THE FUTURE OF SECURE IDENTITY: A SYSTEMATIC REVIEW OF PASSWORDLESS AUTHENTICATION METHODS AND CHALLENGES

ABSTRACT

The increasing frequency of data breaches and credential theft has exposed the inherent weaknesses of traditional password-based authentication. Passwordless authentication methods, such as biometrics, hardware tokens, and public key cryptography, have emerged as promising alternatives to enhance security and usability. This study systematically reviews recent advancements in passwordless authentication technologies and presents an integrated framework that combines biometric verification, cryptographic key management, and contextual access control for secure digital identity. The proposed model addresses issues of scalability, privacy preservation, and cross-platform interoperability, offering a future-ready approach to identity security.

Keywords: Passwordless Authentication, Digital Identity, Biometrics, Cryptography, Multi-Factor Authentication, Security Framework.

EXISTING SYSTEM

Existing authentication systems in digital environments still rely heavily on passwords, one-time passcodes (OTPs), and multifactor authentication (MFA) that use SMS or email verification. Although these mechanisms have provided a baseline of security for decades, they are now inadequate against modern cyber threats. Password reuse, phishing, brute-force attacks, and credential stuffing have rendered conventional methods increasingly vulnerable. Even advanced MFA methods depend on shared secrets or third-party communication channels, both of which can be intercepted or socially engineered.

In enterprise contexts, password-based systems contribute to high maintenance costs due to frequent password resets, account recovery requests, and user frustration. Moreover, organizations often fail to properly enforce password complexity policies, leading to predictable credential patterns. From a security standpoint, passwords represent a single point of failure; once compromised, attackers gain direct access to accounts without further validation. Additionally, storing password hashes, even when encrypted, poses risks if databases are breached. These inherent weaknesses call for an architectural shift toward systems that remove passwords altogether and replace them with more secure and intuitive identity verification methods.

Disadvantages of the Existing System:

1. High vulnerability to attacks such as phishing, credential stuffing, and brute-force password guessing.

2. Poor user experience due to forgotten passwords, frequent resets, and authentication friction.

3. High operational and maintenance costs associated with password management and recovery processes.

PROPOSED SYSTEM

The proposed system introduces a comprehensive passwordless authentication framework combining biometric verification, public key cryptography, and contextual access control to achieve secure and seamless digital identity management. Instead of relying on passwords, the framework leverages a two-tier mechanism: a local authentication layer using biometrics (e.g., fingerprint or facial recognition) and a remote verification layer based on asymmetric cryptography. During registration, each device generates a unique cryptographic key pair, with the private key stored securely within a trusted hardware module. When a user attempts to authenticate, the system verifies their biometric signature locally and uses the corresponding public key to validate access on the server without transmitting sensitive data.

To ensure adaptability, the system integrates contextual authentication parameters such as device trust level, user location, and session history. If anomalies are detected—for instance, a login from an unfamiliar device—the system triggers secondary verification through hardware tokens or one-time biometric prompts. Blockchain-based decentralized identity management is also incorporated to maintain tamper-proof identity records and enhance interoperability across services. This ensures that users can authenticate securely across platforms without sharing personal data with centralized authorities.

Experimental evaluation shows that the proposed framework reduces authentication latency while maintaining high security assurance. It eliminates the need for password storage, minimizes phishing risks, and prevents unauthorized access through compromised credentials. Furthermore, the system ensures compliance with data protection standards such as GDPR by keeping biometric templates encrypted and locally confined.

Advantages of the Proposed System:

1. Enhanced security through biometric and cryptographic integration, eliminating password-based vulnerabilities.

2. Improved user convenience via fast, frictionless, and secure authentication without memorized credentials.

3. High scalability and interoperability through blockchain-backed decentralized identity management.

SYSTEM REQUIREMENTS

- **H/W System Configuration:-**

➢ Processor	-	Pentium –IV
➢ RAM	-	4 GB (min)
➢ Hard Disk	-	20 GB
➢ Key Board	-	Standard Windows Keyboard
➢ Mouse	-	Two or Three Button Mouse
➢ Monitor	-	SVGA

SOFTWARE REQUIREMENTS:

❖ **Operating system**	**:**	Windows 7 Ultimate.
❖ **Coding Language**	**:**	Python.
❖ **Front-End**	**:**	Python.
❖ **Back-End**	**:**	Django-ORM
❖ **Designing**	**:**	Html, css, javascript.
❖ **Data Base**	**:**	MySQL (WAMP Server).