

Endpoint DLP for Clipboard Monitoring

The **Endpoint Data Loss Prevention (DLP) for Clipboard Monitoring** project is designed to enhance cybersecurity by monitoring clipboard activities for sensitive data. This tool helps prevent accidental data leakage by detecting and managing sensitive information copied to the clipboard. It offers real-time notifications, immediate clipboard clearing, logging of detected sensitive data to MySQL database storage for easier management and review.

Features

- Monitors the clipboard continuously.
- Detects sensitive data types including:
 - Aadhaar number
 - PAN number
 - Phone number
 - Email address
 - Bank account number
 - Driving license number
- Clears the clipboard if sensitive data is detected.
- Sends desktop notifications when sensitive data is detected.
- Logs the sensitive data with timestamp to MySQL database for further review.
- Integrated login system using Tkinter to ensure that only authorized users can access the program.

As an endpoint DLP solution, this tool protects individual workstations, which are often the weakest link in a company's security infrastructure. By securing endpoints, the overall security posture of the company is improved.

Project Link:-

<https://github.com/workwithnaveen7/Endpoint-DLP-for-Clipboard-Monitoring>

Tech Stack

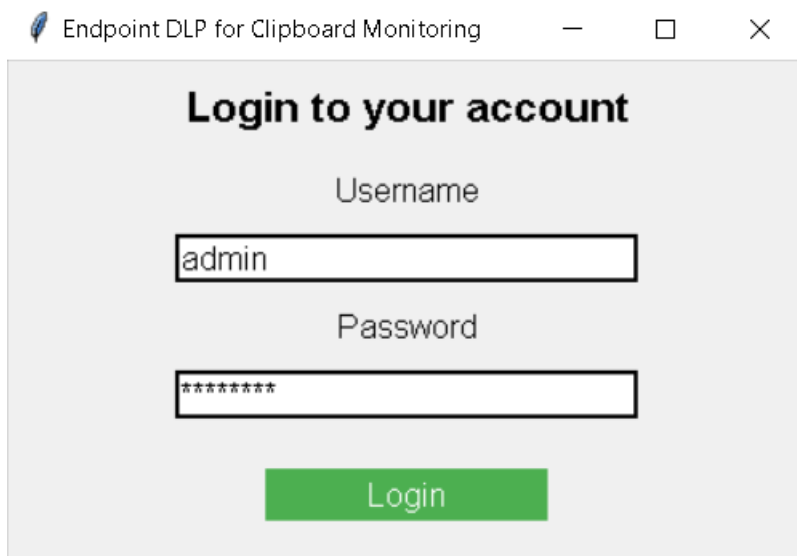
- Programming Language – Python
- MySQL: Used to store logs of sensitive data, allowing for easier data management and reporting.

Python Libraries used-

- pyperclip: Used for clipboard operations, enabling the program to access and modify clipboard content.
- plyer: Provides cross-platform desktop notifications to alert users in real-time.
- re: Utilized for regular expression-based detection of sensitive data patterns.
- datetime: Used for timestamping logs to track when sensitive data is detected.
- Tkinter: used for creating the login interface and authentication system.

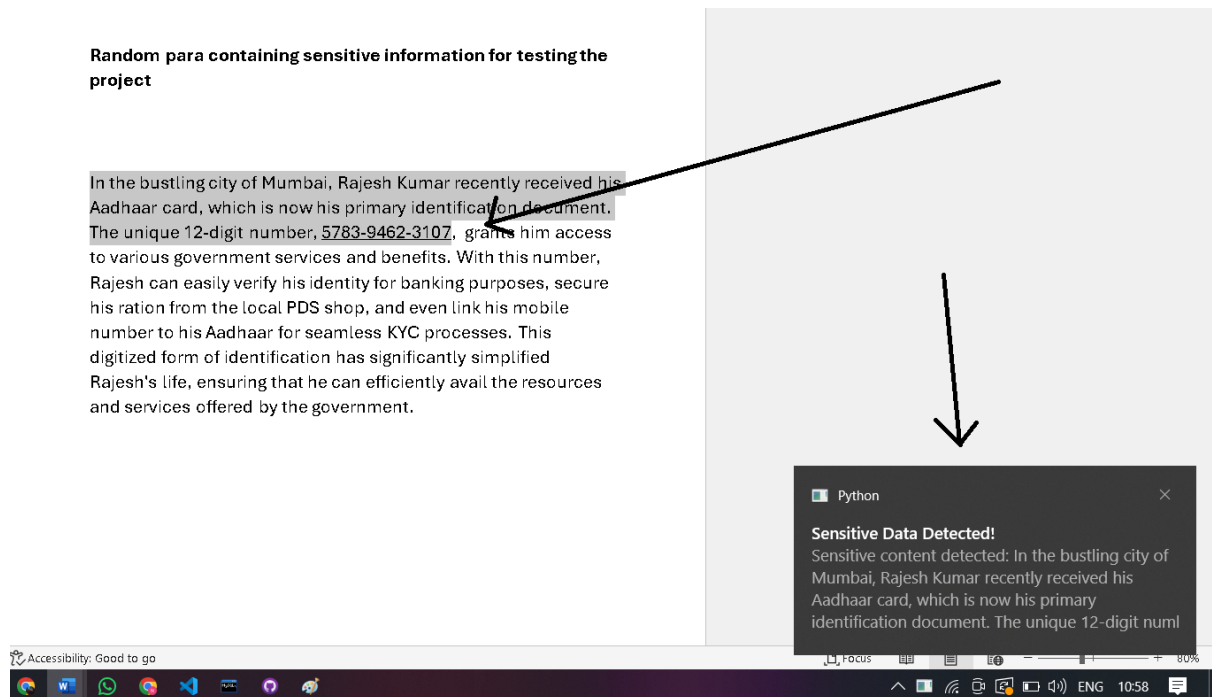
Working:

User Authentication



The image shows a screenshot of a login window titled "Endpoint DLP for Clipboard Monitoring". The window has a light gray background and a dark gray border. At the top, the title bar shows the window title and standard minimize, maximize, and close buttons. The main content area has a light gray background. The title "Login to your account" is centered at the top in a bold, black font. Below the title, the label "Username" is centered, followed by a text input field containing the text "admin". Below the username field, the label "Password" is centered, followed by a text input field containing seven asterisks "*****". At the bottom center, there is a green rectangular button with the text "Login" in white.

Notifying user that sensitive content is detected



Clearing the clipboard

```
Clipboard updated: In the bustling city of Mumbai, Rajesh Kumar recently received his Aadhaar card, which is now his primary identification document.
The unique 12-digit number, 5783-9462-3107
Sensitive data detected! Clearing clipboard...
Clipboard cleared.
Sensitive data logged to MySQL database
Clipboard updated:
```

Logging the data in MySQL database for review

```
mysql> select * from logs;
```

id	content	timestamp
1	yo@gmail.com	2024-11-23 00:57:42
2	yo@gmail.com	2024-11-23 00:58:59
3	1234-5678-9012	2024-11-23 01:00:32
4	ABCDE1234F	2024-11-23 01:00:57
5	9876543210	2024-11-23 01:01:14
6	1234567890123456	2024-11-23 01:01:34
7	testing@gmail.com	2024-11-23 01:01:54
8	1234-5678-9012	2024-11-23 01:27:46
9	ABCDE1234F	2024-11-23 01:29:20
10	testing@gmail.com	2024-11-23 01:31:58
11	9876543210	2024-11-23 01:34:58
12	9876543210	2024-11-23 01:35:36
13	1234-5678-9012	2024-11-23 01:41:25
14	1234-5678-9012	2024-11-23 02:03:32
15	ABCDE1234F	2024-11-23 02:04:48
16	In the bustling city of Mumbai, Rajesh Kumar recently received his Aadhaar card, which is now his primary identification document. The unique 12-digit number, 5783-9462-3107	2024-11-23 10:57:49

16 rows in set (0.00 sec)

```
mysql>
```

Conclusion:

Using the **Endpoint DLP for Clipboard Monitoring** project can significantly improve data loss prevention efforts in any organization. It provides real-time detection and management of sensitive data, enhances user awareness, ensures compliance, and strengthens endpoint security, making it an invaluable tool in the fight against data breaches and accidental data leaks.

