International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Innovative Keystroke Dynamics and Ensuring Secure Email Authentication

Sanjay R[1], Vignesh S[2]

[1]**Master of Science Specialization in Information Security and Cyber Forensic Bharathiyar University-India**
[2]**Department of Computer Science Rathinam College of Arts and Science, India**
[1]**Sanjusanjusanjay2001@gmail.com**, [2]**vignesh.sinfotech@gmaiil.com**

ABSTRACT

With the rise of sensitive information stored on computers, reliable user identification is crucial. Passwords, the traditional approach, have limitations. A compromised password grants unauthorized access. To address this, research explores using a user's unique computer interaction patterns for authentication. The most promising techniques analyze typing patterns, specifically the timing between keystrokes, which we'll call "biometric keystroke authentication." This paper focuses on using these time intervals to differentiate authorized users from imposters. A Multilayer Perceptron (MLP) neural network is employed to train and validate the user's unique typing rhythm. The system analyzes these patterns to verify the user and adapts to slight variations over time.

Keywords: Keystroke Biometrics, user authentication, neural network, keystroke timing.

1. Introduction

The internet has become an essential part of our lives. We use it for work, communication, and entertainment. But with this convenience comes a risk: unauthorized access to our data. Network security is the shield that protects us from this risk. It safeguards computers, users, and programs from various threats like hacking, malware, and data breaches.

Imagine a castle with secure walls. That's how network security works for businesses. It surrounds their IT infrastructure (hardware, software, data) with protective measures like firewalls and intrusion detection systems. These act as guards, keeping out unwanted intruders and preventing attacks.

However, the way we use the internet is changing. Businesses are moving towards cloud-based systems and employees are accessing data on different devices. This traditional "castle wall" approach is no longer enough. Here's where the concept of "zero trust" comes in. This approach assumes no one is inherently trustworthy and verifies every access attempt.

How Network Security Works: A Multi-Layered Approach

Network security relies on a combination of access control and threat control measures implemented throughout a network. Think of it as a layered defense system.

Access Control: This is the first line of defense, preventing unauthorized users from entering the network. It's like having a guard at the castle gate, checking everyone's credentials before letting them in.

Threat Control: Even with access control, threats can slip through. Imagine a spy with stolen credentials. This is where threat control comes in. It analyzes network traffic to identify and stop malicious activities, like malware attacks or data leaks.

Essential Tools for Network Security

A multi-layered approach uses various tools at different points within the network to provide comprehensive protection. Here are some key players:

Firewall: This acts as a barrier between trusted and untrusted zones, controlling access based on IP addresses. It's like the castle wall, separating the inside from the outside world.

Load Balancer: This distributes network traffic evenly across servers, ensuring smooth performance and preventing overload. Think of it as a traffic manager, directing visitors to different roads within the castle to avoid congestion.

IDS/IPS: These systems monitor network traffic and identify suspicious activities based on known attack patterns. Imagine them as guards within the castle, constantly on the lookout for suspicious behavior.

Sandbox: This is a virtual environment that safely tests unknown files or programs to see if they are malicious. Think of it as a controlled space outside the castle walls, where potential threats can be contained and analyzed.

NTA/NDR: These tools analyze network traffic patterns and use statistical methods to detect anomalies that might indicate a threat. Imagine them as detectives in the castle, studying patterns and identifying unusual activity.

Email Security: This encompasses safeguards specifically designed to protect email accounts and data from malicious attacks. It's like adding extra security measures to the castle gates specifically for incoming messages.

2. Project overview

In today's digital world, verifying a user's identity (authentication) is crucial for protecting sensitive information and resources. Passwords are the traditional method, but they have limitations. A stolen password grants access to unauthorized users. Researchers are exploring ways to use a user's unique interaction patterns with a computer for authentication. This paper proposes a system that uses implicit passwords for banking applications. Implicit passwords allow users to choose any image and a sequence of points within that image as their password.

Modules

This system is built on several modules:

Email Framework Creation: This module sets up the core infrastructure, similar to a mail server, that manages users and data.

User Enrollment: Users register by providing basic information and creating a keystroke pattern during password setup. This pattern includes typing speed and rhythm.

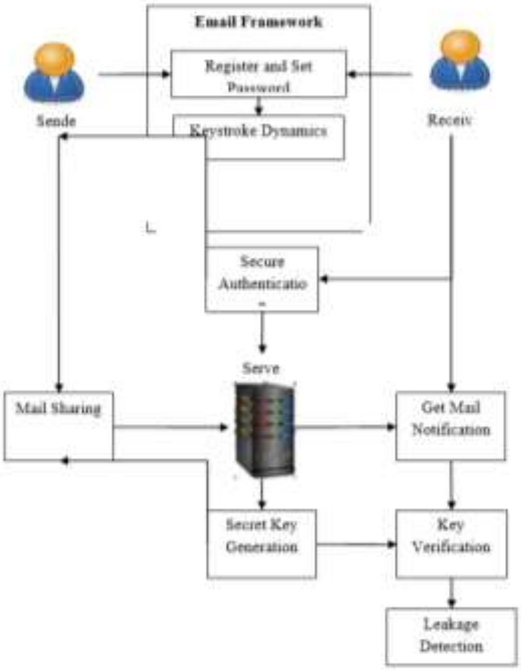
Keystroke Authentication: During login, the system analyzes the user's keystroke pattern (typing speed and rhythm) along with their password to verify their identity.

Content Sharing: Authorized users can securely compose and share emails within the system.

Mail Access: The system controls access to emails. Authorized users can view their mail, while unauthorized users are blocked or prompted for additional verification.

3.System Architecture

A system architecture is a blueprint that defines how a system works, what its parts are, and how they interact. It's like a map for building a system, ensuring all the pieces fit together and function as intended. Some even use special languages to precisely describe these architectures.



4. Proposed System

Email is one of the crucial aspects of web data communication. The increasing use of email has led to a lucrative business opportunity called This email system tackles authentication and data leakage issues by using two techniques: keystroke authentication and random key sharing via SMS.

There are two types of keystroke authentication: static and continuous. Static analysis happens only during login, while continuous monitors typing speed throughout the session to detect unauthorized user access after login. This system uses the static method.

During enrollment, the system records each user's unique typing patterns (keystroke values) as a reference.

To prevent data leakage, the system uses random key sharing. When a message is shared, a secret key is generated and sent to the system's authority. The receiver needs this key to access the message. If someone tries to view the message without the key, the system will notify the authority of unauthorized access.

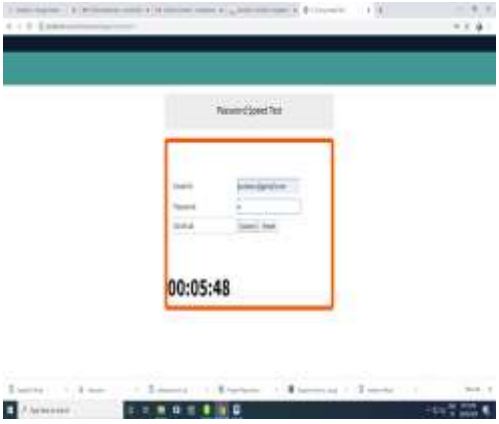
Benefits:

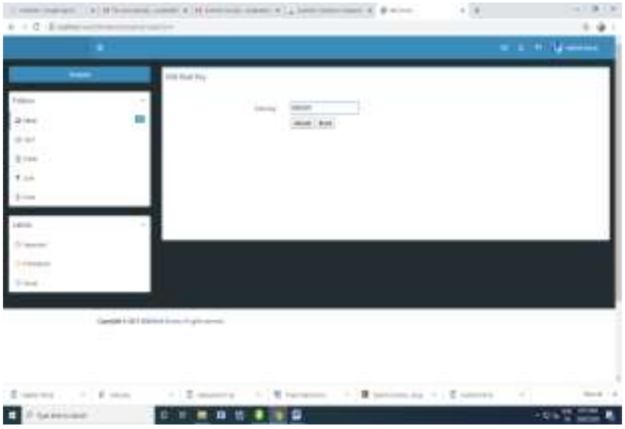
Strong authentication through keystroke analysis.

Only authorized users can access emails.

Fast key generation and distribution process.

Output





5.Conclusion

Data Distribution Strategies: These strategies help identify potential leakers by analyzing how data is distributed.

Keystroke Authentication: This method strengthens user verification during login and email access.

Here's how it works:

During registration, users provide their details and establish their unique keystroke patterns (keystroke values).

Login involves verifying both password and keystroke patterns for enhanced security.

Additionally, a one-time password (OTP) can be generated for further user authorization when accessing email content.

Future Enhancements:

The framework could be expanded to analyze multimedia content, including duplicate detection for images and videos. This would be beneficial due to the large storage requirements of multimedia content.

References

□**1.**ASP.NET Core in Action, Second Edition Annotated Edition by Andrew Lock, 2021.

2.An Atypical ASP.NET Core 6 Design Patterns Guide: .A SOLID adventure into architectural principles and design patterns using .NET 6 and C# 10, 2nd Edition 2nd ed. Edition, 2022, by Carl-Hugo Marcotte (Author), Abdelhamid Zebdi (Foreword)

□**3.**.ASP.NET Core 5 and React: Full-stack web development using .NET 5, React 17, and TypeScript 4, 2nd Edition 2nd ed. Edition, 2021, by Carl Rippon

□**4.**C# 9 and .NET 5 – Modern Cross-Platform Development: Build intelligent apps, websites, and services with Blazer, ASP.NET Core, and Entity
5.Framework Core using Visual Studio Code, 5th Edition 5th ed. Edition, 2020, by Mark J. Price

6.Essential ASP.NET Web Forms Development: Full Stack Programming with C#, SQL, Ajax, and JavaScript 1st ed. Edition, 2020, by Robert E. Beasley