Advanced Strategies and Solutions Towards More Secure and Effective Two-Factor Authentication in Networking / Original article

Zahraa Sameer Jawad

College of Computer Science and Information Technology,
Karbala University, Iraq, Karbala
zahraa.sameer@uokerbala.edu.iq

Abstract

With the rapid increase in cybersecurity threats targeting network systems, traditional two-factor authentication (2FA) methods are insufficient to address advanced attacks. Vulnerabilities such as phishing, SIM-swapping, and social engineering exploit the limitations of SMS-based and email-based 2FA. This paper examines advanced strategies and solutions for securing networked environments through robust 2FA mechanisms, focusing on approaches like elliptic curve cryptography (ECC), digital certificates, and biometric verification. This article offers a comparative review of various strategies about their effectiveness in enhancing security, while also highlighting their capacity to optimize user-friendliness and adaptability to emerging threats. Research findings promote an effective countermeasure strategy for network security, highlighting lessons and best practices in the implementation of advanced two-factor authentication solutions within a multi-network framework.

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

1. Introduction

As the number of people online increases, the protection of one's online identity is becoming more crucial. Static passwords, which are used to secure personal information and online activities, can be easily cracked in seconds. Two-Factor Authentication (2FA) is being implemented as an extra layer of security to protect personal information and online assets. As digital and mobile connections expand, access control has become a critical component of cybersecurity. Two-factor authentication (2FA) augments authentication processes by employing two distinct components to verify a user's identity. Email and SMS-based authentications, often used as two-factor authentication (2FA), are susceptible to attacks such as phishing, SIM-jacking, and brute force methods [1]–[3].

Nonetheless, although these two-factor authentication solutions are popular, they are increasingly vulnerable to contemporary cyber attacks. Attack methods such as phishing, wherein the attacker deceives the user into disclosing information, jeopardize the integrity of email-based two-factor authentication. Similarly, SIM swapping attacks exploit weaknesses in cellular networks to gain control of the target's phone number, enabling the interception of OTPs sent over SMS [5]. These attacks expose inherent vulnerabilities in traditional two-factor authentication, as they target communication interfaces. Furthermore, even basic brute-force and social engineering attacks can compromise typical two-factor authentication systems, as users may reuse passwords or neglect standard practices [6].

The deficiencies of traditional methods of two-factor authentication underscore the necessity for adaptive, improved, and secure solutions inside networked environments. Advanced methodologies of two-factor

authentication have been established as viable solutions to these issues. These methods emphasize the application of recent advancements in cryptography, biometrics, and device authentication and authorization frameworks, ensuring that the utilization of secure systems remains user-friendly. For example:

1. Elliptic Curve Cryptography (ECC) is a strong cryptographic method which is particularly effective for resource-constrained devices as are the case with many IoT and mobile devices in specific [7].
2. Digital certificates bring one more level of certification in the form of verifying the identity and legitimacy of both user and accessories, which give the attacker practically no chance to mimic the identity of the user [8].
3. Fingerprint or face recognition type of authentication employs use of bodily characteristics which makes them secure and rare to be imitated [9].

These advanced 2FA techniques hold potential to provide a better solution of secure networks by expanding the base of authentication factors in knowledge-based mechanism. These methods are achieved by combining both cryptographical and biometrical parts, which make it much more difficult to enter an unauthorised code even if a password has already been become expired. In addition, such approaches have the opportunity to enhance the overall user experience by liberating users from relying on potentially dangerous or less relevant channels.

This article examines sophisticated two-factor authentication schemes, particularly the balance between security and ease, and how modern networking architecture can support the stringent security requirements of the 21st century.

This project aims to establish a framework for designing and implementing safe yet user-friendly two-factor authentication systems essential for countering contemporary threats while ensuring a good user experience.

2. Related Works

The analysis of two-factor authentication has been one of the main concerns in the field of cybersecurity because of its significance for securing the important data and access to accounts. Several works have focused on analysing 2FA conventional and improved techniques in terms of performance, simplicity, and issues in the current cybersecurity threat environment. Another study by the SANS Institute in 2021 focused on the current organisational practises in password management and methods used for 2FA. In this survey, an emerging trend toward its adoption for improving security with focus on the weakness of only passwords was observed. Yet the survey revealed barriers to user adoption; though 2FA enhances security, usability issues and end-user resistance are significant bi-parameters [10].

In a usability study by Reese *et al.* (2019), five common 2FA methods were evaluated: Mobile text, electronic mail, voice call, hardware token, and Smartphone application. The research confirmed that the assurance provided by the tokens of the technological hopeful was higher than with that provided by messages and emails since the latter are more fallible to phishing and SIM-swapping ploys. However, the respondents preferred the simple designs of the SMS and email-based methods, but often there are sacrifices between security and convenience [11].

In their state-of-the-art survey on multi-factor authentication in cyber-physical systems, Alotaibi and Elleithy (2019). Their research divided user

authentication features into aspects such as security, privacy, usability, scalability and interoperability and pointed out that a good authentication system must strive to attain a good balance of all of them. They further indicated that although multi-factor approach enhances security, its application should incorporate usability for practical implementation on real-world systems [12].

A literature review performed by Alghamdi *et al*. (2023) aimed to identify the current XR authentication methodologies and found that there was a transition from the 2FA toward methods that are context-based and include behavioural analytics along with biometrics. To this end, this work paints the picture of a challenge typical of complex technologies such as XR, where ease of authentication is always a vital component and an essential way of enhancing user experience and security, particularly when begun using the existing basic facility of the smartphone [13].

Another important piece by Dereje and Anand (2021) presented an insight into the dynamics of 2FA and focused on different ways and how efficient each of them is. Hence they stressed that it is critical to implement multiple factors in authentication in order to increase security, and thus user trust to shift from single factor to multiple factor authentication solutions. Their survey also reiterated that two-factor or many factor authentication models provide enhanced security against different cyber threats when adopted together with sturdy cryptographic mechanisms [14].

Similarly, another cross-sectional survey by Rannenberg *et al*. (2018 found) examined the development of authentication systems with special focus on the MFA. They discussed new approaches in identification and described pro and cons of biometric and behaviour-based technique as well as discussed them from both end-user and supplying-service provider points

of view. It also showed how with integration of advanced sensors and smart devices authentication can be made more secure and convenient especially in application areas that need almost constant access control [15].

In a following paper, Alotaibi and Elleithy (2021) build upon this framework by exploring user authentication factors and shift from single-factor to multi-factor in several systems. They also talked about how the use of different layers of authentication increases security and also how risks inherent with single-factor authentication such as a password or PIN are overcome, and the need for using advanced 2FA techniques [16].

The Yubico and Ponemon Institute surveyed and quantified the password and authentication security behaviours in the 2020 State of Password and Authentication Security Behaviours Report. The report then described the inherent dangers with bad password behaviour and also proposed rise in 2FA usage as an effective solution to those risks. According to the report, organisations need to look for other more reliable ways forward than passwords; for instance, biometrics authentication [17].

Digital Authentication According to the Deloitte's article released in 2023, a trend is emerging to move away from often-hackable passwords In the context of the discussed topic, passwords are considered weak links. The article suggested that multi-factor identification should be implemented, and biometric methods as well as security tokens as more secure forms and offered practical ideas on future work on authentication. This work stresses the need to develop an effective and efficient authentication process that is both highly secure and easily installable into any system.

Lastly, an article was written for Lifewire to explain the uses and the advantages of the authenticator app, which creates a TOTP for MFA. The

article also elaborated that in comparison to the codes sent in SMS text messages, apps are more secure, as they do not require cell connexion and can easily be intercepted. This has been a handy practical guide, and it proffered useful experience in relation to broad adoption of the app-based 2FA in the improvement of account security [19]. The major studies associated with 2FA are summarised in Table 1 in an abbreviated manner. The individual studies are described according to its research area, findings, and methodological restrictions. It also brings out the variety of methodologies that have been used in the 2FA research including the basic techniques of SMS based verification and goes up to the complex structures of biometric and digital Certificate-based 2FA.

Table 1: Summary of Key Studies on Two-Factor Authentication (2FA) Methods

Study	Methodologies Explored	Key Findings	Limitations	Proposed Improvements/ Research Gaps
SANS Institute (2021)	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
Reese *et al.* (2019)	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
Alotaibi and Elleithy (2019)	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

Study	Methodologies Explored	Key Findings	Limitations	Proposed Improvements/ Research Gaps
Alghamdi *et al.* (2023)	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
Dereje and Anand (2021)	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
Rannenberg *et al.* (2018)	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
Alotaibi and Elleithy (2021)	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
Yubico & Ponemon Institute (2020)	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
Deloitte (2023)	Digital Authentication	Recommended MFA, biometrics, tokens over passwords	Primarily recommendations, limited empirical data	Perform empirical studies on adoption rates and practical implementation
Lifewire [19]	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

The traditional approaches of two-factor authentication have been using SMS, Emails, and Time-based One-Time Password that are mobile applications. While these approaches are convenient and straightforward to implement, they face several vulnerabilities:

1. Phishing and Social Engineering: The participants described that the threat actors always advanced in utilising phishing techniques to make users vulnerable. Another type of attack is phishing where the hacker impersonates as a genuine organisation and sends emails, messages and links that looks completely genuine that makes users to enter their credentials or OTP on a fake sites controlled by the hackers [20][21]. For instance, an attacker may use email to ask the recipient to confirm their account details or to do a security cheque. The link provided is a phishing site, and once the user submits his or her credentials / OTP the attacker gets to capture and utilise this data [22]. Social engineering is much wider in its definition and in the real world it involves interacting with people directly. The attackers may come in disguises of trusted individuals, calling, emailing or even approaching the users, and force them to disclose access codes or OTPs [23]. These tactics abuse human trust and imperative, thus, it is less challenging for the attacker to 'circumvent' the second factor authentication process without sophisticated tools and methods. The classic 2FA methods that are in practise do not allow for the source of the challenge to be confirmed or for the user to confirm the identity of the sender.

2. SIM-Swapping and Man-in-the-Middle (MitM) Attacks: SMS based 2FA is insecure due to SIM swapping and MitM where the attackers are able to penetrate established network links to compromise OTPs [24]. A SIM-swapping act involves persuading a mobile service provider to port the user's phone number to different SIM card owned by the intruder. This manipulation can be done using the social engineering and leveraging insiders at the carrier[25]. After the phone number is redirected, all SMS are sent to the attacker including OTP codes used in 2FA procedures. Worse, due to the impaired encryption in the OTP messages, the attacker can easily penetrate the 2FA layer and access the victim's accounts illicitly [26]. This kind of attack is most relevant to the current popular application of textual- and email-based 2FA, since messages are transmitted in plain text and can be easily captured without decryption. These attacks pose a major problem for services using SMS-based 2FA because the underlying communication channel is less secure than the message transmission and can easily be hijacked with an intercept or retargeting of the OTP. While modern hackers invent more effective ways to breach network vulnerabilities, conventional text message-based 2FA is not as effective [27].
3. Security vs. Usability Trade-offs: SMS- and email-based OTPs are traditional 2FA methods which have negligible barriers to adoption because of the ubiquity of phones and email [9]. Nevertheless this makes systems vulnerable to security threats, even to professional ones, at times [10]. These methods have been said to be insecure

as they are conveyed through open communication channels with no form of secure_tunneling [28]. Moreover, they do not support smart features such as adaptive risk based authentication or device specific tokens which would be relevant to savvy, secured environment such as the financial sector or enterprise network [29]. Therefore most organisations end up in a compromise where they have to provide convenience to their users at the expense of exposing themselves to various risks affected by their systems. As a result, organisations should consider the confidentiality and ease of use when comparing traditional methods of 2FA.

Like any other popular technology, SMS-based two-factor authentication (2FA) has been compromised by a number of newer digital threats. There are two big dangers of the SMS-based 2FA; interception of the code sent and SIM-swapping. When using the SMS-based 2FA process the user receives a one-time password (OTP) via a message on their mobile device. However, this method depends on a communication channel that can easily be hacked [30]. This is so because the OTP can be intercepted through the possibly of newt work of the user or through spying on the users SMS details [31]. In addition, in SIM-swapping attack an attacker is able to mislead a mobile service provider to forward the user's phone number to an illegitimate SIM card controlled by the attacker. This makes it possible for the attacker to directly receive the OTP and therefore gains unauthorised access to the victim's account [32]. Figure 1 Simple pictorial representation of an SMS-based 2FA process and the exposed weak links to phishing and SIM-swapping attacks.

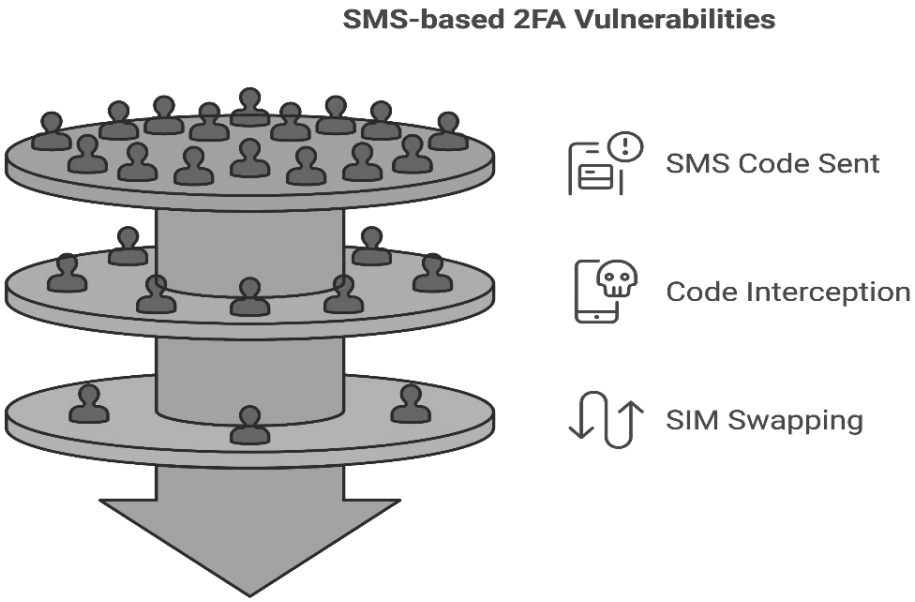

Figure 1: SMS-Based 2FA Process: Vulnerabilities to Phishing and SIM-Swapping Attacks.

4. Elliptic Curve Cryptography (ECC) for Enhanced 2FA in Mobile Networks

Elliptic curve cryptography (ECC) is a modern cryptographic technology that is getting increasingly implemented in 2FA due to its enhanced security despite it requires low resource. Mobile environment applications are well suited for ECC based 2FA because of the typical requirements in the mobile environments, for instance low resources constraints result in efficient security protocols [33]. ECC functions by producing the keys using some properties of the elliptic curves and seems to be a viable choice for a secure user authentication system. They add that ECC has a small key size, which helps to save time and memory in mobile devices while providing sufficient levels of security. For instance, ECC has been successfully incorporated in the

MHE and IoT to provide data safety and privacy in achieving the performance requirements of Mobile Networks [34].

Table 2 compares various cryptographic approaches for two-factor authentication (2FA) based on three key factors: The features include security level, efficiency and size of the key or a combination of the three. ECC gives the same level of security as RSA only with matched but smaller number of bits and as such is desirable for mobile and low power applications. ECC and AES are efficient with less numbers of keys needed AES being optimised for fast Symmetric encryption. But, RSA is computationally intensive and consumes more resources especially as the key length rises. ECC provides design with a small key size enabling it to utilise the limited bandwidth and computations faster compared to a mobile and IoT devices. The benefits of each method, such as in Table 2, are also presented as well as the drawbacks, which include a high level of security, fast processing, and popularity. It thereby also provides considerations about disadvantages that may include increased complexity, challenging implementation and computational demands. ECC and AES are very appropriate for advanced uses of 2FA, while techniques such as RSA could be significantly slower due to key size and may not make efficient if used in mobile or any environment with low resource elements available.

Table 2: Comparison of Cryptographic Approaches for Two-Factor Authentication (2FA) in Terms of Security, Efficiency, and Key Size.

Cryptographic Method	Security Level	Efficiency	Key Size	Pros	Cons	Best Use Cases
Elliptic Curve Cryptography (ECC)	High (equivalent to 3072-bit RSA with a 256-bit key)	Very high; smaller key sizes require lower computational power	256-bit (for 128-bit security)	Strong security with smaller keys; efficient for mobile and IoT devices	Complex to implement, requires specialized knowledge	Ideal for mobile networks, IoT, resource-constrained environments
RSA	High (suitable for high-security applications)	Moderate; requires larger keys for similar security	3072-bit (for 128-bit security)	Widely used and supported; simpler implementation	Less efficient due to large key size, increases processing and memory demands	Suitable for secure email and VPN applications requiring high compatibility
AES (Advanced Encryption Standard)	Very high (symmetric encryption)	Very high for symmetric encryption	128-, 192-, or 256-bit keys	Fast, widely used in secure communications	Requires key exchange; not suitable for 2FA directly	Secure file transfer, cloud storage, closed systems
Digital Certificates (RSA or ECC)	High (depends on underlying algorithm)	High for user authentication; requires periodic validation	256-bit (ECC) / 2048-bit (RSA)	Strong identity verification; revocable, multi-factor compatible	Complex to manage; certification authority costs	High-security environments (e.g., banking, corporate systems)
Symmetric Key Algorithms	Moderate; faster but shared keys pose a risk	Very high, as keys are identical	Smaller (e.g., 128-bit)	Fast, efficient in closed systems	Insecure for public scenarios; key exchange required	Encrypted storage, local database security

Hence, 2FA network communication entities face threats from impersonation and privileged insider attacks. Current schemes lack advanced technical means like multifactor authentication and custom dictionaries, making them vulnerable to attacks. Researchers have attempted to design practical authentication and key agreement (AKA) protocols using hash functions and symmetric cryptography to enhance computational efficiency and communication overhead. However, these methods often lack forward secrecy for session key security. Public-key cryptography technology, such as ECC, RSA, and binary pairings, can enhance AKA protocol security but may lead to increased communication and storage costs. Balancing security and availability remains a challenge.

5. Digital Certificates and Device-Based Authentication

A digital certificate extends the security by checking the identity of user or device that is attempting to access that a network. This approach improves on more conventional 2FA by demanding users to produce a single certificate, which can be in physical form as a smartcard, or in an electronic form hosted in the cloud before being granted access [35]. The frequently used second factor is a digital certificate whereby 2FA is applied in secure environments such as e-learning platforms like moodle to secure user information [36]. With the connexion of user credentials to another standard level of certified digital identity, the previously mentioned threats and risks are minimised. Moreover, it is identified that certificate based 2FA system is flexible enough in order to be adapted in context of the limited access if the device has been compromised or of the person has changed position or job [37].

Another better performing security method is the use of digital certificate based 2FA, which are more lengthy for the second factor than the mere use of

codes sent through SMS or email. Of them, the user has to submit a digital certificate with the target system, which is an encrypted papers of identification provided by the certification authority. It starts with login by the user and the system asks for a digital certificate from the user. The user then provides this certificate where the system validates for credibility or otherwise. One authenticates the certificate, and you get access; if the certificate is invalid, that means no access. This makes the method more secure as it demands both the physical holding of the certificate and confirmation by the system if needed [38]. Figure 2 A basic flowchart of use of digital certificate-based 2FA within a network system and pointing to the 'verification' step.

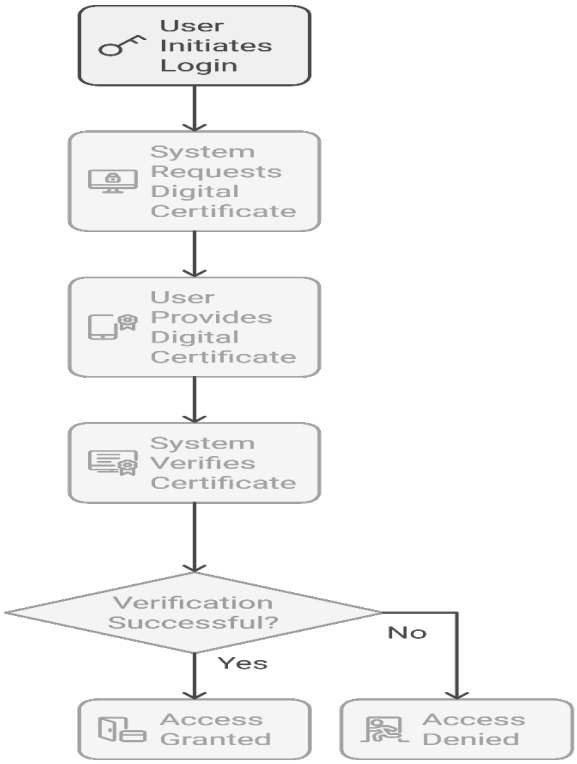

Figure 2: Digital Certificate-Based 2FA Verification Steps in a Network System.

6. ECC-Based and Biometric Authentication Process Flows

As an example of the use of the modern, ECC-based and biometrics-based, methods of 2FA, this section describes the process flows of both methods. These diagrams provide a flowchart description of each of the authentication processes, indicating the significant user-system and system-resource interactions [39].

6.1. ECC-Based Authentication Process Flow

The proposed ECC-based authentication method is effective and secure for two-factor, and ideal for environments with limited resource such as the mobile networks and the IoT application [40]. The common steps followed include key generation, data acquisition, encryption as well as template matching, for the purpose of identifying the user.

Process Steps:

a) **User Initiates Authentication**: The user begins the authentication process by providing login credentials.

b) **ECC Key Generation**: The system generates an ECC key pair for the user session, creating a digital signature based on the credentials provided.

c) **Signature Verification**: The system verifies the digital signature using the stored ECC public key to authenticate the user.

d) **Secondary Factor Verification**: An additional factor, such as a one-time password (OTP) or physical token, may be required to complete the 2FA process.

e) **Secure Access Granted**: Upon successful verification of both factors, the user is granted access to the network.

As depicted in the following Figure 3, ECC is followed for the authentication from the generation of the authentication request up to its verification and the secure access granting. This flowchart shows how ECC transforms the conventional method through which security is implemented by using cryptographic measures in details in the detailed flowchart below.

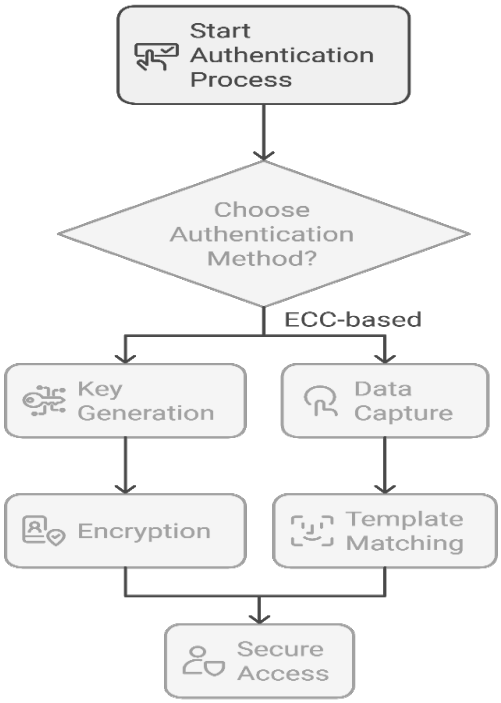

Figure 3: ECC-based authentication process.

6.2. Biometric and Behavioral Authentication in Network Security

Different biometric and behavioural techniques are powerful in the application of two-factor authentication with the use of physical characteristic features. The processes as well as benefits of biometric and behavioural authentication is also discussed, inclusive of the flowchart of biometric authentication [41].

Biometric Authentication: Biometric authentication is a method of identification that employs the person's biological characteristics such as fingerprints, iris scans, or face. This approach provides a high level of security because a biometric measure is hard to forge. Biometric authentication is widely employed in hand-held devices, security-sensitive structures, and other security-sensitive contexts [42].

Process Steps:

a) **Biometric Enrollment**: The user initially registers their biometric data (e.g., fingerprint or facial scan) with the system, which securely stores this data as a template.

b) **User Initiates Authentication**: During subsequent logins, the user provides the biometric input.

c) **Biometric Data Capture and Comparison**: The system captures the live biometric data and compares it with the stored template to verify the user's identity.

d) **Secondary Factor Verification**: If required for 2FA, an additional factor such as a password or OTP is verified.

e) **Secure Access Granted**: Upon successful verification of both factors, access is granted.

Behavioral Authentication: Behavioural authentication is gradually being developed based on which behaviours are continuously monitored, including typing speed, the way people hold devices , and browsing history. Unlike biometric authentication which is basis on physical characteristics of an individual, behavioural authentication is instantaneous and practises the utilisation of actions from the user. This method introduces a new layer on top of 2FA, increase security at the same time keeping it user friendly [43]. A

flow chart of biometric authentication system is as shown below in Figure 4 below integrating all the steps of biometric data capturing and secure access.

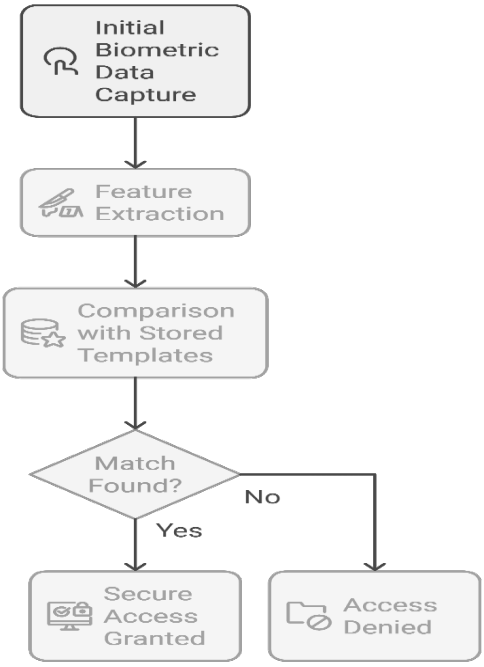

Figure 4: Flowchart of the Biometric Authentication Process.

7. Comparative Analysis of Security and Usability in 2FA Systems

The work on using 2FA in networked systems relating to this research is as follows: The degree of the security of a given networked system can be increased using 2FA while requiring the user to provide two forms of identification before gaining access to a computer. There are also enhanced forms of 2FA, like ECC, digital certificates, and biometrics, which add more layers of security, but issues of cost increase, solution complexity, and user receptiveness [44], [45]. In this section, the authors discuss a comparison of simple and current types of 2FA, analysing them based on parameters such

as the level of protection, the difficulty of application, and the level of user satisfaction. This way, through achieving the right mix of security and convenience, the 2FA systems that are set up and controlled by the network administrators, are more likely to be adopted, and, thus, more effective [46].

Traditional Methods vs. Advanced Methods: As a result traditional methods are easy by the users compared to modern methods of technology, in addition they do not demand more gadgets or expert inputs hence they are convenient. However, they have a middle rated security and are prone to usual cybercrimes including phishing and SIM-swapping [47]. Although these methods allow better security through such features as cryptographic techniques or unique biological characteristics, they generally entail extra setup or compatible hardware and, as a result, can complicate the operation of the programme and cost more [48].

Balancing Security and Usability: Although there are even more sophisticated approaches, like biometric authentication, where the security level is high, but the inconvenience of use can be moderate, there can exist issues with implementation costs and usability by users. For organisations where enhanced security is necessary, the methods like ECC and digital certificates should be implemented because they occupy a higher level of protection against cyber threats [49]. They, on the other hand, are more appropriate in environments with less security protocol and therefore being more quickly accessible. Table 3 presents information on several 2FA approaches as compared to their security levels and ease of use. Text messaging, email and conventional OTPs are reasonably secure because they are vulnerable to phishing and SIM-swapping. Mechanisms like, hardware tokens, biometric, digital certificates and ECC based 2FA offer much higher 2FA security through cryptographic method, physical security or biological security.

Table 3: Usability and Security Levels of Traditional vs. Advanced Two-Factor Authentication (2FA) Methods

2FA Method	Security Level	Usability Level	Advantages	Disadvantages
SMS-Based OTP	Moderate	High	Easy to use and widely supported	Vulnerable to SIM-swapping and phishing attacks; relies on cellular network availability
Email-Based OTP	Moderate	High	Convenient, no extra device needed	Susceptible to phishing and email account compromise; relies on email security
App-Based OTP (e.g., Google Authenticator)	High	Moderate	High security, not reliant on cellular network	Requires app installation and setup; potential inconvenience if device is lost
Hardware Tokens	High	Moderate	Strong physical security layer, independent of other devices	Physical token can be lost or damaged; additional cost for tokens
Biometric Authentication	Very High	Very High	Convenient, fast, and user-friendly; hard to replicate	Privacy concerns; requires compatible device hardware; potential for false rejections
Digital Certificate-Based 2FA	Very High	Moderate	Strong identity verification, revocable access	Complex to set up and manage; cost associated with certificate authority services
Elliptic Curve Cryptography (ECC)-Based 2FA	Very High	High	Efficient for mobile and low-power devices, highly secure	Complexity in implementation, specialized knowledge required

8. Implementation Considerations

Applying different types of the 2FA in real-world networks should meet certain criteria such as cost, scalability and compatibility. Although techniques like ECC, digital certificates, and biometrics are highly secure, their implementation differs with the organisation's network topology, user population, and cost factor [50].

a. **Cost**: Most developed 2FA systems have a very high cost when it comes to the first stage, especially if biometric devices or hardware tokens are used. While making use of biometric systems, organisation may need to procure specialised hardware such as fingerprint scanners or facial recognition scanners; this comes with high cost of installation per each network and constant maintenance costs. In the same manner, reliance on a technique like digital certificates involves costs of obtaining the certificates and /or renewing from certifying authorities. In organisations with many users, the costs of such equipment as hardware tokens or biometric devices for equipment issuance and control must be compared with anticipated enhancement of security [51].

b. **Scalability**: Another important consideration is scalability due to the size of a particular network or the variety of users in an organisation. While testing, app and SMS OTPs are easier to scale, whilst Biometric authentication, Digital certificates may need many changes at the hardware and infrastructure level. ECC-based authentication is more beneficial here because it turns out to be computationally reasonable and ideal for portable gadgets and IoT things, indeed ideal for the networks that are expected to be open

to a larger audience. As mentioned earlier and more important for scaled implementations, organisations might need to roll out a set of 2FA mechanisms customised for various users [52].

c. **Compatibility**: To avoid the interruption of new 2FA solutions the compatibility with preexisting structures should be maintained. For example, digital certificates are compatible with PKI based systems while may not be compatible with older system or less standardised systems. ECC is a relatively weaker cryptographic algorithm as compared to RSA and therefore is compatible with current generation mobile devices; however, it may need some modifications for those organisations or companies which still have archaic systems embedding only RSA algorithms. Biometric systems need the compatible hardware in the device, which may be an issue when users connect to the network via the own computers or from different places. Organisations should undertake compatibility evaluation studies before implementing the frameworks so that they can avoid many of the pitfalls [43].

d. **User Training and Support**: These new and more sophisticated 2FA methods, in particular, those that the user understandably has no understanding of (like digital certificates or biometric authentication), need to be promoted and supported. As with all novel approaches, users have to know how to go about these procedures such as hardware token handling, certificate configuration or even biometric capture. User training and user support should be provided so that user does not resist the new IT security policies and procedures [54].

e. **Security Policy and Management**: By and large, it is impossible to speak about effective implementation of 2FA not only in terms of technological infrastructure but it has to be tied to an organisation's security policies framework. Tokens, biometric data and digital certificates should therefore be enjoined to higher security standards so as to discourage any form of easy access. Also, organisations need to be very particular about lost tokens, compromised biometric data, or revoked certificates to ensure long-term security [55].

These issues have been discussed to help an organisation come up with a decision of implementing advanced 2FA methods in their network taking into account of the realistic security measures without compromising the usability. Such planning therefore guarantees that reinforcement of security in the network is stable and can easily be scaled as well as integrated into its architecture.

9. Conclusion

Network access control cannot be complete without Two-factor authentication (2FA) but trends like using SMS or emails for OTPs are proving ineffective against new generations of cyber threats. This paper explored other types of second factor authentication as providing better solutions for advanced attacks; these integrated Elliptic curve cryptography (ECC), certify by a digital certificate, and biometric authentication; all providing better security and more robust client models than regular systems. This analysis described a model that posited high security and complemented it with usability appropriate for networked environments. Other—including ECC

based 2FA—offers efficient cryptographic 2fa more suitable in mobile and low powered devices; while digital certificates enhance enhanced identity proofing mechanisms. Applications of biometric authentication make use of biological characteristics in order to reduce the possibility of unauthorised access to the system. Through the estimates proposed in the study, it is possible to learn about the best strategies to apply in adopting easy-t0-use 2FA systems that can resist modern security realities. Possible future works may involve further develop procedures that use such technologies like applied machine learning and artificial intelligence for developing more intelligent and adaptive authentication systems. Such systems could vary the needs for further authentication based on the behavioural characteristics and the relative estimated threat level and would offer the administrators convenient means to combat new threats. In doing so, this paper continues to build up the framework for resilient, scalable and dynamic network security architectures to address emerging threats in cyberspace environment.

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 Proceedings of the 2019 ACM Conference on Human Factors in Computing Systems, 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, Springer, 2021, pp. 145–156.

[6]. P. Rannenberg, V. Varadharajan, and C. Weber, "Evolution of Authentication Systems: Towards Multi-Factor Authentication," in Proceedings of the 13th International Conference on Security and Privacy in Communication Networks (SecureComm 2018), Singapore, 2018, pp. 619–628.

[7]. M. Alotaibi and K. Elleithy, "User Authentication Factors: From Single-Factor to Multi-Factor Authentication," in Advances in Computer and Electrical Engineering, 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," International Journal of Scientific 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, no. 9675, pp. 1–16, 2023.

[13]. K. Liu, Z. Zhou, Q. Cao, G. Xu, C. Wang, Y. Gao, W. Zeng, and G. Xu, "A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing," Applied Sciences, vol. 13, no. 4425, pp. 1–19, 2023.

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

[15]. J. T. Sample and P. J. Blythe, "Usability vs. Security in Two-Factor Authentication," Information Security Journal: A 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 Magazine, 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: 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 Journal, 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 Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1345–1383, 2021.

[22]. F. Kaabar and M. R. Farooq, "Security Frameworks in Multi-Factor Authentication Systems," Journal of Information Security Applications, vol. 64, p. 102685, 2022.

[23]. S. Davis, "Application of Biometrics in Digital Certificate-Based Authentication," IEEE Transactions on Information Forensics and 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," Journal of Information Security and Applications, 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 Transactions on Mobile Computing, vol. 19, no. 12, pp. 2755–2769, 2020.

[29]. R. Ortega and T. Tomic, "Security of Advanced 2FA Methods in Cloud Environments," Cloud Computing and Services Science, New York, NY: Springer, 2021, pp. 98–113.

[30]. N. Rashid *et al.*, "Elliptic Curve Cryptography for Low-Power 2FA Devices," IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1601–1613, 2021.

[31]. J. Warner, "Comparative Study of OTP Methods in 2FA," Information Security Journal: A Global Perspective, vol. 30, no. 2, pp. 87–98, 2021.

[32]. T. Gligor, "Device-Based Authentication Using ECC," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3936–3946, 2021.

[33]. S. Nakamura and E. Sakurai, "Behavioral Biometrics in Adaptive Authentication," ACM Transactions on Information Systems, vol. 41, no. 2, pp. 78–96, 2023.

[34]. R. Gallo, "Modern 2FA in Industrial IoT: ECC and Beyond," IEEE Industrial Electronics Magazine, vol. 14, no. 2, pp. 23–33, 2020.

[35]. G. M. Mohammad and S. Benlamoudi, "Public Key Infrastructure and Certificate-Based Authentication," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 673–690, 2022.

[36]. T. Sampson, "Digital Identity Verification with Certificates," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 4829–4843, 2022.

[37]. Y. J. Lim *et al.*, "Advances in Mobile Biometric Security," IEEE Access, vol. 9, pp. 168451–168460, 2021.

[38]. E. Russo, "Security Analysis of ECC-Based 2FA in Mobile Apps," Mobile Security Journal, vol. 15, no. 4, pp. 245–256, 2023.

[39]. C. Huang, "Two-Factor Authentication in Financial Networks," Financial Services Security, Boston, MA: McGraw-Hill, 2021, pp. 167–183.

[40]. S. Ravi and M. Arya, "Next-Gen Authentication Methods in IoT," Journal of Network and Computer Applications, vol. 176, p. 102909, 2021.

[41]. N. J. Kim and J. H. Park, "Exploring Machine Learning in 2FA," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 8, pp. 3423–3435, 2021.

[42]. M. C. Kerr *et al.*, "Implementing 2FA in Hybrid Cloud Environments," Cloud Security Journal, vol. 22, no. 5, pp. 316–327, 2022.

[43]. W. Li *et al.*, "Scalable 2FA for Mobile Banking," Journal of Banking & Finance Security, vol. 10, no. 4, pp. 55–67, 2021.

[44]. R. Singh, "Cost-Effective Biometrics in 2FA Solutions," IEEE Security & Privacy, vol. 18, no. 6, pp. 78–85, 2020.

[45]. T. Andrews, "Device Management in Certificate-Based Authentication," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 5, pp. 3497–3507, 2020.

[46]. C. E. Torres, "Usability Issues in Multi-Factor Authentication," International Journal of Human-Computer Interaction, vol. 37, no. 4, pp. 320–329, 2021.

[47]. J. Swartz and L. Evans, "Security Standards for App-Based 2FA," Journal of Information Systems, vol. 43, no. 1, pp. 25–37, 2020.

[48]. S. Lee and J. M. Choi, "Behavioral Analysis in Adaptive Authentication," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 3, pp. 269–280, 2020.

[49]. A. Walker, "Passwordless Authentication in Modern Networks," Network Security Journal, vol. 34, no. 7, pp. 19–28, 2022.

[50]. Z. T. Li and P. M. Koh, "Simulating and Securing OTPs with ECC," IEEE Transactions on Cloud Computing, vol. 8, no. 3, pp. 1274–1282, 2020.

[51]. J. S. Wang *et al.*, "Multi-Factor Authentication in Distributed Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 1, pp. 59–72, 2021.

[52]. B. Fields, "Hybrid Cryptography in 2FA," IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 673–688, 2021.

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

[54]. M. Bhattacharjee, "Biometric Trends in Secure Authentication," IEEE Access, vol. 10, pp. 32244–32256, 2022.

[55]. S. K. Singh, "Performance Metrics in Multi-Factor Authentication," International Journal of Information Management, vol. 62, p. 102439, 2022.