Team Details

a. **Team name:** Black Bird
b. **Team leader name:** Anuj Khandelwal
c. **Problem Statement:** PS-1: Enhancing Cybersecurity with Targeted Vulnerability Prevention

Demo Link: Video🔗

SBI Life
Apne liye. Apno ke liye.

HACK-AI-THON
2024

POWERED BY H2S HACK2SKILL

SOLUTION BRIEF

CodeShield

FORTIFY YOUR CODE, SECURE YOUR FUTURE.

PROTOTYPE-LINK

WHAT IS IT?

CodeShield is an **Advanced, AI-Driven security plugin** for Visual Studio Code that revolutionizes the way developers approach code security

Objective

Key Components

Why Use It?

AI-POWERED VULNERABILITY DETECTION AND REMEDIATION

Utilizes **Advance AI** to scan code for OWASP Top 10, SANS Top 25, and custom vulnerabilities. Provides intelligent recommendations and **Automatic Code Rewrites** to fix detected issues

SEAMLESS INTEGRATION WITH DEVELOPMENT WORKFLOW

Integrates directly into VS Code, providing security feedback without disrupting coding. Supports multiple programming languages and frameworks, adapting to various project types

REAL-TIME COLLABORATION

Enables team members to discuss and address security concerns in real-time. Implements a **Gamified Approach** to security, encouraging developers to improve practices

COMPREHENSIVE VISUALIZATION AND REPORTING

Provides intuitive visualizations of detected vulnerabilities and their interconnections. Generates **detailed reports on security status**, including a "Security Debt" tracker over time

PROACTIVE SECURITY INTEGRATION

Embeds security directly into the development process, catching vulnerabilities before they reach production

COMPREHENSIVE SECURITY COVERAGE

Addresses a wide range of vulnerabilities including **OWASP Top 10, SANS Top 25 across multiple programming languages** and frameworks.

DEVELOPER'S SKILL ENHANCEMENT

Educates developers on security best practices through real-time feedback and secure code suggestions

COST-EFFECTIVE SECURITY MANAGEMENT

Reduces the need for extensive manual code reviews and expensive security audits

SBI Life
Apne liye. Apno ke liye.

HACK-AI-THON 2024

POWERED BY H2S HACK2SKILL

CHALLENGES AND SOLUTIONS

SECURITY-DELAYS

CodeShield provides **real-time vulnerability scanning** directly within several IDE's. Its AI-powered engine **proactively analyzes code** as it's written and instantly flags security vulnerabilities.

EVOLVING THREATS

The plugin continuously **updates its knowledge base**, adapting to new vulnerabilities and attack vectors. This ensures that your codebase remains **protected against the latest cybersecurity challenges.**

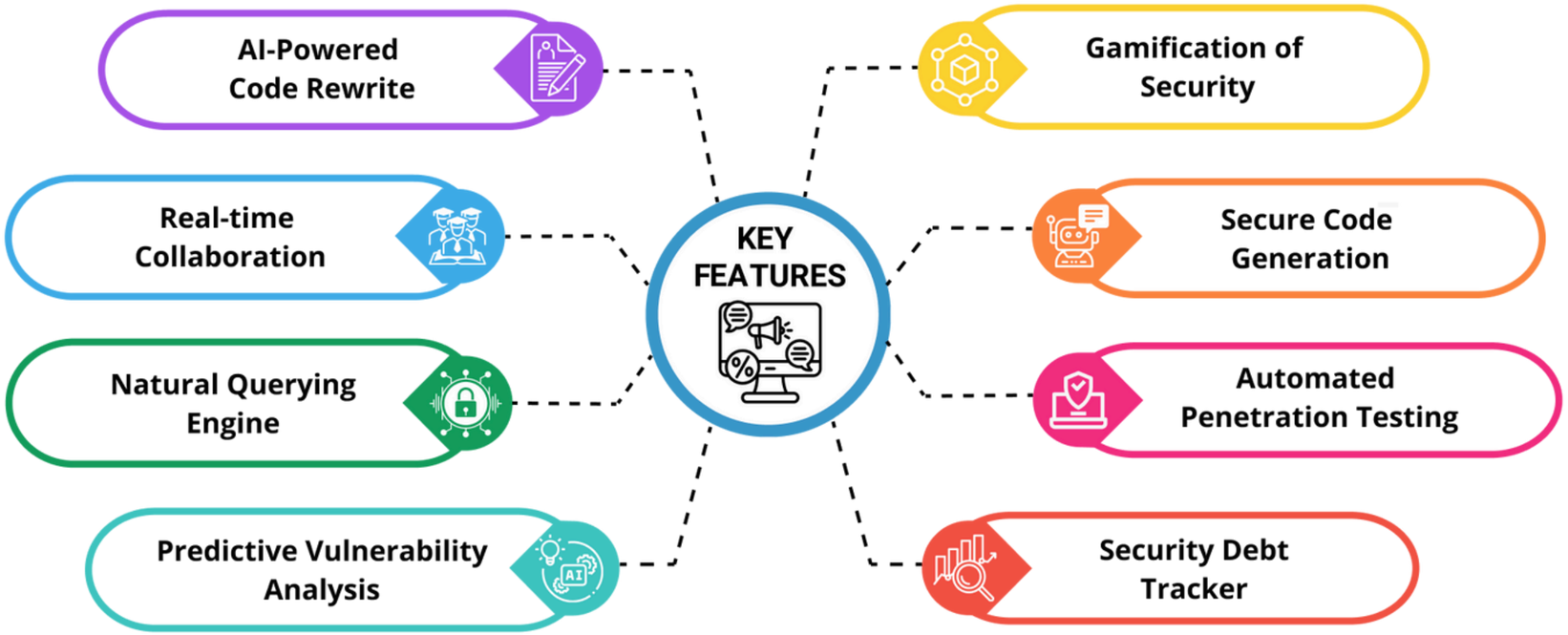
KNOWLEDGE GAP

CodeShield acts as an AI-powered security expert, **offering context-aware suggestions** and automatic **code rewrites.** It educates developers on security best practices through real-time feedback.

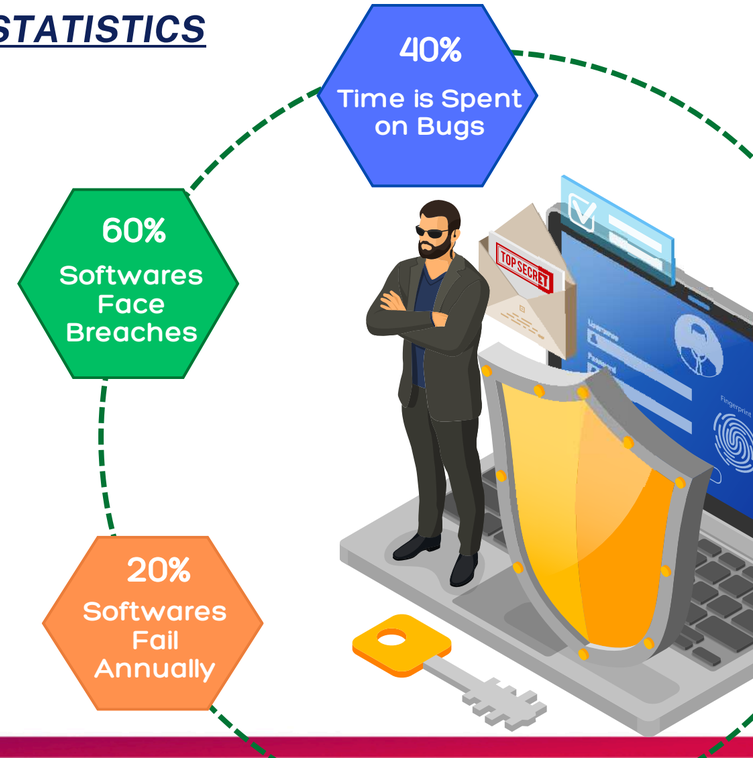
SILOED PRACTICES

CodeShield integrates security directly into the development workflow with its collaborative dashboard. It **centralizes security findings**, enabling **team-wide vulnerability management** and fostering collaboration.

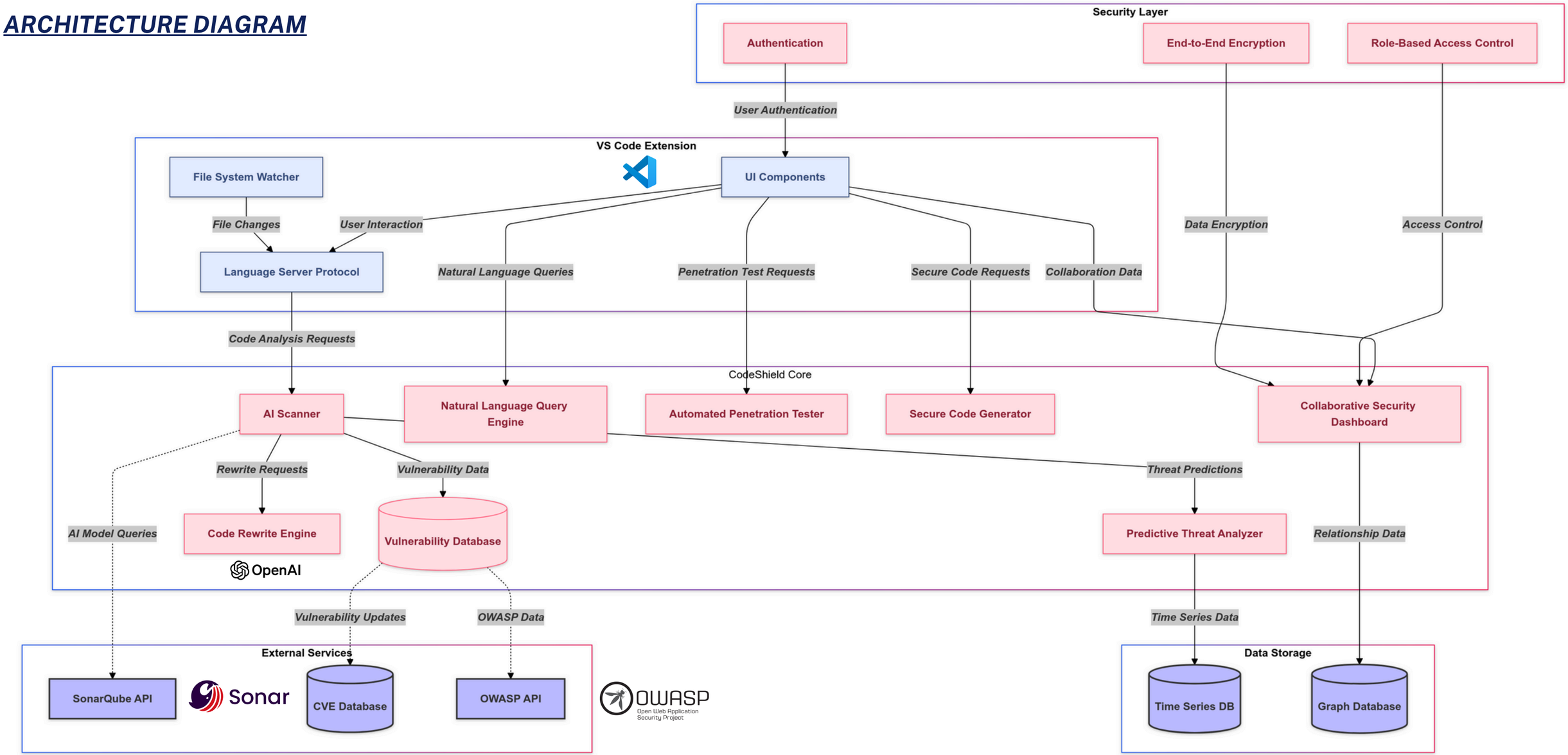
SOLUTION USP



STATISTICS



ARCHITECTURE DIAGRAM

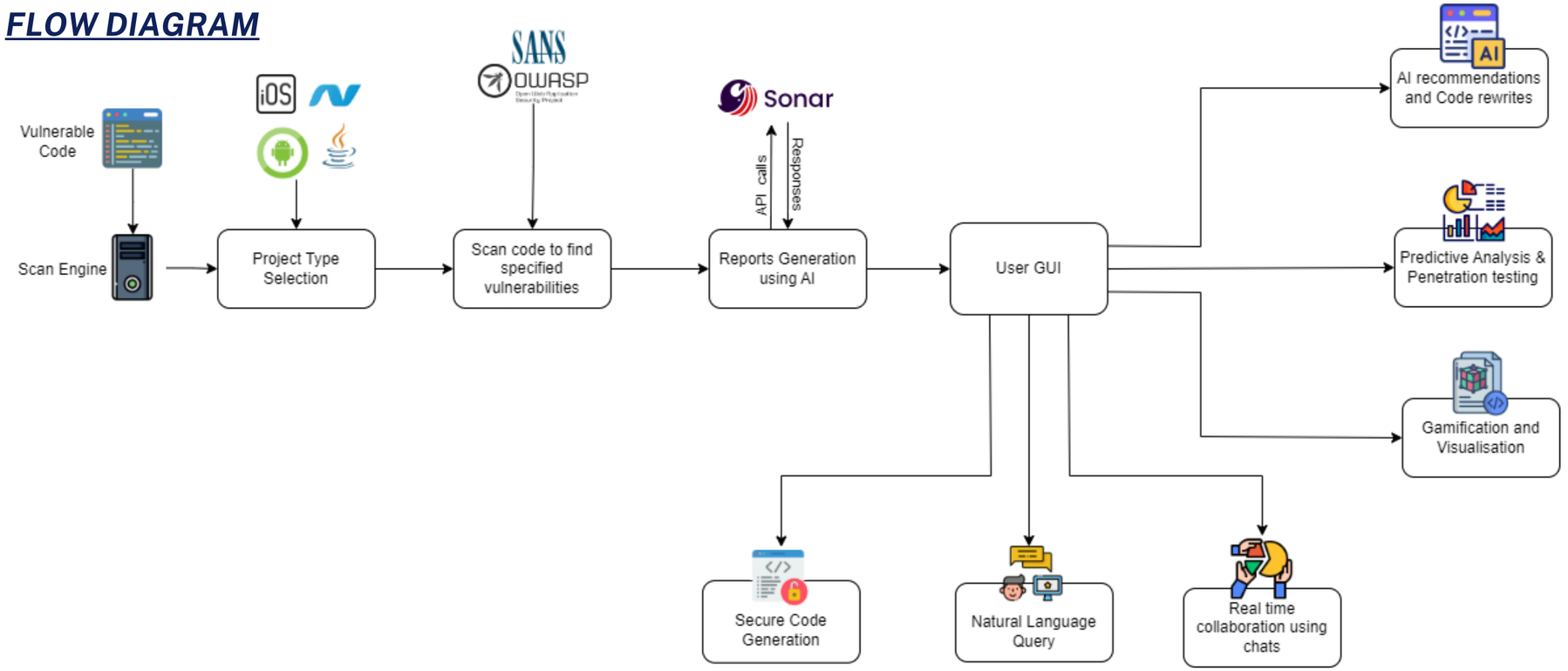


SBI Life
Apne liye. Apno ke liye.

HACK-AI-THON 2024

POWERED BY H2S

FLOW DIAGRAM



Technology Stack

Frontend

Backend

Machine Learning & APIs

MAJOR API'S

01 SonarQube

For static **code analysis**, identifying vulnerabilities, and generating **detailed reports** on code quality.

02 OWASP ZAP

For dynamic application security testing (**DAST**) and identifying **runtime vulnerabilities**.

03 Github Copilot

For **natural language processing** tasks such as analyzing code, suggesting fixes for vulnerabilities, and **AI-based code rewrites**.

Mock Diagrams

Project Selection

Project Type

.NET

- Dashboard
- Scan Results
- AI Recommendations
- AI Code Rewrite
- Visualization
- Collaboration
- Gamification
- Natural Language Query
- Predictive Analysis
- Secure Code Gen
- Pen Testing
- Security Debt
- Settings

Dashboard

Security Scanner

Quick Scan | Generate Report | Configure AI

Vulnerability Types

OWASP Top 10 | SANS Top 25 | Business Logic | Emerging Threats

Quick Scan
Start Scan

Secure Code Generation
Generate Code

Penetration Testing
Start Test

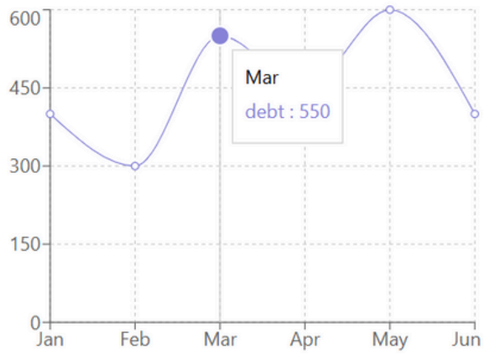
Security Debt
400 pts
+21 from last week

Scan Results

Type	Name	Severity	Location
OWASP Top 10	Injection	High	src/main.js:42
SANS Top 25	Use of Hard-coded Credentials	Medium	src/auth/login.js:15
Business Logic	Insufficient Access Control	High	src/api/users.js:78
Emerging Threats	API Key Exposure	Medium	src/config/api.js:5

Security Dept

Security Debt Tracker



Current Security Debt: 400 points

Security debt represents the accumulation of unaddressed vulnerabilities and technical shortcomings in your system's security posture.

AI Recommendations

Fix SQL Injection Vulnerability

Use parameterized queries or prepared statements to prevent SQL injection attacks.

```
// Instead of:
String query = "SELECT * FROM users WHERE username = '" + username + "'";

// Use:
String query = "SELECT * FROM users WHERE username = ?";
PreparedStatement stmt = connection.prepareStatement(query);
stmt.setString(1, username);
```

Resources:

- OWASP SQL Injection Prevention Cheat Sheet

Apply Fix

SBI Life
Apne liye. Apno ke liye.

PRESENTS

HACK-AI-THON 2024

POWERED BY H2S HACK2SKILL

Thank You!