International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Evaluating the Effectiveness of Two-Factor Authentication: A Comparative Analysis of Security and Usability

Rohit P. Deshmukh[1], Prathamesh K. Gandhare[2], Dr. D. S. Deshmukh[3]
[1,2,3]*MCA II yr Sem IV P.G. Dept of Computer Applications, PRMITR Badnera City-Amravati country- India*

***Abstract*--While passwords are the most common way we lock our digital accounts, they are no longer enough to keep hackers out. To fix this, most apps and websites now use Two-Factor Authentication (2FA), which asks for a second piece of information—like a code sent to your phone—before letting you in. This report looks at how well 2FA actually works. We studied different methods, from simple text message codes to high-tech security keys built into smartphones.**

Our research found that while 2FA makes accounts much safer, it isn't perfect. Some systems have "loopholes" that hackers can use to bypass the second step, especially when websites try to make things too "convenient" for the user (like the "Remember this Device" feature). We also looked at the human side of things: if a security step takes too long or is too confusing, people are less likely to use it correctly. Ultimately, this paper shows that for 2FA to be truly effective, it needs to be easy for people to use while keeping the two security steps completely separate so that a hacker can't break both at once..

***Keyword*-- Account security, user experience, mobile security, login codes, website vulnerabilities, smart cards, digital safety, password apps.**

I. INTRODUCTION

In today's digital world, almost everything we do—from banking and shopping to staying in touch with friends—happens online. To keep these activities private, we use a process called **authentication**. Simply put, authentication is the digital version of showing an ID card; it is the way a website or app verifies that you are actually who you say you are before letting you into your account. For a long time, the main way we proved our identity was by using a **password**. This is known as "knowledge-based" authentication because it relies on something you know. However, passwords have become a weak link in modern security. Because we have so many accounts, most people find it impossible to remember dozens of long, complex, and unique passwords. As a result, many people fall into risky habits, like using "123456," using their pet's name, or—most dangerously—using the same password for every website. This makes a hacker's job easy. If a criminal steals your password from one leaked database, they can often use it to break into your email, your social media, and even your bank account.

To fix this problem, the security world has moved toward **Two-Factor Authentication (2FA)**. The idea behind 2FA is simple: even if a hacker steals your password, they still shouldn't be able to get into your account. By adding a second "factor," you provide two different types of proof. Usually, this means combining **something you know** (your password) with **something you have** (like a code sent to your phone or a physical security key).

2FA is incredibly important because it stops the most common types of cyberattacks. For example, when Google automatically turned on two-step verification for millions of users, they saw account hacks drop by 50%. However, 2FA isn't a perfect fix. Sometimes it can be annoying to use, taking extra time and effort every time you log in. Also, some hackers have found clever ways to bypass 2FA by tricking users or stealing the "cookies" that tell a website to "remember this device."

This report will look at how effective 2FA really is. We will explore the different types of 2FA, how hackers try to break them, and how companies are trying to make security stronger without making it too difficult for the average person to use.

II. LITERATURE REVIEW

The evolution of Two-Factor Authentication (2FA) has moved from theoretical cryptographic protocols to practical, hardware-integrated solutions, yet the balance between security and user experience remains a central challenge in the literature.

Early academic focus was heavily centered on the cryptographic integrity of 2FA schemes. **Ding Wang and colleagues (2016)** conducted a comparative evaluation of smart-card-based systems, pointing out a critical theoretical flaw: many schemes failed to provide "true" two-factor security. They argued that if a physical factor like a smart card is compromised, it often allows an attacker to mount offline attacks to discover the second factor (the password), effectively collapsing the security back to a single point of failure. As mobile devices became the primary vehicle for 2FA, research shifted toward the vulnerabilities inherent in commodity hardware.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Radhesh Krishnan Konoth and his team (2020) highlighted that most mobile-based 2FA is weaker than assumed because the "two factors"—the device and the credential—often reside on the same potentially compromised Operating System. To solve this, they proposed **SecurePay**, which uses ARM TrustZone technology to isolate sensitive transaction data from the main phone system, ensuring that even a fully "rooted" or infected phone cannot manipulate the authentication process.

Recent empirical studies have exposed how modern "usability" features can inadvertently create new security gaps. **Zhi Wang and co-authors (2024)** analyzed realworld implementations and found that features like "Remember this Device" often rely on insecure browser cookies. Their findings revealed that attackers could bypass 2FA entirely by stealing these cookies, effectively rendering the second factor useless without the user ever knowing. This highlights a persistent tension: as 2FA becomes easier to use, it often becomes easier to circumvent. This tension is further explored through the lens of user perception. **Ghulam Mustafa Khaskheli and others (2022)** conducted experiments showing that while users acknowledge 2FA is significantly more secure than simple passwords, they consistently rate it lower in terms of usability due to the extra time and effort required. This "usability tax" can lead to dangerous behaviors, such as "click-through habituation." As **Mohammed Jubur and his colleagues (2025)** noted in their comprehensive survey, users of push-based 2FA often develop a habit of blindly approving requests, which attackers can exploit through "push fatigue" attacks.

Collectively, the literature suggests that while 2FA is a vital defense-in-depth strategy, its effectiveness is limited by implementation flaws in "remember me" features, the lack of true hardware isolation in mobile devices, and the human tendency to prioritize convenience over rigorous verification.

III. How Two-Factor Authentication Works

In simple terms, two-factor authentication (2FA) works by asking you for two different types of proof to show who you are. Instead of just relying on a password, 2FA uses three main categories: something you **know** (like a PIN), something you **have** (like your phone), or something you **are** (like your fingerprint).

A. Authentication Process (Handshake Mechanism): The way 2FA actually starts is pretty straightforward. First, you type in your username and password like normal. Once the website sees your password is correct, it starts a "challenge" to check your second factor. Usually, this means the site sends a short code—called a One-Time Password (OTP)— to your phone. You then type that code into the login screen. This is secure because the code only works once and usually expires in about 30 seconds. Another important point is how these codes are made. Most apps use a system called TOTP, which stands for Time-based One-Time Password.

Basically, your phone and the website's server both have the same "secret key" and the same clock. They use the current time to create a matching code. If the numbers match, you're in. Some fancier versions use "security keys" (like a YubiKey). In this case, the key holds a digital signature that never leaves the hardware, making it almost impossible for a hacker to copy.

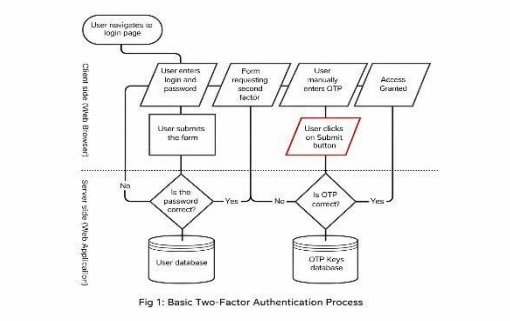

Fig.1 Basic Two-Factor Authentication Process

B. Isolation of Factors: For 2FA to really work, the two steps need to be kept far apart. This is called "isolation." If a hacker breaks into your computer, they shouldn't be able to get into your 2FA app on your phone. However, things get tricky when you are doing everything on one smartphone. To fix this, modern phones have a "secure world" built into their chips, often called a Trusted Execution Environment (TEE). Think of the TEE as a private safe inside your phone's processor. While your apps and games run in the "normal world," your 2FA secrets stay locked in the "secure world." When you go to log in, the phone quickly switches to this safe zone to handle the security check. This way, even if your phone has a virus or is "rooted," the hacker still can't see what's happening inside that private safe.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

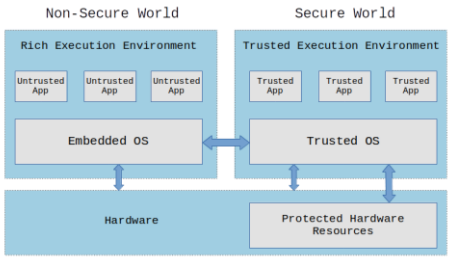

Fig.2 Isolation of Authentication Factors using Trusted Execution Environment (TEE)

C. User Verification and Presence: The final part of the process is making sure a human is actually involved. Many 2FA systems now use "Push Notifications" where a message pops up on your screen asking you to "Approve" or "Deny" a login. This requires you to physically tap a button, which proves you are at your device and aware of what's happening. In high-security apps, like mobile banking, the system will even show you exactly what you are authorizing—for example, "Transfer $500 to John Doe." This is a huge help because it prevents a "Man-in-the-Middle" attack. Even if a hacker tries to change the transaction details behind the scenes, you will see the real numbers on your 2FA screen and can hit "Deny" before any money moves.

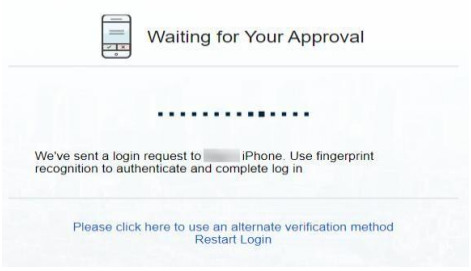

Fig.3 Push-Based User Verification in TwoFactor Authentication

IV. Types Of 2FA Methods

The effectiveness and adoption of 2FA depend heavily on the specific method chosen. Each type offers a different balance of security, usability, and cost.

SMS-Based One-Time Password (OTP): This is one of the most widely used 2FA methods. The system sends a 4–6 digit code to the user's registered mobile number.

- *Usability:* Very high, as it requires no additional setup
- *Security:* Relatively low due to risks such as SIM-swapping and network interception

Software Tokens (Authenticator Applications): Applications such as Google Authenticator generate time-based one-time passwords (TOTP) on the user's device.

- *Usability:* Moderate, requires installation and setup
- *Security:* Higher than SMS, but vulnerable to malware attacks

Push Notification-Based Authentication: Users receive a notification on their device to approve or deny login attempts.

- *Usability:* Very high, as no manual code entry is required
- *Security:* Good, but vulnerable to "push fatigue" attacks

Hardware Security Keys: Devices such as YubiKey provide authentication using physical hardware.

- *Usability:* Moderate, requires carrying a physical device
- *Security:* Very high, resistant to phishing and remote attacks

Proximity and Context-Based Methods: These methods use environmental factors such as sound or location for authentication.

- *Usability:* Very high, often automatic
- *Security:* Variable, depends on environmental reliability

Table 1:
Comparison of Different TwoFactor Authentication Methods

2FA Metho d	Primary Factor	Usabili ty	Main Security Threat
SMS-OTP	Possession (Phone)	Very High	SIM-jacking, network sniffing
Softwa re Token	Possession (App)	High	Malware on OS, seed theft
Push2FA	Possession (App)	High	User habituation (accidental tap)
Securit y Key	Possession (Hardware)	Mediu m	Physical theft, loss of token
Audio-Proxim ity	Context (Environm ent)	Very High	Sound recording/manipul ation

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

V. Problem Statement

Despite the theoretical strength of two-factor authentication (2FA), its real-world implementation faces several challenges that reduce its overall effectiveness.

Two-Factor Dependency on Mobile Devices

The fundamental principle of 2FA is the independence of authentication factors. However, in modern usage, both factors are often used on the same device, especially smartphones. For example, users may log in to a banking application and receive the OTP on the same device. This creates a security risk, as attackers who gain control over the device can access both factors simultaneously. As a result, the effectiveness of 2FA is reduced in such scenarios.

Usability–Security Trade-off

While 2FA improves security, it also increases login time and user effort. Studies show that a password-based login takes around 7–8 seconds, whereas 2FA may take more than 30 seconds. This additional time can lead to user frustration. To reduce this, many platforms use "Remember Device" features. However, these often rely on browser cookies, which can be stolen through attacks such as Cross-Site Scripting (XSS), allowing attackers to bypass 2FA completely.

Lack of Standard Evaluation Framework

Another major issue is the absence of a standardized method to evaluate 2FA systems. Many authentication schemes are proposed and later found to be vulnerable. This creates a continuous "break-fix" cycle in security research. Additionally, some systems fail to consider real-world attack scenarios such as device theft or sidechannel attacks, which further reduces their reliability.

Transaction Integrity Issues

Most 2FA systems focus only on verifying the user's identity, but not the actual transaction being performed. For example, a user may approve a transaction believing it to be small, while an attacker modifies it to a larger amount. Without a secure and independent way to display transaction details, 2FA cannot fully guarantee transaction integrity.

VI. Benefits Of Two-Factor Authentication

When implemented correctly, two-factor authentication (2FA) provides several advantages that significantly improve security compared to password-only systems.

Reduction in Account Compromise

One of the major benefits of 2FA is its ability to prevent large-scale automated attacks. Many cyber attacks rely on stolen passwords (credential stuffing).

Since 2FA requires an additional verification factor, these stolen credentials alone are not sufficient to access accounts. Studies have shown that enabling 2FA can reduce account theft significantly, with reports indicating up to a 50% decrease in such incidents.

Protection Against Phishing Attacks

Advanced 2FA methods, such as hardware security keys and passkeys, offer strong protection against phishing attacks. These methods use cryptographic verification linked to the original website domain. As a result, even if a user enters credentials on a fake website, the authentication process will fail, preventing unauthorized access.

Improved Security with Password Managers

Combining 2FA with password managers creates a highly secure authentication system. Password managers generate and store strong passwords, while 2FA adds an additional layer of protection. Even if the master password is compromised, attackers cannot access accounts without the second authentication factor.

Transaction Security and Integrity

Modern 2FA systems, especially those using Trusted Execution Environments (TEE), ensure that users can verify the exact details of a transaction before approval. This helps prevent unauthorized changes during financial transactions. For example, users can confirm payment details securely before completing a transaction.

Flexibility and Scalability

2FA systems can be adapted for different use cases. High-security environments such as banking systems may use hardware tokens, while general applications like social media may use OTP or push notifications. This flexibility makes 2FA suitable for a wide range of applications.

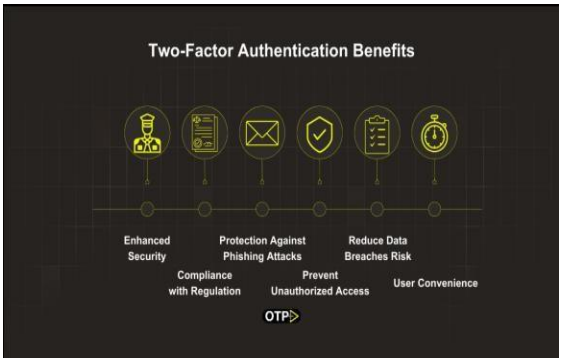

Fig.4 Benefits of Two-Factor Authentication

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

VII. Challenges And Limitations

Despite its advantages, two-factor authentication (2FA) faces several challenges that can affect its usability and effectiveness.

Physical and Cognitive Burden

The possession factor depends on devices such as smartphones or hardware tokens. If these devices are lost, recovering access becomes difficult. Additionally, switching between devices to complete authentication can increase user effort and lead to fatigue.

Compatibility and Environmental Limitations

Some 2FA methods require specific conditions or device support. For example, hardware keys may not work on all devices, and audio-based methods depend on environmental factors. This can lead to inconsistent user experience.

Vulnerability to Social Engineering

Human behavior plays a major role in security. Users may accidentally approve unauthorized login requests due to repeated notifications. SMS-based systems are also vulnerable to SIM-swapping attacks.

Implementation Weaknesses

Features like "Remember Me" can introduce security risks. If cookies are not properly secured, attackers may bypass 2FA completely.

Hardware and Side-Channel Risks

Hardware tokens are not completely secure over time. Advanced attacks can extract sensitive data, especially if the device is physically accessed.

VIII. Evaluation Of Effectiveness

The effectiveness of two-factor authentication (2FA) can be evaluated based on usability, security performance, and real-world implementation analysis.

Usability–Security Trade-off: To evaluate 2FA performance, it is important to analyze how it affects user experience. A study comparing single-factor authentication (SFA) and 2FA shows a clear trade-off between usability and security.

Table 2:
Comparison of Usability and Performance between SFA and 2FA

Metric	SingleFactor (SFA)	TwoFactor (2FA)	Difference (%)
Mean Completion Time	7.795 seconds	34.578 seconds	+343%
Usability Score (1-7)	5.56	5.31	-4.5%
Aegis Time (avg)	N/A	37.734 seconds	N/A
Google Auth Time (avg)	N/A	< 32.000 seconds	N/A
Microsoft Auth Time (avg)	N/A	34.570 seconds	N/A

The results show that 2FA significantly increases login time compared to single-factor authentication. However, the usability score remains relatively similar, indicating that users are adapting to the additional security layer

Cookie-Based Risk Analysis (SE2FA): To understand real-world implementation issues, an empirical study analyzed websites using "Remember Me" functionality.

Table 3:
Analysis of Cookie-Based Device Recognition in 2FA Systems

Category of Implementation	Number of Websites	Percentage (%)
Cookie-Only Reliance	93	51.6%
Cookie + Other (Fingerprint/IP)	87	48.4%
Total with "Remember Me"	180	100%

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

The findings reveal that more than 50% of websites rely only on cookies for device recognition. This creates a major vulnerability, as attackers can bypass 2FA by stealing these cookies.

Performance of TEE-Based Systems: Modern 2FA systems use Trusted Execution Environments (TEE) to improve security and efficiency.

Table 4:
Performance Evaluation of TEE-Based 2FA Systems

SecurePay Operation	Mean Time (Seconds)	Compliance (< 2s)
2048-bit RSA Key Generation	1.34 seconds	Yes
Key Generation + QR Display	1.91 seconds	Yes
Summary Decryption & Display	1.29 seconds	Yes

The results indicate that TEE-based systems perform efficiently, with all operations completing within acceptable time limits. This shows that high security can be achieved without affecting performance.

Smart Card Attack Analysis: To evaluate robustness, 2FA systems must also be tested against physical attacks.

Table 5:
Classification of Smart Card-Based Attacks

Attack Type	Strategy	Weakness Exploited
Type I	Passive	No verification during password change
Type II	Passive	Definite verifiers stored for PW change
Type III	Passive	Partitioning of non-group password logic
Type IV	Passive	Intercepting protocol flow + card data
Type V	Passive	Pre-computation of flow and math
Type VI	Passive	Pre-computation of specific flow 1
Type VII	Hybrid	Using server as an oracle for flow 2
Type VIII	Hybrid	De-synchronization of flow 3

The analysis highlights that many 2FA systems fail to address multiple attack strategies. This demonstrates the need for stronger evaluation frameworks and more secure designs.

IX. Future Scope

The future of two-factor authentication (2FA) is expected to evolve towards more intelligent, user-friendly, and secure systems. Emerging technologies will play a key role in improving both security and usability.

AI-Driven Personalized Authentication

Artificial Intelligence (AI) is expected to transform authentication systems by making them adaptive. Instead of always requiring a second factor, AI-based systems can analyze user behavior such as typing patterns, login location, and usage habits. Based on this analysis, the system can decide whether additional verification is needed. This approach improves user experience while maintaining strong security.

Hardware-Based Secure Environments

The use of Trusted Execution Environments (TEE) is likely to become more common in future authentication systems. These secure hardware environments protect sensitive operations from external threats. As technology advances, such features may become standard across devices, ensuring consistent and reliable security.

Passwordless and Risk-Based Authentication

Future systems are moving towards passwordless authentication methods such as biometrics and FIDO2based systems. These methods reduce reliance on passwords and improve security. Additionally, riskbased authentication allows systems to adjust security requirements based on context. For example, login from a trusted device may require minimal verification, while unusual activity may trigger additional checks.

Secure Digital and Educational Platforms

With the growth of online services and digital learning platforms, secure authentication will become increasingly important. Future 2FA systems must support users with limited access to advanced devices or high-speed internet. This may include lightweight authentication methods and institutional verification systems to ensure accessibility and security for all users.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

X. CONCLUSION

Two-factor authentication (2FA) plays a crucial role in modern digital security. However, its effectiveness largely depends on proper implementation and evaluation. This study shows that while 2FA can significantly reduce account compromise, it is often weakened by poor design choices, such as insecure "Remember Device" mechanisms that may allow attackers to bypass authentication.

For 2FA to be truly effective, certain principles must be followed. First, there should be clear separation between authentication factors to prevent both from being compromised simultaneously. Technologies such as Trusted Execution Environments (TEE) provide stronger protection by isolating sensitive operations. Second, there is a need for standardized evaluation frameworks that consider a wide range of attack scenarios, including physical and software-based threats.

In addition, the balance between security and usability must be carefully managed. Simplified authentication methods, such as push-based approval systems and password manager integration, can improve user experience without compromising security. As authentication systems continue to evolve towards AIdriven and passwordless approaches, it is essential to apply the lessons learned from current 2FA systems to develop more secure and user-friendly solutions.

REFERENCES

[1] R. K. Konoth, B. Fischer, W. Fokkink, E. Athanasopoulos, K. Razavi, and H. Bos, "SecurePay: Strengthening Two-Factor Authentication for Arbitrary Transactions," in Proc. IEEE European Symposium on Security and Privacy (EuroS&P), 2020, pp. 569–586.

[2] M. Jubur, P. Shrestha, and N. Saxena, "An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools," ACM Computing Surveys, vol. 57, no. 5, pp. 1–32, Jan. 2025.

[3] Z. Wang et al., "Simple But Not Secure: An Empirical Security Analysis of Two-Factor Authentication Systems," arXiv preprint arXiv:2411.11551, Nov. 2024.

[4] G. M. Khaskheli, M. Sherbaz, and U. R. Shaikh, "Users' Opinion Regarding Comparison Between SingleFactor and Two-Factor Authentication Using Parameters of Security and Usability in Social Media Application," Tropical Scientific Journal, vol. 1, no. 1, pp. 17–27, 2022.

[5] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes," in Proc. ACM Asia Conference on Computer and Communications Security (AsiaCCS), 2016, pp. 475–486.

[6] A. V. Dongre, O. S. Gorle, and R. R. Sherekar, "A diligent survey of the Future of Education: Personalized learning and online learning," Journal of Computer Applications, vol. 9, no. 2, pp. 368–378, 2024.

[7] J. H. Saltzer and M. Schroeder, "The protection of information in computer systems," Proceedings of the IEEE, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.

[8] X. Li, J. Niu, and M. Khan, "An enhanced smart card based remote user password authentication scheme," Journal of Network and Computer Applications, vol. 36, no. 5, pp. 1365–1371, 2013.

[9] H. Sun, K. Sun, Y. Wang, and J. Jing, "TrustOTP: Transforming smartphones into secure one-time password tokens," in Proc. ACM Conference on Computer and Communications Security (CCS), 2015, pp. 976–988.

[10] S. Kumari and M. K. Khan, "Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme," International Journal of Communication Systems, vol. 27, no. 12, pp. 3939– 3955, 2014.