ABSTRACT

The Ransomware File Protector is a web-based cybersecurity tool designed to detect, monitor, and mitigate ransomware attacks in real time. It leverages Python and the Flask framework to provide an intuitive user interface, while integrating file system monitoring using the Watchdog library. The system continuously tracks selected folders for suspicious file behavior, such as unauthorized encryption or extension changes. A hybrid encryption-decryption mechanism using RSA and AES ensures safe file recovery, and automatic backups are triggered for suspicious changes.

To enhance threat detection accuracy, the tool incorporates DeepSeek AI, which analyzes file activity patterns and flags potential ransomware behavior. Users can toggle AI mode, view real-time logs, decrypt files, and explore a visual dashboard that summarizes suspicious vs. safe file trends using Chart.js. The integration of backend automation, frontend analytics, and AI reasoning provides a practical and scalable defense mechanism against ransomware threats. This solution is ideal for educational institutions, organizations, or individuals seeking an intelligent approach to securing sensitive file systems.

TABLE OF CONTENTS