PIP2001 Capstone Project
Review-3

Batch Number:CCS

PENDRIVE COPY PROTECTION

ROLL NO	NAME
20211CCS0063	Mohammed Faiz
20211CCS0069	Thaman Tharanath
20211CCS0072	Sathvik U
20211CCS0091	Abel Abraham
20211CCS0149	Snigdha Shetty

Under the Supervision of,

Mr Tanveer Ahamed,
Professor,
School of Computer Science and Engineering,
Presidency University.

Name of the Program: B.TECH
Name of the HoD: Dr Anand Raj
Name of the Program Project Coordinator:
Name of the School Project Coordinators:

CONTENT

- INTRODUCTION
- Literature Review
- Existing method Drawback
- Proposed Method
- Objectives
- Methodology/Modules
- Architecture
- Hardware/software components

- Timeline of Project
- Expected Outcomes
- Conclusion
- Github link
- References
- Project work mapping with SDG

PROBLEM STATEMENT

In today's digital age, USB flash drives (pendrives) are widely used for data storage and transfer due to their portability and convenience. However, their accessibility makes them vulnerable to unauthorized copying, data breaches, and misuse, which can lead to severe consequences such as intellectual property theft, privacy violations, and financial losses. Existing security measures, such as simple password protection or encryption tools, often fail to provide comprehensive protection, as they lack mechanisms to prevent copying or unauthorized use of data on untrusted devices.

Additionally, many solutions are either too complex for general users or too costly for widespread adoption. This creates a critical need for a cost-effective, user-friendly, and secure pendrive system that not only encrypts data but also prevents unauthorized access, copying, and misuse, ensuring data confidentiality and integrity in a portable and reliable manner.

This project aims to address these challenges by designing a pendrive copy protection system with advanced security features, such as device binding, multi-factor authentication, and anti-copy mechanisms, while maintaining usability and affordability for a broad range of users.

Introduction

- The widespread use of USB drives (pendrives) for data sharing poses significant risks, including unauthorized copying and data breaches.
- The aim of this project is to design a secure pendrive system with embedded protection mechanisms to prevent unauthorized copying, ensuring data integrity and confidentiality.
- This project combines encryption techniques and access control mechanisms to achieve effective protection.

Literature Review

Literature Review

1. **Basic Encryption Tools**:
   Widely used tools like **BitLocker** (Windows-specific) and **VeraCrypt** (cross-platform) offer robust encryption. However, they require manual configuration and are often underutilized due to the technica**ker** integrates with Windows for drive encryption but needs activation and appropriate settings for optimal security.
   - ○ **VeraCrypt** provides additional customization, such as hidden volumes, but its interface can be daunting for non-technical users.
2. **Password-Protected Zip Files**:
   A popular, quick-fix approach due to its simplicity and compatibility across platforms. However:
   - ○ Password-protected zip files use weaker encryption standards compared to dedicated tools.
   - ○ They are highly susceptible to brute-force attacks, particularly if users rely on weak or predictable passwords.l know-how required. For example:
   - ○ **BitLoc**

Research Insights:

- Studies reveal that existing solutions often prioritize encryption but neglect anti-copy mechanisms.
- Hardware-based protection, like TPM (Trusted Platform Module), shows promise but is costly.

Advantages

- **Enhanced Data Security**
  - Prevents unauthorized copying and distribution of sensitive files.
  - Protects data from being accessed by untrusted devices.
- **Encryption Integration**
  - Ensures data confidentiality with advanced encryption techniques (e.g., AES-256).
  - Protects against data breaches even if the pendrive is lost or stolen.
- **Access Control**
  - Multi-factor authentication (MFA) adds an extra layer of security.
  - Ensures that only authorized users can access the data.
- **Portability**
  - Retains the convenience of a standard pendrive while adding robust protection mechanisms.
- **User-Friendly**
  - Simplifies secure file management through an intuitive interface.
  - Eliminates the need for manual encryption processes.

Existing method Drawback

EXISTING METHOD DRAWBACKS

1. **Encryption Tools**:
   - Do not prevent copying; files can still be transferred to unauthorized devices.
   - Heavily reliant on the user to secure the key/password.
2. **Password Protection**:
   - Weak against brute-force or dictionary attacks.
   - Lacks comprehensive access control.
3. **Hardware-Based Solutions**:
   - Expensive and not widely accessible for everyday users.
   - Require dedicated hardware modules.

Proposed Method

- **Dynamic Copy Prevention System**:
  - Prevent unauthorized copying by binding the pendrive to specific devices (e.g., MAC address-based restriction).
  - Implement dual-layer encryption with unique keys tied to the pendrive.
- **Real-Time Monitoring**:
  - Employ software that monitors access attempts and logs unauthorized activities.
- **Authentication System**:
  - Multi-factor authentication (MFA) for accessing protected files.
- **Self-Destruct Mechanism**:
  - Optionally, erase or disable content if unauthorized access is detected.

Objectives

1. Ensure that data on the pendrive cannot be copied or transferred to unauthorized systems.
2. Integrate encryption and access control for enhanced security.
3. Develop a user-friendly interface for secure file management.
4. Minimize the cost and complexity of implementation for broad usability.

Methodology/Modules

1.Encryption Module

- Secures data using AES-256 encryption to prevent unauthorized access.
- Restricts pendrive use to authorized devices via unique identifiers like MAC address or system ID.

2.Access Control Module

- Implements multi-factor authentication (e.g., password/PIN, biometric verification).

3.Anti-Copy Module

- Prevents unauthorized copying or transfer of files with real-time monitoring and restrictions.

4.Monitoring and Logging Module

- Tracks and logs all access attempts and alerts users about suspicious activities.

5.User Interface Module

- Provides an intuitive interface for configuring security settings and managing the pendrive.

6.Emergency Recovery Module

- Allows secure data recovery through authorized recovery keys or remote recovery methods.

Architecture

1. **Hardware Layer**:
   - Pendrive with embedded microcontroller for security functions.
   - Support for secure hardware storage (optional).
2. **Software Layer**:
   - Driver and access control software installed on the host system.
   - Real-time monitoring and alert system for unauthorized access.
3. **Communication Layer**:
   - Interface between pendrive hardware and user devices (USB interface).
4. **Encryption Layer**:
   - Handles encryption, decryption, and secure key management.

Hardware/software components

- **USB Flash Drive**:
  - High-speed, high-capacity USB 3.0/3.1 pendrive for fast operations.
- **Microcontroller**:
  - Secure microcontroller for encryption and key storage (e.g., STM32, Atmel).
- **Power Source**:
  - USB-powered, no external power required.Programming Language:
  - Python/C++ for software development.
- **Encryption Libraries**:
  - OpenSSL, PyCrypto, or Libsodium for AES encryption.
- **Access Control Framework**:
  - Implement using APIs for biometric/PIN-based authentication.
- **Monitoring Tool**:
  - Log generation and access alert system using Python or Java.

Timeline of Project

- Research and Analysis: September 2024 -October 2024
- Development of App(Frontend&Backend): October 2024 - November 2024
- Testing and Refinement: December 2024
- Final Report and Presentation: January 2025

(it will take around 3 to 4 months)

Expected Outcomes

Prevent Unauthorized Copying

- Data on the pendrive will be accessible only on authorized devices, eliminating the risk of data transfer to unverified systems.

Enhanced Data Confidentiality

- Implementation of AES encryption ensures that files remain secure, even if the pendrive falls into the wrong hands.

Improved Access Control

- Multi-factor authentication (e.g., PIN, password, or biometrics) will ensure that only verified users can access the data.

Reduced Data Breaches

- The combination of encryption and access restriction will significantly lower the likelihood of data breaches and leaks.

Real-Time Threat Detection

- The system will detect and log unauthorized access attempts, providing users with alerts and audit trails for security monitoring.

Device-Specific Functionality

- Binding the pendrive to specific devices (e.g., via MAC address) ensures that the data remains confined to trusted environments.

Expected Outcomes

Data Integrity Maintenance

- Unauthorized modification or tampering of files will be prevented, ensuring that data remains authentic and unaltered.

Improved User Experience

- A user-friendly interface for managing secure files will make the system accessible to non-technical users without compromising security.

Secure Self-Destruct Mechanism

- If unauthorized tampering or multiple failed login attempts are detected, the system will optionally erase or lock the data, preventing misuse.

Compliance with Data Protection Standards

- The system will align with data security standards, such as GDPR or HIPAA, making it suitable for sensitive industries like healthcare and finance.

Portable and Cost-Effective Security Solution

- A lightweight and affordable tool offering robust security, usable across different industries and personal applications.

Broader Market Applicability

- The system's adaptability makes it suitable for industries like education, corporate environments, government agencies, and personal use cases requiring secure file sharing.

Conclusion

The **Pendrive Copy Protection System** is a robust and innovative solution addressing the critical need for data security in portable storage devices. By integrating encryption, device binding, multi-factor authentication, and anti-copy mechanisms, the system ensures that sensitive information remains protected against unauthorized access and copying.

This solution offers a balance between security, usability, and cost-effectiveness, making it accessible for both personal and professional applications. With features such as real-time monitoring, self-destruct mechanisms, and user-friendly interfaces, the system not only safeguards data but also enhances user confidence in secure file management.

The expected outcomes, including prevention of data breaches, improved confidentiality, and compliance with data protection standards, position this system as a versatile tool for industries like education, healthcare, finance, and government.

In conclusion, the Pendrive Copy Protection System is a forward-thinking approach to modern data security challenges, ensuring that the integrity, confidentiality, and availability of information are maintained in an increasingly interconnected world.

Github Link

- .

The Github link provided should have public access permission.

Github Link: https://github.com/Sathvi1/Project

References

[1] Anderson, R. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
[2] Brier, E., Clavier, C., & Olivier, F. (2004). Correlation Power Analysis with a Leakage Model. IEEE Transactions on Computers.
[3] Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. SIAM Journal of Computing.
[4] Boyen, X. (2007). Reusable Cryptographic Fuzzy Extractors. ACM CCS.
[5] Burrows, M., Abadi, M., & Needham, R. (1990). A Logic of Authentication. ACM Transactions on Computer Systems.
[6] Chari, S., Jutla, C., Rao, J., & Rohatgi, P. (1999). Towards Sound Approaches to Counteract Power-Analysis Attacks. Springer.
[7] Clark, J., & Jacob, J. (2012). A Survey of Authentication Protocol Literature: Version 1.0. Springer.
[8] Diffie, W. (1988). The First Ten Years of Public Key Cryptography. Proceedings of the IEEE.
[9] Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory.
[10] Dolev, D., & Yao, A. (1983). On the Security of Public Key Protocols. IEEE Transactions on Information Theory.
[11] Ferguson, N. (2001). Improved Cryptanalysis of RC4. Springer.
[12] Ferguson, N., & Schneier, B. (2003). Practical Cryptography. Wiley.
[13] FIPS PUB 197 (2001). Advanced Encryption Standard (AES). NIST.
[14] Goldreich, O. (2001). Foundations of Cryptography. Cambridge University Press.
[15] Gura, N., Patel, A., & Wander, A. (2004). Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs. IEEE Transactions on Computers.
[16] Halderman, J. A., & Schoen, S. D. (2008). Lest We Remember: Cold Boot Attacks on Encryption Keys. USENIX Security Symposium.
[17] Juels, A., & Sudan, M. (2006). A Fuzzy Vault Scheme. Springer.
[18] Kaliski, B. (2003). The Mathematics of the RSA Public-Key Cryptosystem. RSA Laboratories Bulletin.
[19] Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. CRC Press.
[20] Kelsey, J., Schneier, B., Wagner, D., & Hall, C. (1997). Side Channel Cryptanalysis of Product Ciphers. Springer.

Thank You