CAMBRIDGE INSTITUTE OF TECHNOLOGY

K R PURAM, BANGALORE-560036

Department of Computer Science & Engineering

Final Year B.E Project work: 2024-25

Synopsis

Students Name: 1) Shreevatsa PU	USNs: 1) 1CD21CS146
2) Sai Spandan	2) 1CD21CS134
3) Udbhav Kumar	3) 1CD21CS176

Batch No: 46

Title: Secure Access

Introduction

The project focuses on enhancing the security of digital payment transactions and net-banking operations that utilize One-Time Passwords (OTPs) for authentication. Given the rise in OTP-related fraud, the invention proposes a novel system and method aimed at safeguarding OTPs from various types of attacks, particularly social engineering and passive interception.

Background

OTPs have become a standard mechanism for ensuring secure access in digital transactions, primarily due to their single-use nature, which mitigates the risk of replay attacks. However, vulnerabilities persist as attackers can intercept OTPs during transmission or manipulate users into revealing them. The frequency of OTP fraud cases highlights the urgent need for improved security measures.

Objectives

The primary objective of this project is to develop a robust system that secures OTP-based access and transactions while maintaining user-friendliness. The proposed solution aims to:

- Protect OTPs from unauthorized use even if they are intercepted.
- Implement a dual-layer authentication process where OTPs serve as a second factor.
- Utilize innovative techniques such as digit permutation and challenge-response mechanisms to enhance security.

Methodology

The invention introduces a **Churn Module** that modifies the original OTP by reordering its digits before delivery to the end-user. This "churning" process makes it difficult for attackers to utilize intercepted OTPs. The following key components are integral to the system:

1. **Churn Module**: Accepts generated OTPs, applies a permutation algorithm, and sends the modified OTP to the user.
2. **Challenge Module**: Engages users in a challenge-response dialogue to verify their identity. This module utilizes an "un-churn key" that allows legitimate users to revert the churned OTP back to its original form.
3. **Server Interaction**: The server generates the initial OTP and validates it against the un-churned version provided by the user after successful challenge completion.

Workflow

The process can be summarized in several steps:

1. The user logs into the server with their credentials.
2. Upon verification, the server generates an OTP and passes it to the Churn Module.
3. The Churn Module reorders the digits of the OTP and sends it along with an un-churn key to the Challenge Module.
4. The user receives the churned OTP and inputs it back into the system.
5. The Challenge Module verifies the user's identity through a series of challenges, applying the un-churn key to restore the original OTP.
6. Finally, the server matches this restored OTP with its generated version to grant access or complete transactions.

Conclusion

This project presents a comprehensive approach to securing OTP-based transactions through innovative methodologies that address existing vulnerabilities while ensuring ease of use for end-users. By implementing this system, organizations can significantly reduce instances of fraud related to digital payments and enhance overall transaction security.

Name of the Guide: Dr. Shreekanth M Prabhu   Signature of Guide: Date:

Signature of Project coordinator: