# SYSTEM SURVEILLANCE USING KEYLOGGER

**Prof. . Dr. Vilas Joshi**
Divya Prakash[2], Kishlay Kumar[3], Shubham[4], Shubham[5]
Computer Engineering Department, ISBM College of Engineering Nande, Pune-412115, India,
Savitribai Phule Pune University

***Abstract: The System Surveillance using Keylogger project aims to provide an efficient and comprehensive system for monitoring computer activity by capturing keystrokes and screenshots. This research paper presents the design, implementation, and evaluation of the system. The project utilizes various Python libraries, including pyscreenshot, FTP, keyboard, and SMTP, to capture and store the data securely. The captured keystrokes and screenshots are sent to an online cloud storage service, specifically DriveHQ, ensuring remote access and storage. The paper discusses the architecture, advantages, limitations, and potential applications of the system, highlighting its effectiveness in providing real-time system surveillance.***

## I. INTRODUCTION

In today's digital era, effective system surveillance is crucial for security, troubleshooting, and user behavior analysis. This research paper introduces the System Surveillance using Keylogger project, which captures keystrokes and screenshots on a computer system to monitor and record user activity. The project leverages Python and various libraries to achieve its objectives.

## II. MOTIVATION

Tt aims to contribute to the existing body of knowledge in system surveillance, provide insights into the implementation and utilization of keylogger tools, and encourage discussions on ethical usage and security considerations. The motivation on the System Surveillance using the Keylogger project stems from several key factors:

- **Security Enhancement:** In an increasingly digital world, the need for robust security measures is paramount. This project addresses the need for effective system surveillance by capturing keystrokes and screenshots, enabling users to detect potential security breaches, unauthorized access, or suspicious activities on their computer systems.
- **User Behavior Analysis:** Monitoring and analyzing user behavior can provide valuable insights for various purposes, such as identifying productivity trends, troubleshooting issues, or detecting malicious activities. By capturing keystrokes and screenshots, the System Surveillance using Keylogger project offers a comprehensive view of user actions, allowing for in-depth behavior analysis.
- **Remote Access and Cloud Storage:** The utilization of online cloud storage services, like DriveHQ, provides the advantage of remote access to captured data. This ensures that users can conveniently monitor their systems and retrieve captured information from anywhere, adding flexibility and convenience to system surveillance.
- **Ethical Considerations:** While keyloggers can be misused, conducting research and writing a research paper on this topic allows for an exploration of ethical considerations surrounding such tools. Addressing privacy concerns, consent, and responsible usage within the research paper contributes to raising awareness and promoting ethical practices in system surveillance.
- **Practical Applications:** The research paper showcases the practical applications of the System Surveillance using Keylogger project, including employee monitoring, parental control, and system security auditing. These applications highlight the relevance and usefulness of the project in real-world scenarios, further motivating its exploration and study.

## III. LITERATURE SURVEY

Author: Robbi Rahim, Heri Nurdiyanto, Ansari Saleh A, Dahlan Abdullah, Dedy Hartama and Darmawan Napitupulu.

The development of technology is very fast, especially in the field of Internet technology that at any time experiencing significant changes, The development also supported by the ability of human resources, Keylogger is a tool that most developed because this application is very rarely recognized a malicious program by antivirus, keylogger will record all activities related to keystrokes, the recording process is accomplished by using string matching method. The application of string matching method in the process of recording the keyboard is to help the admin in knowing what the user accessed on the computer.

Author: Preeti Tuli, Priyanka Sahu

The goal of this paper is to give an idea about some of the benefits that anyone can get from the complete monitoring of the system network. Keylogging programs, commonly known as keyloggers, are a type of malware that maliciously tracks user input from the keyboard in an attempt to retrieve personal and private information. Keystroke logging, also known as key logging, is the capture of typed characters/number [2]. The data captured can include document content, passwords, user ID’s, and other potentially sensitive bits of information. The program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. It also notes the window captions and all URLs visited with a web browser. This allows you to review all the text written by your employer/user, whether it was created with a text editor, email client or an on-line text control on a web page. You can view all the pages visited by your employ/user and the passwords for all their on-line accounts. For easier monitoring, you can also turn on automatic screenshot capture.

Author: Stig Arild Ysterud

One goal of this research is to investigate keyloggers and ways to monitor detecting methods that are used in attacks through the usage of honeypots.
First of all the difference of this subject title "Honeynets and Honeypots" is explained: Honeynet is a computer network specifically to be attacked. The hosts that comprise a honeynet and serve as attack targets are called Honeypots. A honeypot is a trap set to detect, deflect or in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

## *IV.* SUMMARY

This research paper presents the System Surveillance using Keylogger project, which aims to provide a comprehensive system for monitoring computer activity by capturing keystrokes and screenshots. The project utilizes Python and various libraries such as pyscreenshot, FTP, keyboard, and SMTP. The captured data is securely stored and sent to an online cloud storage service, DriveHQ, allowing for remote access. The paper discusses the system architecture, advantages, limitations, and potential applications. The research paper contributes to the field of system surveillance and highlights the effectiveness of the project in real-time monitoring and analysis of computer activity.

## V. CONCLUSION

The System Surveillance using Keylogger project presents a robust and efficient system for monitoring computer activity through the capture of keystrokes and screenshots. The integration of Python and various libraries such as pyscreenshot, FTP, keyboard, and SMTP enables seamless implementation and functionality. The system architecture ensures secure storage and remote access to the captured data, providing flexibility and convenience for users.

## VI. ACKNOWLEDGMENT

We would like to express our sincere gratitude to all individuals and organizations who have contributed to the successful completion of this research paper on System Surveillance using Keylogger project.First and foremost, we would like to thank our advisor/mentor Prof. Dr. Vilas Joshi , for their invaluable guidance, support, and expertise throughout the duration of this project. Their insightful feedback and constructive criticism have been instrumental in shaping the direction and content of this research paper.
We would also like to extend our appreciation to the research participants who willingly volunteered their time and consented to participate in the evaluation and testing of the System Surveillance using Keylogger project. Their

contribution has been vital in validating the effectiveness and performance of the system.

## VII. REFERENCES

● S. Moses, J. Mercado, A. Larson and D. Rowe, "Touch interface and keylogging malware," 2015 11th International Conference on Innovations in Information Technology (IIT), Dubai, 2015, pp. 86-91.doi:10.1109/INNOVATIONS.2015.738152 0

● Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap and L. S. Vignesh, "Keyloggers software detection techniques," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016,pp.1-6,doi:10.1109/ISCO.2016.7726880

● Advanced Keylogger- A Stealthy Malware for Computer Monitoring, Asian Journal of Convergence in Technology ISSN NO: 2350-1146 I.F5.11 Volume VII and Issue I, Aarushi Dwivedi, Krishna Chandra Tripathi, M.L. Sharma.

● University of Oslo- Keylogging of user interaction in physical and virtual environments and its implications for honeypot analysis Stig Arild Ysterud stigay@ifi.uio.no Network and System Administration 20th May 2014

● M. Dadkhah, A. Ciobotaru, et. al, “An Introduction to Undetectable Keyloggers with Experimental Testing”, International Journal of Computer Networks and Communications Security - September 2014 ● Enhancement Keylogger Application for Parental Control and Monitor Children's Activities, Mohamad Yusof Darus, Muhammad Azizi Mohd Ariffin, Journal of Positive School Psychology http://journalppw.com 2022, Vol. 6, No. 3, 8482–8492