Effective And Secure Two-Factor Multi Server Authentication Scheme Without Password

R.Vaishnavi
Software Engineering Kakatiya Institute Of Technology & Science
Warangal, India
rayabharapuvaishnavi@gmail.com

Dr.C.Srinivas
Associate Professor,CSED, Kakatiya Institute Of Technology & Science
Warangal, India cs.cse@kitsw.ac.in

***Abstract*— This paper presents a secure two-factor, password-less authentication scheme designed for multi-server environments. The proposed approach eliminates the use of traditional passwords to address common security vulnerabilities and enhance system security. It combines asymmetric cryptography with Time-Based One-Time Passwords (TOTP) to provide strong user authentication. In this scheme, a user signs a server-generated challenge using a private key, which is verified by the server through the corresponding public key. An additional layer of security is provided by validating a TOTP generated through an authenticator application within a defined time window. The architecture separates registration and authentication across multiple servers, improving scalability and flexibility. The scheme effectively resists brute-force, phishing, and replay attacks while maintaining a smooth and user-friendly authentication experience.**

I. INTRODUCTION

Authentication is a fundamental aspect of security in modern digital systems, as it protects sensitive information and prevents unauthorized access to electronic resources. Traditional password-based authentication methods have become increasingly vulnerable to attacks such as phishing, brute-force attempts, password hijacking, and social engineering. Despite the widespread adoption of multi-factor authentication (MFA), many systems continue to rely heavily on passwords, which remain a major source of security risk.

To overcome these challenges, this work introduces an effective and secure two-factor, password-less scalability and ensures secure authentication without requiring users to remember or manage passwords.

By combining strong cryptographic techniques with two-factor authentication, the proposed password-less scheme offers a secure, flexible, and standardized solution for modern cybersecurity requirements. It effectively addresses the limitations of existing authentication mechanisms and provides robust protection against common attacks such as password hijacking, brute-force attacks, and replay attacks, thereby contributing a promising direction for next-generation authentication systems.

A. ***GOAL***

The primary goal of this project is to design and implement an effective and secure two-factor, password- less authentication scheme for multi-server environments. The system replaces traditional password- based authentication with a password-less approach using asymmetric cryptography (digital signatures) and Time-Based One-Time Passwords (TOTP).

The project aims to enhance security by protecting against common cyber-attacks such as phishing, brute- force, replay, and man-in-the-middle attacks. By adopting a multi-server architecture that separates registration and authentication processes, the system improves scalability, reliability, and performance.
Overall, the goal is to provide a secure, scalable, and user-friendly authentication solution suitable for modern web and distributed applications.
authentication scheme for multi-server environments. The proposed approach completely eliminates the use of passwords and replaces them with a more secure and user-friendly authentication mechanism based on cryptographic signatures and Time-Based One-Time Passwords (TOTP). By employing asymmetric cryptography for identity verification and time-stamped tokens as an additional security layer, the scheme strengthens the authentication process and mitigates vulnerabilities inherent in password-based systems.

The proposed system adopts a multi-server architecture to enhance scalability and reliability. A dedicated registration server securely manages user cryptographic keys and TOTP secrets, while application servers perform authentication by validating cryptographic signatures and one-time passwords. This separation of responsibilities improves system

B. ***OBJECTIVES***

The primary objectives of the Effective and Secure Two-Factor Multi-Server Authentication Scheme without Passwords are to eliminate the use of traditional passwords and thereby reduce security risks such as password theft, phishing, and weak credential practices. The system aims to enhance authentication security by incorporating cryptographic signatures and Time-Based One-Time Passwords (TOTP), while utilizing asymmetric cryptography through public–private key pairs for secure identity verification. By employing layered protection with time-limited one-time passwords and a multi-server architecture that separates registration and authentication processes, the scheme ensures scalability, reliability, and improved performance.
Additionally, the project seeks to deliver a seamless, password-less user experience, protect against common cyber-attacks such as brute-force and man-in-the-middle attacks, and provide flexibility for integration into existing systems, making it suitable for large-scale deployment in modern web and distributed applications.

C. METHODOLOGY

The proposed system adopts a multi-server architecture to implement a secure, password-less authentication mechanism. A dedicated registration server handles user enrollment, cryptographic key pair generation, and Time-Based One-Time Password (TOTP) secret creation. An application server is responsible for processing login requests by verifying digital signatures and validating TOTP codes.

Asymmetric cryptography is used to authenticate users through public–private key pairs, where the private key is securely stored on the user's device and the public key is maintained on the server. During authentication, the user signs a server-generated challenge, which is verified by the application server, along with a TOTP generated through an authenticator application. Authentication is granted only when both verifications succeed, ensuring enhanced security, scalability, and resistance to common cyber-attacks..

D. ALGORITHMIC COMPONENTS AND THEIR WORKING

1) User Regestration and Key Generation

The registration algorithm initiates when a user interacts with the registration server through a secure interface.
During this process, the system generates a unique RSA public–private key pair associated with a unique user identifier. The private key is securely transmitted to the user and stored on a user-controlled device, while the public key is stored securely in the system database. This step establishes the cryptographic identity of the user and removes the need for password-based credentials.

2) TOTP Secret Generation and Configuration

After key generation, the system generates a unique Time-Based One-Time Password (TOTP) secret using Base32 encoding. This secret is converted into a QR code and provided to the user for configuration in a TOTP-compatible authenticator application such as Google Authenticator. The TOTP secret is securely stored on the server and linked to the user's identity, enabling time-based verification during authentication.

3) Challenge Generation and User Initiation Algorithm

When a user initiates the login process, the application server generates a random challenge string (nonce). This challenge is unique for each session and prevents replay attacks. The generated challenge is sent to the user and acts as the input for cryptographic signature creation.

4) Digital Signature Verification

The user signs the server-issued challenge using their private RSA key. The application server verifies the received digital signature using the corresponding public key stored during registration. Successful verification confirms the authenticity of the user and ensures that the request has not been tampered with during transmission.

5) TOTP Verification and Authentication Decision

In parallel with signature verification, the user submits a TOTP generated by the authenticator application. The server retrieves the stored TOTP secret and validates the submitted code against the expected value for the current time window. Authentication is granted only when both the digital signature and TOTP verification are successful. If either check fails, access is denied and the attempt is flagged for further review.

6) Security Logging and Monitoring Algorithm

In parallel with signature verification, the user submits a TOTP generated by the authenticator application. The server retrieves the stored TOTP secret and validates the submitted code against the expected value for the current time window. Authentication is granted only when both the digital signature and TOTP verification are successful. If either check fails, access is denied and the attempt is flagged for further review.

E. MODEL TRAINING AND SYSTEM OPTIMIZATION

To evaluate the effectiveness of the proposed Effective and Secure Two-Factor Multi-Server Authentication Scheme without Passwords, a comprehensive set of experiments was conducted to simulate real-world authentication scenarios. The evaluation focused on system security, performance efficiency, and overall user experience under various test conditions.

After deployment, system performance is evaluated using metrics such as accuracy, response rate, and reminder success ratio. A confusion matrix is used to compare scheduled reminders with actual responses.

When performance is suboptimal, key parameters—such as reminder intervals, notification types, and alert repetition frequency—are fine-tuned to enhance system reliability.

F. SYSTEM FUNCTIONALITY

The experimental environment was configured using Python as the programming language and Flask as the backend framework to simulate server-side APIs. Security-related operations were implemented using cryptographic libraries such as cryptography for asymmetric encryption and pyotp for Time-Based One-Time Password generation.
Authentication testing was performed using standard authenticator applications for TOTP validation. All experiments were executed on a Windows operating system using a local environment.

Testing and Verification :

A structured testing and verification process was followed to validate system reliability, security, and correctness.

Functional Testing:

Functional testing confirmed that all system components operated as expected, including key generation and user registration, digital signature verification, TOTP generation and validation, and secure communication between servers.

Security Testing :

Security testing verified protection against common cyberattacks. Replay attacks were prevented through time-limited TOTP validation, man-in-the-middle attacks were mitigated using asymmetric encryption, and brute-force attacks were effectively eliminated by removing password-based authentication entirely.

Performance Testing :
System performance was evaluated based on response time and scalability. Multiple simultaneous authentication requests were generated to stress-test the backend. The response times for digital signature verification and TOTP validation were analyzed to ensure acceptable performance under load.

Multi-Server Communication Verification :
Testing was conducted to validate secure and reliable communication between the registration server and the authentication server. Public key sharing and verification processes were tested to ensure data integrity and correct synchronization across servers.

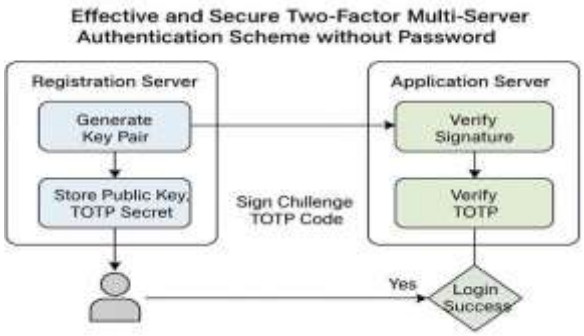
Usability Evaluation :
Usability testing confirmed a positive user experience. End users were able to authenticate successfully without remembering passwords, relying instead on private keys and one-time passwords. This significantly reduced cognitive load while maintaining strong security.

Error Conditions and Logging :
Error handling was tested using invalid OTPs, expired tokens, and corrupted cryptographic keys. All error events were accurately logged, and log entries were verified to support effective monitoring, debugging, and security auditing without exposing sensitive information

G. INNOVATIVENESS

The proposed system introduces an innovative password-less authentication approach by combining asymmetric cryptography with Time-Based One-Time Passwords (TOTP) in a multi-server environment. Unlike traditional authentication methods that rely on static passwords, the system eliminates password-related vulnerabilities such as phishing and brute-force attacks. The separation of registration and authentication across multiple servers enhances scalability, reliability, and security. By providing strong two-factor protection with a seamless user experience, the system offers a modern, secure, and adaptable solution for next-generation web and distributed applications.

Fig. 1. Flow Diagram



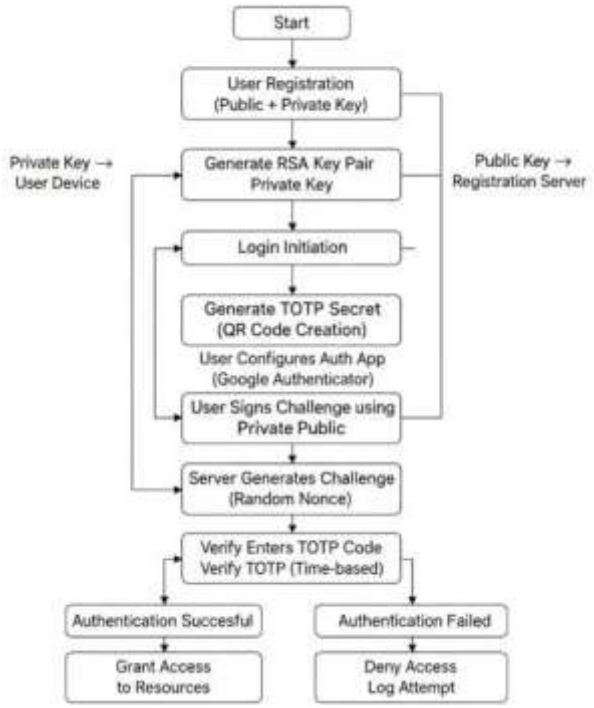


Fig. 2. Activity Diagram of Authentication

- **Successful Password-less Authentication:**

Users were able to authenticate securely and accurately using only a cryptographic key pair and a Time-Based One-Time Password (TOTP), completely eliminating the need for traditional passwords.

- **Enhanced Security:**

The system effectively resisted common cyber- attacks, including brute-force attacks due to the absence of passwords, replay attacks through time- limited TOTP validation, and man-in-the-middle attacks using digital signatures and encrypted communication. Sensitive credentials such as private keys were never transmitted over the network.

- **Multi-Server Architecture Validation:**

Secure interaction between the registration server and the authentication server functioned as expected. Public keys and shared secrets were exchanged and verified correctly, demonstrating the reliability of the multi-server model.

- **Scalability and Performance:**

Authentication requests were processed within acceptable time limits, making verification delays negligible. The system successfully handled multiple concurrent authentication requests, indicating good scalability and suitability for real- world deployment.

The real-time performance was further validated by simulating multiple overlapping schedules. Even under maximum load, the system delivered notifications promptly:

I. CONCLUSION

This work presented an effective and secure two-factor, password-less authentication scheme designed for multi-server environments. By eliminating traditional passwords and combining asymmetric cryptography with Time-Based One-Time Passwords (TOTP), the proposed system significantly reduces common security vulnerabilities such as brute-force, phishing, replay, and man-in-the-middle attacks. The multi-server architecture successfully separates registration and authentication processes, improving scalability, reliability, and system performance.
Experimental evaluation demonstrated secure authentication, efficient response times, and support for concurrent users. Overall, the proposed scheme offers a secure, scalable, and user-friendly authentication solution
suitable for modern web and distributed applications.

H. EXPERIMENTS & RESULTS

The implementation and testing of the proposed Effective and Secure Two-Factor Multi-Server Authentication Scheme without Passwords produced the following key outcomes:

J. FUTURE SCOPE

The proposed password-less two-factor multi-server authentication scheme can be further enhanced in several ways. Future work may include integrating biometric

authentication to provide an additional security layer alongside cryptographic keys and TOTP. The system can also be extended to support cloud-based deployment and large-scale distributed environments for enterprise applications. Incorporating adaptive or AI-based risk analysis can help dynamically adjust authentication strength based on user behavior. Support for hardware security modules (HSMs) and secure enclaves can further protect private keys. These enhancements would improve security, scalability, and applicability of the system in next-generation cybersecurity solutions.

REFERENCES

[1] D. Florencio and C. Herley, “A large-scale study of web password habits,” *Proc. 16th Int. World Wide Web Conf. (WWW)*, pp. 657–666, 2007.

[2] F. Aloul, S. Zahidi, and W. El-Hajj, “Two factor authentication using mobile phones,” *Proc. IEEE/ACS Int. Conf. Computer Systems and Applications (AICCSA)*, pp. 641–644, 2009.

[3] R. Gennaro, H. Krawczyk, and T. Rabin, “Secure hash-and-sign signatures without the random oracle,” *Advances in Cryptology – EUROCRYPT*, pp. 123–139, 1999.

[4] J. Patel and K. Shah, “A cloud-enabled healthcare solution for automated medicine dispensing and monitoring,” *Proc. IEEE Int. Conf. Smart Computing (SMC)*, pp. 650–655, 2022.

[5] N. Haller, C. Metz, P. Nesser, and M. Straw, “A one-time password system,” *RFC 2289*, Internet Engineering Task Force, Feb. 1998. [6] A. Verma and T. Prasad, “IoT-based patient monitoring with automated alerts and
reporting features,” *IEEE Sensors J.*, vol. 20, no. 15, pp. 8561–8569, Aug. 2020.

[6] J. Bonneau et al., “SoK: Towards the science of security and human factors,” *IEEE Symp. Security and Privacy*, pp. 110–124, 2012.

[7] T. O. Hardjono and N. Smith, “Decentralized trusted computing base for secure authentication,” *IEEE Security & Privacy*, vol. 14, no. 5, pp. 48–56, Sep.–Oct. 2016.

[8] S. Halevi and H. Krawczyk, “Public-key cryptography and password protocols,” *ACM Trans. Information and System Security*, vol. 2, no. 3, pp. 230–268, Aug. 1999.