Chapter 8
Hybrid Authentication System Using Image-Based Multi-Factor Verification

Golla Sandhyakumari
https://orcid.org/0000-0002-4755-0873
Siddharth Institute of Engineering and Technology, India

M. Bharathi
https://orcid.org/0000-0002-8633-1921
Sri Venkatesa Perumal College of Engineering and Technology, India

V. Madhurima
https://orcid.org/0000-0001-5553-6839
SV College of Engineering, India

ABSTRACT

Multi-Factor Authentication (MFA) is a secure electronic verification method that allows users to access an application or website only after completing multiple layers of authentication. While protecting sensitive data and systems from cyber threats is critical, traditional text-based authentication methods fail to provide sufficient security. Current systems enhance security by incorporating additional layers, such as OTPs sent to mobile phones or emails, or biometric verification using facial recognition. However, these systems often rely on costly hardware, limiting their accessibility. This paper proposes an integrated Authentication System designed to achieve high levels of security using low-cost equipment. The proposed system eliminates the need for expensive hardware by utilizing images as passwords in a

DOI: 10.4018/979-8-3373-1832-5.ch008

novel three-step authentication process. The system effectively counters various cyber threats, including malware attacks, phishing, and SQL injection, offering a cost-effective and robust solution for secure authentication.

1. INTRODUCTION

Authentication is a critical component of cybersecurity, ensuring that only authorized users can access sensitive data, applications, or systems. Traditional authentication methods, such as text-based passwords, have long been the primary means of verifying user identity. However, these methods are increasingly vulnerable to various cyberattacks, including phishing, brute force, and malware attacks. The growing need for stronger security measures has led to the adoption of multi-factor authentication (MFA), which combines multiple verification steps, such as one-time passwords (OTPs), biometrics, and hardware tokens. While MFA enhances security, the high costs associated with advanced hardware and infrastructure often limit its adoption. To address these challenges, this paper introduces an innovative, low-cost authentication system that leverages easily accessible technology. The proposed system combines traditional login methods with image-based passwords and face verification, providing a robust, three-step authentication process without the need for expensive equipment. By offering enhanced protection against various cyber threats, this system aims to balance security, affordability, and ease of implementation.

Authentication serves as the backbone of modern cybersecurity, playing a pivotal role in safeguarding sensitive data, critical applications, and systems against unauthorized access. As the digital landscape continues to evolve, the threat of cyberattacks grows exponentially, putting traditional authentication methods under immense scrutiny. Text-based passwords, though widely used, are often insufficient to counteract sophisticated attacks such as phishing, brute force attacks, malware intrusions, and SQL injections. Their reliance on human memory and predictable patterns further exacerbates vulnerabilities, making systems prone to breaches.

Authentication systems are essential for verifying user identity and securing access to sensitive data or systems. These systems can be broadly categorized based on their approach. Knowledge-based authentication relies on information the user knows, such as text-based passwords, security questions, or pattern-based methods. Possession-based authentication verifies users based on something they have, like one-time passwords (OTPs) sent via SMS or email, hardware tokens, smart cards, or QR codes. Inherence-based authentication, also known as biometric authentication, uses unique physical or behavioral traits such as fingerprints, facial recognition, iris scanning, voice recognition, or even behavioral biometrics like typing speed or mouse movements.