GAS Journal of Engineering and Technology (GASJET)

OPEN ACCESS

Volume 2, Issue 8, 2025 Journal Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800
Email: editor@gaspublishers.com

Enhancing Digital Security: A QR Code and OTP-Based E-Authentication Systems

M.A YA'A[1], Adenomon Monday O.[2], Dr. GT Obadiah[3], Gilbert I.O. Aimufua[4], Mohammed Idris[5]& Yakubu Saidu[6]

[1]PhD Student, Centre for Cyberspace Studies, Department of Cybersecurity, Nasarawa State University, Keffi. Nigeria
[2]Center for Cyberspace, Department of Cybersecurity, Nasarawa State University, Keffi, Nigeria
[3]Dean, Faculty of African Languages and Development, Omni University, Imo State, Nigeria
[4]Director, Center for Cyberspace, Nasarawa State University, Keffi, Nigeria
[5]Doctorate Candidate, Security and Strategic Studies, Institute Of Government and Department Studies, Nasarawa State University, Keffi
[6]Computer Science Department, Faculty of Natural and Applied Sciences, Nasarawa state university, Keffi

Received: 29.08.2025 | **Accepted:** 21.09.2025 | **Published:** 25.09.2025

***Corresponding Author:** M.A YA'A

DOI: *10.5281/zenodo.17203514*

Abstract **Original Research Article**

In an era where digital security is paramount, the Quick Response (QR) Code and One-Time Password (OTP)-Based E-Authentication System proposes an innovative approach to enhance user authentication. With the rapid proliferation of wireless communication technology, the importance of user authentication is growing to ensure the security of the system. An essential role in the authentication process is played by passwords. In the authentication procedure, the user's password is transmitted along with the traffic to the authentication server, enabling the server to grant access to the legitimate user. Adversaries may exploit this opportunity to attempt to intercept other individuals' passwords to engage in illicit activities under false identities, thereby evading detection. Various strategies have been proposed to enhance the security of wireless communication technologies in response to these challenges. The suggested approach will be employed to enhance the security of the system in this investigation. One-time passwords, hashing, and two-factor authentication have been selected as the resolution. Additionally, a novel solution utilizing QR codes will be introduced to store more information securely. The objective of the system's outcome is to enhance the current login authentication mechanism. It offers methodologies to heighten the complexity of password cracking and encourage individuals to opt for and utilize intricate passwords.

Keywords: E-Authentication, Two-Factor Authentication (2FA), QR Code Security, One-Time Password (OTP), Digital Security Systems.

1. INTRODUCTION

In today's interconnected world, digital security has become an indispensable aspect of daily life, impacting individuals, businesses, and governments alike. The pervasive use of online services, from banking and e-commerce to social media and cloud computing, necessitates robust authentication mechanisms to protect sensitive information and prevent unauthorized access. However, traditional authentication methods, primarily relying on static usernames and passwords, have proven increasingly vulnerable to sophisticated cyber threats. The confidentiality of passwords is often compromised due to weak password practices, phishing attacks, keyloggers, and data breaches, leading to significant financial losses and privacy infringements (Alexandre. 2018).

The rapid expansion of wireless communication technologies has further exacerbated these security concerns. As more transactions and interactions migrate to digital platforms, the attack surface for malicious actors widens (Ataelfadiel, 2022). Cybercriminals continuously devise intricate methods to target online consumers, making it challenging to detect and prevent attacks that often originate from the legitimate user's web browser. This can lead to user account information being covertly altered, resulting in substantial monetary losses. For instance, the financial services sector has experienced a surge

in cyber-attacks globally, with losses reaching billions of dollars annually (Edwards, 2018).

2. RESEARCH PROBLEM

The primary problem addressed by this paper is the inadequacy of conventional single-factor authentication systems, such as username and password combinations, in safeguarding against modern cyber threats. These systems are susceptible to various attacks, including brute-force attacks, dictionary attacks, phishing, and replay attacks. When a user's password is transmitted over a network, even if encrypted, there remains a risk of interception and exploitation by adversaries. This vulnerability allows unauthorized individuals to gain access to legitimate user accounts, leading to data theft, identity fraud, and other illicit activities.

Furthermore, the reliance on human memory for complex passwords often results in users opting for simple, easily guessable passwords, or reusing passwords across multiple services, thereby diminishing the overall security posture. The existing literature, despite exploring various methodologies, often lacks definitive or universally applicable solutions for establishing a dependable and secure authentication framework that can effectively counter these evolving threats without introducing significant usability drawbacks.

3. OBJECTIVES OF THE RESEARCH

This paper aims to propose and analyze an innovative e-authentication system that integrates QR Code and One-Time Password (OTP) technologies to significantly enhance digital security. The main objectives of this system are:

i. To enhance the security of user authentication: By combining multiple authentication factors, the system aims to create a more robust defense against unauthorized access, making it significantly harder for adversaries to compromise user accounts.

ii. To mitigate vulnerabilities associated with traditional passwords: The system seeks to reduce reliance on static passwords by introducing dynamic, time-sensitive authentication credentials.

iii. To improve the user experience while maintaining high security: The goal is to provide a secure authentication method that is also convenient and intuitive for users, encouraging widespread adoption.

iv. To provide a comprehensive framework for secure online transactions: The system intends to offer a reliable mechanism for authenticating users in various online contexts, thereby safeguarding sensitive data during transmission and interaction.

v. To explore the integration of modern technologies: The paper will delve into how QR codes and OTPs can be effectively combined to create a synergistic authentication solution that leverages the strengths of both technologies.

4. SCOPE OF THE STUDY

This paper will focus on the theoretical framework, architectural design, and security implications of a QR Code and OTP-Based E-Authentication System. It will cover the fundamental principles of QR codes and OTPs, their individual advantages and limitations in security, and how their synergistic integration can address the shortcomings of traditional authentication methods. The scope includes:

i. A detailed literature review of existing authentication systems.

ii. An in-depth explanation of QR code and OTP technologies.

iii. A proposed system architecture and authentication process flow.

iv. A discussion on the security features, potential vulnerabilities, and mitigation strategies.

v. A comparative analysis with other authentication approaches.

While the paper will discuss implementation considerations conceptually, it will not delve into the specifics of coding or deployment of a fully functional system. The primary emphasis is on the design principles and security benefits of the proposed hybrid authentication model.

5. LITERATURE REVIEW

The literature review highlights the integration of QR codes and OTPs as a hybrid authentication model enhancing digital security. Conceptually, it balances usability and protection; theoretically, it aligns with multi-factor and cryptographic frameworks; empirically, studies confirm reduced phishing risks but emphasize the need for robust usability and implementation strategies.

5.1 Conceptual Review

The conceptual framework for a QR code and OTP–based e-authentication system conceptualizes authentication as layered verification combining “something you have” and “something you know” with temporal constraints. QR codes are treated as session-specific visual tokens bound to a registered mobile device, establishing device-session linkage when scanned. OTPs—time-based or counter-based—introduce ephemeral numeric proofs ensuring freshness. The framework models interactions among user identity, device integrity, session context, credential lifecycle, and threat vectors. It incorporates threat detection nodes, fallback paths for device loss, privacy-preserving storage, and design guidelines that balance robustness with minimal user friction.

Historically, authentication systems have predominantly relied on single-factor methods, primarily usernames and passwords. While seemingly straightforward, these methods suffer from significant limitations that render them increasingly inadequate in the face of evolving cyber threats. The fundamental flaw lies in their susceptibility to various attack vectors. For instance, passwords can be easily guessed, cracked through brute-force

or dictionary attacks, or compromised via phishing scams and keyloggers. Users often contribute to this vulnerability by choosing weak passwords, reusing them across multiple platforms, or failing to update them regularly (IEEE,).

Moreover, the transmission of passwords, even when encrypted, presents an opportunity for adversaries to intercept and exploit sensitive data. This risk is particularly pronounced in environments with lax security protocols or when users are unaware of potential vulnerabilities in their systems (Jain, 2004). The consequences of compromised traditional authentication methods are severe, ranging from unauthorized access to personal accounts and data breaches to significant financial losses and reputational damage for organizations.

5.2 Theoretical Review

The theoretical review synthesizes multi-factor authentication theory, Kerckhoffs's principle, and formal security models to analyze QR+OTP systems. It references TOTP/HOTP design principles and protocol analysis for secrecy and freshness properties. Human-computer interaction theories (cognitive load, affordance) clarify usability-security tradeoffs, while economic adoption frameworks explain organizational constraints. Game-theoretic attacker-defender models illustrate adversary incentives for phishing, relay, or replay attacks. Privacy minimization and threat modeling inform data storage and logging decisions. Together, these theoretical lenses predict that device-bound QR tokens plus ephemeral OTPs increase attacker cost but require careful UX and fallback design to ensure adoption.

The shortcomings of traditional password-based authentication have spurred the development of more sophisticated e-authentication systems. The evolution has been driven by the continuous arms race between cybercriminals and security professionals. Early enhancements included the introduction of multi-factor authentication (MFA), which requires users to provide two or more verification factors to gain access to a resource. These factors typically fall into three categories: something the user knows (e.g., password), something the user has (e.g., a token or smartphone), and something the user is (e.g., biometric data) (Karim, 2015).

Further advancements have seen the integration of various technologies, such as smart cards, biometric authentication (fingerprint, facial recognition, iris scan), and token-based systems. The goal has been to create more robust and user-friendly authentication experiences. However, each of these methods comes with its own set of challenges, including implementation complexity, cost, and potential vulnerabilities. For example, while biometrics offer convenience, they raise concerns about privacy and the immutability of biometric data if compromised.

Figure 1: the evolution of Authentication methods

5.3 Empirical Review

Empirical studies report security benefits yet mixed usability outcomes for combined QR and OTP approaches. Controlled lab experiments show reduced successful phishing and improved session binding when QR scans accompany OTPs, but usability tests reveal longer task times and occasional scan failures in poor lighting or on older devices. Field deployments in banking and enterprise single-sign-on contexts document fewer account takeovers, though implementations suffered from QR generation latency, synchronization errors, and increased support load. Studies recommend comprehensive user testing, accessible fallback methods, robust server-side logging, and performance tuning. Overall, empirical evidence supports security gains contingent on quality engineering and UX optimization.

QR codes, or Quick Response codes, have emerged as a promising component in e-authentication systems due to their ability to store a significant amount of information and their ease of use. A QR code is a two-dimensional barcode that can be scanned by a mobile device to quickly access embedded data. In authentication, QR codes are often used to facilitate a seamless login process without requiring manual entry of credentials. For instance, a user might scan a QR code displayed on a login screen with their registered mobile device, which then sends an authentication request to a server.

Existing QR code-based systems often leverage the mobile device as a trusted authenticator. The QR code itself might contain encrypted session tokens, temporary login credentials, or a unique identifier that links to the user's account. When scanned, the mobile application processes this information and communicates with the authentication server to verify the user's identity. This approach reduces the risk of phishing attacks, as

the user is not directly typing credentials into a potentially malicious website. However, QR code-based systems can be vulnerable to attacks if the QR code itself is tampered with or if the communication channel between the mobile device and the server is not adequately secured.

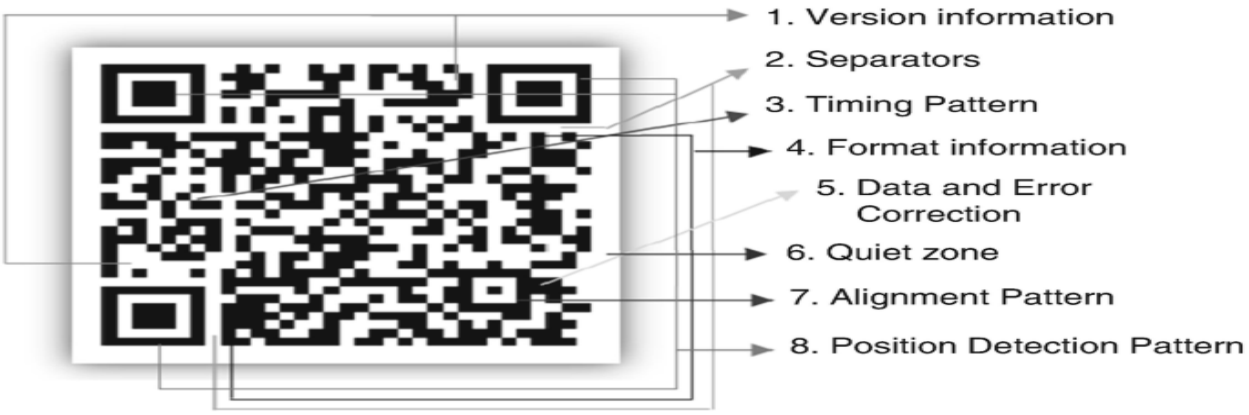


Figure 2: QR Code-Based Authentication Systems

One-Time Passwords (OTPs) have been widely adopted as a second factor in authentication due to their time-sensitive and single-use nature. An OTP is a password that is valid for only one login session or transaction and typically expires after a short period (e.g., 30-60 seconds) or after its first use. This characteristic significantly enhances security by mitigating the risks associated with static passwords, such as replay attacks and credential stuffing.

There are primarily two types of OTPs: Time-based One-Time Passwords (TOTP) and HMAC-based One-Time Passwords (HOTP). TOTPs are generated using a shared secret key and the current time, making them synchronized with a server. HOTPs, on the other hand, are event-based, generated using a shared secret and a moving counter. OTPs are typically delivered via SMS, email, or generated by authenticator applications (e.g., Google Authenticator). While highly effective against many common attacks, OTPs can still be vulnerable to man-in-the-middle attacks if not implemented correctly, where an attacker intercepts the OTP and uses it before the legitimate user (Karim, 2016).

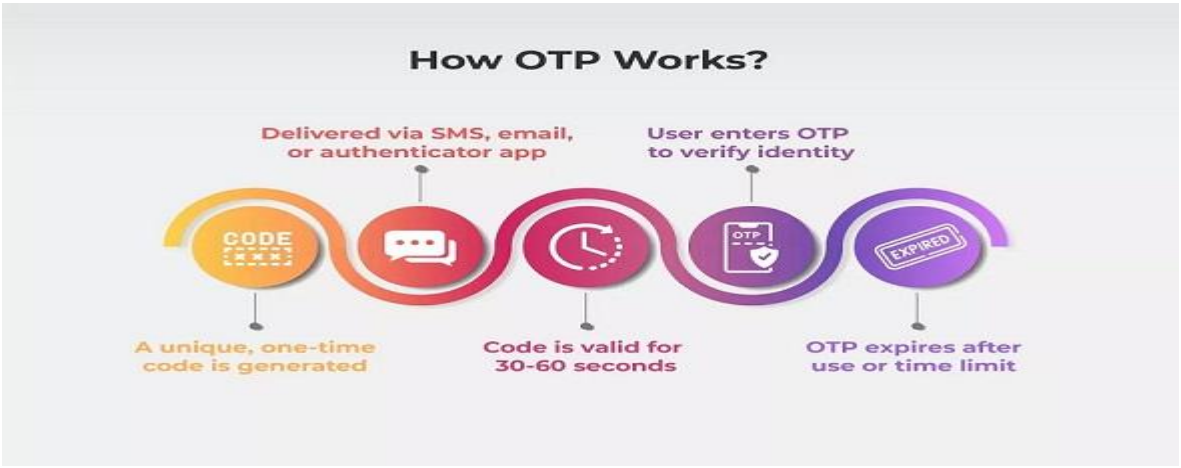


Figure 2.4 OTP-Based Authentication System

6. DISCUSSION

The Quick Response (QR) code, a type of two-dimensional barcode, was first developed in 1994 by Denso Wave, a subsidiary of Toyota, for tracking vehicles during manufacturing. Its primary purpose was to allow for high-speed component scanning. Unlike traditional one-dimensional barcodes, which can only store data horizontally, QR codes

encode information both horizontally and vertically, enabling them to store significantly more data. This enhanced data capacity and rapid readability quickly led to its adoption beyond the automotive industry, finding applications in logistics, advertising, and eventually, digital security (Karim, et al).

Working Principle

A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera and processed using Reed-Solomon error correction until the image can be appropriately interpreted (Jain, et al). The required data is then extracted from patterns present in both horizontal and vertical components of the image. The structure of a QR code includes several key components:

Finder Patterns: Three identical square patterns located at the corners of the QR code, used to orient the code for scanning.

Alignment Patterns: Smaller squares, present in larger QR codes that help to correct for distortion.

Timing Patterns: A line of alternating black and white modules that runs between the finder patterns, used to determine the coordinate system of the data modules.

Version Information: Specifies the version of the QR code standard being used (e.g., Version 1 to 40).

Format Information: Contains data about the error correction level and mask pattern used.

Data and Error Correction Keys: The actual data encoded in the QR code, along with error correction codes that allow the code to be read even if it is partially damaged or obscured.

Advantages in Security

In the context of digital security, QR codes offer several advantages:

i. **Ease of Use:** Scanning a QR code is often faster and less prone to human error than manually typing in URLs or complex codes. This convenience can encourage users to adopt more secure authentication practices.

ii. **Reduced Phishing Risk:** By eliminating the need to type credentials into a browser, QR codes can help mitigate certain types of phishing attacks. Users scan a code with a trusted device, which then handles the authentication process securely (Moini, 2009).

iii. **Data Capacity:** QR codes can store a substantial amount of data, including encrypted session tokens, temporary credentials, or unique identifiers, making them versatile for various authentication schemes (Okada, 2019).

iv. **Offline Capability:** QR codes can be generated and displayed in offline environments, providing flexibility in authentication scenarios where internet connectivity might be intermittent or unavailable on one of the devices (Sharma, 2020).

Limitations and Vulnerabilities

Despite their advantages, QR codes are not without limitations and potential vulnerabilities in security applications:

i. **Visual Tampering**: Malicious actors can replace legitimate QR codes with fraudulent ones, redirecting users to phishing sites or downloading malware. Users may not be able to visually distinguish between a genuine and a malicious QR code (Saranya, 2016).

ii. **Man-in-the-Middle (MitM) Attacks:** If the communication channel between the scanning device and the authentication server is not adequately secured, an attacker could intercept the data transmitted via the QR code (Srivastava, 2016).

iii. **Lack of User Verification:** The act of scanning a QR code itself does not verify the user's identity. Additional authentication factors are necessary to ensure that the person scanning the code is the legitimate user (Jain, et al).

iv. **Dependency on Scanning Device:** The security of a QR code-based system relies heavily on the security of the scanning device (e.g., smartphone). If the device is compromised, the authentication process can be undermined (Sharma, et al).

One-Time Password (OTP)

One-Time Passwords (OTPs) are dynamic authentication codes that are valid for a single login session or transaction. They are a crucial component of multi-factor authentication (MFA) systems. There are two primary types of OTPs:

i. **Time-based One-Time Password (TOTP):** TOTPs are generated using a shared secret key and the current time. Both the authentication server and the user's device (e.g., a smartphone app) generate the OTP independently but synchronously. The OTP typically changes every 30 or 60 seconds. This time-sensitive nature makes TOTPs highly resistant to replay attacks, as an intercepted OTP quickly becomes invalid (Tesla, 2016).

ii. **HMAC-based One-Time Password (HOTP):** HOTPs are event-based, meaning they are generated using a shared secret key and a moving counter. Each time an OTP is requested or used, the counter increments. Both the server and the client maintain synchronized counters. If an OTP is used, the counter on both sides' advances. HOTPs are less common in consumer applications but are used in specific security contexts (Okada, et al.).

Working Principle

The general working principle of an OTP system involves a shared secret key known only to the user's authenticator (e.g., a mobile app or hardware token) and the authentication server. When a user attempts to log in or perform

a transaction, the server requests an OTP. The user then generates an OTP using their authenticator, which applies a cryptographic algorithm (e.g., HMAC-SHA1 for HOTP, or a similar algorithm incorporating time for TOTP) to the shared secret and a variable parameter (time or counter). The generated OTP is then entered by the user and sent to the server. The server independently calculates its own OTP using the same shared secret and variable parameter. If the two OTPs match (within a small-time window for TOTP or counter deviation for HOTP), the authentication is successful.

Advantages in Security

OTPs offer significant security advantages over static passwords:

i. **Immunity to Replay Attacks:** Since each OTP is valid only once, an attacker who intercepts an OTP cannot reuse it to gain unauthorized access.

ii. **Protection against Phishing**: Even if a user falls victim to a phishing attack and enters their OTP on a fake website, the OTP will likely expire or be used by the attacker before the legitimate user can complete their login, thus limiting the attacker's window of opportunity.

iii. **Resistance to Brute-Force Attacks**: The short validity period and single-use nature of OTPs make brute-force attacks impractical, as the attacker would need to guess a new code within a very narrow timeframe for each attempt (Sharma, et al).

iv. **Enhanced Credential Security**: OTPs add a layer of security that does not rely on the user's memory, reducing the risk associated with weak or reused passwords.

Limitations and Vulnerabilities

Despite their strengths, OTPs also have limitations and potential vulnerabilities:

i. **Man-in-the-Middle (MitM) Attacks**: Sophisticated MitM attacks can still compromise OTPs if the attacker can intercept both the user's credentials and the OTP in real-time and use them before the legitimate user.

ii. **SMS-based OTP Vulnerabilities:** OTPs delivered via SMS can be vulnerable to SIM-swapping attacks, where an attacker takes control of the user's phone number and receives the OTPs [1].

iii. **Usability Challenges**: While generally convenient, some users may find the process of generating and entering OTPs cumbersome, especially if they are not accustomed to using authenticator apps or if network delays affect SMS delivery.

iv. **Shared Secret Compromise:** If the shared secret key used to generate OTPs is compromised, the entire system's security is at risk.

Proposed QR Code and OTP-Based E-Authentication System

To address the limitations of traditional authentication methods and enhance digital security, this paper proposes a hybrid e-authentication system that synergistically combines QR Code and One-Time Password (OTP) technologies. This integrated approach aims to leverage the strengths of both methods while mitigating their individual vulnerabilities, thereby providing a more robust, user-friendly, and secure authentication framework.

System Architecture

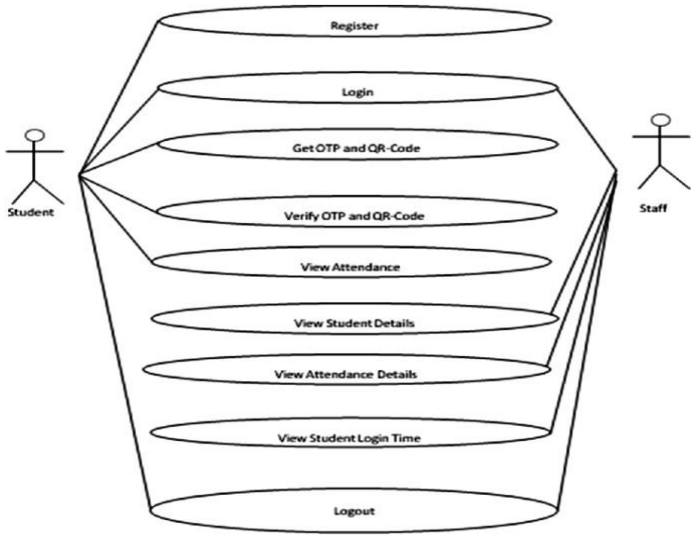
The proposed system comprises several key components working in concert to facilitate secure user authentication. A high-level architectural overview includes:

i. **User Device (Client):** This is typically a smartphone or a computer with a camera and an installed authenticator application. The authenticator app is responsible for scanning QR codes, generating OTPs, and securely communicating with the authentication server.

ii. **Authentication Server**: This central component manages user accounts, stores shared secrets for OTP generation, validates QR code data, verifies OTPs, and authorizes access to protected resources. It is equipped with robust cryptographic modules and secure database management.

iii. **Web Application/Service**: The application or service that requires user authentication. It interacts with the authentication server to delegate the authentication process.

iv. **Database:** A secure database stores user credentials (hashed passwords), shared secrets for OTPs, user profiles, and logs of authentication attempts. It is crucial that this database is protected against unauthorized access and data breaches.



Authentication Process Flow (Sharma, et al)

The authentication process in the proposed system involves a multi-step, two-factor mechanism designed to ensure both security and usability:

i. **Initiation of Login:** The user navigates to the login page of the web application/ service. Instead of immediately prompting for a username and password, the application displays a unique, dynamically generated QR code on the screen.

ii. **QR Code Generation and Session ID:** The web application requests the Authentication Server to generate a temporary session ID and embed it, along with a timestamp and other relevant metadata, into a QR code. This QR code is then displayed to the user.

iii. **User Scans QR Code**: The user opens their dedicated authenticator application on their smartphone and scans the displayed QR code. The authenticator app decrypts the QR code to extract the session ID and other embedded information.

iv. **OTP Generation:** Upon successful scanning, the authenticator app, using a pre-shared secret key (established during initial registration) and the current time (for TOTP), generates a One-Time Password (OTP).

v. **Submission of Credentials**: The authenticator app then securely transmits the generated OTP, along with the user's username (or a derived identifier), and the session ID to the Authentication Server. This communication is encrypted using secure protocols (e.g., HTTPS).

vi. **Server-Side Verification:** The Authentication Server receives the submitted data. It retrieves the corresponding shared secret for the user from its secure database and independently generates an OTP using the same algorithm and parameters (session ID, timestamp, shared secret). It then compares the usersubmitted OTP with its internally generated OTP.

vii. **Authorization:** If the OTPs match and the session ID is valid and within its active timeframe, the Authentication Server verifies the user's identity. It then issues an authentication token (e.g., a JWT) to the web application/service, granting the user access to the requested resources.

viii. **Access Granted:** The web application/service receives the authentication token and allows the user to access their account.

This process ensures that even if an attacker manages to intercept the QR code or the OTP, they cannot easily replay the authentication, as the OTP is time-sensitive and the session ID is unique to each login attempt.

Security Features and Mechanisms (Tesla, et al)

The proposed system incorporates several security features to enhance protection against various cyber threats:

Two-Factor Authentication (2FA): By requiring both

Something the user has (the authenticator app generating the OTP) and something the user knows (their username/password for initial access or registration), the system significantly elevates the security posture beyond single-factor methods.

i. **Time-Sensitive OTPs:** The use of TOTP ensures that each generated password is valid for a very short duration, making replay attacks extremely difficult. An intercepted OTP quickly becomes useless to an attacker.

ii. **Dynamic QR Codes:** The QR codes are dynamically generated for each login attempt, embedding unique session identifiers and timestamps. This prevents attackers from using static, pre-captured QR codes for unauthorized access.

iii. **Encrypted Communication**: All communication between the user device, authentication server, and web application is secured using industry-standard encryption protocols (e.g., HTTPS/TLS). This protects against man-in-the-middle attacks and ensures the confidentiality and integrity of transmitted data.

iv. **Shared Secret Protection**: The shared secret keys used for OTP generation are stored securely on both the user's authenticator app and the authentication server's database, typically encrypted and protected against unauthorized access. They are never transmitted over the network in plain text.

v. **Hashing and Salting**: User passwords (if used for initial registration) are stored as cryptographic hashes with unique salts in the database, preventing direct retrieval even if the database is compromised.

vi. **Session Management**: Robust session management ensures that authenticated sessions are properly maintained, invalidated upon logout, and protected against session hijacking.

Advantages of the Proposed System (Jain, et al)

The integration of QR codes and OTPs offers several distinct advantages over standalone authentication methods:

i. **Enhanced Security:**The combination of two distinct authentication factors (QR code for session initiation and OTP for verification) creates a strong barrier against various cyber threats, including phishing, replay attacks, and credential stuffing.

ii. **Improved User Experience**: Scanning a QR code is often quicker and more convenient than manually typing complex passwords or waiting for SMS-based OTPs. The authenticator app provides a seamless experience, reducing friction in the login process.

iii. **Reduced Reliance on SMS**: By primarily using authenticator apps for OTP generation, the system reduces dependency on SMS, which can be vulnerable to SIM-swapping attacks and network delays.

iv. **Offline OTP Generation:** Authenticator apps can generate TOTPs even without an internet connection on the user's device, providing flexibility and reliability.

v. **Scalability and Flexibility:** The modular design allows for easy integration into various web applications and services, and it can be scaled to accommodate a large number of users.

vi. **Cost-Effectiveness:** Compared to hardware tokens, software-based authenticator apps are more cost-effective to deploy and maintain.

Implementation Details (Conceptual)

While this paper primarily focuses on the theoretical framework and architectural design of the QR Code and OTP-Based E-Authentication System, a conceptual overview of its implementation details is essential to understand its practical feasibility. The system can be developed using a client-server architecture, with distinct components for the frontend (user interface), backend (server-side logic), and database (data storage).

Frontend Implementation

The frontend component would be responsible for presenting the user interface for login and interaction. This would typically involve:

i. **Web Interface:** A web-based login page developed using modern web technologies such as HTML, CSS, and JavaScript (with frameworks like React, Angular, or Vue.js). This page would display the dynamically generated QR code and provide input fields for the username and OTP (if required for initial setup or fallback). The frontend would communicate with the backend API to initiate authentication requests and receive responses.

ii. **Mobile Authenticator Application**: A dedicated mobile application (for iOS and Android) would serve as the primary authenticator. This app would be developed using native languages (Swift/Kotlin) or cross-platform frameworks (React Native, Flutter). Its core functionalities would include:

iii. **QR Code Scanner:** Utilizing the device's camera to scan and parse the QR code displayed on the web interface.

iv. **OTP Generator:** Implementing the TOTP algorithm to generate timesensitive one-time passwords based on a shared secret key.

v. **Secure Communication Module**: Encrypting and transmitting the generated OTP and user identifiers to the authentication server via secure API calls.

vi. **User Enrollment:** A process within the app to securely provision the shared secret key during initial user registration (Tiwari, 2016).

Backend Implementation

The backend forms the core logic of the authentication system, handling all serverside operations. It can be implemented using robust programming languages and frameworks such as Python (with Flask or Django), Node.js (with Express), Java (with Spring Boot), or Go. Key backend modules would include:

i. **API Endpoints:** RESTful APIs to handle various authentication requests, including QR code generation, OTP validation, user registration, and session management.

ii. **QR Code Generation Service:** A module responsible for generating unique QR codes for each login attempt, embedding session IDs, timestamps, and other encrypted metadata. This service would ensure the QR codes are dynamic and single-use.

iii. **OTP Validation Service:** This module would implement the TOTP algorithm to independently generate and verify OTPs. It would compare the OTP submitted by the user with the server-generated OTP, accounting for time drift.

iv. **User Management Module:** Handling user registration, password hashing and storage, and shared secret key management for OTPs.

v. **Session Management**: Creating, validating, and invalidating user sessions, issuing authentication tokens (e.g., JSON Web Tokens - JWTs), and ensuring secure session lifecycle.

vi. **Logging and Auditing**: Comprehensive logging of all authentication attempts, successes, and failures for security auditing and incident response (Tiwari, et al).

Database Design

A secure and efficient database is critical for storing user information and authentication-relate data. A relational database (e.g., PostgreSQL, MySQL) or a NoSQL database (e.g., MongoDB) could be used, depending on scalability and data structure requirements. Key tables/collections would include:

i. **Users Table:** Stores user credentials (hashed passwords and salts), unique user IDs, email addresses, and other profile information.

ii. **OTP Secrets Table:** Stores the securely encrypted shared secret keys for each user, essential for OTP generation and validation. These secrets must be protected with strong encryption at rest.

iii. **Sessions Table:** Manages active user sessions, storing session IDs, associated user IDs, creation and expiration timestamps, and other session-related metadata. * **Audit Logs

iv. **Table:** Records all authentication events, including timestamps, user IDs, IP addresses, and outcomes (success/failure), crucial for security monitoring and compliance.

All sensitive data within the database, especially shared secrets and hashed passwords, must be encrypted and protected with appropriate access controls to prevent unauthorized disclosure. Regular security audits and penetration testing would be essential to ensure the integrity and confidentiality of the stored data (Sharma, et al).

SECURITY ANALYSIS AND DISCUSSION

6.1 Comparison with Existing Systems

The proposed QR Code and OTP-Based E-Authentication System offers significant security enhancements when compared to traditional single-factor authentication methods and even some existing two-factor solutions. Traditional username/ password systems are highly vulnerable to phishing, brute-force attacks, and credential stuffing, as static credentials can be easily compromised and reused. The proposed system mitigates these risks by introducing dynamic, time-sensitive factors.

Compared to SMS-based OTP systems, our approach reduces the vulnerability to SIM-swapping attacks, as the primary OTP generation relies on a dedicated authenticator application rather than network-dependent SMS delivery. While SMS OTPs are convenient, their reliance on mobile network security introduces a potential weak point. Furthermore, the integration of QR codes streamlines the initial authentication step, offering a more user-friendly experience than manually entering codes or waiting for SMS messages.

Biometric authentication systems, while offering convenience and strong identity verification, face challenges related to privacy concerns and the immutability of biometric data. If biometric data is compromised, it cannot be easily changed, unlike a password or a shared secret for OTP. The proposed system avoids these specific biometric vulnerabilities while still providing a strong second factor of authentication (IEE, et al).

6.2 Threat Model and Mitigation Strategies

Despite its robust design, any security system must consider potential threats. This section outlines a threat model for the proposed system and discusses corresponding mitigation strategies:

Phishing Attacks:

Threat: An attacker creates a fake login page that mimics the legitimate one, attempting to trick users into scanning a malicious QR code or entering their OTP.

Mitigation: The system design inherently reduces phishing risk by not requiring users to type credentials directly into the web page. The authenticator app should be designed to verify the legitimacy of the QR code's origin (e.g., by checking the domain embedded in the QR code against a whitelist) before generating an OTP. User education on verifying URLs and using trusted authenticator apps is crucial.

Man-in-the-Middle (MitM) Attacks:

Threat: An attacker intercepts communication between the user's device and the authentication server, potentially capturing session IDs or OTPs.

Mitigation: All communication channels must be secured using strong encryption protocols (e.g., HTTPS/TLS with strict certificate pinning). The dynamic nature of QR codes and time-sensitive OTPs further limits the window of opportunity for an attacker to use intercepted data (Tiwari, et al).

QR Code Tampering/Substitution:

Threat: An attacker physically replaces a legitimate QR code with a malicious one (e.g., on a public terminal) or digitally alters the QR code displayed on a compromised screen.

Mitigation: The system should implement mechanisms for the authenticator app to verify the integrity and authenticity of the scanned QR code, possibly through digital signatures embedded within the QR code data. Users should be advised to be cautious of QR codes in untrusted environments.

Authenticator App Compromise:

Threat: The user's smartphone or the authenticator application itself is compromised by malware, allowing an attacker to generate or intercept OTPs.

Mitigation: The authenticator app must be developed with robust security practices, including secure storage of shared secrets, code obfuscation, and tamper detection. Users should be encouraged to keep their devices updated and use reputable security software.

Shared Secret Compromise:

Threat: The shared secret key used for OTP generation is stolen from the authentication server's database.

Mitigation: secrets must be stored encrypted at rest and protected by multiple layers of security controls, including strong access management, intrusion detection systems, and regular security audits. Key rotation policies should also be in place.

6.3 Potential Vulnerabilities and Future Enhancements (Tiwari, et al)

While the proposed system significantly enhances security, it is important to acknowledge potential vulnerabilities and areas for future improvement:

Usability vs. Security Trade-off: While QR codes and OTPs improve usability over complex passwords, some users might still find the multi-step process cumbersome. Future enhancements could explore adaptive authentication, where the level of security required adjusts based on user behavior and risk context.

Recovery Mechanisms: Secure account recovery mechanisms are critical. If a user loses their device or forgets their credentials, a robust and secure recovery process must be in place without introducing new vulnerabilities.

Advanced Threat Detection: Integrating advanced threat detection mechanisms, such as behavioral analytics and machine learning, could help identify and respond to novel attack patterns that might bypass current authentication checks.

Hardware Security Modules (HSMs): For extremely high-security environments, storing shared secrets in Hardware Security Modules (HSMs) could provide an even stronger level of protection against server-side compromises.

Decentralized Identity: Exploring integration with decentralized identity solutions (e.g., block chain-based identities) could offer enhanced privacy and user control over their authentication credentials in the long term.

7. CONFLICT OF INTEREST

Conflict of interest in developing or evaluating QR code and OTP-based e-authentication systems arises when researchers, developers, or stakeholders hold financial, professional, or personal interests that may bias outcomes. For instance, developers affiliated with cybersecurity firms may overstate effectiveness, while funders could influence results to favor adoption. Such conflicts risk undermining credibility, transparency, and objectivity in system design or evaluation. To mitigate this, disclosure of affiliations, independent audits, and adherence to ethical guidelines are essential. Acknowledging and managing conflicts ensures trust, integrity, and fairness in advancing secure, reliable, and user-centered authentication technologies across diverse application domains.

8. ETHICAL CONSIDERATION

Ethical considerations in implementing QR code and OTP-based e-authentication systems focus on safeguarding user privacy, data protection, and informed consent. Personal identifiers, QR codes, and OTP records must be securely encrypted, stored minimally, and accessed only by authorized entities. Users should be clearly informed about data collection practices, potential risks, and system limitations. Accessibility and inclusivity are essential to ensure no group is excluded due to device, literacy, or disability barriers. Compliance with regulations such as GDPR and NDPR must guide design. Ultimately, ethical responsibility ensures that enhanced security does not compromise human rights, fairness, or user trust.

9. CONCLUSION

In conclusion, the increasing sophistication of cyber threats necessitates a paradigm shift in digital security, moving beyond the vulnerabilities inherent in traditional single-factor authentication

Methods. This seminar paper has proposed and analyzed a robust e-authentication system that synergistically combines QR Code and One-Time Password (OTP) technologies to address these contemporary security challenges. By integrating the convenience and data capacity of QR codes with the time-sensitive, single-use nature of OTPs, the system establishes a formidable multifactor authentication framework.

The proposed system significantly enhances digital security by mitigating common attack vectors such as phishing, replay attacks, and credential stuffing. It offers a more secure alternative to SMS-based OTPs by leveraging dedicated authenticator applications, thereby reducing susceptibility to SIM-swapping. Furthermore, the dynamic generation of QR codes, coupled with encrypted communication channels and secure storage of shared secrets, fortifies the system against various forms of tampering and interception. While acknowledging potential vulnerabilities and the continuous evolution of cyber threats, the system's design prioritizes both security and user experience, aiming to foster broader adoption of stronger authentication practices.

Ultimately, this hybrid QR Code and OTP-Based E-Authentication System represents a significant step forward in securing digital interactions. Its architectural design and proposed mechanisms lay a strong foundation for future research and development in adaptive authentication, advanced threat detection, and integration with emerging identity solutions, paving the way for a more secure and trustworthy

digital ecosystem.

10. RECOMMENDATION

Recommendations for QR code and OTP-based e-authentication systems emphasize strengthening security, usability, and scalability. Developers should adopt strong encryption standards, secure key management, and real-time monitoring to mitigate threats. Usability testing must address accessibility issues, ensuring inclusivity across devices and user groups. Organizations are advised to implement backup authentication methods to prevent lockouts. Regular updates, audits, and compliance with data protection laws like GDPR and NDPR should be maintained. Integration with biometrics may further enhance multi-factor protection. Finally, promoting user awareness and training fosters trust and reduces human error, ensuring the system's effectiveness in real-world applications.

REFERENCES

Alexandre, B., Reynaud, E., Osiurak, F., & Navarro, J. (2018). Acceptance and acceptability criteria: A literature review. Cognition, Technology & Work, 20(2), 165–

Ataelfadiel, M. A. (2022, September). E-Authentication System Using QR Code & OTP. Research Journal of Innovations in Engineering and Technology - IRJIET, pp. 75-81.

E-Authentication System using QR Code and OTP. (n.d.). Retrieved from [https:// ijarsct.co.in/Paper14204.pdf](https://ijarsct.co.in/Paper14204.pdf)

Edwards, C., Holmes, W., Whitelock, D., & Okada, A. (2018). Student trust in e-authentication. In Proceedings of the Fifth Annual ACM Conference on Learning at Scale, UK, Article No.: 42, 1–4. https://doi.org/10.1145/3231644.3231700.

IEEE International Conference on Engineering and Technology (ICETECH) (pp. 173-177). IEEE.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4– 20. https://doi.org/10.1109/TCSVT.2003.818349.

Karim, N. A., & Shukur, Z. (2015). Review of user authentication methods in online examination. Asian Journal of Information Technology, 14(5), 166–175.

Karim, N. A., & Shukur, Z. (2016). Proposed features of an online examination interface design and its optimal values. Computers in Human Behavior, 64, 414–

Moini, A., & Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: A systems

Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2019). E-authentication for online assessment: A mixed-method study. British Journal of Educational Technology, 50(2), 861– 875. https://doi.org/10.1111/bjet.12608.

perspective. IEEE Systems Journal, 3(4), 469–

Saranya, K., Reminaa, R. S., & Subhitsha, S. (2016, March). Modern applications of QR-Code for security. In 2016

Sharma, M. K., & Nene, M. J. (2020). Dual factor thirdparty biometric-based authentication scheme using quantum onetime passwords. Security and Privacy, 3(6), e129.

Srivastava, S., & Sivasankar, M. (2016, August). On the generation of alphanumeric one time passwords. In 2016 International Conference on Inventive Computation Technologies

TeSLA. (2016). The TeSLA project home page. https://tesla-project.eu/. Accessed 18 Feb 2018.

The downloaded PDF file also mentions reference 13: OTPs address numerous issues associated with traditional passwords, notably mitigating vulnerabilities such as susceptibility to replay attacks and phishing scams. Unlike standard passwords, an expired OTP cannot be exploited by an adversary who intercepts it post-use, thereby enhancing security. Nevertheless, a drawback of OTPs is their inherent complexity, posing a challenge for users to memorize them.

for security. In 2016 IEEE International Conference on Engineering and Technology (ICETECH) (pp. 173-177). IEEE.

Tiwari, S. (2016, December). An introduction to QR code technology. In 2016 international conference on information technology (ICIT) (pp. 39-44). IEEE.

(ICICT) (Vol. 1, pp. 1-3). IEEE.

177. https://doi.org/10.1007/s10111-018-0459-1.

422. https://doi.org/10.1016/j.chb.2016.07.013.

476. https://doi.org/10.1109/JSYST.2009.2038957.