security assessment. While emerging standards attempt to address these issues, their adoption remains inconsistent, particularly in rapidly evolving technological areas. This situation highlights the need for more coordinated standardization efforts that can accommodate technological advancement while ensuring security and interoperability.

6.5. Future research and development priorities

Based on our comprehensive analysis, several key areas emerge as priorities for future research and development. The advancement

of adaptive authentication systems represents a particularly promising direction, with the potential to fundamentally transform how security measures are implemented and managed. These systems could leverage artificial intelligence and machine learning to provide dynamic, context-aware security that adapts to changing threat landscapes and user behaviors.

Integration of emerging technologies, particularly blockchain and advanced AI systems, offers significant potential for enhancing authentication security. However, successful implementation requires careful consideration of practical constraints and user needs. Privacy-preserving authentication methods represent another critical area for development, particularly as biometric authentication becomes more prevalent.

6.6. Practical implications and recommendations

The findings of our analysis have significant implications for practitioners and system designers. The development of authentication systems should prioritize risk-based approaches that can adapt to different security contexts while maintaining usability. Regular security assessments and updates are essential, as is the development of clear security policies that address both technical and human factors.

Investment in user education and awareness remains crucial for the successful implementation of any authentication system. Organizations should develop comprehensive training programs that help users understand and effectively utilize security features while maintaining awareness of potential threats.

In conclusion, while significant progress has been made in the implementation of multi-factor authentication, considerable work remains in bridging the gap between theoretical capabilities and practical implementations. Future developments should focus on creating more adaptive, context-aware systems that maintain high security while ensuring user convenience. Success in this endeavor will require continued collaboration between academic researchers, industry practitioners, and regulatory bodies to develop and implement effective, user-friendly authentication solutions.

7. Related work

Through a preliminary review, we assessed the strengths, weaknesses, objectives, and resources discussed in these articles, comparing them to our own findings as detailed in Table 11. To elucidate the rationale and structure of this table, it is designed to systematically juxtapose our work with existing literature in the domain of MFA and security. This comparative approach is crucial for understanding the diverse methodologies and evaluation standards employed within the field.

Table 11 facilitates a structured analysis across several key dimensions. The column 'Standard for Analysis' serves to identify the benchmark frameworks utilized by each study, such as recognized standards like NIST, ISO/IEC, or eIDAS. This is instrumental in gauging the rigor and accepted industry practices adopted in their security assessments. Furthermore, the column 'MFA tools analysis' indicates whether the research analyzed the MFA support capabilities in any industry-based authentication tools. The 'Relative works' column provides context by outlining the specific contributions and focus of each study, allowing for a direct comparison of research scopes. Lastly, 'Period of time' specifies the temporal context of each study, which is essential for understanding the evolution of research and practices in this dynamic field.

By employing these defined columns, our comparative methodology enabled a systematic and rigorous evaluation of the selected articles. This structured approach allowed us to identify not only the commonalities and divergences in their contributions but also any potential limitations or gaps in their approaches. Consequently, these comprehensive evaluations have been invaluable in identifying a suitable development direction and providing valuable insights to refine the research direction of our paper, ensuring it is both relevant and impactful within the broader academic landscape.

From the analysis of related works, a significant gap in the existing research is the lack of a well-defined evaluation standard for selecting relevant studies on MFA and 2FA. Most prior studies either do not specify any selection criteria or rely on security recommendations from organizations like NIST and EBA solely for defining concepts rather than as a basis for data selection.

Additionally, another limitation is the insufficient use of MFA tools to assess the effectiveness of authentication methods. While some studies attempt to implement fraud detection models using machine learning, it is unclear whether this approach is applied to evaluate MFA itself. Therefore, this study addresses these gaps by proposing a well-defined evaluation standard for selecting relevant literature and leveraging MFA tools to provide more accurate assessments of security mechanisms. This approach enhances objectivity and reliability compared to previous research.

In the 3 subsections of this section, we review relevant studies on multi-factor authentication in three main areas: Payment Systems, Edge and Cloud Communications, and E-Commerce/Online Retail. To compare these works with ours, we employ a systematic set of criteria: (1) Key Findings and Contributions, assessing the novelty and value each study brings to the MFA field; (2) Relation to Our Objective, examining compatibility with our goal of evaluating MFA in digital payment systems against NIST SP 800-63 standards; and (3) Critical Analysis and Limitations, identifying strengths, weaknesses, and gaps to highlight research needs. For instance, Konoth et al. [42] propose a practical 2FA solution for mobile payments, emphasizing usability, yet lack alignment with NIST guidelines—a gap our study addresses by evaluating both academic proposals and industry tools (e.g., 13 tools, 33% OTP-reliant) against these standards, revealing a theory-practice divide absent in prior work. We categorized these studies into distinct topics and conducted a qualitative analysis based on novelty, practical impact, and relevance to digital payment security. This structured comparison, summarized in Table 11, highlights similarities (e.g., focus on usability in payment systems), differences (e.g., our NIST-centric evaluation vs. others' implementation focus), and shortcomings (e.g., limited biometric integration in 40% of studies despite 60% adoption trends), elucidating general trends like biometric growth and informing future research directions.

7.1. Multi-factor authentication in payment systems

Key Findings and Contributions: The collection of relative works on "Multi-Factor Authentication in Payment Systems" provides valuable insights and contributions to enhancing the security and effectiveness of authentication in various financial contexts. These works highlight the vulnerabilities and limitations of existing authentication schemes, identify threat models, and propose countermeasures to mitigate risks. They shed light on adoption patterns, design choices, and compliance with regulations in the banking and e-Banking sectors. The works also explore machine learning techniques, user authentication approaches, and authentication methods in information systems, offering a comprehensive understanding of current trends and advancements. Overall, these works contribute to the identification of security concerns and the exploration of novel authentication mechanisms to improve the trust, integrity, and confidentiality of payment transactions.

Relation to the Survey Paper's Objective: Relative works contributes to the survey paper's objective of evaluating multi-factor authentication practices comprehensively in payment systems. While each work focuses on different aspects within the broader domain of authentication and security, they collectively provide valuable insights into specific areas such as mobile money authentication, online banking,

Table 11
Comparisons of related works and our work.

No.	Paper	Standard for analysis	MFA tools analysis	Relative works.	Period of time
1	Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. [16]	No (not mentioned any standard)	No	97 papers focused on the threat models in the 2FA scheme for mobile money.	after 2019
2	A survey on multi-factor authentication for online banking in the wild. [17]	No (just using standard for defining MFA concepts)	No	MFA solutions adopted by 30 banks operating.	before 30/9/2018
3	Strong Authentication for e-Banking: A Survey on European Regulations and Implementations. [107]	No	No	The strong authentication mechanisms implemented by 26 major EU and non-EU banks.	before 2017
4	Effects of PSD2 on security architecture of mobile banking: a review of literature. [108]	No (just focus on PSD2)	No	22 academic publications about the security architecture.	before 2017
5	A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection. [109]	No (just present an overview of authentication methods)	No	Classical machine learning models and techniques of user authentication.	2004–2015
6	A Review of Secure Authentication based e-Payment Protocol. [110]	No	No	Review 58 papers related to mobile payment schemes, smart cards, security, and privacy-based encryption	2004–2016
7	A review on electronic payments security. [111]	No	No	131 research articles published on electronic payment.	2010–2020
8	Authentication methods review: How to enhance identity trust in authentication. [112]	No	No	40 papers, articles and publications.	before 2017
9	Recent trends in user authentication–a survey. [113]	No (just focus on defining and implementing authentication methods)	No	New mechanisms to authenticate the users.	before 2019
10	Strong Electronic Identification: Survey & Scenario Planning. [114]	No	No	44 researches conducted on e-payment system on e-commerce between the years 2008–2018 from various countries	before 2016
11	A survey of Mobile Ticketing Services in Urban Mobility Systems. [115]	No	No	Electronic ticket schemes and the most used technologies to provide the service.	before 2020
12	Key Growth Drivers and Barriers to Adoption of E-Payments: A Review. [116]	No	No	Exploratory research and secondary data.	2014–1015
13	A survey on Classification of Cyber-attacks on IoT and IIoT devices. [117]	No	No	The attacks that an attacker can launch against these devices and antiattacks methods.	before 2020
14	A survey on edge computing for wearable technology. [118]	No	No	Survey on existing works from four aspects, i.e., computation scheduling, information perception, energy-saving.	before 2022
15	A survey on smartphones security: software vulnerabilities, malware, and attacks. [24]	No (investigate about sensitive security issues affecting on smartphones)	No	Security solutions, threats, and vulnerabilities on smartphones security.	2011–2017
16	Systematic identification of threats in the cloud: A survey. [119]	No	No	Vulnerabilities to threats by relating vulnerabilities-to-attacks, and then relating attacks-to-threats.	2008–2016
17	A survey on smartphone authentication. [120]	No (comparison and discussion of different approaches based on authentication mechanisms)	No	A discussion on real-world experience of smartphone authentications	2005–2013
18	Adoption of Cashless Economy in the World: A Review. [121]	No (present an overview of types of cashless, challenges and opportunities of non-cash methods)	No	57 articles on cashless economy and methods used to make non-cash payments.	before 2022
19	A survey based on E-commerce website for visually impaired people. [122]	No	No	20 Research works on increased of Ecommerce business.	2016–2021

(*continued on next page*)

Table 11 (*continued*).

No.	Paper	Standard for analysis	MFA tools analysis	Relative works.	Period of time
20	Online Retailer Survey 2021: empirical findings on the e-commerce boom in Switzerland and Austria. [123]	No	No	The online survey with 365 online retailers.	2021
21	A review of e-payment system in e-commerce. [124]	No (re-analyze the findings from studies that have been statistically analyzed based on collected primary data)	No	Literature for e-payment systems on e-commerce	2002–2018
22	REVIEW OF TEXT BASED PASSWORD AND OTHER AUTHENTICATION METHODS FOR E-COMMERCE DATA PROTECTION. [125]	No (analyze pros and cons of authentication methods and type of attacks can occur)	No	Authentication methods, pros and cons, types of attacks, and the importance of an authentication system.	2016–2020
23	Online Banking User Authentication Methods: A Systematic Literature Review. [22]	No (Present an overview of existing authentication methods in online banking and the associated cyber threats)	No	Discuss the pros and cons and analyze the role of authentication methods (KBA, PBA, BBA) and identifies various cyber threats.	2013–2023
24	Examining User Verification Schemes, Safety and Secrecy Issues Affecting M-Banking: Systematic Literature Review. [126]	No	No	Assess 38 papers that examined m-banking authentication, protection, and secrecy challenges.	2013–2021
25	A Systematic Review of User Authentication Security in Electronic Payment System. [23]	No (analyze recently released user authentication documents)	No	Identify the user authentication techniques and threats to the electronic payment methods of 142 papers.	2013–2021
26	Our paper	Yes	Yes	Academic literature and utilized in industry tools	2017–2023

strong authentication in e-Banking, the impact of regulatory frameworks like PSD2, credit card fraud detection, e-payment protocols, electronic payment security, authentication methods, recent trends in user authentication, and strong electronic identification. By considering these works together, the survey paper gains a comprehensive understanding of multi-factor authentication practices, identifies trends and gaps, and offers opportunities for further research and improvement in authentication practices within payment systems.

Critical Analysis and Limitations: Related works provide valuable insights into multi-factor authentication, particularly in Payment Systems, but they exhibit limitations that our study systematically addresses. Studies like Konoth et al. [42] with SecurePay and Jamil et al. [48] with PetroBlock introduce practical innovations – mobile 2FA and blockchain-based payments – enhancing transaction security. However, these works often focus narrowly on specific solutions, lack comprehensive evaluation frameworks, and overlook vulnerabilities assessment, as seen in Tran [45]'s regional focus on MOMO in Vietnam or Bhargava et al. [46]'s UPI study absent NIST alignment. In contrast, our research evaluates 70 papers and 13 industry tools against NIST SP 800-63 standards, revealing gaps like 33% OTP reliance despite advanced alternatives in literature (e.g., 60% biometric adoption). While prior works may suffer from potential biases in literature selection or outdated contexts, our dual academic-industry lens offers a standardized, rigorous framework. This approach not only identifies trends but also bridges the theory-practice divide, providing greater depth, practicality, and relevance to guide future MFA enhancements.

7.2. Multi-factor authentication in edge and cloud communication

Key Findings and Contributions: The relative works on "Edge and Cloud Communication" provide valuable insights and contributions to their respective topics. These works offer thorough surveys, critical analyses, and classification frameworks that enhance our understanding of mobile ticketing services, e-payment adoption factors, cyber-attacks on IoT and IIoT devices, edge computing for wearable technology, smartphone security concerns, threat identification in the cloud, and smartphone authentication techniques. The key findings and contributions of these works contribute to the current knowledge, shape research directions, and provide practical insights to improve the respective domains.

Relation to the Survey Paper's Objective: Relative works share a common interest in technology and security but have distinct focuses and objectives. While our survey paper evaluates MFA practices in payment systems, assessing their alignment with NIST standards, the other works explore topics such as mobile ticketing services, e-payment adoption, cyber-attacks on IoT devices, edge computing for wearables, smartphone security, threats in the cloud, and smartphone authentication. Although the papers differ in their specific domains, they all contribute to a broader understanding of technological systems and their implications within different contexts. Relative works share a common interest in technology and security but have distinct focuses and objectives. While our survey paper evaluates MFA practices in payment systems, assessing their alignment with NIST standards, the other works explore topics such as mobile ticketing services, e-payment adoption, cyber-attacks on IoT devices, edge computing for wearables, smartphone security, threats in the cloud, and smartphone authentication. Although the papers differ in their specific domains, they all contribute to a broader understanding of technological systems and their implications within different contexts.

Critical Analysis and Limitations: Related works provide valuable insights, with strengths including thorough surveys and frameworks that enhance understanding of MFA in diverse contexts (e.g., IoT and smartphone security [117,120]). However, they also have certain limitations. These limitations include the absence of in-depth analyses of specific aspects, reliance on secondary data sources, lack of empirical evaluations, time frame constraints, and focus on specific methodologies or technologies. Future research should address these limitations by conducting more extensive analyses, incorporating primary data collection methods, performing empirical evaluations, considering the latest developments, and exploring emerging trends and challenges. Overcoming these limitations would enhance the relevance, robustness, and applicability of the findings in the field of edge and cloud communication.

7.3. Multi-factor authentication in E-commerce and online retail

Key Findings and Contributions: The relative works on "E-commerce and Online Retail" contribute to the understanding and improvement of various aspects of digital transactions and online retail experiences. These works explore the adoption of cashless economies worldwide, enhance the accessibility and usability of e-commerce websites for visually impaired individuals, provide empirical insights into the e-commerce boom in specific regions, review e-payment systems in e-commerce, and evaluate authentication methods for data protection in e-commerce. Together, these works offer valuable insights into the factors influencing digital payment adoption, inclusive online experiences, industry growth, payment systems, and authentication security. They contribute to shaping a more robust, accessible, and secure e-commerce ecosystem.

Relation to the Survey Paper's Objective: The relative works provide valuable insights into different aspects of digital transactions and online retail experiences. While our survey paper focuses specifically on evaluating multi-factor authentication practices in payment systems, the other works explore the adoption of cashless economies, enhance the accessibility of e-commerce websites for visually impaired individuals, examine empirical findings on the e-commerce boom in specific regions, and review e-payment systems and authentication methods for data protection in e-commerce. Although there may be some overlap in the context of digital transactions, the specific objectives and scopes of the papers differ, contributing to a comprehensive understanding of various aspects of e-commerce and online retail.

Critical Analysis and Limitations: Related works provide valuable insights into various aspects of the topic, with strengths such as actionable insights into payment adoption and accessibility improvements (e.g., cashless economy trends [121] and e-commerce for visually impaired [122]). However, they also have certain limitations that should be considered. These limitations include the reliance on generic review approaches, the need for additional primary research or case studies, potential challenges in implementing accessibility features for visually impaired users, limited generalizability of survey findings, the absence of comprehensive evaluations of specific e-payment systems or security mechanisms, and the lack of coverage of all authentication methods used in e-commerce. Addressing these limitations through further research and analysis would enhance the understanding and applicability of the findings in the field of e-commerce and online retail.

The survey of related works on designing authentication models for payment processes revealed common themes and trends as well as identified gaps and areas not covered. Common themes and trends observed include the lack of emphasis on industry-based tools to support developers and the absence of specific assessments for Identity Assurance Levels (IALs) and Authenticator Assurance Levels (AALs) outlined in SP 800-63 A and SP 800-63B. Gaps and areas not covered include the lack of focus on industry-based tools and the absence of assessments for IALs and AALs. These gaps hinder the practical implementation of authentication systems and compromise the security and reliability of e-payment systems.

In conclusion, our survey paper comprehensively reviewed and evaluated MFA practices in payment systems, with a specific focus on their alignment with NIST standards. We compared our work with related studies in the authentication and security domain, highlighting the specialization of our analysis in MFA within payment systems. Our paper made significant contributions by analyzing the current state of MFA, identifying gaps and trends, and evaluating adherence to industry guidelines. We also identified future research directions, including addressing gaps in NIST alignment, integrating emerging technologies, and considering the human factor in MFA adoption. Our findings provide valuable insights for researchers, practitioners, and policymakers to improve MFA practices and enhance the security and usability of payment systems.

8. Conclusion

Our comprehensive analysis of MFA in digital payment systems reveals both significant progress and persistent challenges in achieving robust security while maintaining usability. The evaluation of 70 academic papers and 13 industry tools against NIST standards has highlighted a substantial gap between theoretical capabilities and practical implementations, particularly in the adoption of advanced authentication methods. While academic research proposes sophisticated approaches, industry solutions predominantly rely on simpler mechanisms like OTP, potentially compromising optimal security for implementation practicality. The varying levels of regulatory compliance across different sectors underscore the need for more standardized approaches, especially in emerging domains like IoT and E-Services. The widespread adoption of biometric authentication represents a positive trend towards stronger security, though implementation challenges remain.

CRediT authorship contribution statement

Phat T. Tran-Truong: Writing – original draft, Software, Methodology, Conceptualization. **Minh Q. Pham:** Writing – original draft, Methodology. **Ha X. Son:** Writing – original draft, Software, Methodology, Conceptualization. **Dat L.T. Nguyen:** Writing – original draft, Methodology. **Minh B. Nguyen:** Writing – original draft, Methodology. **Khiem L. Tran:** Writing – original draft, Methodology. **Loc C.P. Van:** Writing – original draft, Methodology. **Kiet T. Le:** Writing – original draft, Methodology. **Khanh H. Vo:** Supervision, Methodology. **Ngan N.T. Kim:** Writing – review & editing, Writing – original draft, Methodology. **Triet M. Nguyen:** Writing – review & editing, Methodology. **Anh T. Nguyen:** Writing – review & editing, Methodology.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We acknowledge the support of time and facilities from Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for this study.

Availability of data and material

The authors declare that all the data used in experiments in this paper are freely available via the mentioned sources in the corresponding sections.

Data availability

No data was used for the research described in the article.

References

[1] A.M. Balloon, From wax seals to hypertext: electronic signatures, contract formation, and a new model for consumer protection in internet transactions, Emory LJ 50 (2001) 905.

[2] J.-J. Kim, S.-P. Hong, A method of risk assessment for multi-factor authentication, J. Inf. Process. Syst. 7 (1) (2011) 187–198.

[3] R.K. Konoth, V. van der Veen, H. Bos, How anywhere computing just killed your phone-based two-factor authentication, in: Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20, Springer, 2017, pp. 405–421.

[4] J. Bonneau, C. Herley, P.C. Van Oorschot, F. Stajano, Passwords and the evolution of imperfect authentication, Commun. ACM 58 (7) (2015) 78–87.

[5] D. Dasgupta, A. Roy, A. Nag, Toward the design of adaptive selection strategies for multi-factor authentication, Comput. Secur. 63 (2016) 85–116.

[6] R. Banyal, V. Jain, P. Jain, Dynamic trust based access control framework for securing multi-cloud environment, in: Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 2014, pp. 1–8.

[7] A. Bhargav-Spantzel, A. Squicciarini, E. Bertino, Privacy preserving multi-factor authentication with biometrics, in: Proceedings of the Second ACM Workshop on Digital Identity Management, 2006, pp. 63–72.

[8] E.M. Scheidt, E. Domangue, Multiple Factor-Based User Identification and Authentication, Google Patents, 2006, US Patent 7, 131, 009.

[9] D. Wang, W. Li, P. Wang, Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inform. 14 (9) (2018) 4081–4092.

[10] D. Wang, P. Wang, Two birds with one stone: Two-factor authentication with security beyond conventional bound, IEEE Trans. Dependable Secur. Comput. 15 (4) (2016) 708–722.

[11] D. Wang, D. He, P. Wang, C.-H. Chu, Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment, IEEE Trans. Dependable Secur. Comput. 12 (4) (2014) 428–442.

[12] A.M. Aburbeian, M. Fernández-Veiga, Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning, AI 5 (1) (2024) 177–194.

[13] A.K. Wee, E.G. Chekole, J. Zhou, Excavating vulnerabilities lurking in multi-factor authentication protocols: A systematic security analysis, 2024, arXiv preprint arXiv:2407.20459.

[14] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, Y. Koucheryavy, Multi-factor authentication: A survey, Cryptography 2 (1) (2018) 1.

[15] A.M. Mostafa, M. Ezz, M.K. Elbashir, M. Alruily, E. Hamouda, M. Alsarhani, W. Said, Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication, Appl. Sci. 13 (19) (2023) 10871.

[16] G. Ali, M. Ally Dida, A. Elikana Sam, Two-factor authentication scheme for mobile money: A review of threat models and countermeasures, Futur. Internet 12 (10) (2020) 160.

[17] F. Sinigaglia, R. Carbone, G. Costa, N. Zannone, A survey on multi-factor authentication for online banking in the wild, Comput. Secur. 95 (2020) 101745.

[18] P.A. Grassi, N.B. Lefkovitz, J.M. Danker, Y.-Y. Choong, K.K. Greene, M.F. Theofanos, Digital Identity Guidelines: Enrollment and Identity Proofing, NIST Special Publication 800-63A, National Institute of Standards and Technology, 2017, URL: https://doi.org/10.6028/NIST.SP.800-63a.

[19] P.A. Grassi, M.E. Garcia, J.L. Fenton, Digital Identity Guidelines: Authentication and Lifecycle Management, NIST Special Publication 800-63B, National Institute of Standards and Technology, 2017, URL: https://doi.org/10.6028/NIST.SP.800-63b.

[20] P.A. Grassi, M.E. Garcia, J.L. Fenton, Digital Identity Guidelines: Federation and Assertions, NIST SpecialPublication 800-63C, National Institute of Standards and Technology, 2017, URL: https://doi.org/10.6028/NIST.SP.800-63c.

[21] M.H. Barkadehi, M. Nilashi, O. Ibrahim, A.Z. Fardi, S. Samad, Authentication systems: A literature review and classification, Telemat. Inform. 35 (5) (2018) 1491–1511.

[22] N.A. Karim, O.A. Khashan, H. Kanaker, W.K. Abdulraheem, M. Alshinwan, A. Albanna, Online banking user authentication methods: A systematic literature review, IEEE Access (2023).

[23] M.A. Hassan, Z. Shukur, A systematic review of user authentication security in electronic payment system, in: Proceedings of International Conference on Data Science and Applications: ICDSA 2022, vol. 1, Springer, 2023, pp. 121–138.

[24] M.T. Ahvanooey, Q. Li, M. Rabbani, A.R. Rajput, A survey on smartphones security: software vulnerabilities, malware, and attacks, 2020, arXiv preprint arXiv:2001.09406.

[25] L.J. Chetalam, Enhancing Security of MPesa Transactions by Use of Voice Biometrics (Ph.D. thesis), United States International University-Africa, 2018.

[26] G.J. Harkácsi, L.P. Szegfű, The role of the compliance function in the financial sector in the age of digitalisation, artificial intelligence and robotisation, Financ. Econ. Rev. 20 (1) (2021) 152–170.

[27] B. Mega, Framework for Improved Security on Usage of Mobile Money Application Based on Iris Biometric Authentication Method in Tanzania (Ph.D. thesis), The University of Dodoma, 2020.

[28] S. Midha, S. Verma, M. Mittal, N. Jhanjhi, M. Masud, M.A. AlZain, et al., A secure multi-factor authentication protocol for healthcare services using cloud-based SDN, Comput. Mater. Contin. 74 (2) (2023).

[29] T. Suleski, M. Ahmed, W. Yang, E. Wang, A review of multi-factor authentication in the Internet of Healthcare Things, Digit. Heal. 9 (2023) 20552076231177144.

[30] J. Mehtälä, et al., User-centred design of M-government services in namibia: Prototyping mobile identification, 2019.

[31] T. Zhu, Z. Qu, H. Xu, J. Zhang, Z. Shao, Y. Chen, S. Prabhakar, J. Yang, RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild, IEEE Trans. Mob. Comput. 19 (2) (2019) 466–483.

[32] W. Yu, Q. Yin, H. Yin, W. Xiao, T. Chang, L. He, L. Ni, Q. Ji, A systematic review on password guessing tasks, Entropy 25 (9) (2023) 1303.

[33] W. Fernando, D. Dissanayake, S. Dushmantha, D. Liyanage, C. Karunatilake, Challenges and opportunities in password management: a review of current solutions, Sri Lanka J. Soc. Sci. Humanit. 3 (2) (2023).

[34] National Cyber Security Centre, Problems with forcing regular password expiry, 2016, URL: https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry. (Accessed 22 February 2025).

[35] National Cyber Security Centre, Password administration for system owners, 2018, URL: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach. (Accessed 22 February 2025).

[36] D. Wang, Q. Gu, X. Huang, P. Wang, Understanding human-chosen pins: characteristics, distribution and security, in: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017, pp. 372–385.

[37] K. Sadeghi, A. Banerjee, J. Sohankar, S.K. Gupta, Geometrical analysis of machine learning security in biometric authentication systems, in: 2017 16th IEEE International Conference on Machine Learning and Applications, ICMLA, IEEE, 2017, pp. 309–314.

[38] H. Zhu, M. Xiao, D. Sherman, M. Li, SoundLock: A novel user authentication scheme for VR devices using auditory-pupillary response, in: NDSS, 2023.

[39] Y.C. Feng, P.C. Yuen, Binary discriminant analysis for generating binary face template, IEEE Trans. Inf. Forensics Secur. 7 (2) (2011) 613–624.

[40] D. Wang, H. Cheng, P. Wang, X. Huang, G. Jian, Zipf's law in passwords, IEEE Trans. Inf. Forensics Secur. 12 (11) (2017) 2776–2791.

[41] K. Inthavisas, D. Lopresti, Secure speech biometric templates for user authentication, IET Biom. 1 (1) (2012) 46–54.

[42] R.K. Konoth, B. Fischer, W. Fokkink, E. Athanasopoulos, K. Razavi, H. Bos, Securepay: Strengthening two-factor authentication for arbitrary transactions, in: 2020 IEEE European Symposium on Security and Privacy, EuroS&P, IEEE, 2020, pp. 569–586.

[43] A.-a.M. Ibrahim, M.H. Hashim, Secure Model for M-payment Transaction Using Two Factor Authentication and Tokenization (Master's thesis), University of Science and Technology, 2018.

[44] P.T. Wolters, B.P. Jacobs, The security of access to accounts under the PSD2, Comput. Law Secur. Rev. 35 (1) (2019) 29–41.

[45] T.M.A. Tran, Mobile payment security: A case study of digital wallet MOMO, 2020.

[46] A. Bhargava, M. Ubaid, Y. Khan, P.C. Gupta, Expansion of unified payment interface, Ann. Rom. Soc. Cell Biol. 25 (6) (2021) 12491–12499.

[47] A. Bartoszczyk-Brzoskowski, The purpose and impact of the second payment service directive on cyber security of, 2019.

[48] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, M.A. Ferrag, PetroBlock: A blockchain-based payment mechanism for fueling smart vehicles, Appl. Sci. 11 (7) (2021) 3055.

[49] A. Omotubora, S. Basu, Regulation for e-payment systems: Analytical approaches beyond private ordering, J. Afr. Law 62 (2) (2018) 281–313.

[50] S. Abraham, Unified payment interface: Towards greater cyber sovereignty, ORF Issue Brief (380) (2020).

[51] L.F. Petry, J. Moormann, Mobile payment in the connected car: Developing services based on process thinking, Bus. Syst. Res.: Int. J. Soc. Adv. Innov. Res. Econ. 11 (3) (2020) 63–77.

[52] A. Antonio Martinez Villegas, P. Ashraf Zarif, J. Shokry, Investigating Factors Affecting Small Business' Owner's Decisions to Use the Electronic Payment Services (Application on the National Awareness Campaign of the Benefits of Electronic Payment Initiated by The Central Bank of Egypt), MSA UNIVERSITY, 2021.

[53] G. Ramesh, A. Jangid, L. Sivamalai, A.B. Rebelly, NPCI: chartering a payment freeway, IIM Bangalore Res. Pap. (626) (2020).

[54] R. D'souza, Cashless India: Getting Incentives Right, ORF Occasional Paper, Mumbai, Observer Research Foundation, 2018.

[55] J. Geewax, Design principles for third-party initiation in real-time payment systems, 2021.

[56] D. Basin, R. Sasse, J.L. Toro Pozo, Card brand mixup attack: Bypassing the PIN in non-visa cards by using them for visa transactions, in: Proceedings of the 30th USENIX Security Symposium, USENIX Security 21, USENIX Association, 2021, pp. 179–194.

[57] R. Kumar, S. Kishore, H. Lu, A. Prakash, Security analysis of unified payments interface and payment apps in India, in: Proceedings of the Usenix Security Symposium 2020, 2020.

[58] F. Tommasi, C. Catalano, M. Fornaro, I. Taurino, Mobile session fixation attack in micropayment systems, IEEE Access 7 (2019) 41576–41583.

[59] A. Ciccarello, Design of a Mobile Payment Application and Performance Comparison with the Lightning Network (Ph.D. thesis), Politecnico di Torino, 2021.

[60] J. Sturgess, S. Eberz, I. Sluganovic, I. Martinovic, WatchAuth: User authentication and intent recognition in mobile payments using a smartwatch, in: 2022 IEEE 7th European Symposium on Security and Privacy, EuroS&P, IEEE, 2022, pp. 377–391.

[61] G. Ali, M.A. Dida, A. Elikana Sam, A secure and efficient multi-factor authentication algorithm for mobile money applications, Futur. Internet 13 (12) (2021) 299.

[62] O.R. Vincent, T. Okediran, A. Abayomi-Alli, O.J. Adeniran, An identity-based elliptic curve cryptography for mobile payment security, SN Comput. Sci. 1 (2020) 1–12.

[63] M.F. Oladapo, Development of a Multi-level Security Model for Mobile Payment System (Ph.D. thesis), Federal University of Technology, Akure, 2021.

[64] M.A. Hassan, Z. Shukur, Device identity-based user authentication on electronic payment system for secure E-wallet apps, Electronics 11 (1) (2022) 4.

[65] M.P. Centeno, Applying Machine Learning to Enhance Payments Systems Security (Ph.D. thesis), Newcastle University, 2020.

[66] M. Massoth, S.L. Ahier, Fast Electronic Identification at Trust Substantial Level using the Personal Online Bank Account, CYBER, 2020.

[67] J. N'Gumah, Evaluating security in cryptocurrency wallets, 2021.

[68] N.T.N. Thuy, T.T. Kiet, P.H. Cuong, V.D. Quy, N.C. Trung, Ho chi minh city university of technology and education students' satisfaction with e-wallet service, Linguist. Cult. Rev. 6 (S5) (2022) 15–31.

[69] P. Shipalana, Digitising Financial Services: a Tool for Financial Inclusion in South Africa? South African Institute of International Affairs (SAIIA), 2019.

[70] O.E. Morakinyo, A Secure Bank Login System Using a Multi-Factor Authentication, Mountain Top University, 2021.

[71] A. Avdić, Use of biometrics in mobile banking security: case study of Croatian banks, IJCSNS Int. J. Comput. Sci. Netw. Secur. 19 (2019) 83–89.

[72] S. Iqbal, M. Irfan, K. Ahsan, M.A. Hussain, M. Awais, M. Shiraz, M. Hamdi, A. Alghamdi, A novel mobile wallet model for elderly using fingerprint as authentication factor, IEEE Access 8 (2020) 177405–177423.

[73] S. Kim, H.-J. Mun, S. Hong, Multi-factor authentication with randomly selected authentication methods with DID on a random terminal, Appl. Sci. 12 (5) (2022) 2301.

[74] D. Jayasinghe, S. Cobourne, K. Markantonakis, R.N. Akram, K. Mayes, Philanthropy on the blockchain, in: Information Security Theory and Practice: 11th IFIP WG 11.2 International Conference, WISTP 2017, Heraklion, Crete, Greece, September 28–29, 2017, Proceedings 11, Springer, 2018, pp. 25–38.

[75] M. Guerar, M. Migliardi, F. Palmieri, L. Verderame, A. Merlo, Securing PIN-based authentication in smartwatches with just two gestures, Concurr. Comput. Pr. Exp. 32 (18) (2020) e5549.

[76] A. Dey, S. Jain, Automated POS system based on face recognition and password, 2019.

[77] B.M. Nguyen, T.-C. Dao, B.-L. Do, Towards a blockchain-based certificate authentication system in Vietnam, PeerJ Comput. Sci. 6 (2020) e266.

[78] K. Okokpujie, E. Noma-Osaghae, O. Okesola, O. Omoruyi, C. Okereke, S. John, I.P. Okokpujie, Fingerprint biometric authentication based point of sale terminal, in: Information Science and Applications 2018: ICISA 2018, Springer, 2019, pp. 229–237.

[79] İ. Türk, NFC Feature Box: an Open, Nfc Enabler Independent Mobile Payment and Identification Method, Middle East Technical University, 2019.

[80] K.S. Kumar, P. Govardhan Reddy, A. Sivakumar, et al., A two factor image based authentication system, in: Proceedings of the International Conference on Innovative Computing & Communication, ICICC, 2021.

[81] S. Zheng, R.W.O. Rahmat, F. Khalid, N.A. Nasharuddin, Learning scale-variant features for robust iris authentication with deep learning based ensemble framework, 2019, arXiv preprint arXiv:1912.00756.

[82] P. Ranabhat, Secure Design and Development of IoT Enabled Charging Infrastructure for Electric Vehicle: Using CCS Standards for DC Fast Charging, Metropolia Ammattikorkeakoulu, 2018.

[83] M. Santoro, L. Vaccari, D. Mavridis, R. Smith, M. Posada, D. Gattwinkel, et al., Web Application Programming Interfaces (APIs): General-Purpose Standards, Terms and European Commission Initiatives, Technical Report, European Commission, Louxembourg, 2019.

[84] M.H. Sadi, E. Yu, RAPID: a knowledge-based assistant for designing web APIs, Requir. Eng. 26 (2021) 185–236.

[85] O.P. Onyinyechi, O.A. Ifeanyi, E.N. Nnabuchi, I.P. Nwakaego, Enhanced business marketing for small scale enterprises via the quick response code technology, Frontiers 1 (1) (2021) 7–13.

[86] Z. Han, L. Yang, S. Wang, S. Mu, Q. Liu, Efficient multifactor two-server authenticated scheme under mobile cloud computing, Wirel. Commun. Mob. Comput. 2018 (2018).

[87] H.U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, F. Ali, Role of authentication factors in Fin-tech mobile transaction security, J. Big Data 10 (1) (2023) 138.

[88] U. Kishnani, I. Cardenas, J. Castillo, R. Conry, L. Rodwin, R. Ruiz, M. Walther, S. Das, Towards perceived security, perceived privacy, and the universal design of E-payment applications, 2024, arXiv preprint arXiv:2407.05446.

[89] B. Venkatraman, H. Jain, An analytical study on the security features of digital payment systems with special reference to blockchain technology, 2023.

[90] D. Mondego, E. Gide, Cloud-based payment systems in Australia: How security affects consumer satisfaction, Eng. Proc. 55 (1) (2024) 89.

[91] N. Hanbali, A. El-Yahyaoui, O. Ali, E. Chaima, Exploring Cybersecurity in Apple Pay: A Study of Attacks and Vulnerabilities, Technical Report, EasyChair, 2024.

[92] A.H.Y. Mohammed, R.A. Dziyauddin, L.A. Latiff, Current multi-factor of authentication: Approaches, requirements, attacks and challenges, Int. J. Adv. Comput. Sci. Appl. 14 (1) (2023).

[93] H. Purohit, M. Dadhich, P.K. Ajmera, Analytical study on users' awareness and acceptability towards adoption of multimodal biometrics (MMB) mechanism in online transactions: a two-stage SEM-ANN approach, Multimedia Tools Appl. 82 (9) (2023) 14239–14263.

[94] J. Thomas, S. Akhtar, Cyber forensics in the age of AI: Investigating cyber crimes with advanced multi-factor authentication and adaptive threat mitigation, 2024.

[95] A. Alabdulatif, R. Samarasinghe, N.N. Thilakarathne, A novel robust geolocation-based multi-factor authentication method for securing ATM payment transactions, Appl. Sci. 13 (19) (2023) 10743.

[96] A. Stęchły, A. Szpunar, Analysis of potential risks of SMS-based authentication, Adv. Web Dev. J. 1 (1) (2023).

[97] R.H. Anwar, S.R. Hussain, M.T. Raza, In wallet we trust: Bypassing the digital wallets payment security for free shopping, in: 33rd USENIX Security Symposium, USENIX Security 24, 2024, pp. 541–558.

[98] T. Wang, T. Liu, H. Zhu, Cybersecurity challenges in mobile payment systems: A case study of alipay in Chinese cities, Innov. Sci. Technol. 3 (1) (2024) 51–58.

[99] C. Saxena, A secure and structured environment for reliable and trustworthy contactless digital payments, 2024, Available at SSRN 4833175.

[100] C. Igwesi, Enhancing Authentication and Fraud Detection in Financial Technology And Wireless Payments, OSF, 2023.

[101] O.P. Olaiya, T.O. Adesoga, A.A. Adebayo, F.M. Sotomi, O.A. Adigun, P.M. Ezeliora, Encryption techniques for financial data security in fintech applications, Int. J. Sci. Res. Arch. 12 (1) (2024) 2942–2949.

[102] M.R. Ramakrishnan, S. Vanisri, D. Yuvalakshmi, Unified payment interface seamless transaction using rnn model, 2024.

[103] H. Alamleh, A.A.S. AlQahtani, B. Al Smadi, Secure mobile payment architecture enabling multi-factor authentication, in: 2023 Systems and Information Engineering Design Symposium, SIEDS, IEEE, 2023, pp. 19–24.

[104] S. Pawar, A. Dhutonde, An in-depth analysis of & performance comparison security models used in banking scenario, 2023.

[105] E.E. Archibong, B.U.-A. Stephen, P. Asuquo, Analysis of cybersecurity vulnerabilities in mobile payment applications, Arch. Adv. Eng. Sci. (2024) 1–12.

[106] X. Chen, Network security risks caused by third-party payment: a case study of apple pay, 2024.

[107] F. Sinigaglia, R. Carbone, G. Costa, et al., Strong authentication for e-banking: A survey on European regulations and implementations, in: SECRYPT, 2017, pp. 480–485.

[108] L. Kaipainen, Effects of PSD2 on security architecture of mobile banking: a review of literature, 2017.

[109] N. Yousefi, M. Alaghband, I. Garibay, A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection, 2019, arXiv preprint arXiv:1912.02629.

[110] B. Ratnakanth, P. Avadhani, A review of secure authentication based e-payment protocol, Int. J. Adv. Comput. Sci. Appl. 8 (3) (2017).

[111] M.A. Hassan, Z. Shukur, M.K. Hasan, A.S. Al-Khaleefa, A review on electronic payments security, Symmetry 12 (8) (2020) 1344.

[112] E. Patmanidou, I. Tsilikas, Authentication methods review: How to enhance identity trust in authentication, 2018.

[113] S.W. Shah, S.S. Kanhere, Recent trends in user authentication–a survey, IEEE Access 7 (2019) 112505–112519.

[114] O. Agbede, et al., Strong electronic identification: Survey & scenario planning, 2018.

[115] M.C. Ferreira, T.G. Dias, J.F. e Cunha, A survey of mobile ticketing services in urban mobility systems, Int. J. Smart Sens. Technol. Applications (IJSSTA) 1 (2) (2020) 17–35.
[116] A. Lohar, M.Y.Y. Gajare, A. Kumar, Key growth drivers and barriers to adoption of E-payments: A review, Natl. J. Res. Mark. Financ. HRM (2017) 1.
[117] Y. Shah, S. Sengupta, A survey on classification of cyber-attacks on IoT and IIoT devices, in: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, IEEE, 2020, pp. 406–413.
[118] X. Jin, L. Li, F. Dang, X. Chen, Y. Liu, A survey on edge computing for wearable technology, Digit. Signal Process. 125 (2022) 103146.
[119] J.B. Hong, A. Nhlabatsi, D.S. Kim, A. Hussein, N. Fetais, K.M. Khan, Systematic identification of threats in the cloud: A survey, Comput. Netw. 150 (2019) 46–69.
[120] S. Vongsingthong, S. Boonkrong, A survey on smartphone authentication, Walailak J. Sci. Technol. (WJST) 12 (1) (2015) 1–19.
[121] A. Kirobo, J. Lissah, M.M. Govella, Adoption of cashless economy in the world: A review.
[122] V.M. Rajaselvi, A survey based on E-commerce website for visual impaired people, 2022.
[123] D. Zumstein, C. Oswald, C. Brauer, Online Retailer Survey 2021: Empirical Findings on the E-Commerce Boom in Switzerland and Austria, ZHAW Zürcher Hochschule für Angewandte Wissenschaften, 2021.
[124] S. Fatonah, A. Yulandari, F.W. Wibowo, A review of e-payment system in e-commerce, J. Phys. Conf. Ser. 1140 (1) (2018) 012033.
[125] H. Malau, V. Yovira, Review of text based password and other authentication methods for e-commerce data protection, J. Theor. Appl. Inf. Technol. 100 (6) (2022).
[126] N. Cavus, Y.B. Mohammed, M. Bulama, M.L. Isah, Examining user verification schemes, safety and secrecy issues affecting m-banking: Systematic literature review, SAGE Open 13 (1) (2023) 21582440231152379.

Msc. Phat Tuan Tran-Truong is currently a lecturer/researcher at the Department of Software Engineering, Faculty of Computer Science & Engineering, Ho Chi Minh City University of Technology, Vietnam National University (HCMUT, VNU-HCM). He completed both a research-based Master's degree and a Bachelor's degree (Honors) in Computer Science from HCMUT, VNU-HCM in 2023 and 2020 respectively. His research interests delve into the areas of Trustworthy AI, Machine Learning, Security & Privacy, and Blockchain.

Mr. Pham Quang Minh is a student at Ho Chi Minh City University of Technology, Vietnam National University (HCMUT, VNU-HCM). His research interests are Computer Science, Computer Security & Privacy. Email: minh.pham2212075@hcmut.edu.vn

Dr. Son Xuan Ha is lecturer in Blockchain enabled business at RMIT University Vietnam, Saigon South Campus. Before joining RMIT, he was a Marie Curie Fellow in the Real-time Analytics for Internet of Sports (RAIS) project. His research is interested in the Cryptography, Security, Privacy, Access Control, and Blockchain.

Mr. Nguyen Le Tan Dat is a student at Can Tho University of Technology. His research interests are Computer Science, Computer Security & Privacy. Email: nltdat2101364@student.ctuet.edu.vn

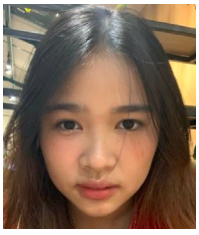
Mr. Nguyen Binh Minh is a student at Can Tho University of Technology. His research interests are Computer Science, Computer Security & Privacy. Email: nbminh2101381@student.ctuet.edu.vn

Msc. Tran Luong Khiem received his Master's in Security and Cloud Computing from Aalto University, Finland. Currently, he is a Backend Engineer, Founder of the company Imutably Oy, Finland. Email: khiemfle@imutably.com

Mr. Loc Van Cao Phu is a student at FPT University. His research interests are Computer Science, Information Systems and Blockchain. Email: locvcpce160307@fpt.edu.vn

Mr. Kiet Le Tuan is a student at FPT University. His research interests are Computer Science, Information Systems and Blockchain. Email: KietLTCE160373@fpt.edu.vn

Msc. Vo Hong Khanh received his Master's in Information System from Can Tho University (CTU), Vietnam, in 2017. Currently, he is a lecturer of Software Engineering of FPT University-campus Can Tho (FPTU). His research interests are Computer Science, Information Systems, Algorithms, Computer Vision, AI, Deep Learning and Blockchain.



Ms. Ngan Nguyen Thi Kim is a student at FPT Polytechnic. Her research interests are Computer Science, Information Systems and Blockchain.

Msc. Minh Triet Nguyen received his Master's in Information System from Can Tho University (CTU), Vietnam, in 2017. Currently, he is a lecturer of Information Assurance of FPT University - campus Can Tho (FPTU). His research interests are Computer Networking, Cyber Security and Computer Vision.

Msc. Anh Nguyen The is a student at FPT University. His research interests are Computer Science, Information Systems and Blockchain.