JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A STUDY ON THE ADOPTION AND SECURITY PERFORMANCE OF QR CODE-BASED TWO-FACTOR AUTHENTICATION IN WEB APPLICATION

Akshay Satish Koli[1], Shreya Bhaskar Thakare[2], Prof. Shivaji Bachchhav[3], Prof. Shubhangi Shinde[4]
[12]MCA Department, Dr. D.Y. Patil Centre of Management and Research, Pune, India
[34]Assistant Professor, MCA Department, Dr. D.Y. Patil Centre of Management and Research, Pune, India

Abstract*:* Cyber threats targeting web applications have increased significantly with the expansion of online services in banking, e-commerce, and communication platforms. Traditional password-based authentication is proving inadequate due to issues such as password reuse, credential stuffing, brute force attacks, and phishing. Two-Factor Authentication (2FA) has emerged as one of the most widely adopted countermeasures. Among the various 2FA methods, QR code-based authentication is gaining momentum for its simplicity, cross-platform compatibility, and potential security advantages.

Keywords: QR Code Authentication, Two-Factor Authentication, Web Application Security, SMS OTP, TOTP, Phishing Attacks, Cybersecurity, User Perception, MITM Attack, Authentication Technologies

1. INTRODUCTION

The rapid digitalization of services has led to increased usage of web applications for financial transactions, bill payments, shopping, education, and communication. This growth has simultaneously attracted cybercriminals, resulting in a rise in password-related breaches. Studies show that more than 60% of data breaches involve stolen or weak passwords.

To address these challenges, web applications are increasingly adopting Two-Factor Authentication (2FA), which combines a password with a second verification factor such as an OTP, mobile app confirmation, QR scan, or biometric verification. Among these, QR code-based authentication has gained popularity due to its ease of implementation, quick login process, and elimination of manual OTP entry.

This study attempts to answer these questions through a structured data-driven approach involving adoption scanning, user surveys, and controlled testing.

2. REVIEW OF LITERATURE

2FA literature emphasizes its role in strengthening authentication. SMS OTP, one of the oldest forms, is widely deployed but severely vulnerable to SIM swapping, telecom interception, malware, and phishing. TOTP authentication, generated via apps like Google Authenticator, offers improved security but requires technical understanding and secure seed storage.

QR code-based authentication is observed in modern systems such as WhatsApp Web Login, Microsoft Authenticator, and enterprise single sign-on systems. These systems leverage QR codes for device binding, session authentication, and cross-device login.

However, research also highlights risks associated with “quishing” (QR phishing), where attackers replace legitimate QR codes with malicious ones, redirecting users to fake websites. Studies show that users often fail to verify the authenticity of QR codes, making them susceptible to redirection attacks.

Despite growing interest, few studies have conducted comprehensive comparisons of QR-based 2FA with SMS and TOTP methods in both usability and security contexts. This research aims to fill that gap.

3. OBJECTIVES OF STUDY

The primary objective of the study is to examine the adoption and security performance of QR code-based 2FA in web applications.The specific objectives are:

1. To assess QR code-based 2FA adoption across different categories of web applications.
2. To evaluate user perceptions regarding usability, convenience, and security.
3. To analyze the effectiveness of QR-based 2FA against phishing, replay, and MITM attacks.
4. To compare QR-based 2FA with SMS OTP and TOTP authentication.
5. To identify barriers affecting the adoption of QR-based 2FA.

4. RESEARCH METHODOLOGY

A mixed-methods approach was adopted, combining descriptive and experimental techniques.
Sample Selection:

- 20 web applications across finance, social media, e-commerce, and cloud services.
- 100 survey participants with prior experience using 2FA.
- Controlled test environment implementing three authentication methods.

Data Collection Methods:

1. Adoption Analysis: Manual scanning of 20 popular sites using their security settings.
2. User Survey: Structured questionnaire addressing usability, trust, and convenience.
3. Security Testing:

o Phishing attacks via fake login pages
o Replay attacks using intercepted codes
o MITM attacks simulating traffic interception

Data Analysis:

- Descriptive statistics for adoption and survey responses.
- Comparative matrices for security test outcomes.
- Graphical representation of survey results.

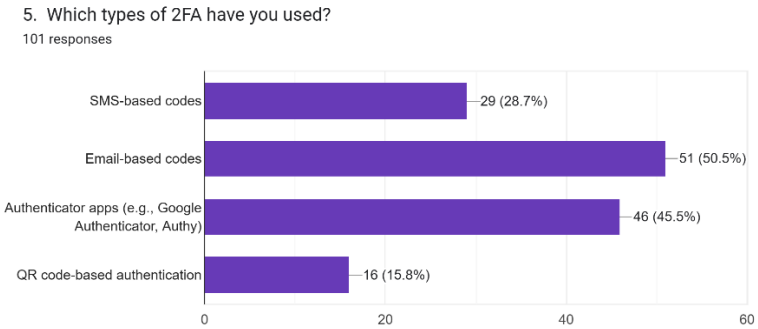
5. DATA ANALYSIS AND INTERPRETATION

1. location of the respondents

2FA Type	Adoption Rate	Examples
SMS OTP	60%	Paytm, IRCTC, Banking apps
TOTP App	75%	Google, Amazon, GitHub
QR-Based 2FA	30%	WhatsApp Web, Microsoft Authenticator

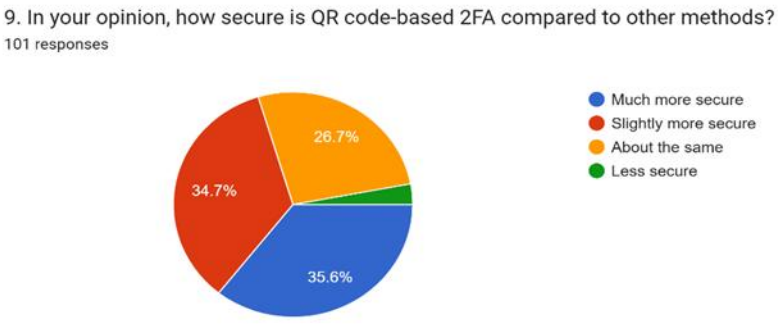
Interpretation:
QR code-based 2FA is still emerging and not yet widely adopted, primarily due to lack of standardization and developer knowledge.

7.2 User Survey (100 participants)



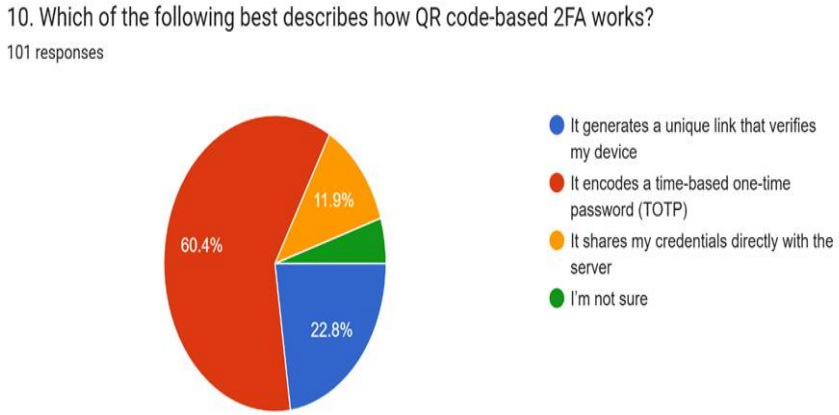
Results from your chart:

2FA Method	Responses	Percentage
Email-based codes	51	50.5%
Authenticator apps (Google Authenticator, Authy)	46	45.5%
SMS-based codes	29	28.7%
QR code-based authentication	16	15.8%



3.What type of internet connection do you mainly use for learning?

Response Category	Percentage (%)
Much more secure	35.6%
Slightly more secure	34.7%
About the same	26.7%
Less secure	3% (approx)



4. Which digital devices do you primarily use for studying online?

Option	Responses (%)
It encodes a time-based one-time password (TOTP)	60.4%
It generates a unique link that verifies my device	22.8%
It shares my credentials directly with the server	11.9%
I'm not sure	-5%

Usability Ratings (1–5 scale)
- QR 2FA: 4.1 average
- TOTP: 4.4 average
- SMS OTP: 3.2 average

Security Perception
- QR: 70% users believe it is more secure than SMS
- TOTP: 82% users believe it is the most secure
- SMS OTP: Only 40% users trust its security

Convenience
- 68% found QR authentication faster
- 74% found SMS OTP irritating due to delays or non-delivery
- 59% found TOTP slightly difficult to set up

7.3 Security Testing

Attack Type	QR 2FA	SMS OTP	TOTP
Phishing	Moderate risk	High Risk	Low Risk
Replay Attack	Low Risk	Medium Risk	Low Risk
MITM Attack	Medium Risk	High Risk	Medium Risk

Interpretation:
QR code-based 2FA is significantly stronger than SMS OTP but still requires enhanced QR validation to reach TOTP-level security.

6. FINDINGS OF THE STUDY

1. QR-based 2FA adoption remains low but is gradually increasing with modern applications.
2. Users find QR 2FA more convenient than SMS and nearly as easy as TOTP.
3. Security testing confirms QR-based authentication is more secure than SMS OTP.
4. QR 2FA is still vulnerable to phishing attacks involving QR code manipulation.
5. TOTP remains the most secure method overall.
6. Major barriers include low awareness, dependency on smartphones, and limited availability.

7. CONCLUSION

QR code-based authentication has the potential to become a mainstream 2FA method due to its convenience and enhanced security compared to SMS OTP. While it still faces usability and implementation challenges, it performs strongly in controlled security environments and is well-received by users.
The study concludes that QR code-based 2FA offers a practical balance between usability and security, with room for improvement through user education, secure QR generation, and integration with advanced authentication technologies.

8. REFERENCES

1.Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

2. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

3. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.

4. RFC 6238: M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). TOTP: Time Based One-Time Password Algorithm. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc6238

5. RFC 4226: M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). HOTP: An HMAC-Based One-Time Password Algorithm. IETF. https://datatracker.ietf.org/doc/html/rfc4226

6. Burp Suite. (2024). Web Security Testing Guide. Retrieved from https://portswigger.net/burp