International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Emerging Trends and Innovations in Web-Based Applications and Technologies
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Strengthening Transaction Authentication: A Study on the Effectiveness of One-Time Passwords (OTP)

Anshul Kumbhare[1], Aditya Tripathi[2], Usha Kosalkar[3], Shubhra Chinchmalapure[4], Prof. Anupam Chaube[5]

[1,2,5]Department of Science and Technology,
[4]Department of Computer Science,
[1,2,4,5]G H Raisoni College of Engineering and Management, Nagpur, Maharashtra, India
[3]Department of Artificial Intelligence, G H Raisoni College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

In the digital era, transaction security is a growing concern due to increasing cyber threats. One-Time Passwords (OTPs) are widely used as an additional authentication layer to protect sensitive transactions. This study examines the effectiveness of OTPs in securing transactions, their advantages, vulnerabilities, and potential alternatives. By analyzing case studies and security trends, the research highlights the strengths and weaknesses of OTP authentication and proposes improvements to enhance transaction security.

1. INTRODUCTION

1.1. Background

With the rise of digital transactions, ensuring authentication security has become critical. OTPs, typically sent via SMS, email, or authentication apps, serve as a temporary verification code for transaction approval. Despite their widespread use, OTPs have limitations, including phishing attacks, SIM swapping, and interception risks.

1.2. Research Problem

While OTPs add an extra layer of security, their effectiveness is often challenged by evolving cyber threats. This study seeks to evaluate whether OTPs provide sufficient protection for transactions and explore possible enhancements.

1.3. Research Objectives

To assess the effectiveness of OTPs in transaction authentication.

To identify the vulnerabilities and security risks associated with OTPs.

To explore alternative authentication methods for enhanced security.

1.4. Research Questions

How effective are OTPs in preventing unauthorized transactions?

What are the common vulnerabilities of OTP authentication?

What improvements can be made to strengthen OTP security?

2. Literature Review

Several studies have explored the role of OTPs in multi-factor authentication (MFA). According to security experts, OTPs reduce fraud risks but are not foolproof against social engineering attacks. Research highlights that hackers exploit vulnerabilities such as SIM swapping and man-in-the-middle (MITM) attacks. Alternative authentication mechanisms, including biometric verification, token-based authentication, and behavioral analytics, have been proposed to mitigate these risks.

3. Methodology

3.1. Research Design

This study adopts a mixed-method approach, incorporating:

- A security analysis of OTP mechanisms in different authentication frameworks.
- A case study of past OTP-related fraud incidents.
- A survey of users and cybersecurity professionals regarding OTP security concerns.

3.2. Data Collection Methods

Reviewing cyber attack reports and OTP-related fraud cases.

Conducting interviews with cybersecurity experts.

Surveying users on their experiences with OTP security.

4. Findings and Discussion

4.1. Strengths of OTP Authentication

Enhanced security: OTPs provide a second layer of verification beyond passwords.

Ease of use: Users can easily receive OTPs via SMS, email, or authentication apps.

Temporary validity: OTPs expire quickly, reducing the risk of reuse.

4.2. Weaknesses and Vulnerabilities

Phishing attacks: Cybercriminals trick users into revealing OTPs.

SIM swapping: Attackers clone SIM cards to intercept OTPs.

Network interception: OTPs sent via SMS can be intercepted using sophisticated attacks.

4.3. Alternative Authentication Methods

Biometric authentication (fingerprint, facial recognition, iris scan).

Hardware security tokens (e.g., YubiKey, RSA SecurID).

Behavioral authentication (AI-driven analysis of user behavior).

5. Conclusion and Recommendations

5.1. Summary of Findings

While OTPs offer an extra layer of security, they are not foolproof against evolving cyber threats. Attackers exploit

vulnerabilities such as SIM swapping and phishing to bypass OTP protection.

5.2. Recommendations

Implementing multi-factor authentication (MFA) that combines OTPs with biometric verification.

Encouraging users to switch to app-based authentication instead of SMS OTPs.

Enhancing OTP security with encrypted transmission and AI-based fraud detection.

6. References

[1] "A New One-Time Password Method" by Yong Wang, Jianming Fu, and Yuliang Lu https://www.researchgate.net/publication/270937234_A_new_One-time_Password_Method

[2] "An Improved Time-Based One-Time Password Authentication Framework for Electronic Payments" by Mohammad A. Hassan, Zaid Shukur, and Md. Khadim Hasan https://thesai.org/Publications/ViewPaper?Code=IJACSA&Issue=11&SerialNo=46&Volume=11

[3] "An Empirical Study of SMS One-Time Password Authentication in Android Apps" Yue Zhou and Yajin Zhou https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=5631&context=sis_research

[4] "Under The Microscope: The Risks Of One-Time Passwords" https://www.forbes.com/councils/forbestechcouncil/2024/07/12/under-the-microscope-the-risks-of-one-time-passwords-vulnerabilities/

[5] "One-Time Password Security Might Fail 80% of the Time. IAM is Better." https://securityintelligence.com/articles/one-time-password-security-fails-80-percent-iam-better/

[6] "The State of Password Security 2024 Report" https://bitwarden.com/resources/the-state-of-password-security/