International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02956
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

KEYLOGGER - INNOVATIVE KEYSTROKE DYNAMICS AND ENSURING SECURE AUTHENTICATION

B.VINOTH KUMAR, R.ALAGU, S.KAVIYARASAN

1,2,3.B.sc ISCF students, DR.M.G.R Educational and Research Institute Deemed to be University, Chennai.
Corresponding Email ID: kumarvinoth53497@gmail.com

4. Professor, DR.M.G.R Educational and Research Institute, Deemed to be University , Chennai.

5. Assistant Professor, DR.M.G.R Educational and Research Institute, Deemed to be University,Chennai

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02956
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

ABSTRACT

In the digital era, the need for secure and reliable user authentication mechanisms has become more critical than ever. Traditional password-based authentication systems are increasingly vulnerable to threats such as keylogging, phishing, and brute-force attacks. To address these issues, keystroke dynamics has emerged as an innovative and promising solution. Keystroke dynamics is a behavioral biometric technique that analyzesthe unique typingpatterns of individuals. Every person has a distinct way of typing, characterized by the speed of key presses, the time interval between each keystroke, and the overall typing rhythm. These patterns are difficult to replicate, making keystroke dynamics a powerful tool for enhancing security.

INTRODUCTION

A key area in modern security research is user authentication—the process of verifying whether a user should be granted access to a

system or resource. Authentication serves as the first and most critical line of defense in ensuring the confidentiality, integrity, and availability of protected data and systems. In an increasingly digital world, users interact with numerous platforms that require authentication, such as banking systems, corporate databases, mobile applications, and web services. The common reliance on passwords poses significant challenges, including password fatigue, where users have to remember multiple complex passwords, and the risk of security breaches due to weak or reused credentials. The vulnerability of passwords to attacks like phishing, brute force, and keylogging has prompted the need for more secure and user-friendly authentication methods. and meet regulatory expectations.

2. REQUIREMENT ANALYSIS

2.1 OBJECTIVE OF THE PROJECT

The primary objective of this project is to design and implement a more secure and user-friendly email authentication system using keystroke dynamics, a behavioral biometric authentication technique. In the current digital landscape, security threats such as passive and active attacks are major concerns for network systems. Passive attacks involve unauthorized entities trying to capture information, while active attacks aim to disrupt network communication and damage the user's productivity. Traditional password-based authentication systems are vulnerable to various attacks, such as password theft, phishing, and brute-force attacks. These vulnerabilities highlight the need for stronger, more reliable authentication methods that do not solely rely on static passwords.

The user clicks the login button. This opens a mail to link that directs the person to pre-written email that includes an encrypted token.

The user sends the email. The message already comes with a recipient address so the user doesn't need to enter any information.

The server verifies the request. Using a combination of token-based security checks, the user's identity is verified.

SIGNIFICANT OF THE PROJECT

Traditional authentication methods such as

passwords are susceptible to hacking, phishing, and brute-force attacks. Implementing keystroke dynamics adds an additional layer of security that is difficult for malicious actors to bypass. Unauthorized access to email accounts can lead to various security breaches, including data theft, identity theft, and unauthorized use of confidential information. By implementing a robust authentication system based on keystroke dynamics, the project helps prevent unauthorized access to mail server accounts, thereby safeguarding sensitive data and information. Despite the enhanced security measures, the project ensures a seamless and convenient user experience. Users are not burdened with additional authentication steps or complicated procedures. Instead, the authentication process is integrated seamlessly into the

login process, requiring only the user's natural typing behavior for verification. Implementing a keystroke dynamics-based authentication system can be cost- effective compared to other biometric authentication methods that require specialized hardware or software. Keystroke dynamics can be captured using existing keyboard input devices, eliminating the need for additional investment in biometric sensors or equipment. The project offers scalability and flexibility, making it suitable for a wide range of applications and environments. As technology evolves and security threats continue to evolve, it's essential to adopt advanced authentication methods that can withstand emerging challenges. The project's focus on keystroke dynamics-based authentication ensures a future-proof solution that can adapt to evolving security threats and technological advancements. By introducing innovative authentication techniques such as keystroke dynamics, the project contributes to the advancement of cybersecurity practices and encourages further research and innovation in the field. It serves as a demonstration of how biometric authentication can be effectively applied to enhance security in real-world applications.

2.2 EXISTING SYSTEM

In today's digital world, email has become an indispensable tool for communication, both personally and professionally. Millions of people rely on email for various functions, including business correspondence, social media logins, and managing sensitive tasks such as banking and online shopping. Email services have evolved to become a vital part of most individuals' daily lives, making it crucial to ensure that these communication channels are secure. However, the security of email systems, particularly in terms of authentication, remains a significant concern.

Data Leakage Risks: Sensitive data transmitted via email is vulnerable to interception during transmission. Even with encryption, attackers can still find ways to access unprotected data, leading to potential data leakage. .

Password Theft: Traditional password- based systems are prone to hacking, where attackers use techniques like keylogging, phishing, or brute-force attacks to steal login credentials and gain unauthorized access to email accounts.

Lack of Unauthorized Access Detection: In the current system, there is no way to detect or prevent unauthorized access to email accounts once the user is logged in. This presents a significant security gap, as attackers can continue to exploit the system without being detected until the damage is done.

2.3 PROPOSED SYSTEM

Email has become one of the most essential forms of communication in the digital age, widely used for both personal and professional purposes. However, as the use of email has increased, so have the risks associated with unauthorized access, data leakage, and malicious activities such as spamming. To mitigate these security challenges, the proposed system introduces an innovative approach to email authentication and data protection, combining keystroke dynamics with key sharing techniques to enhance the overall security of email systems.

To further enhance the security of the system, a key-sharing mechanism via SMS is employed to prevent unauthorized access to sensitive email messages. When an email is sent, a secret key is generated and securely distributed to the sender and receiver through SMS. This key is used to authenticate the recipient and ensure security, reducing the risk of email interception and unauthorized access. If an unauthorized party attempts to access the message, the system will trigger an alert, notifying the authorities of the potential security breach.

The advantages of this proposed system include the following:

Access Control: Only authorized individuals are allowed to read and interact with email messages. The combination of keystroke authentication and SMS key-sharing ensures that unauthorized access is prevented.

Reduced Time for Key Generation and Distribution: The use of SMS-based key sharing is a fast and efficient method for distributing

encryption keys. The process does not require complex infrastructure, making it easier to implement and maintain.

3. REQUIREMENT SPECIFICATIONS

3.1 HARDWAREREQUIREMENTS

that only authorized individuals can access the contents of the email. The key value acts as an additional layer of

- Processor : Dual core processor 2.6.0 GHZ
- RAM : 8GB
- Hard disk : 160 GB
- Compact Disk : 650 Mb

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02956
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

3.2 SOFTWARE REQUIREMENTS

- Operating system : Windows OS
- Front End : Html, css, javascript – Frontend
- Back End : Python flask, sqlite
- IDE : Pycharm,Visual Studio Code

Application Web application

4.1 ARCHITECTURE DIAGRAM

The architecture diagram is an essential visual representation that outlines the key components of the system, their relationships, and their interactions.

In the context of the proposed email authentication system using keystroke dynamics, the architecture diagram will represent how different subsystems, such as the user interface, the keystroke analysis module, the server, and the SMS-based key-sharing mechanism, interact and communicate with each other.

The architecture for the system can be divided into the following key components:

1. User Interface (UI):

The user interface serves as the entry point for the users of the system. It allows the user to interact with the email authentication application.

It facilitates user login by capturing typing patterns and other input data, such as keystroke timing, during the login process.

2. Keystroke Dynamics Module: This module captures the user's typing patterns during the login process and compares them with stored keystroke profiles.

Keystroke dynamics data, such as typing speed, rhythm, and key hold duration, are analyzed to authenticate the user.

3. **Email Server:**

The email server is responsible for handling email communications between the sender and receiver.

4. **SMS Key Sharing Service:** This component ensures secure communication by generating a secret key when an email is sent. The key is then securely transmitted to both the sender and receiver via SMS.

The key is required for decrypting the message, ensuring that only authorized users can access the email content.

The SMS key-sharing service ensures additional security for sensitive data being transferred via email, reducing the risks of unauthorized access.

5. **Security Authority:**

The security authority manages the monitoring of unauthorized access attempts and sends notifications in the case of suspicious activities.

6. **Database:**

The database stores the keystroke dynamics data for each registered user. This includes data such as the user's typing patterns, keystroke timings, and login history.

It is also responsible for storing user credentials and the encrypted key used for SMS key sharing during email communication.

Flow of Operation:

1. Login Process:

The user enters their username and password via the user interface. o The keystroke dynamics module captures the user's typing patterns and compares them to the stored data in the database. If the keystroke match is within the accepted threshold, access is granted; otherwise, access is denied.

2. Email Authentication:

When an email is sent, a secret key is generated and sent to both the sender and receiver via SMS.

The receiver must authenticate themselves by entering the key received via SMS to access the email content.

If the user is authorized, the email is decrypted and read; if not, an alert is triggered and sent to the security authority.

3. Continuous Monitoring:

The system continuously monitors the user's typing behavior during the session to detect any unusual changes in the keystroke dynamics.

If a discrepancy is found (e.g., a different person uses the system after login), an alert is triggered to notify the security authority of a potential security breach.

Advantages of the Architecture: Modular and Scalable: The architecture allows for easy scaling and modular upgrades. Each component (e.g., keystroke dynamics module, SMS key-sharing service) can be updated or replaced independently without disrupting the entire system.

Improved Security: By combining both keystroke dynamics and SMS- based key-sharing, the system offers a multi-layered authentication mechanism, significantly enhancing the security of email communications.

Efficient User Authentication: The static keystroke method ensures a quick and efficient authentication process, minimizing delays during login and email access.

DESCRIPTION

Email Framework Creation:

The email framework forms the backbone of the system, providing the infrastructure for managing email communications between users.

A mail server, or Mail Transfer Agent (MTA), is responsible for receiving incoming emails from local and remote users, as well as forwarding outgoing emails. The mail server also handles routing and delivery of messages. In this module, we create a similar structure for the system, where the server acts as the core hub for user interactions. The server will store critical user information, such as authentication details, keystroke patterns, and other personal data. Multiple users can interact with the server to send, receive, and manage emails securely.

User Enrolment:

User enrolment is the initial process that sets up an individual's account in the email system. For users to participate in the authentication process, they must first register with the server by providing necessary details such as username, email ID, contact number, and primary and confirm passwords. In addition to these traditional credentials, the user must also undergo a keystroke analysis during the password typing process.

Keystroke Authentication:

Keystroke authentication is a critical security feature of the system. Unlike traditional methods that rely solely on passwords, this method analyzes the user's typing rhythm and speed. In the verification phase, when the user attempts to log in, the system compares their keystroke dynamics — such as the time between keystrokes and the overall speed of typing — with the stored data in the server's database.

Content Sharing:

Once users have successfully logged in and passed the authentication check, they are allowed to compose and send emails. The content sharing module enables users to send secure emails to other registered users. Users can add the recipient's details, compose their message, and send it over the secure email channel.

Mail Access:

In case an unauthorized individual attempts to read the email, the system will prevent the email's contents from being displayed. Additionally, notifications are sent to the email owner and the security authority, alerting them of the unauthorized access attempt. This ensures that any attempts to access sensitive data are detected and addressed promptly, significantly reducing the risk of data leaks and unauthorized information access.

IMPLEMENTATION

Implementation is the critical phase in which the theoretical design and planning of a project are translated into a functional and operational system. It is the stage where all the design concepts and methodologies discussed earlier are converted into a working system that can be used effectively.

The implementation phase begins with careful planning. The first step is to evaluate the current system and its constraints, identifying any challenges or limitations that may affect the new system's performance or integration. This step is followed by the design of strategies for overcoming these limitations and ensuring that the new system can be seamlessly implemented. A detailed plan is created, outlining the necessary resources,

equipment, and the testing activities required for successful deployment.

Ease of Design-to-Code Translation: The design models should be easily translatable into the programming language, which helps avoid errors and inefficiencies during coding.

Code Efficiency: The code should be optimized for performance, ensuring that the system can handle the expected number of users and requests without slowdowns or failures.

Memory Efficiency: The system should use memory resources efficiently, preventing memory leaks and ensuring that the system operates smoothly even under heavy load.

Maintainability: The code should be clean, modular, and well-documented to allow easy updates and modifications in the future. This is essential for long- term success as the system may need updates, bug fixes, or new features

CONCLUSION

In conclusion, our proposed system addresses the growing need for more secure and efficient methods of email authentication by combining the power of keystroke dynamics with OTP-based security and potential multimedia content analysis. By offering continuous, realtime authentication and reducing the risks of unauthorized access and data leakage, our framework provides a robust solution for enhancing the security of email communications in today's increasingly digital world.