Babylonian Journal of Networking
Vol.2025, **pp**. 185–196
DOI: https://doi.org/10.58496/BJN/2025/017; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Optimized Solutions for Robust and Efficient Two-Factor Authentication in Networking Environments

Hussein Alkattan [1,2,*], Raad S. Alhumaima [3], Amr Badr [4], Peter Mwangi [5]

[1] *Department of System Programming, South Ural State University, Chelyabinsk, Russia.*

[2] *Directorate of Environment in Najaf, Ministry of Environment, Najaf, Iraq.*

[3] *Brunel University, Uxbridge UB8 3PH, UK.*

[4] *School of Science and Technology -University of new England, Armidale, Australia.*

[5] *Department of computer science, Murang'a University of Technology, Kenya.*

ARTICLE INFO

Article History

Received 5 Sep 2025
Revised 15 Oct 2025
Accepted 11 Nov 2025
Published 13 Dec 2025

Keywords
Two-Factor Authentication (2FA), Network Security, Elliptic Curve Cryptography (ECC), Biometric Authentication, Digital Certificates, Behavioral Biometrics, Phishing, SIM-Swapping, Multi-Network Environments.

ABSTRACT

With the rise of escalating cyber threats to the present-day networking environment, the traditional two-factor authentication (2FA) mechanisms remain ineffective in mitigating the sophisticated attack vectors like phishing, SIM-swapping and social engineering. These loops holes, specifically in SMS- and email-based 2FA, are opening users and network infrastructure up to substantial danger. This paper presents optimized and robust enhancements to 2FA technology, and points out cryptographic technologies like ECC, the addition of X.509 digital certificates, and biometric and behavioral authentication solutions. Then, the performance of these distributed trust models is compared, in terms of security efficiency, usability, and deploy ability, with a complete comparative study of these models in dynamic networking. The paper also includes real-world examples of implementing such multi-layered 2FA schemes being tensioned between a strong security protection and what is deemed to be user acceptable. The results showcase best practices and challenges in building secure and efficient as well as future-proof authentication systems that match the requirements of complex network environments.

1. INTRODUCTION

a cyber priority. Static passwords, previously the primary method of authentication, are considered inadequate because they are prone to brute-force attacks, password reuse, and bad user habits. In reaction to this threat, Two-Factor Authentication (2FA) has become a popular security practice, which adds an extra layer of identity verification by asking the user for two different and independent pieces of information: something they know (like a password) and something they have or are (like a code or biometric characteristic) [1-3]. However, traditional 2FA solutions - especially those which are SMS or email-based, such as One-Time Passwords - are more and more under attack from the most advanced vectorial attack like phishing, SIM-swapping, social engineering. These techniques take advantages of those insecure communication channels to intercept authentication tokens or manipulate users into leaking secret credentials. Even brute-force type of attacks, which many systems commonly use, are effective if password complexity and user behavior are not taken into account [4-5]. The deficiencies of these old-fashioned methods challenge those solutions should adapt to the need, automatically generating matching authentication specifications on the fly to critically support scalable and robust authentication over today's network infrastructure [6].

*Corresponding author. Email: alkattan.hussein92@gmail.com

As threats change, so too the means to defend against them must change. Next-generation 2FA is starting to take advantage of innovations in cryptography, biometrics, and mobile device-level authentication to improve the usability and security of access control systems. Key advancements include:

a) Elliptic Curve Cryptography (ECC) A light weight yet very strong cryptographic method able to deployed in both resource-limited environment like IoT and resourceful environment like mobile device [7].
b) Digital Certificates: They offer verifiable identity assurance, rendering it much more complex to fake valid users [8].
c) Biometric Authentication: Fingerprint or facial recognition is ease of an individual's unique physiological characteristic which is unlikely to be imitated and can achieve high level assurance from the user with a low effort [9].

With the cryptographic security and the unique-ness of biometrics combined, today's 2FA systems make it very difficult for an unauthorized user to cross the line—even if they have access to your password. Additionally, these methods mitigate the dependencies on fragile mediums such as SMS and email, providing a frictionless user experience that's in line with the usability expectations of the modern digital experience. To make two-factor authentication more robust and efficient in the networking environment is studied in this paper. We emphasis on the trade-off between security, performance, and user convenience for authentication systems that are secure against current threats. This framework provides best practices and design guidelines for the development of modern 2FA systems able to satisfy the modern cybersecurity's stringent requirements.

2. RELATED WORKS

Two-Factor Authentication (2FA) is still an important and active research area in cybersecurity as it plays a fundamental role in protecting user credentials, digital resources and network access. Many academic and commercially motivated studies have studied traditional and modern 2FA solutions considering dimensions such as security strength, usability, resistance to adoption barriers, and resilience to new threats. Sponsored A report from the SANS Institute delves into password protection and 2FA adoption by organizations. There is a notable trend to begin and accelerate 2FA adoption to deal with the weaknesses of passwords. Nevertheless, the study identified major challenges including user resistance and usability which are still prevalent barriers to its use [10]. carried out a user-centered investigation on five major 2FA solutions — SMS, email, voice calls, hardware tokens, and mobile application-based. Hardware tokens and authenticator apps offered better security, but participants still preferred the SMS and email approaches, pointing to the trade-off between user experience and security assurance that persists today [11]. In a pioneering study on Multi-Factor Authentication (MFA) in Cyber-Physical Systems, the necessity to find the right trade-off among security, privacy, usability, scalability, and interoperability was highlighted. While MFA can greatly improve system security, they pointed out that the practical value heavily relies on how easy it can be integrated and how user-friendly it is to people [12]. They also provided a literature review about authentication in Extended Reality (XR) environments. The research noticed a focus on context-aware and behavior-based 2FA mechanisms, including the use of biometrics or behavioral analytics. However, mainly considered applications and opportunities are within XR scopes, counterpart findings highlight the importance of user-friendly and non-intrusive authentication mechanisms on upcoming digital platforms [13]. One comparative research paper was considered which identified a range of 2FA mechanisms and noted the importance of multilayered mechanisms to build user's trust and prevent the over-reliance on the use of single factor 2FA. Their research promoted integrating cryptographic mechanisms with multi-factor authentication to combat the growing threats in cyber security [14]. Also studied the development of authentication systems from a technical and human point of view." They proposed to use smart sensors and the behavior-based authentication system in sensitive environments in order to establish the continuous access control, but did not target cryptographic lightweight concepts such as ECC [15]. Extended their work by considering the transition from single-factor to multi-factor schemes in different systems. They emphasized the need for multiple layers of security as a means to mitigate the weakness, but failed to provide a comprehensive overview of today's 2FA practices [16]. One report put numbers on password management practices and illustrated how bad habits still create big risks. The piece recommended a need for much more solid based on OTP. requirements for mash, 2FA with biometric authentication for a genuine accessibility model [14]. The report was an echo of these feelings, warning that as a matter-of-fact conventional of passwords have increasingly exposed as a fundamental breaking point in digital security. The article promoted multi-factor identification based on biometrics, security tokens, and other methods as more secure and scalable. It further suggested that future studies should investigate to the smooth and efficient incorporation of both these mechanisms into current systems [18]. Finally, an article described the advantages of login with authenticator apps (like Time-Based One-Time Passwords (TOTP)) over SMS-based methods. These applications function without the need for data connections and

are facilitated to be more secure and less vulnerable to snooping, thus providing more freedom to users out of the mobile space [19]. Table I provides an overview of the collected studies including the methods used, main findings, limitations, and possible further investigations. In sum, the literature indicates a consensus on the appreciation for more secure, efficient and user-centered 2FA solutions based on contemporary cryptography and biometric methods.

TABLE I: SUMMARY OF KEY STUDIES ON TWO-FACTOR AUTHENTICATION (2FA) METHODS

Methodologies Explored	Key Findings	Limitations	Proposed Improvements/Research Gaps
Password Management, 2FA Methods	Shift towards 2FA adoption; user resistance remains a challenge	Did not analyze advanced 2FA solutions (e.g., biometrics, certificates)	Examine user education approaches for better adoption of secure 2FA methods
SMS, Email, Phone Call, Hardware, App-based 2FA	Hardware and apps offer higher security; users prefer SMS/email for convenience	Limited to comparing five 2FA methods	Study additional 2FA methods like biometrics and digital certificates
MFA in Cyber-Physical Systems	Emphasized balance of security, privacy, usability	Focused primarily on cyber-physical systems	Apply findings to general networked environments; examine biometric impacts
Authentication in Extended Reality (XR)	Advanced methods, especially behavioral biometrics, needed for XR	Narrow application to XR environments	Investigate generalizability of behavioral biometrics beyond XR
Trends in 2FA	Multi-layered 2FA improves security and user trust	Limited analysis of specific 2FA methods	Explore the impact of specific 2FA combinations in varying threat landscapes
Evolution of MFA	Advanced sensors enable secure, convenient authentication	No focus on emerging cryptographic methods like ECC	Investigate ECC-based authentication and other lightweight cryptography
User Authentication Factors	Layered authentication reduces vulnerabilities	Focused on user authentication without extensive 2FA analysis	Extend findings to include comparative analysis of multi-layer 2FA methods
Password & Authentication Security	Highlighted risks in password practices; rising 2FA adoption to mitigate risks	Did not address advanced 2FA methods beyond traditional OTP	Explore biometric and certificate-based 2FA integration for higher security
Digital Authentication	Recommended MFA, biometrics, tokens over passwords	Primarily recommendations, limited empirical data	Perform empirical studies on adoption rates and practical implementation
Authenticator Apps	Authenticator apps offer secure alternative to SMS-based 2FA	Basic overview, no in-depth analysis	Investigate scalability of app-based 2FA across various user demographics

3. TRADITIONAL TWO-FACTOR AUTHENTICATION AND LIMITATIONS

Conventional mechanisms for Two-Factor Authentication (2FA)—such as those that are based on SMS, email, and time-based one-time password (TOTP) produced by mobile applications—have been well-establish because they are easy to deploy and convenient for the user. However, in spite of their wide adoption, these approaches are plagued by several severe security restrictions, which make them increasingly inadequate to address modern cyber-attacks.

3.1 Phishing and Social Engineering Attacks

Phishing is still the single most common attack vector against traditional 2FA. In these attacks, attackers pretend to be trusted entities and send phasing message/mail that includes a link to phishing website where they capture user's credentials or OTPs [20,21]. For example, an adversary can masquerade as a benign network operator and ask users to verify their accounts, causing users to submit personal information to fake web pages [22]. These risks are further heightened by social engineering, which subverts the human psyche. Attackers can even masquerade as the support desk, coworkers or other known entities to ask users on the phone, via messages or in person to give them an OTP or to provide credentials [23]. Conventional 2FA solutions do not have a direct way of authenticating the challenge originator because challenge could have been initiated by an attacker who can manipulate the context-rendering users susceptible to those sophisticated impersonation tricks.

3.2 SIM-Swapping and Man-in-the-Middle (MitM) Attacks

SMS 2FA is especially vulnerable to SIM-swapping attacks, when attackers find and exploit vulnerabilities in mobile carrier networks. Attackers trick the service provider to move the phone number of a victim to a SIM card controlled by the attacker (e.g., through social engineering or insider exploitation) [24,25]. Once succeeded, each and every SMS message (including

OTP) is forwarded to the attacker, thus providing unauthorized access to secured accounts [26]. Also, unencrypted communication between the user and the authentication servers is utilized by Man-in-the-Middle (MitM) attacks. 1 Time-based one-time passwords sent in the clear as SMS or email can be intercepted in transit or by local malware on infected device [27]. "These weaknesses highlight the fragility of SMS-based authentication in hostile network environment.

3.3 The Trade-off Between Security and Usability

Email and SMS as a common 2FA modality is mainly due to their ease and low barriers to entry as smartphones are already pervasive devices and so are email servers [9,10]. But ease of use can also equal lack of security. These techniques do not have more advanced security capabilities including secure tunneling, device fingerprinting, or risk-based adaptive authentication' [28, 29]. This often forces organizations to pick between providing a slick user experience and a set of strong, if somewhat clunky, security systems. 2FA and the risk of its failure are especially worrisome for high-secure industries like finance, medicine, enterprise networks, and the like – industries where confidentiality and trust are key. SMS-based authentication and email-based authentication can also not satisfy nature of modern threat model, so it requires development of more resilient and intelligent authentication framework [30]. While Figure 1 presents a simplified visual of how an SMS-based 2FA implementation looks like, it reveals the weaknesses that are exposed during common phishing and SIM-swapping attacks.

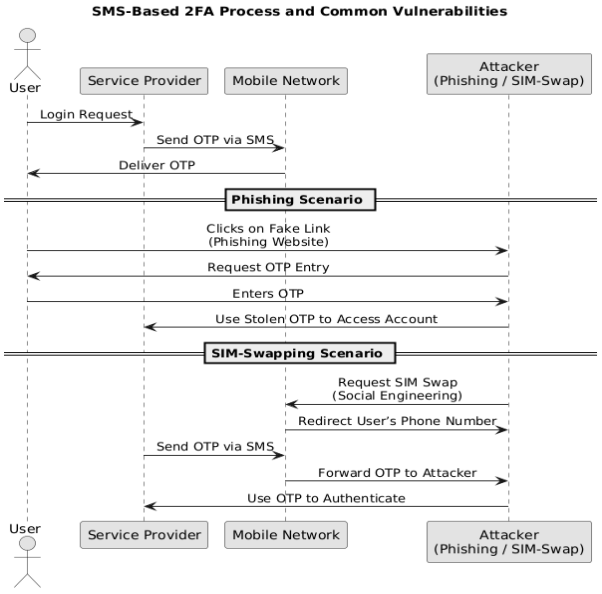

Fig1. SMS-Based 2FA Process and Common Vulnerabilities to Phishing and SIM-Swapping Attacks.

4. ELLIPTIC CURVE CRYPTOGRAPHY (ECC) FOR ENHANCED 2FA IN MOBILE NETWORKS

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

4.1 Authors and Affiliations

Elliptic Curve Cryptography (ECC) is becoming a successful cryptographic mechanism in the enhancement of Two-Factor Authentication (2FA) especially for both mobile and resource constrained networks. ECC is becoming more popular than traditional public-key cryptography due to its strong security assurance and support for lower key length (in addition to small memory footprint and less energy consumption), especially for many applications in which resources are power and memory restricted, such as mobile devices and IoT [31-33]. ECC derives its security by the use of the mathematically properties of elliptic curves over finite fields and the properties of the algebraic structure of elliptic curves handles the public key generation. One of the ECC's most attractive aspects is its capability to achieve the security equivalent to RSA with much smaller key sizes, thus diminishing the computation cost and memory usage. For example, a 256-bit ECC public key has equivalent security to a 3072-bit RSA public key, which renders ECC a good option for contemporary 2FA systems over mobile networks [34]. Several realizations of ECC have already been effectively used in mobile health environments (MHE), IoT devices and secure messaging systems with low computational overhead. ECC based 2FA not only provides the guarantee of authentication integrity, but also improves the security properties such as data confidentiality and system

scalability. To highlight the strengths and weaknesses of ECC compared to other cryptographic schemes, consider Table II, which presents a survey of ECC with other cryptosystems based on degree of security, efficiency, key and message lengths, and common applications.

TABLE II: COMPARISON OF CRYPTOGRAPHIC APPROACHES FOR TWO-FACTOR AUTHENTICATION (2FA)

Cryptographic Method	Security Level	Efficiency	Key Size	Pros	Cons	Best Use Cases
Elliptic Curve Cryptography (ECC)	High (equiv. to 3072-bit RSA with 256-bit key)	Very High	256-bit	Strong security, low resource usage; ideal for mobile/IoT	Complex implementation; specialized expertise required	Mobile networks, IoT, resource-limited environments
RSA	High (suitable for high-security applications)	Moderate (large key sizes)	3072-bit	Well-supported; simple conceptually	Computationally intensive; large memory/storage needed	VPNs, secure emails, traditional desktop systems
AES (Symmetric Encryption)	Very High (symmetric)	Very High	128–256-bit	Fast encryption/decryption; low overhead	Not suitable for 2FA directly; key exchange required	File transfer, cloud storage, closed systems
Digital Certificates (RSA/ECC)	High (depends on underlying algorithm)	High (strong authentication)	256-bit (ECC) / 2048-bit (RSA)	Provides identity assurance; supports MFA	Requires certificate authorities; revocation complexity	Banking, corporate security systems
Symmetric Key Algorithms	Moderate	Very High	~128-bit	Fast in controlled systems	Risk of key leakage; weak in open networks	Local storage, offline access control

Facing the implementation challenges of ECC, as well as other public-key cryptography approaches, such as complexity, vulnerability to erroneous configurations, and reliance at the key exchange level on secure protocols, provide some reasons in favor of further R&D into quantum-resistant algorithms. Besides, although ECC delivers good security and efficiency, ensuring forward secrecy and resistance to insider threats are also essential for full-fledged 2FA in distributed networks. A number of studies have suggested the use of ECC in AKA protocols to get rid of shortcomings in conventional hash-based or symmetric key schemes. Symmetric cryptography is faster but does not have forward secrecy. ECC or RSA can fill out the deficit, but require more communication and storage overhead. As such, an optimal 2FA strategy with ECC should carefully balance the security strength, on one hand, efficiency and resource needs, on the other, in view of mobile-first infrastructures.

5. DIGITAL CERTIFICATES AND DEVICE-BASED AUTHENTICATION

Digital certificates have become a strong contender in improving Two-Factor Authentication (2FA), especially when indivisibility of the user and system integrity is required. Unlike typical OTP-based techniques, certificate-based 2FA ties a user's identity to a digitally signed certificate, which is issued by a trusted CA (Certificate Authority). This credential could be stored (e.g., on a smart card, USB token, or in trusted software/vault (e.g., Cloud based keychain)) and is used as a necessary second factor of the secure systems [35]. The idea is to use the 2 elements: a log in credential (the first factor) and a verified digital certificate (the second factor), so as to add another line of defense against unauthorized access. There was a common usage of this subject matter in areas like enterprise systems, e-learning systems (i.e., Moodle), and governmental services, where privacy has an importance above other applications [36]. Additionally, digital certificate 2FA boasts advanced policy-based abilities to revoke or control access in the event of device compromise, user role changes, and organization offboarding. It is this flexibility that enables on-demand security enforcement where security policies are context-sensitive, e.g., in zero-trust environments and RBAC environments [37]. To authenticate, the following would be the simplified flow:

a) The user initiates a login request.
b) The system prompts for a digital certificate.
c) The user submits a certificate issued by a CA.
d) The system validates the certificate’s authenticity and integrity.
e) If verified, access is granted; otherwise, access is denied.

Unlike SMS or email codes, digital certificates are cryptographically signed and difficult to copy, and they are tied to a specific user or device. It protects them from phishing, SIM-swapping and other impersonation attacks [38]. What's more, the requirement of having an actual item in your possession adds a layer of security in line with the "something you have" part of 2FA. A high-level concept of operation of digital certificate based 2FA in a network system is shown in Figure 2, with the verification flow is being focused on, and with particular attention to the role of the certification authority.

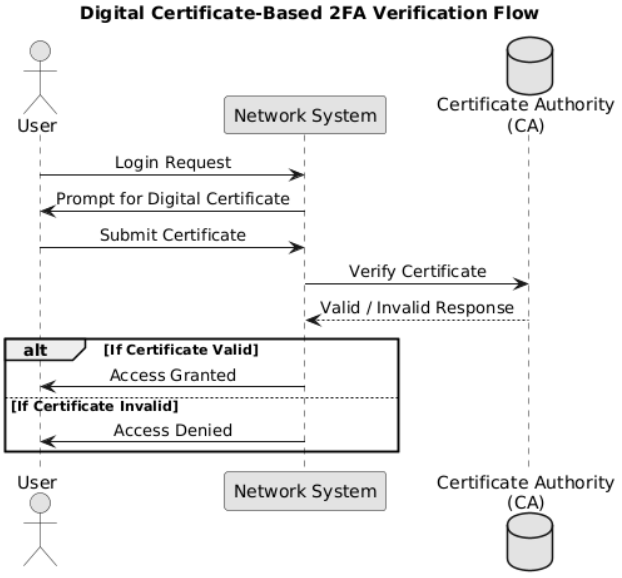

Fig 2. Digital Certificate-Based 2FA Verification Steps in a Network System.

6. ECC-BASED AND BIOMETRIC AUTHENTICATION PROCESS FLOWS

To show the practical use of more sophisticated Two-Factor-Authentications (2FA) protocols, the following summarizes the procedure flow of two 2FA mechanisms such as Elliptic Curve Cryptography (ECC)-based authentication as well as biometric/behavioral authentication (without measurable values) (both) based authentication. These flows focus on the secure steps for user to system interactions and illustrate how contemporary 2FA mechanisms increase security in a networked environment with layered levels of authentication [39].

6.1 ECC-Based Authentication Process Flow

ECC-based authentication is particularly suitable for such constrained environments as mobile networks and Internet of Things (IoT) systems. This technique uses low-cost cryptography to achieve strong security assurance at low computational and memory costs [40]. Process Steps:

a) **User Initiates Authentication**: The user begins by submitting login credentials (e.g., username and password).
b) **ECC Key Generation**: The system generates a session-specific ECC key pair and produces a digital signature using the private key.
c) **Signature Verification**: The system verifies the signature using the ECC public key stored in the server.
d) **Secondary Factor Verification**: The user may be prompted to provide an additional factor (e.g., OTP, hardware token) to complete 2FA.
e) **Access Granted**: Upon successful verification of both factors, access is securely granted.

This approach strengthens conventional authentication by adding a cryptographic layer that resists replay attacks and impersonation. The process is depicted in **Figure 3** below.

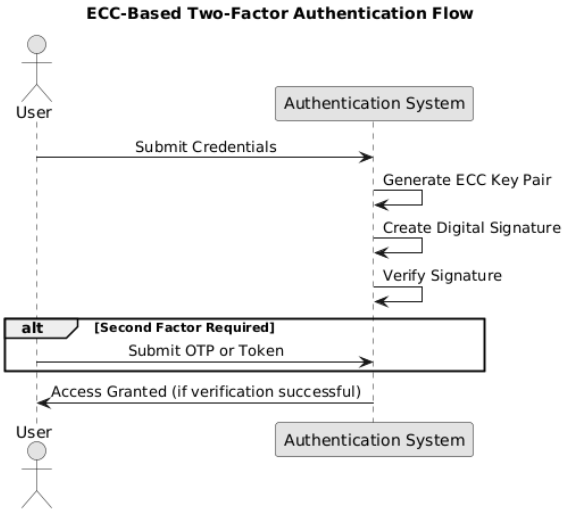

Fig 3. ECC-Based Authentication Process.

6.2 Biometric and Behavioral Authentication in Network Security

Biometric verification relies on the physical characteristics (e.g. fingerprint, face recognition, iris scan) of a person to confirm his identity. It is non-trivial to reproduce these features, which makes them well suited for high-security applications like mobile banking, medical applications and enterprise networks [41, 42]. Biometric Authentication Process Steps:

a) **Enrollment**: The user registers biometric data, which is stored as a secure template.
b) **Authentication Initiation**: During login, the user presents biometric input (e.g., fingerprint scan).
c) **Data Capture and Matching**: Live biometric data is captured and compared with the stored template.
d) **Secondary Factor Verification (if required)**: The user may be asked to submit an OTP or password.
e) **Secure Access Granted**: If both factors are validated, the system grants access.

Real-time behavior-based authentication, on the other hand, verifies identity and ensures security quality from typing speed, device handling to navigation behavior. This technique passive authentication, which both increase the security and the user experience at the same time, does not require explicit user input and can run the user in the back ground constantly [43]. Figure 4 shows the flowchart of the biometrics authentication steps.

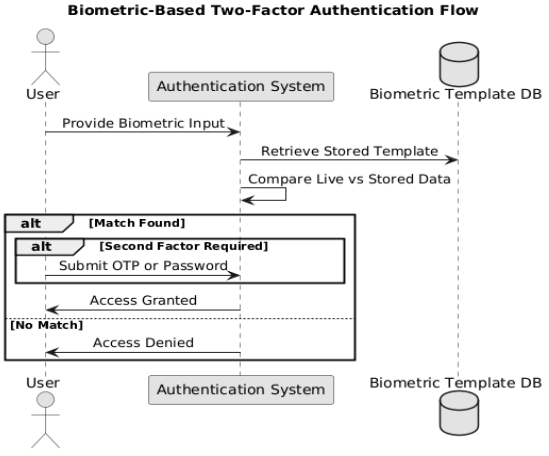

Fig 4. Flowchart of the Biometric Authentication Process

These flows illustrate how ECC and biometrics operate to supplement 2FA schemes, through the provision of robust proof, enabled with strong cryptographic binding, and unique human-centered aspects. When used in conjunction with behavioral analysis, these technologies help to enforce continuous authentication, reduce the need to rely on comprisable channels (such as SMS) and introduce pattern-driven access control.

7. COMPARATIVE ANALYSIS OF SECURITY AND USABILITY IN 2FA SYSTEMS

Two-Factor Authentication (2FA) has emerged as an indispensable tool to increase the security level in networked systems by asking users to present evidence of two different factors. Although traditional 2FA solutions such as SMS and email-based OTPs provide usability and wide availability, they do not provide strong resistance against advanced attacks such as phishing, SIM swiping, and credential interception [44, 45]. Contemporary 2FA methods, from Elliptic Curve Cryptography (ECC) to digital certificates to biometrics, add strong security to the mix with crypto or physical identity tokens. Nevertheless, these sophisticated approaches bring back problems with implementation complexity, user acceptance, hardware requirements, and cost of deployment [46]. In this section, we provide a systematic comparison of traditional and advanced 2FA approaches, with reference to three key criteria:

a) **Security Level**
b) **Usability Level**
c) **Trade-offs between convenience and protection**

Such analysis is vital to the decision-makers and system designers to drive the system to be more practical to deploy and to achieve a balance between security and usability, and hence have a probability to be adopted at the large scale in enterprise and consumer domains [46,47].

7.1 Traditional vs. Advanced 2FA Mechanisms

For instance, SMS based 2FA is convenient and is barely supported everywhere, but is transmitted over insecure channels and can be bypassed trivially via SIM-swapping. In contrast, ECC- based 2FA provides high level of cryptographic security, and it is suitable for IoT and mobile environments; however, it has high integration knowledge and expert effort [48]. Bi-directional authentication is indeed highly secure and user-friendly, but it is not privacy-friendly and it requires alternative hardware. Digital certificates provide revocable, verifiable identity assurance but come at the cost of the complexity and expense of a public key infrastructure, or certificate authority (CA) services [49]. To further underline the challenge of balancing security strength with implementation complexity, we summarize in Table III a comparison of traditional and advanced 2FA designs. He outlines the fundamental benefits and drawbacks of each category, providing decision-makers with a guide to determining which path is most suitable to their organization's requirements and threat environment.

TABLE III: COMPARATIVE EVALUATION OF 2FA METHODS BASED ON SECURITY AND USABILITY ATTRIBUTES

2FA Method	Security Level	Usability Level	Advantages	Disadvantages
SMS-Based OTP	Moderate	High	Simple, widely supported	Prone to phishing & SIM-swapping; depends on cellular networks
Email-Based OTP	Moderate	High	Convenient, no extra hardware required	Vulnerable to email breaches; phishing threats
App-Based OTP (e.g., Authenticator)	High	Moderate	Secure, offline-capable	Requires setup; user inconvenience if phone is lost
Hardware Tokens	High	Moderate	Strong physical factor; independent of other devices	Tokens can be lost or damaged; added costs
Biometric Authentication	Very High	Very High	Fast, user-friendly; hard to spoof	Privacy issues; hardware dependency; potential false positives/negatives
Digital Certificate-Based 2FA	Very High	Moderate	Strong identity assurance; revocable	Complex setup; reliance on trusted CA; maintenance overhead
ECC-Based 2FA	Very High	High	High security with small key size; resource-efficient	Requires cryptographic expertise; initial complexity

Balancing security with usability is a key challenge in 2FA system design. Old-school approaches could be viable in low-risk environments or user-operated platforms focused on usability first. At the other extreme, more sophisticated 2FA methods including ECC and biometrics are deemed appropriate for high-security environments like finance, government, healthcare and corporate infrastructures. This comparative analysis consolidates the notion that there is no one-size-fits-all solution. System administrators have to weigh up their threat models, their users' requirements, and their infrastructure capabilities when deciding how to approach authentication.

8. IMPLEMENTATION CONSIDERATIONS

To adopt 2FA into their real-world networking environment, designers and managers need to take into account a number of practical aspects: the cost, scalability, 1 compatibility, user preparedness, and policy compliance. While more advanced 2FA methods (e.g., ECC (Elliptic Curve Cryptography), digital certificates, and biometric authentication) provide better security, the utility of such options depends on an organization’s IT systems, users, and financial resources [50].

1. Cost: cost is still a major consideration withholding the use of advanced 2FA solutions. For example, biometric systems typically utilize dedicated hardware (e.g., fingerprint scanners, facial recognition hardware), the setup cost is high, and the maintenance cost is also expensive. Likewise, hardware tokens or digital certificates introduce costs such as device issuance, certificate purchase, and renewal from CAs, and the integration with infrastructure [51]. Within a large-scale deployment, these costs must be weighed against the predicted cost reductions in security, particularly given the general move to secure its critical systems.
2. Scalable: Scalability is an issue with increasing populations and network complexities. Solutions based on traditional methods including SMS- and app-based OTPs are cost-effective and easy to scale with less infrastructure modifications. In the other hand, we will ensure that biometric systems and digital certificates do not require hardware upgrade and backend changes. ECC 2FA gives a good trade-off in between since small computational costs and small key lengths are ideal for mobile and IoT networks, allowing a compromise between good scalability and performance [52]. Hybrid or role based 2FA solutions may be adopted by the organization to cater for different user requirement and context.
3. Compatibility: Compatibility with other systems is a key factor to avoid operational disruptions. For instance, digital certificates are interoperable with PKI-based environments, but not with legacy or non-standardized environments. Modern devices adoptions of ECC are also growing, however the large number of existing systems which use only RSA algorithms may need to be retrofitted. Biometric systems also need suitable devices and drivers, which can be problematic in remote or Bring Your Own Device (BYOD) settings. A comprehensive compatibility check is necessary prior to deployment [53-58].
4. User Training and Support -- Advanced 2FA technologies may present new procedures to end users, especially in systems applying digital certificates or biometric enrollment. Effective utilization requires clear user training programmers, step by step onboarding, and technical support. End user understanding of procedures including how to handle hardware tokens, enroll biometric templates, and manage certificate lifecycles is critical to reducing resistance to change and guarantee acceptance [59-64].
5. Security Policy and Management – Deployment of technology should be consistent with the overall organization's security policy. This encompasses procedures to deal with lost or stolen tokens, revoked or expired certificates, and compromised biometric data. In addition, we should provide guidelines for how 2FA credentials are issued, monitored, and revoked by policies. Integrations with central access management and audit logging are also necessities for long-term security and compliance with data protection standards [65-68].

By attending to these implementation concerns, organizations can properly deliberate whether to deploy advanced 2FA mechanisms that are secure but also usable, scalable, and consistent with operational practice. Strategic planning will help to identify, evaluate, and successfully integrate security advancements that are strategically incorporated into the network infrastructure in order to respond to changes in security threats and user requirements.

9. CONCLUSION

Two-Factor Authentication (2FA) continues to be an essential part of network access security; however, classical offerings such as SMS- and email-delivered OTPs are becoming vulnerable to increasingly sophisticated cybercriminal methods such as phishing, SIM-swapping and interception attacks. This work provided a thorough investigation of advanced 2FA schemes such as ECC, PKI-based authentication, and biometric-based verification that offer superior security and flexibility to changing network scenarios. ECC offers lightweight yet strong cryptographic authentication for mobile and IOT types

of systems, digital certificates enhance identity assurance with trusted, revocable certificates, and biometrics offer a layer of physical identity validation that is impervious to impersonation. Comparing different 2FA solutions, a balance between security, usability, scalability, and compatibility was clearly shown to be a key-aspect when deploying modern 2FA schemes in real-world infrastructures. Moreover, this work advocates a tactical departure from outdated models to smarter and robust authentication systems to thwart present-day cybersecurity threats. In addition, future developments need to concentrate on the introduction of machine learning and AI paradigms into 2FA frameworks, so that adaptive models that dynamically react according to the end users' behavior and the risk assessment would be created. " In doing so, businesses can construct saleable, context-aware, future-ready security architectures to protect digital assets across multiple networked environments.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

Non.

References

[1] SANS Institute, SANS 2021 Password Management and Two-Factor Authentication Methods Survey. SANS Institute, 2021.

[2] R. Reese, B. Smith, and C. Johnson, “Usability analysis of two-factor authentication methods,” in Proc. ACM Conf. Human Factors Comput. Syst. (CHI), Glasgow, UK, 2019, pp. 1–12.

[3] A. Alotaibi and H. Elleithy, “Multi-factor authentication in cyber physical systems: A state-of-the-art survey,” IEEE Access, vol. 7, pp. 128845–128866, 2019.

[4] K. Alghamdi, S. Alharbi, and M. Alzahrani, “Recent trends of authentication methods in extended reality: A survey,” Applied Sciences, vol. 13, no. 3, p. 9675, 2023.

[5] T. Dereje and D. Anand, “Trends in two-factor authentication: A survey,” in Advances in Intelligent Systems and Computing, vol. 1158. Cham, Switzerland: Springer, 2021, pp. 145–156.

[6] P. Rannenberg, V. Varadharajan, and C. Weber, “Evolution of authentication systems: Towards multi-factor authentication,” in Proc. 13th Int. Conf. Security Privacy Commun. Netw. (SecureComm), Singapore, 2018, pp. 619–628.

[7] M. Alotaibi and K. Elleithy, “User authentication factors: From single-factor to multi-factor authentication,” Adv. Comput. Electr. Eng., vol. 2, no. 1, pp. 1–15, 2021.

[8] Yubico and Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, 2020. [Online]. Available: https://www.yubico.com/authentication-report

[9] Deloitte, Digital Authentication: Moving Beyond Passwords, 2023. [Online]. Available: https://www2.deloitte.com/global/en/pages/risk/articles/digital-authentication.html

[10] Lifewire, “What is an authenticator app and how does it work?” [Online]. Available: https://www.lifewire.com/what-is-an-authenticator-app-5180855

[11] I. A. Jaddoa and A. T. Kurnaz, “Developing a two-factor authentication system to identify vulnerabilities in public Wi-Fi,” Int. J. Sci. Trends, vol. 2, no. 7, pp. 1–6, 2023.

[12] V. Banes, C. Ravariu, B. Appasani, and A. Srinivasulu, “A novel two-factor authentication scheme for increased security in accessing the Moodle e-learning platform,” Applied Sciences, vol. 13, p. 9675, pp. 1–16, 2023.

[13] K. Liu et al., “A robust and effective two-factor authentication (2FA) protocol based on ECC for mobile computing,” Applied Sciences, vol. 13, p. 4425, pp. 1–19, 2023.

[14] NIST, Digital Identity Guidelines, Special Publication 800-63B. Gaithersburg, MD, USA: Natl. Inst. Standards Technol., 2020.

[15] J. T. Sample and P. J. Blythe, “Usability vs. security in two-factor authentication,” Inf. Security J.: Global Perspective, vol. 26, no. 2, pp. 87–98, 2017.

[16] J. G. Vives and K. Sanchez, “Biometric authentication: Advances in behavioral biometrics,” IEEE Security Privacy, vol. 18, no. 4, pp. 48–55, 2020.

[17] G. Ziegler and C. Allen, “Evaluating mobile app-based two-factor authentication,” in Mobile Computing and Network Security. New York, NY, USA: Springer, 2022, pp. 232–249.

[18] C. A. Gelin, “The role of elliptic curve cryptography in mobile device security,” Wireless Networks, vol. 26, no. 5, pp. 1937–1952, 2020.

[19] D. Anand and S. Datta, “2FA in IoT systems: Security and challenges,” Sensors, vol. 21, no. 8, pp. 2671–2679, 2021.

[20] P. Ahmad, “Advanced two-factor authentication for healthcare IoT,” Health Informatics J., vol. 27, no. 3, pp. 2653–2674, 2021.

[21] M. Wazid, A. K. Das, and N. Kumar, “An advanced survey on security and privacy in IoT-based 2FA,” IEEE Commun. Surveys Tuts., vol. 23, no. 3, pp. 1345–1383, 2021.

[22] F. Kaabar and M. R. Farooq, “Security frameworks in multi-factor authentication systems,” J. Inf. Security Appl., vol. 64, p. 102685, 2022.

[23] S. Davis, “Application of biometrics in digital certificate-based authentication,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 456–465, 2021.

[24] T. Zhu et al., “Exploring SIM-swap vulnerabilities in 2FA protocols,” Computer Networks, vol. 197, p. 108268, 2021.

[25] H. Y. Kim, “Challenges in implementing biometric and certificate-based 2FA in smart cities,” IEEE Access, vol. 8, pp. 171285–171299, 2020.

[26] M. Y. Lee and R. A. Brison, “Usability and security in mobile device authentication,” J. Inf. Security Appl., vol. 51, p. 102511, 2020.

[27] A. B. Ali, “Examining cyber attacks targeting traditional 2FA,” IEEE Security Privacy, vol. 18, no. 6, pp. 59–65, 2020.

[28] A. Beltran and B. C. Lynn, “Efficiency in cryptographic protocols for mobile networks,” IEEE Trans. Mobile Comput., vol. 19, no. 12, pp. 2755–2769, 2020.

[29] R. Ortega and T. Tomic, “Security of advanced 2FA methods in cloud environments,” in Cloud Computing and Services Science. New York, NY, USA: Springer, 2021, pp. 98–113.

[30] N. Rashid et al., “Elliptic curve cryptography for low-power 2FA devices,” IEEE Internet Things J., vol. 8, no. 3, pp. 1601–1613, 2021.

[31] J. Warner, “Comparative study of OTP methods in 2FA,” Inf. Security J.: Global Perspective, vol. 30, no. 2, pp. 87–98, 2021.

[32] T. Gligor, “Device-based authentication using ECC,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 3936–3946, 2021.

[33] D. Abu Laila, “Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the IoT-based IDS,” STAP J. Security Risk Management, vol. 2025, no. 1, pp. 59–70, 2025, doi: 10.63180/jsrm.thestap.2025.1.3.

[34] A. Ali, “Adaptive and context-aware authentication framework using edge AI and blockchain in future vehicular networks,” STAP J. Security Risk Management, vol. 2024, no. 1, pp. 45–56, 2024, doi: 10.63180/jsrm.thestap.2024.1.3.

[35] Q. Al-Na’amneh et al., “Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments,” STAP J. Security Risk Management, vol. 2025, no. 1, pp. 85–114, 2025, doi: 10.63180/jsrm.thestap.2025.1.5.

[36] M. Almaayah and R. B. Sulaiman, “Cyber risk management in the Internet of Things: Frameworks, models, and best practices,” STAP J. Security Risk Management, vol. 2024, no. 1, pp. 3–23, 2024, doi: 10.63180/jsrm.thestap.2024.1.1.

[37] S. Alsahaim and M. Maayah, “Analyzing cybersecurity threats on mobile phones,” STAP J. Security Risk Management, vol. 2023, no. 1, pp. 3–19, Aug. 2023, doi: 10.63180/jsrm.thestap.2023.1.2.

[38] R. Almanasir et al., “Classification of threats and countermeasures of cloud computing,” J. Cyber Security Risk Auditing, vol. 2025, no. 2, pp. 27–42, 2025, doi: 10.63180/jcsra.thestap.2025.2.3.

[39] A. A. Almuqren, “Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions,” J. Cyber Security Risk Auditing, vol. 1, no. 1, pp. 1–11, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.1.

[40] R. S. Mousa and R. Shehab, “Applying risk analysis for determining threats and countermeasures in workstation domain,” J. Cyber Security Risk Auditing, vol. 2025, no. 1, pp. 12–21, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.2.

[41] S. R. Addula and A. Ali, “A novel permissioned blockchain approach for scalable and privacy-preserving IoT authentication,” J. Cyber Security Risk Auditing, vol. 2025, no. 4, pp. 222–237, 2025, doi: 10.63180/jcsra.thestap.2025.4.3.

[42] S. Nakamura and E. Sakurai, “Behavioral biometrics in adaptive authentication,” ACM Trans. Inf. Syst., vol. 41, no. 2, pp. 78–96, 2023.

[43] R. Gallo, “Modern 2FA in industrial IoT: ECC and beyond,” IEEE Ind. Electron. Mag., vol. 14, no. 2, pp. 23–33, 2020.

[44] G. M. Mohammad and S. Benlamoudi, “Public key infrastructure and certificate-based authentication,” IEEE Commun. Surveys Tuts., vol. 24, no. 1, pp. 673–690, 2022.

[45] T. Sampson, “Digital identity verification with certificates,” IEEE Trans. Inf. Forensics Security, vol. 17, pp. 4829–4843, 2022.

[46] Y. J. Lim et al., “Advances in mobile biometric security,” IEEE Access, vol. 9, pp. 168451–168460, 2021.

[47] E. Russo, “Security analysis of ECC-based 2FA in mobile apps,” Mobile Security J., vol. 15, no. 4, pp. 245–256, 2023.

[48] C. Huang, “Two-factor authentication in financial networks,” in Financial Services Security. Boston, MA, USA: McGraw-Hill, 2021, pp. 167–183.

[49] S. Ravi and M. Arya, “Next-generation authentication methods in IoT,” J. Netw. Comput. Appl., vol. 176, p. 102909, 2021.

[50] N. J. Kim and J. H. Park, “Exploring machine learning in 2FA,” IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 8, pp. 3423–3435, 2021.

[51] M. C. Kerr et al., “Implementing 2FA in hybrid cloud environments,” Cloud Security J., vol. 22, no. 5, pp. 316–327, 2022.

[52] W. Li et al., “Scalable 2FA for mobile banking,” J. Banking Finance Security, vol. 10, no. 4, pp. 55–67, 2021.

[53] R. Singh, “Cost-effective biometrics in 2FA solutions,” IEEE Security Privacy, vol. 18, no. 6, pp. 78–85, 2020.

[54] T. Andrews, “Device management in certificate-based authentication,” IEEE Trans. Syst., Man, Cybern.: Syst., vol. 50, no. 5, pp. 3497–3507, 2020.

[55] C. E. Torres, “Usability issues in multi-factor authentication,” Int. J. Human–Computer Interaction, vol. 37, no. 4, pp. 320–329, 2021.

[56] J. Swartz and L. Evans, “Security standards for app-based 2FA,” J. Inf. Syst., vol. 43, no. 1, pp. 25–37, 2020.

[57] S. Lee and J. M. Choi, “Behavioral analysis in adaptive authentication,” IEEE Trans. Biometrics, Behavior, Identity Sci., vol. 2, no. 3, pp. 269–280, 2020.

[58] A. Walker, “Passwordless authentication in modern networks,” Network Security J., vol. 34, no. 7, pp. 19–28, 2022.

[59] S. R. Addula, S. Norozpour, and M. Amin, “Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing,” Jordanian J. Informatics Comput., vol. 2025, no. 1, pp. 38–48, 2025, doi: 10.63180/jjic.thestap.2025.1.5.

[60] M. Alshinwan et al., “Unsupervised text feature selection approach based on improved prairie dog algorithm for text clustering,” Jordanian J. Informatics Comput., vol. 2025, no. 1, pp. 27–36, 2025, doi: 10.63180/jjic.thestap.2025.1.4.

[61] H. Albinhamad et al., “Vehicular ad-hoc networks (VANETs): A key enabler for smart transportation systems and challenges,” Jordanian J. Informatics Comput., vol. 2025, no. 1, pp. 4–15, 2025, doi: 10.63180/jjic.thestap.2025.1.2.

[62] Z. T. Li and P. M. Koh, “Simulating and securing OTPs with ECC,” IEEE Trans. Cloud Comput., vol. 8, no. 3, pp. 1274–1282, 2020.

[63] J. S. Wang et al., “Multi-factor authentication in distributed systems,” IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 1, pp. 59–72, 2021.

[64] B. Fields, “Hybrid cryptography in 2FA,” IEEE Trans. Cloud Comput., vol. 9, no. 2, pp. 673–688, 2021.

[65] A. Coleman and R. Davis, “The importance of ECC in 2FA,” in Security and Privacy in Computing Systems. Berlin, Germany: Springer, 2021, pp. 58–73.

[66] M. Bhattacharjee, “Biometric trends in secure authentication,” IEEE Access, vol. 10, pp. 32244–32256, 2022.

[67] S. K. Singh, “Performance metrics in multi-factor authentication,” Int. J. Inf. Management, vol. 62, p. 102439, 2022.

[68] E. Spahiu, D. Xhako, N. Hyka, and S. Hoxhaj, “3D magnetic resonance image segmentation using HD brain extraction in 3D Slicer,” J. Trans. Syst. Eng., vol. 3, no. 1, pp. 340–348, 2025.