AI-Powered Encrypted Keylogger - Project Report

1. Project Title:

AI-Powered Encrypted Keylogger

2. Objective:

To design a smart keylogger that not only captures keystrokes, but also analyzes the typing pattern using an AI model to identify behavior types such as password input, commands, URLs, or general typing. The logs are securely encrypted for privacy and stored safely.

3. Tools and Technologies Used:

- Programming Language: Python 3.9
- Libraries: TensorFlow, Keras, Cryptography, Pynput, Argparse
- AI Model: LSTM (Long Short-Term Memory Neural Network)
- OS: Kali Linux (or any Linux-based system)

4. System Workflow:

- When user starts the logger, each keystroke is recorded.
- The time between each keystroke is measured.
- These delays are passed into a pre-trained LSTM model.
- Based on the timing patterns, the model classifies the input behavior.
- The output along with typed data is written to a plaintext log file and an encrypted binary file using Fernet.

5. Key Features:

- Predicts typing behavior in real-time.
- Encrypts logs securely using a symmetric encryption key.

- Command-line interface with options to start logging, analyze logs, and decrypt logs.
- Modular and easy-to-extend code.

6. Use Cases:

- Cybersecurity learning projects (ethical hacking, red teaming)
- Behavioral biometrics research
- Insider threat simulations in security training
- Portfolio project for interviews

7. Results:

The tool successfully logged keystrokes, generated behavior labels based on keystroke dynamics, and encrypted all logs securely. It demonstrates how AI can be integrated with security tools for advanced behavior analysis.

8. Future Enhancements:

- Train the model with real user data for higher accuracy.
- Add GUI dashboard for non-technical users.
- Implement real-time alerts if suspicious behavior is detected.
- Upload logs to cloud storage securely.

9. Conclusion:

This project is a powerful demonstration of AI and cybersecurity integration. It reflects skills in machine learning, encryption, system-level programming, and behavior analytics, making it an excellent showcase for cybersecurity roles.