IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 13, Issue 2, April-May 2025
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

A Multi - Factor Authentication Framework Using Keystroke Biometrics and Illusion PIN

Dr. Kavitha R[1], Preethika V[2], Navin Kumar R[3] and Saira Begam S[4]

[1] Professor, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science. Thanjavur, Tamil Nadu - 613006, India
Pits.hod.cse@gmail.com

[2]UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India
preethikavivek005@gmail.com

[3]UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India
rnkumar0264@gmail.com

[4]UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India
sairabegam03@gmail.com

Abstract

In the digital era, securing access to web applications has become a major challenge due to the increasing sophistication of cyber threats, such as credential theft and brute-force attacks. Traditional authentication mechanisms, such as passwords and PINs are no longer sufficient to counter these risks, necessitating the development of robust multi-factor authentication solutions. To address this challenge, the proposed model introduces a enhanced security framework which integrates Keystroke Dynamics and Illusion PIN for enhanced authentication. Keystroke Dynamics analyses users unique typing patterns to ensure continuous authentication and prevent credential-based attacks. Illusion PIN employs a shuffling algorithm to create a dynamic keypad layout, making it resilient against shoulder- surfing and unauthorized access attempts. This authentication framework is demonstrated in healthcare systems, where securing patient records is crucial. By integrating these methods, the system significantly reduces false acceptance rates while maintaining a seamless and user-friendly authentication experience. Experimental results demonstrate its effectiveness in preventing unauthorized access and ensuring the integrity of healthcare data.

Keywords – *Keystroke dynamics, Illusion PIN, Multi- Factor Authentication, User Authentication.*

1. Introduction

Healthcare data security is crucial in modern digital healthcare systems, ensuring the confidentiality, integrity and availability of sensitive patient information. With the widespread adoption of Electronic Health Records (EHRs), telemedicine, wearable devices and cloud-based services, healthcare organizations face increasing security threats such as data breaches, ransomware and identity theft. The high value of medical records makes them a prime target, leading to financial fraud, privacy loss, and regulatory non compliance. Traditional security measures like password based authentication are insufficient against phishing, brute force attacks and keylogging. Additionally, insider threats, where employees or compromised user credentials lead to unauthorized data access, pose a significant risk. To address these challenges, this system proposes a multi-factor authentication system integrating keystroke dynamics and illusion PIN to enhance security and protect sensitive healthcare data. Keystroke dynamics use behavioural biometrics for real-time authentication, analysing user's unique typing patterns to detect unauthorized access. The illusion PIN mechanism mitigates shoulder surfing and keylogging risks by utilizing a dynamic, randomized PIN input interface, ensuring secure record authentication. The proposed system bridges these gaps by continuous authentication and security threat resilience, ensuring robust healthcare security

2. Literature Survey

Guiseppe Strangapede et al. [1] presented a study on keystroke dynamics (KD) for biometric verification, emphasizing its advantages, such as its lightweight processing and non-intrusive nature. The authors highlighted the challenge of heterogeneous experimental protocols and limited dataset sizes in KD research. To address this, they proposed a benchmarking framework based on tweet-length sequences from the Aalto Keystroke Databases, encompassing data from over 185,000 subjects. By employing TypeNet and TypeFormer verification systems, the study demonstrated the potential for a privacy-preserving KD-based authentication system while maintaining

satisfactory performance.

Sabin Shahi et al. [2] examined authentication mechanisms in e-health services, which enable remote storage and retrieval of patient records. The study identified security vulnerabilities in current authentication protocols, particularly those transmitting sensitive data over public networks. The paper reviewed various authentication methods, including biometric and token-based mechanisms, to enhance e-health security. The findings emphasized the importance of robust authentication strategies to safeguard patient data and ensure compliance with regulatory standards such as HIPAA and GDPR.

Athanasios Papadopoulos et al. [3] proposed the Illusion PIN (IPIN) system to counter shoulder-surfing attacks in touchscreen authentication. IPIN employs hybrid images to create two distinct keypads: one visible to the legitimate user and another visible to an attacker from a distance. The system dynamically shuffles the keypad arrangement to prevent memorization-based attacks. A security evaluation involving 84 simulated shoulder-surfing attempts demonstrated that IPIN effectively prevents unauthorized PIN observation. Additionally, the study estimated the minimum distance required for a surveillance camera to capture a user's PIN, confirming the effectiveness of IPIN in public and high-risk environments.

R. F. Olanrewaju et al. [4] proposed the Frictionless and Secure User Authentication system for web-based applications, enhancing security while ensuring seamless access. FSUA uses behavioral profiling (device location, login time, browser, and web activity) to automate dynamically. The system uses four authentication methods password-based, time-constrained key, OTP or digital certificate authentication, minimizing user effort.

Poornima Naga et al. [5] proposed an improved two-factor authentication scheme for healthcare systems to enhance security and privacy in Telecare Medicine Information Systems (TMIS). The system secures Electronic Medical Records (EMR) by combining password and smart card authentication, preventing unauthorized access. Validated using the AVISPA tool, the scheme is resistant to replay, man-in-the-middle, stolen verifier, and impersonation attacks. Compared to existing protocols, it improves computational efficiency, reduces communication costs, and enhances execution time, making it a secure and efficient authentication mechanism for healthcare applications.

Dhananjay Nigam et al. [6] proposed a biometric-based authentication system for intelligent and privacy-preserving healthcare environments, enabling seamless patient identification using face and speech recognition without external devices. Compared to traditional password-based and two-factor authentication (2FA) methods, which are often inconvenient and vulnerable, the system enhances security and usability. A survey of 96 individuals indicated biometric authentication as the most preferred method due to its ease of use and security benefits. The study confirms that biometric authentication resists insider attacks, replay attacks, and identity theft, making it a reliable security solution for modern healthcare systems

Art Conklin et al. [7] proposed a user-centric risk model for password-based authentication, highlighting the security challenges posed by cognitive limitations and password memory aids. The study reveals that users' reliance on password reuse, written notes, and digital storage inadvertently creates security vulnerabilities across interconnected systems. Analyzing threats such as brute force, discovery, and social engineering attacks, the model underscores the need for a system-wide approach to password security. The authors advocate for enhanced authentication mechanisms, including stronger password policies, encryption, multi-factor authentication, and user training. Compared to conventional system-centric models, this approach offers a holistic view of password-based risks and presents scalable security improvements for modern distributed computing environments.

Wang Yuanbing et al. [8] proposed an improved authentication protocol for smart healthcare systems using Wireless Medical Sensor Networks (WMSN) to enhance security and efficiency in patient monitoring. The system secures patient data transmission over public networks by integrating Elliptic Curve Cryptography (ECC) for robust encryption. It addresses vulnerabilities in existing authentication schemes, such as privileged insider attacks, user anonymity issues, and offline password guessing attacks. Security validation using Burrows-Abadi-Needham (BAN) logic and AVISPA tools confirms resistance against replay, impersonation, and stolen smart card attacks. Compared to previous authentication models, the proposed solution ensures higher security while maintaining computational and communication efficiency, making it suitable for real-time healthcare applications.

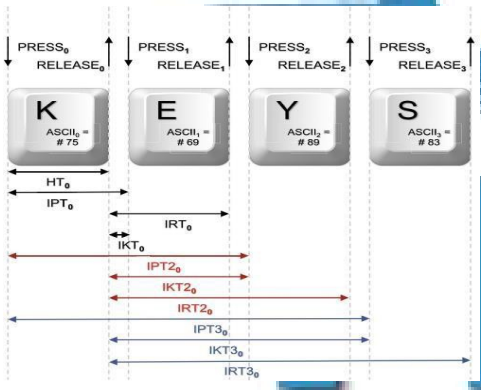
Nafiseh Kahani et al. [9] proposed a secure authentication and access control framework for cloud-based e-Health systems to protect sensitive patient data. The system employs a zero-knowledge authentication protocol and a two stage keyed access control mechanism, dynamically determining minimum necessary access rights for users based on predefined policies. It integrates public key encryption with the Derive Unique Key Per Transaction (DUKPT) scheme, ensuring session keys change per transaction to prevent key compromise. A security analysis confirms resistance against replay attacks, unauthorized access, and data breaches, while experimental results show the system efficiently handles a high number of concurrent authentication requests with minimal response time, making it an effective authentication model for cloud-based e-Health services.

M. Hindusree and Dr. R. Sasikumar [10] proposed an improved Black-White (BW) method and session key method to prevent shoulder surfing attacks during secure transactions. Their approach enhances PIN-based authentication by dynamically altering the keypad layout and using a four-digit randomization technique to extract PIN digits only after user iterations are complete. The method resists covert attention attacks by frustrating adversaries with randomized digit ordering and perceptual grouping complexity. Additionally,

their session key mechanism prevents unauthorized PIN interception by encrypting authentication data before transmission. Compared to existing methods, this approach enhances security, reduces PIN entry time, and improves usability, making it a robust defense against shoulder surfing in crowded environments.

Yu Zhong et al. [11] proposed an improved keystroke dynamics-based authentication scheme for user verification, addressing challenges in scale variations, feature interactions, and outliers. The system enhances security by introducing a novel distance metric that integrates Mahalanobis and Manhattan distances to improve classification accuracy. Validated using the CMU keystroke dynamics benchmark dataset, the scheme demonstrates superior performance over traditional distance metrics, achieving lower equal error rates and enhanced robustness to outliers. Compared to existing methods, it improves authentication accuracy, reduces false alarm rates, and enhances resistance to attacks, making it a reliable and efficient biometric authentication mechanism.

A.F.M. Nazmul Haque Nahin et al. [12] proposed an advanced emotion detection system that integrates keystroke dynamics and text pattern analysis to identify user emotions during computer interactions. The system leverages typing speed, dwell time, and flight time from keystroke patterns, alongside vector space modeling (VSM) with Jaccard similarity for text analysis. The model was trained using machine learning algorithms in Weka and evaluated on a dataset including seven emotional classes. Experimental results demonstrated an accuracy above 80% in recognizing emotions, surpassing individual keystroke or text-based approaches. To enhance



robustness, the system applies feature selection techniques to refine the most relevant keystroke and text-based parameters, reducing computational complexity while maintaining high accuracy. It also adapts dynamically to individual typing behaviors, improving personalization in emotion recognition. By incorporating real-time data processing, the model ensures low latency, making it suitable for interactive applications such as mental health monitoring and adaptive user interfaces. Overall, this fusion of keystroke dynamics and text analysis presents a significant advancement in affective computing, offering a reliable and scalable solution for real-world human-computer interaction scenarios and so on.

3. The Proposed Model

In the current digital era, authentication mechanisms face critical security challenges due to increasing cyber threats such as phishing, unauthorized access and data breaches. Conventional single-factor authentication methods, such as passwords and static PINs, are vulnerable to attacks like shoulder surfing and brute force attempts. To address these challenges, we propose a Multi-Factor Proactive Authentication Solution that enhances security, ensures real time threat detection and provides a seamless user experience. Our model integrates: 1. Keystroke Dynamics – Analysing the unique typing patterns of users to authenticate identity. 2.Illusion PIN – A dynamic PIN-based authentication method that minimizes risks associated with traditional static PINs. This system enhances authentication security by incorporating behavioural and dynamic elements, making it significantly more resistant to unauthorized access and security threats.

2.1 Keystroke Registration

The Doctor Registration Module is the initial step in enabling secure access to the system. When a doctor registers, they provide their personal details, including name, email and a chosen password. In addition to these conventional credentials, the system records their keystroke dynamics, which act as a unique biometric signature. The system captures various parameters such as,

1. Digraph timing – The time taken between pressing two consecutive keys.
2. Start and end time – The total duration taken to type the input.
3. Typing speed – The overall typing rhythm and patterns.

Once the doctor enters their password, the system processes these keystroke features and generates a unique reference template associated with the user's credentials. This template is securely stored in the database for future authentication. To further enhance security, feature extraction techniques are applied to eliminate noise and refine the collected data. This ensures the stored template to accurately represents the doctor's natural typing behaviour. Unlike traditional password-based authentication, where stolen credentials can be misused, keystroke dynamics provide an additional layer of security, making it difficult for attackers to replicate. After successful registration, the doctor is officially added to the system and can proceed with the login process in subsequent sessions.

2.2 Keystroke Authentication

The Doctor Login Module verifies a doctor's identity using multi-factor authentication by combining traditional credentials with keystroke dynamics. When a doctor attempts to log in, they enter their registered email and password. However, instead of merely checking if the password is correct, the system also captures their keystroke behaviour in real time and compares it against the stored reference

template. The verification process involves several key steps:

1. Keystroke Data Collection – The system records the doctor's typing pattern as they enter their password.
2. Feature Matching – The newly captured typing signature is analyzed using a pattern-matching algorithm.

Threshold-Based Decision making where the system calculates a similarity score between the newly entered typing pattern and the stored template. If the score meets a predefined threshold, authentication is successful. Otherwise, the login attempt is rejected.

2.3 Threat Detection and Response

To further enhance security, the system includes a threat detection module that monitors unauthorized login attempts. If an intruder tries to access the system with the correct password but fails to match the expected keystroke dynamics, an alert is triggered. The system performs the following actions, blocks the login attempt to prevent unauthorized access.

By incorporating keystroke-based authentication and threat detection, this module ensures that even if an attacker obtains a doctor's password, they cannot log in unless their typing behaviour matches the registered user. This approach significantly enhances security, reduces the risk of credential based attacks and ensures a more adaptive and resilient authentication process.

2.4 Illusion Pin

The Illusion PIN module is a secure and innovative authentication mechanism designed to enhance traditional PIN- based security by mitigating risks such as shoulder surfing and keylogging attacks. This module works by incorporating

dynamic keypad layouts. Each time a user attempts to authenticate, the keypad layout is shuffled randomly, ensuring that numbers do not appear in their usual sequential order, preventing attackers from memorizing keystroke positions. Instead of entering the actual PIN, users follow a predefined mapping rule known only to them, such as selecting adjacent or mirrored keys based on a secret strategy. This ensures that even if someone observes the input, they cannot deduce the actual PIN. Additionally, the system employs visual distortion elements by modifying the font, colour, or overlaying symbols on the keypad, making it harder for keyloggers or screen capture attacks to recognize the correct PIN. This multi- layered approach significantly enhances security while maintaining a seamless user experience.

2.5 Patient Record Authentication

In the healthcare authentication system, the Illusion PIN module is used to authenticate patients to access their medical records uploaded by doctors. When a patient attempts to log in, they are prompted to enter their PIN using the Illusion PIN interface, where the keypad layout is randomized, and a predefined mapping technique is in place. This ensures that even if an attacker observes the input, they cannot derive the correct PIN. To enhance security, the system employs Multi- Factor Authentication (MFA) by integrating Illusion PIN and Keystroke Dynamics. Keystroke Dynamics analyses typing behaviour to detect inconsistencies and verify the authenticity of the user. If the PIN entry and typing pattern match the stored templates, access is granted.

Once authenticated, the patient can securely access their medical records uploaded by doctors. Additionally, security measures and intrusion detection mechanisms are in place. If multiple incorrect Illusion PIN attempts occur, the Threat Detection Module is triggered, capturing an image of the unauthorized user and sending an email alert to both the patient and the administrator, ensuring proactive security.

4. Conclusion

The proposed Multi-Factor Proactive Authentication Solution effectively strengthens the security of web applications, particularly in healthcare systems where data confidentiality is paramount. By integrating Keystroke Dynamics and Illusion PIN, the model mitigates common authentication vulnerabilities such as phishing, brute-force attacks and shoulder surfing. Keystroke Dynamics continuously verifies users based on unique typing patterns, while the Illusion PIN employs dynamic layouts to prevent unauthorized access. The addition of a threat detection module enhances security by identifying suspicious login attempts and triggering alerts. Experimental results demonstrate that this approach reduces false acceptance rates while maintaining user convenience. Compared to traditional authentication mechanisms, this system offers a more adaptive and resilient security framework. Future improvements could incorporate additional biometric factors such as facial recognition or AI-driven anomaly detection to further enhance protection. This study underscores the importance of evolving authentication methods to counter modern security threats while ensuring usability and efficiency in security solutions.

5.

REFERENCES

[1] Guiseppe Strangapede et al. TypeNet, TypeFormer, "Keystroke Dynamics for Biometric Verification: A Benchmarking Framework Based on Aalto Keystroke Databases", Journal of Biometric Security, 2023.

[2] Sabin Shahi et al. "Authentication Mechanisms in E-Health Services: Enhancing Security in Remote Patient Data Access", IEEE, 2020.

[3] Athanasios Papadopoulos et al. IPIN, "Illusion PIN: Shoulder-Surfing Resistant Authentication for Touchscreens," IEEE TIFS, 2017.

[4] R. F. Olanrewaju et al. FSUA, "A Frictionless and Secure User Authentication in Web-Based Premium Applications", IEEE Access, 2021.

[5] Poornima Naga et al. ITFA, "An Improved and Anonymous Two-Factor Authentication Protocol for Healthcare Applications with Wireless Medical Sensor Networks", Multimedia Systems, 2015.

[6] Dhananjay Nigam et al. BioAuth, "Biometric Authentication for Intelligent and Privacy-Preserving Healthcare Systems", Journal of Healthcare Engineering, 2022.

[7] Art Conklin et al. UserRisk-Auth, "A User-Centric Risk Model for Password-Based Authentication", Journal of Cybersecurity Research, 2004.

[8] Wang Yuanbing et al. SmartHealth-Auth, "An Improved Authentication Protocol for Smart Healthcare System Using Wireless Medical Sensor Network", IEEE Access, 2021.

[9] Nafiseh Kahani et al. AAC-eHealth, "Authentication and Access Control in e-Health Systems in the Cloud," BigDataSecurity, 2016.

[10] M. Hindusree et al. PSS-ST, "Preventing Shoulder Surfing in Secure Transactions", IEEE, 2015.

[11] Yu Zhong et al. KDUA-ML, "Keystroke Dynamics User Authentication Using Advanced Machine Learning Methods", IEEE, 2015.

[12] A.F.M. Nazmul Haque Nahin et al. IE-KDTP, "Identifying Emotion by Keystroke Dynamics and Text Pattern Analysis", Behaviour & Information Technology, 2014.


IJREAT
PRDG