PROJECT AND TEAM INFORMATION

Project Title

Shield AI: Your AI-Powered Code Security Guardian using Js

Student / Team Information

Team Name: *Team #*	*Decepticons*
Team member 1 (Team Lead) *(Last Name, name: student ID: email, picture):*	*Saxena, Vedant –211111012* *6987vedsaxena@gmail.com*
Team member 2 *(Last Name, name: student ID: email, picture):*	*Rawat , Vikas - 23041436* *vikasvikasrawat574@gmail.com*

Team member 3 *(Last Name, name: student ID: email, picture):*	*Shardul –230111404* *shardulsemwal52@gmail.com*
Team member 4 *(Last Name, name: student ID: email, picture):*	*Kirola, Payal – 23012940* *payalkirola50@gmail.com*

PROPOSAL DESCRIPTION

Motivation

With the rise of AI-driven applications and an increasing number of cybersecurity threats, developers often struggle to secure their code effectively. Shield AI is an AI-powered security assistant that automates security analysis, detects vulnerabilities, and suggests fixes.
By leveraging Google's Generative AI (Gemini-1.5 Pro), this tool ensures robust security checks against injection attacks, authentication flaws, and dependency vulnerabilities.
Our motivation is to make security best practices accessible, automated, and efficient for all developers.

State of the Art / Current solution

*Currently, developers rely on **manual security audits, static code analysis tools (like SonarQube, ESLint, or Snyk), and penetration testing** to identify security issues. However, these solutions often require **manual intervention**, are **time-consuming**, and lack real-time monitoring. **Shield AI** enhances security by offering an **AI-driven, interactive, and automated** approach to security analysis and fixing.*

Project Goals and Milestones

- **Phase 1:** Develop core functionalities (AI-driven security checks, automated fixes, real-time monitoring).
- **Phase 2:** Implement a **CLI-based user interface** for ease of use.
- **Phase 3:** Integrate advanced AI models for security threat detection and fix recommendations.
- **Phase 4:** User testing, performance optimization, and release of the **Shield AI** package.

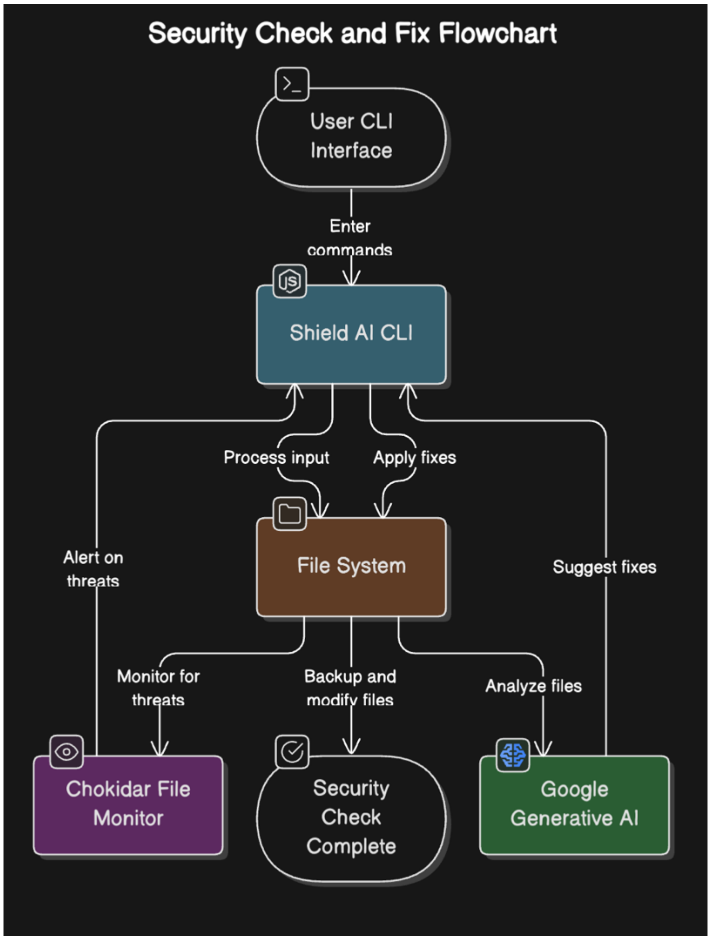
Project Approach

Shield AI is developed as a **Node.js CLI tool** using:

- **Google Generative AI (Gemini-1.5 Pro)** for security analysis.
- **Chalk, Ora, Chokidar and Inquirer** for an interactive UI.
- **File System (fs) module** for secure backups and modifications.

Users can **check and fix** their code using simple CLI commands, and AI will provide **secure coding recommendations** while preserving functionality.

System Architecture (High Level Diagram



Project Outcome /

- A **fully functional CLI tool** for AI-powered security scanning.
- AI-generated **security reports and automated code fixes**.
- Real-time **file monitoring** for security threats.
- **Backup functionality** for modified files.

Assumptions

- Users will have a **Node.js environment (v14+)** installed.
- The AI model requires an **active API key** to function.
- Users will provide **valid file paths** for scanning and fixing.

References

- **Google Generative AI Docs:** https://developers.google.com/generative-ai
- **Chalk Documentation:** https://github.com/chalk/chalk
- **Chokidar File Watching:** https://github.com/paulmillr/chokidar
- **Node.js File System API:** https://nodejs.org/api/fs.html