Volume 12, No.9, September 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

UGC Approved Journal

RESEARCH PAPER

Available online at http://www.jgrma.info

MULTI-FACTOR AUTHENTICATION IN MOBILE APPLICATIONS: A SURVEY OF METHODS AND CHALLENGES

Mr. Sachin Manekar[1]

Sachin.manekar@meu.edu.in

[1] Assistant Professor, Mandsaur University, Mandsaur, Department of Computer Sciences and Applications

Abstract: With the increasing number of attacks on sensitive personal and financial information, Multi-Factor Authentication (MFA) has become an essential security tool and especially in mobile apps. MFA can further increase security by mandating that the user prove their identity using multiple authentication factors, thus providing a more robust security than traditional Single-Factor Authentication (SFA) mechanisms, which are more susceptible to theft and negligence and are also prone to attacks. Advanced modern mobile devices offer the flexibility to integrate MFA, which aligns with regulations, while still being very convenient to use. Through this survey, various MFA techniques deployed on mobile devices will be analyzed, including biometric authentication, hardware and software tokens, SMS-based One-Time Passwords (OTPs), behavioral biometrics, and dynamic authentication schemes. It considers the use, security implications, and implementation difficulty of each method. The paper also discusses real-world scenarios of cyberattacks, assesses prevailing threats, and presents current developments in mobile cybersecurity. The survey concludes with a description of potential future research directions that could enhance the effectiveness and usability of mobile-based MFA systems.

Keywords: Multi-Factor Authentication (MFA), Mobile Security, Authentication Methods, Biometric Authentication, Security Challenges.

1 INTRODUCTION

Authentication has been a crucial process for confirming the identity of a person or system attempting to access sensitive resources. The process is particularly crucial as one tries to deal with sensitive personal, financial or corporate information on mobile platforms[1]. Although PINs and passwords are still used in conventional authentication techniques, they have become increasingly ineffective in the current mobile environment. These credentials tend to be shared, are easily compromised, and can be brute-forced or phished; thus, they cannot adequately protect mobile data.

Mobile applications are dynamic and have security vulnerabilities; therefore, stringent and flexible authentication methods are necessary [2]. Mobile platforms are embracing Multi-Factor Authentication (MFA), and it is becoming increasingly common to see users who must authenticate using two or more independent factors, such as information about them (password), their possessions (device or OTP), and their characteristics (biometrics).

Cybercriminals have an enlarged attack surface, coinciding with the increased proliferation of mobile devices and applications. Mobile devices have begun to generate significant amounts of internet traffic and have become the target of phishing, malware, session hijacking, SIM swapping, and unauthorized access. In many cases, users themselves contribute to these risks quite readily by downloading apps on untrusted sources, using unsecure networks as well as not updating the software timely[3]. Mobile data breaches have been on the rise according to recent threat reports with a large portion of them being directly related to breached authentication credentials[4].

MFA provides more stages of verification, it significantly lowers the risk of identity theft, data breaches, and unauthorized access. MFA examples that can be used in a mobile environment can be biometric scan systems, time-based one-time password (TOTP), hardware tokens, pushing notifications on an app, or SMS/email OTP. Those techniques take advantage of the connectivity and sensors of the mobile devices to enrich security without requiring excessive efforts on behalf of the user[5]. Nevertheless, there are some challenges that come with the integration of MFA in mobile applications [6]. Poor usability, including complexity or even login friction, can be a turnoff to the user. Its effectiveness is also curtailed by privacy issues related to biometric data, technical incompatibility of different operating systems and devices, as well as issues related to phishing, SIM swapping and man-in-the-middle attacks. Push-based MFA has the advantage of requiring a stable internet connection and a functioning device, which is another potential failure point.

There are new movements in mobile MFA, including QR code-based logins, behavioral biometrics, and the use of device-specific identifiers such as MAC addresses to authenticate [7]. With further development of MFA, this survey evaluates the efficacy of current MFA techniques, considers practical issues of direct implementation, and describes the future prospects of the domain. It is expected to provide developers with up-to-date best practices, as well as to outline the areas where additional innovation is needed to ensure secure, seamless, and easy-to-use mobile authentication mechanisms.

1.1 Structure of the paper

This paper is organized as follows: An overview of single-factor versus multi-factor authentication is given in Section II. The categorization of multi-factor authentication techniques in mobile apps is examined in Section III. The challenges of multi-factor authentication for mobile applications are addressed in Section IV. Case studies and pertinent literature are reviewed in Section V, and future study topics are suggested in Section VI.

2 MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that provides a higher level of protection for computing devices and important services, as it requires users to authenticate themselves based on two or more unique factors. They are often categorized into one of three types: the user's possessions (such as a smartphone or security token), knowledge (such as passwords or PINs), or identity (such as fingerprints or facial patterns). The combination of these factors makes MFA a very useful improvement of the authentication procedure over the current password-and username-based single-factor authentication schemes[8]. Even when one of the factors is compromised, the attacker will still have to pierce through the other layers and there is a significant decrease in the chances of unauthorized access. The example of an ATM withdrawal can be used: the physical card (possession) and the PIN (knowledge) are usually required, but one can also add a one-time password (OTP). As a typical part of MFA, biometrics provide automated recognition using behavioral or biological features that create strong security.

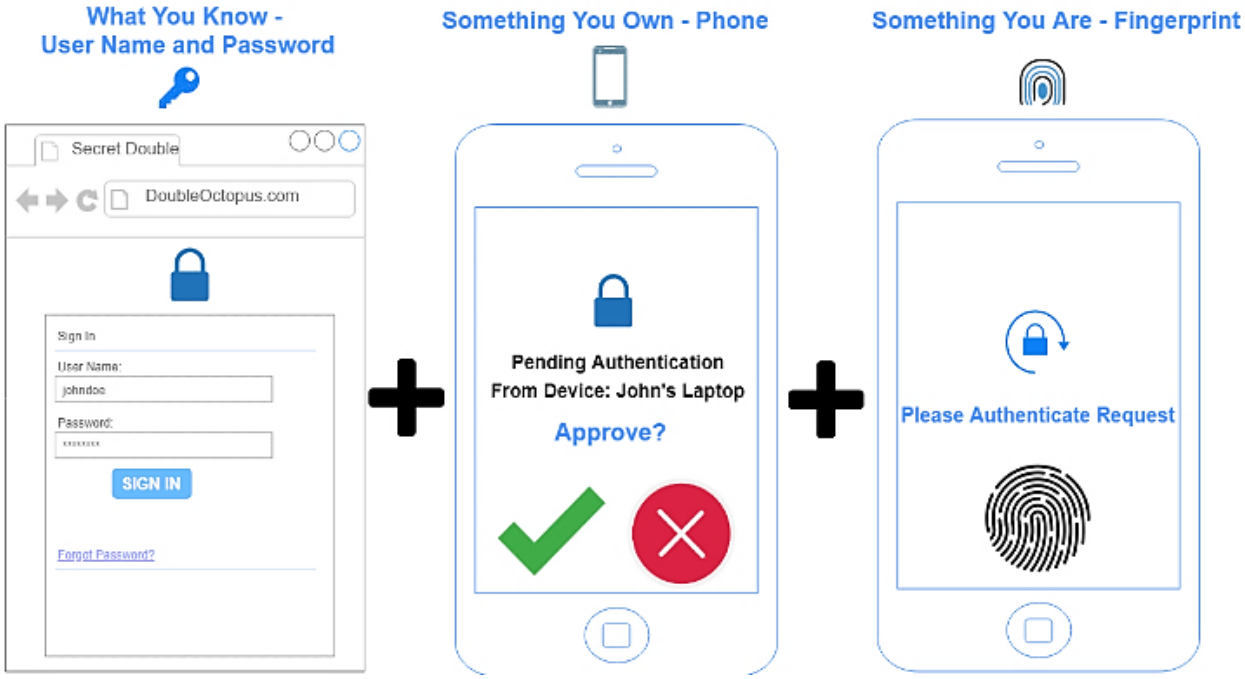

Figure 1: Multi-factor authentication

MFA's basic idea is that the system can stop unwanted logins even if one of the authentication factors is compromised, since further authentication is still needed, as illustrated in Figure 1. It is much better to use this layered approach, as it provides strong protection for systems that rely on just one authentication method.

2.1 Authentication Factors

Multi-Factor Authentication (MFA) enhances security by combining two or more different kinds of authentication elements, include things you possess, something you know, and something you are. Every element contributes a unique degree of security.[9]. Figure 2 illustrates the interplay of these general authentication factors, where one or more combinations are used to confirm a user's identity before allowing access.

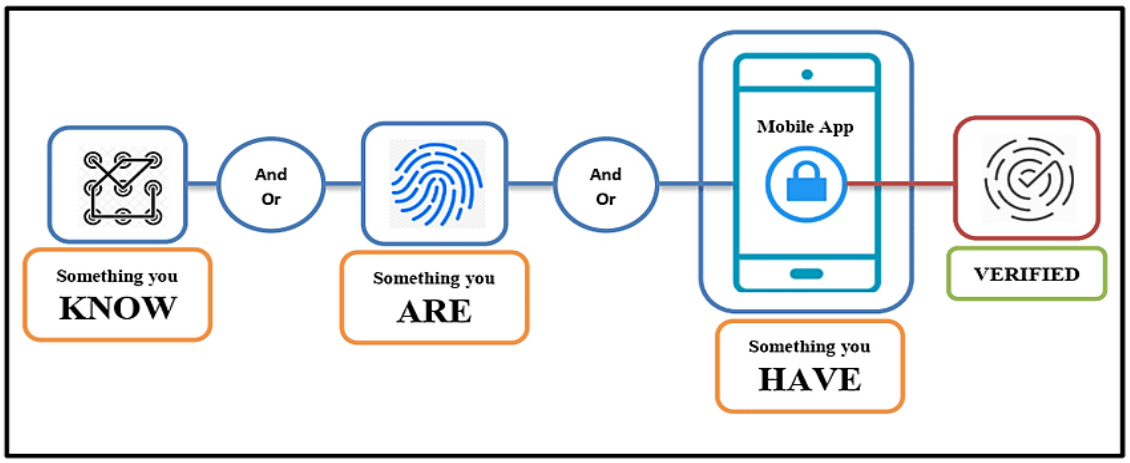

Figure 2: Types of General Authentication Factors

There are three commonly accepted categories of authentication elements:

- Type 1 – Secret handshakes, code phrases, passwords, PINs, and combinations are a few instances of Things You Know. This covers whatever you can remember and, depending on the circumstance, type, say, perform, execute, or remember in another way.
- Type 2 – Keys, mobile phones, smart cards, USB drives, and token devices are all examples of physical objects that fall under the category of "Something You Have." A token device can create a time-based PIN or compute a response from a challenge number provided by the server.
- Type 3 – Anything is including any part of the human body that may be submitted for verification, such as fingerprints, palm scanning, voice verification, facial recognition, retinal and iris scans, and facial recognition.

2.2 Single-Factor vs. MFA and Two-Factor Authentication

Authentication mechanisms can be broadly categorized based on the number and nature of identity verification factors they employ. In this section, a comparison of Single-Factor Authentication (SFA), Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) is made, with focus on their security implications, applicability and practical use[10]. Figure 3 illustrates the authentication method history: Single-Factor Authentication uses knowledge-based authentication such as a password; Two-Factor Authentication includes an additional possession factor, such as a smartphone or OTP; and Multi-Factor Authentication incorporates access authentication such as the application of different biometrics, including facial recognition or fingerprints, for increased security.

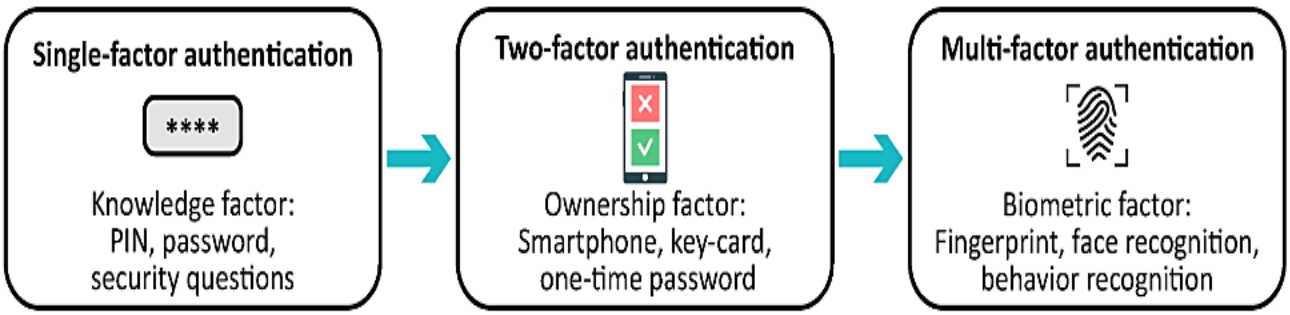

Figure 3: Single-factor vs multi-factor authentication

2.2.1 Single-Factor Authentication (SFA)

Single-factor authentication provides the least protection to an access-control system, as it utilizes only one form of credential, commonly a password or personal identification number (PIN). Although SFA, due to its ease of use and low implementation cost, is widely used, it is more vulnerable to various online dangers, including phishing, credential stuffing, brute-force attacks, and social engineering. When using a singular basis of a knowledge factor (something the user knows), there is a major failure point of failure particularly at instances when the user reuses weak or default passwords across different platforms.

2.2.2 Two-Factor Authentication (2FA)

A PIN delivered by SMS or acquired through an authenticator app is an example of a possession factor. Two-factor authentication strengthens security by combining two authentication factors of distinct kinds[11]. This multi-layer implementation provides

significantly higher degrees of assurance that criminals will be unable to compromise their way to unauthorized access, since, unless a threat actor has physical access to the victim's device, stealing both elements will generally require stealing the victim's device as well as their credentials. 2FA represents a reasonable tradeoff that balances security and user convenience, and therefore has become the go-to security measure for protecting online or web-based accounts, financial networks, and corporate systems.

2.2.3 Multi-Factor Authentication (MFA)

Multi-Factor Authentication is an extension of the 2FA model, adding three or more authentication factors, including but not limited to factors based on locale, factors based on behavior and/or factors based on inherence (biometrics). MFA brings substantial enhancement to the authentication mechanism by adding an extra layer of security in the form of a multifold defense, which limits the chances of account theft even when partial credentials are compromised[12]. Moreover, more complex MFA systems are likely to involve adaptive or risk-based authentication policies, where those needs are scaled in accordance with contextual cues like the location of the login, device fingerprinting, and authentication patterns. Although SFA and 2FA have different levels of security and usability, MFA is the strongest form of authentication in high-stakes and sensitive areas. However, it cannot be applied efficiently without a careful design, user training, and consistent testing of changing threats.

2.3 Evolution of Mobile Security Needs

Since the emergence of smartphones as a necessity for conducting personal and professional tasks, mobile devices have become the most targeted targets. Initially, there were basic defenses, including screen locks and PINs. Nevertheless, the requirements of a stronger security increasingly became context-aware as mobile applications started managing sensitive data, including banking, healthcare, and enterprise data[13]. Contemporary mobile devices are equipped with sophisticated sensors, biometric authentication scanners, and secure hardware, enabling smoother and safer authentication. In an attempt to satisfy user demands pertaining to speed and security, most services, particularly those in the financial industry, have now implemented the concept of adaptive, multi-layered security solutions, taking into consideration contextual aspects, including device location[14]. Additionally, regulatory standards such as GDPR, HIPAA, and PSD2 are mandating Multi-Factor Authentication (MFA) as a regulatory requirement, which continues to spur innovation in mobile-based authentication solutions.

2.4 MFA in Mobile Applications

The necessity of secure and reliable authentication is particularly evident in high-risk areas of mobile application usage. These various applications highlight that trust, user data protection, and compliance are core areas of utilizing MFA through mobile applications, as illustrated in Figure 4.

Figure 4: MFA in Mobile Applications

The critical uses of MFA in Mobile systems include the following ones:

- **Banking and Financial Services**: Financial information is sensitive, so mobile banking apps are the main target of cyber-attacks. MFA is widely used here, often combining passwords with OTPs (one-time passwords), biometric verification, or

app-based push notifications. Regulatory requirements like Strong Customer Authentication (SCA) under PSD2 have made MFA mandatory in many regions.

- **Healthcare**: Mobile health (mHealth) applications manage electronic health records (EHRs), telemedicine, and patient monitoring. Given the sensitivity of patient data, HIPAA compliance in the U.S. and similar regulations globally necessitate robust authentication protocols. Biometric MFA solutions are gaining traction due to their balance of usability and security.
- **E-Commerce**: Online retailers increasingly integrate MFA into their mobile platforms to prevent account takeover and fraud. Adaptive authentication where additional factors are triggered based on transaction value or user behavior is commonly used to balance user convenience and risk management.
- **Enterprise Applications**: Mobile device usage in the workplace, driven by Bring Device (BYOD) policies and remote work trends, has raised concerns about unauthorized access to corporate resources. MFA is essential in securing enterprise mobile apps, often implemented through mobile device management (MDM) and identity federation systems (e.g., SSO combined with MFA).

3 CLASSIFICATION OF MFA METHODS IN MOBILE APPLICATIONS

Mobile applications have become an integral part of everyday life, often handling sensitive data and financial transactions. Multi-factor authentication (MFA) techniques have been numerous to prevent unauthorized use. The section will take a look at the main MFA techniques used in mobile applications and how they work, their strengths, and their weaknesses[15]. All the approaches have a trade-off in terms of security, usability and complexity of implementation. The security needs will determine which MFA technique is used, the demographics of users and the technological capabilities of the mobile app. There are multiple layers of identity verification[16]. used in modern mobile apps because they are based on multiple MFA means. Such methods are usually categorized based on the authentication factor they are based on, Factors based on possession, knowledge, inheritance, and context awareness are among them. The subsequent subsections give the in-depth classification and discussion of the most common approaches to MFA used in the mobile environment.

3.1 Existing MFA Methods and Mobile Systems

Mobile app-specific Multi-Factor Authentication (MFA) options. The analyzed studies introduce creative solutions that enhance security, albeit with some usability and implementation issues. Using passwords, OTPs, security questions, facial recognition, and speech recognition together makes mobile banking transactions safer. Some researchers introduce a new module-based system for push notifications based on Key cloak which makes it simpler to support MFA in several applications. Researchers have proposed an MFA algorithm that uses MAC addresses for secure device-based authentication, which checks QR codes and contains user information. To gain access, individuals are verified using login information and biometric data, which occurs only when they are within a designated area of the access point. By relying on the Internet for MFA logins, people realize that important identity providers raise risks and need better safeguards [17]. All these investigations, taken together, describe how MFA works on mobile devices and highlight different ways to improve security and make authentication easier for users illustrated in Figure 5.

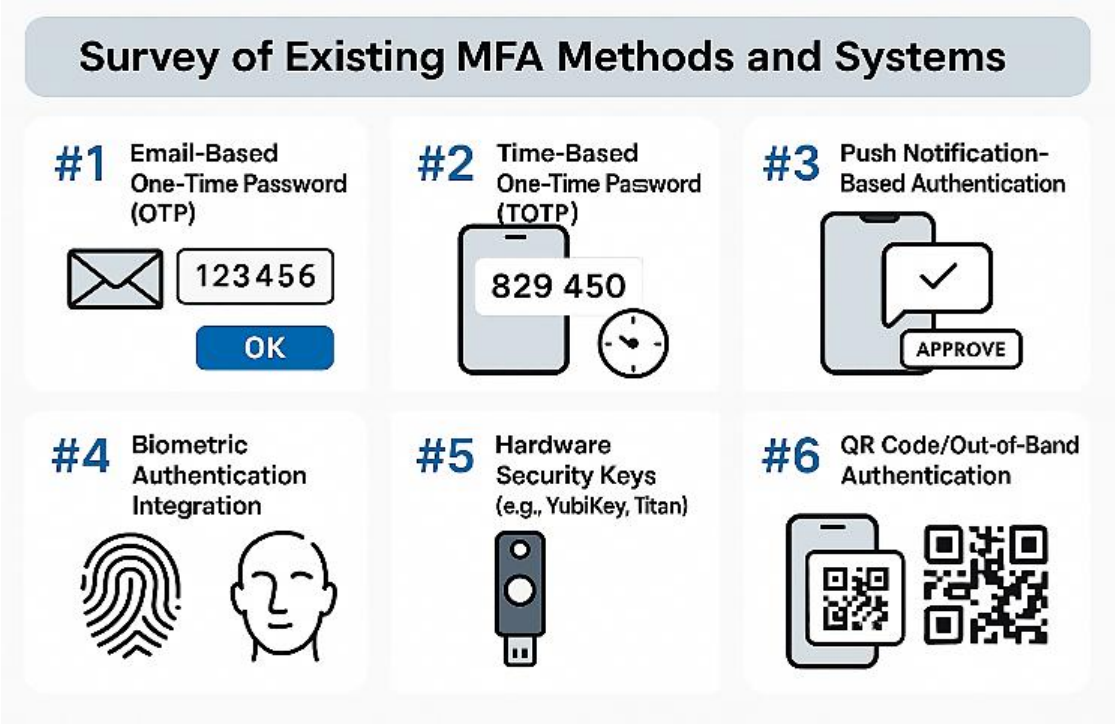

Figure 5: Methods of MFA used in a Mobile application

Here are the MFA techniques used in mobile applications are as follows:

- **Email-based One-Time Passwords (OTP):** Many people use MFA via SMS or email because these methods are straightforward and relatively easy to implement. When users begin logging in, they are sent a one-time code to their phone or email, which they must enter to access the platform. Although it makes things easier, this approach is not secure, as it can be compromised by SIM swapping, phishing, or someone intercepting the signals over an open Wi-Fi network [18]. Despite these issues, SMS and email OTPs remain prevalent in regions where implementing advanced authentication systems is challenging.
- **Time-Based One-Time Passwords (TOTP):** TOTP improves security by producing codes that are only good for a brief period of time, usually 30 seconds. The current timestamp and a shared secret are used to generate these codes, guaranteeing synchronization between the user's device and the authentication server. Authenticator programs that use TOTP, such as Google Authenticator and AUTH, provide a more secure option than OTPs based on SMS. Nonetheless, when the machine containing the authenticator app becomes compromised or lost, users are likely to encounter problems regaining their account.
- **Push Notification-Based Authentication:** The authentication using push notifications is more secure and also more comfortable as users can accept or reject the attempts to log in using their trusted devices. This approach simplifies the process, as there is no need to manually enter codes, making it smooth and easy to use. It, however, is dependent on a working internet connection and can end up being at risk in case the user device is infected. It is necessary to secure the notification channel and the device to preserve the integrity of this authentication mechanism.
- **Biometric Authentication Integration:** Biometric type authentication verifies a user's identity by using their distinguishing physical characteristics, such as fingerprints or facial recognition. The mainstream use of biometric sensors in new smartphones has made it easier to incorporate this technique into the daily life Multi-Factor Authentication (MFA) platform. Biometrics offer strong security and a seamless user experience. However, concerns persist regarding data privacy, the irreversible nature of biometric data, and the potential for spoofing or system manipulation[19].
- **Hardware Security Keys (e.g., YubiKey, Titan):** A very secure kind of multi-factor authentication is offered by hardware security keys, which require users to physically own a specific device, such as a YubiKey or Google Titan, to complete the login process [20]. These keys provide robust protection against phishing, man-in-the-middle attacks, and credential theft, as they comply with open standards such as Universal 2nd Factor (U2F). However, the need to carry an additional device and the associated costs may hinder widespread adoption, especially among casual users or those seeking minimal friction in authentication workflows.
- **QR Code/Out-of-Band Authentication:** QR code-based or out-of-band authentication involves scanning a code displayed on one device using another trusted device, allowing secure login without transmitting credentials over potentially compromised channels [21]. This method helps mitigate risks such as keylogging and phishing attacks by isolating the authentication process. However, its effectiveness depends heavily on the security of both devices involved, as compromise of either can undermine the overall protection.

4 CHALLENGES IN MFA FOR MOBILE APPLICATIONS

The security of the system and the usability of the app may be compromised when Multi-Factor Authentication (MFA) is used in mobile applications. Such problems include having a dependent network, device-related glitches, exposure to hackers, privacy risks, the use of multiple operating systems, and user experience issues[22]. To address these difficulties, businesses should mix new technology, great user design and strong security in their mobile apps to boost the use of MFA, are includes:

4.1 Network Dependency and Interception Risks

Services could be disrupted or stolen if networks are compromised or intercepted. One-Time Passwords (OTPs) and other mobile phone-based methods for MFA need the phone to communicate with a network to work. For example, the reliability of the app may lead to several risks, such as another remote person reading the codes that authorize the activity, either through SIM swapping or a man-in-the-middle attack. The only means to handle these risks should not be secure transmission procedures and MFA which depend on the Internet.

4.2 Device Loss and Identity Lockout

The theft or loss of a mobile device may lead to Users are unable to access their accounts, particularly where the device is used as the primary authentication mode. This scenario presents a major problem, where it may interfere with delivery of vital services, besides putting accounts under serious security threat [23]. Hence, it is crucial to strike a balance between security and usability. Secure, yet user-friendly, recovery schemes should be applied that enable the user to resume use of the system without compromising their integrity.

4.3 Malware and Phishing Attacks

Phishing and malware attacks are also deployed on mobile devices, which represent a potential threat to the efficiency of Multi-Factor Authentication (MFA)[24]. Malicious software can monitor authentication codes or simulate genuine logins, tricking the

user into providing their credentials. Such threats highlight the need of having solid vetting procedures of apps, security maintenance and training of users to detect and avoid such attacks. In addition to enhanced user awareness and safe use of practices, they are critical in ensuring the integrity of MFA systems.

4.4 Privacy Concerns with Biometric Data

Biometric authentication is convenient and easy to use but raises serious privacy concerns. Fingerprints or facial features that are used as biometric identifiers cannot be replaced in case of a breach, as opposed to passwords. Sensitive data that needs to be stored, transmitted, and processed should have high security levels to prevent unauthorized access or misuse. Security of biometrics is a fundamental component in the survival of biometric-based MFA systems as well as ensuring consumer confidence in such systems.

4.5 Compatibility and Platform Fragmentation

The use of MFA on various mobile devices and operating systems is extremely challenging. People use online services with various software and hardware setups; thus, it may result in inconsistent behavior, usability problems, and security risks[25]. Such differences complicate the ability to provide uniform and safe MFA experience across the board. With MFA being deeply embedded in the daily systems, it is crucial to adjust the authentication to be cross-platform and maintain its performance in terms of accessibility and safety by all users.

5 LITERATURE REVIEW

This section presents a comprehensive literature review on Multi-Factor Authentication in mobile applications, highlighting various methods and their associated challenges. A summary of the reviewed studies is provided in Table 1, which includes sections such as study focus, approach, key findings, and identified challenges or limitations, offering a concise overview.

Hasan et al. (2025) examine the evolution of contemporary mobile authentication techniques, classifying them into approaches based on touchscreen, color, biometrics, graphical, behavioral, keyboard, password, and gaze. Examining the advantages and disadvantages, with an emphasis on issues such as security and usability, is its goal. Additionally included are standard datasets and metrics for performance evaluation. Lastly, the research gaps and future goals in this important and developing field of study are examined. Authentication and cybersecurity have become the foundation of the Internet of Things. The most crucial and safest accounts in the world can only be opened with it. Passwords will undoubtedly be present after authentication is finished.[26].

Aciobăniței (2024) introduces a novel integration of a Push Notification module within Keycloak, an established open-source identity and access management solution. Our approach simplifies the deployment of effective MFA by encapsulating the intricacies of push notification services into easily manageable modules. By leveraging Keycloak's extensive capabilities, we enable seamless MFA integration, allowing developers to implement secure and sophisticated authentication mechanisms with minimal effort. Our proof of concept implementation, publicly available on Github, demonstrates a significant reduction in the development overhead associated with MFA, promoting its adoption across various applications[27].

Syahreen et al. (2024) suggest using several authentication procedures to raise a system's security level, whether it is hosted on-site or in the cloud. Nevertheless, little research has been done on standards and suitable authentication frameworks that meet an organization's requirements. Using five main databases—Scopus, IEEE, ScienceDirect, SpringerLink, and Web of Science—a thorough literature review of a Multi-Factor Authentication framework was conducted. To address specific system and data security issues, a range of authentication techniques were implemented. Biometric authentication, which takes into account the individuality of the user's biological identity, is the most widely used authentication technique. A pilot test or experiment is necessary in the future for most of the suggested solutions, which were proof of concept[9].

Salman (2023). Provide a multi-factor authentication-enabled safe access control system included in Android phones. To do this, authorized users are listed in a database that the access control system may access when the user authenticates themselves using both their smartphone's biometric data and a login and password. Once the user reaches within 10 meters of the access control system, they are asked to provide their biometric credentials. The database compares the user's keys and grants access after successful authentication. The goal of this design is to lessen the instances where someone enters a restricted area without authorization. The observed outcomes unmistakably satisfy the physical access control systems' security requirements[28].

Wang and Wang (2022) make a significant first step in methodically investigating security proof failures in mobile device multi-factor authentication systems. Using the random oracle model, they first look at the underlying reasons why insecure multi-factor authentication solutions fail at "provable security," and then they divide them into eight categories based on the five phases of a formal security proof. They then go into detail about each of these eight proof failure types by looking at three common weak protocols and provide appropriate fixes. Lastly, using our expanded assessment criteria, they do a thorough evaluation and comparison of 70 sample multi-factor authentication systems. Our chosen schemes span the years 2009–2022, and the comparative findings indicate that designing better secure multi-factor authentication methods for mobile devices can be aided by an awareness of formal security proof failures[29].

Alshoshan, (2021) suggests a low-cost, user-friendly multi-factor authentication solution. No extra configurations or infrastructure are required for the system. The user selects and commits to memory three photos throughout the registration process since it uses graphical passwords. All the user has to do during the login procedure is select the appropriate photographs in the sequence he thought of during the registration process. Numerous security risks, including shoulder surfing, screen capture attacks, and keyloggers, are defeated by the suggested solution. Using the suggested approach, the 170 participants were divided into groups according to their age, level of education, and previous internet experience; 75% of them were males and 25% were women. On the many security threats, one-third of them lacked sufficient knowledge[30].

Table 1: Multi-Factor Authentication in Mobile Applications and its Methods and Challenges

Reference	Study On	Approach	Key Findings	Challenges and Limitations
Hasan et al., (2025)	Survey of modern mobile authentication schemes	Categorization of authentication types (password, biometric, graphical, gaze, etc.); evaluation of datasets and metrics	Identifies strengths and weaknesses of different methods; discusses research gaps and future directions	Lacks deep technical implementation; limited empirical evaluation
Aciobăniţei, (2024)	Integration of Push Notification module in Keycloak for MFA	Modular push-based MFA system using Keycloak; GitHub proof of concept	Reduces MFA implementation overhead; enables easy integration for developers	Evaluation limited to proof-of-concept; not tested in varied production environments
Syahreen et al., (2024)	Systematic review of MFA frameworks	SLR across 5 major databases; analysis of biometric and hybrid MFA schemes	Biometric is most used; most works are proof-of-concept needing further experimentation	Few practical implementations; lack of standardization or organizational guidelines
Salman et al., (2023)	Secure Android-based access control using MFA	Biometric + password-based access system with proximity sensor (10m range)	Effective for physical access control; enhances security using multi-modal verification	Distance-based functionality may limit flexibility; requires smartphone and biometric access
Wang and Wang, (2022)	Analysis of failures in security proofs in MFA schemes	Evaluated 70 MFA schemes from 2009–2022; classified 8 types of proof failures	Formal security proof failures can undermine MFA; countermeasures proposed for each type	Limited to random oracle model; real-world attack resistance not always tested
Alshoshan, (2021)	Usability-focused MFA using graphical passwords	Image-based authentication with low-cost, infrastructure-free setup	Protects against keyloggers, shoulder surfing; user-friendly design	Some users lacked awareness of security threats; limited scalability in high-risk environments

6 CONCLUSION AND FUTURE WORK

In mobile apps, multi-factor authentication (MFA) strategies are increasingly focused on striking a balance between strong security and user convenience. Common security risks, such as phishing, credential theft, and unauthorized access, are successfully addressed with MFA. However, mobile implementation introduces several challenges, including network dependency, device loss, biometric privacy concerns, and compatibility issues across diverse operating systems and hardware. Despite these limitations, MFA continues to evolve, incorporating advanced features such as push notifications, hardware/software tokens, and biometric recognition to strengthen mobile security. To ensure widespread adoption, MFA systems must be designed with a focus on usability, platform compatibility, and technological feasibility.

Future studies should analyze the development of adaptive authentication processes that integrate behavioral analytics and artificial intelligence to provide security without compromising the user experience. Also, they require offline-ready MFA solutions, as well as more secure and privacy-preserving biometric methods that will safeguard critical information. This would support interoperability and acceptance by having a common use of MFA across multiple mobile platforms in a consistent manner. Additionally, there should be increased awareness and education among users on good cybersecurity practices, particularly in mitigating human-based threats such as phishing and social engineering. Merging innovation with active user training will be imperative to the future of secure and ease-of-use MFA systems.

REFERENCES

[1] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” *Cryptography*, vol. 2, no. 1, 2018, doi: 10.3390/cryptography2010001.

[2] E. Ribeiro de Mello *et al.*, “Multi-factor authentication for shibboleth identity providers,” *J. Internet Serv. Appl.*, vol. 11,

no. 1, p. 8, Dec. 2020, doi: 10.1186/s13174-020-00128-1.
[3] S. Singh, "Enhancing Observability and Reliability in Wireless Networks with Service Mesh Technologies," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 1, pp. 7–17, 2025, doi: 10.48175/568.
[4] Nirav Kumar Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.
[5] V. Panchal, "Thermal and Power Management Challenges in High-Performance Mobile Processors," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 13, no. 11, Nov. 2024, doi: 10.15680/IJIRSET.2024.1311014.
[6] G. Ali, M. A. Dida, and A. E. Sam, "A secure and efficient multi-factor authentication algorithm for mobile money applications," *Futur. Internet*, 2021, doi: 10.3390/fi13120299.
[7] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.
[8] P. T. Tran-Truong *et al.*, "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis," *J. Syst. Archit.*, vol. 162, no. March, p. 103402, May 2025, doi: 10.1016/j.sysarc.2025.103402.
[9] M. Syahreen, N. Hafizah, N. Maarop, and M. Maslinan, "A Systematic Review on Multi-Factor Authentication Framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 5, pp. 1043–1050, 2024, doi: 10.14569/IJACSA.2024.01505105.
[10] S. Subudhi, "Comparative Analysis of Multi-Factor Authentication Mechanisms in Enhancing Cloud Security," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 6, no. 7, pp. 179–188, Jul. 2024, doi: 10.56726/IRJMETS59848.
[11] K. Liu *et al.*, "A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing," *Appl. Sci.*, vol. 13, no. 7, p. 4425, Mar. 2023, doi: 10.3390/app13074425.
[12] S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure," *Futur. Internet*, vol. 15, no. 4, p. 146, Apr. 2023, doi: 10.3390/fi15040146.
[13] R. Patel, "Optimizing Communication Protocols in Industrial IoT Edge Networks : A Review of State-of-the-Art Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 19, 2023, doi: 10.48175/IJARSCT-11979B.
[14] M. Ashawa and S. Morris, "Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies," *J. Inf. Secur. Cybercrimes Res.*, 2021, doi: 10.26735/krvi8434.
[15] G. Ali, M. A. Dida, and A. E. Sam, "Heuristic Evaluation and Usability Testing of G-MoMo Applications," *J. Inf. Syst. Eng. Manag.*, 2022, doi: 10.55267/iadt.07.12296.
[16] V. Shah, "Network Verification Through Formal Methods : Current Approaches and Open Issues," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, 2021.
[17] V. Prajapati, "Exploring the Role of Digital Twin Technologies in Transforming Modern Supply Chain Management," vol. 14, no. 03, pp. 1387–1395, 2025.
[18] S. Singh, "Open Radio Access Networks in Multi - Vendor Environments : A Survey of Interoperability Solutions and Best Practices," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, pp. 57–65, 2025, doi: 10.5281/zenodo.14881343.
[19] S. Hossain, A. Goh, C. H. Sin, and L. K. Win, "Generation of one-time keys for single line authentication," in *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*, 2016. doi: 10.1109/PST.2016.7906957.
[20] R. Patel, "Remote Troubleshooting Techniques for Hardware and Control Software Systems: Challenges and Solutions," *Int. J. Res. Anal. Rev.*, vol. 11, no. 2, pp. 933–939, 2024, doi: 10.56975/ijrar.v11i2.311510.
[21] N. Malali, "The Impact of Digital Transformation on Annuities : Personalization , Investment Strategies , and Regulatory Challenges," *J. Glob. Res. Math. Arch.*, vol. 11, no. 12, pp. 1–7, 2024, doi: 10.5281/zenodo.15279540.
[22] S. A. Lone and A. H. Mir, "A novel OTP based tripartite authentication scheme," *Int. J. Pervasive Comput. Commun.*, 2022, doi: 10.1108/IJPCC-04-2021-0097.
[23] D. Wang, P. Wang, and C. Wang, "Efficient Multi-Factor User Authentication Protocol with Forward Secrecy for Real-Time Data Access in WSNs," *ACM Trans. Cyber-Physical Syst.*, vol. 4, no. 3, pp. 1–26, Jul. 2020, doi: 10.1145/3325130.
[24] S. Gupta and A. Mathur, "Enhanced Flooding Scheme for AODV Routing Protocol in Mobile Ad Hoc Networks," in *2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies*, IEEE, Jan. 2014, pp. 316–321. doi: 10.1109/ICESC.2014.60.
[25] A. Abuarqoub, "D-FAP: Dual-Factor Authentication Protocol for Mobile Cloud Connected Devices," *J. Sens. Actuator Networks*, vol. 9, no. 1, p. 1, Dec. 2019, doi: 10.3390/jsan9010001.
[26] S. S. U. Hasan, A. Ghani, A. Daud, H. Akbar, and M. F. Khan, "A Review on Secure Authentication Mechanisms for Mobile Security," *Sensors*, vol. 25, no. 3, p. 700, Jan. 2025, doi: 10.3390/s25030700.
[27] B.-D. I. I. Aciobăniţei, "Enriching an Open-Source Access Management Platform Using Multi-Factor Authentication," 2024, doi: https://doi.org/10.1109/SACI60582.2024.10619788.
[28] M. I. Abdulkareem, O. I. Ashour, and Y. B. Salman, "Secure IoT Entrance Using Mobile Application," in *2023 7th International Electromagnetic Compatibility Conference (EMC Turkiye)*, IEEE, Sep. 2023, pp. 1–6. doi: 10.1109/EMCTurkiye59424.2023.10287534.
[29] Q. Wang and D. Wang, "Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices," in *IEEE Transactions on Information Forensics and Security*, 2022, pp. 597–612. doi: 10.1109/TIFS.2022.3227753.
[30] B. O. Als. A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," 2021, doi: https://doi.org/10.1109/NCCC49330.2021.9428806.

