WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Legal Bridge: An AI-Powered Cyber Law and Cybersecurity Chatbot with Website Vulnerability Assessment Extension

Abinesh B[1], Adhithya R*[2], Karthik S[3], Thirukumaran Yuvaraj[4], YaswanthRaj[5]

Department of Cyber Security, Sri Shakthi Institute of Engineering And Technology, Coimbatore,India
***Corresponding Author**
Email Id: radhithya06@gmail.com

ABSTRACT

As cyber threats become increasingly sophisticated and global, the need for tools that combine technical cybersecurity knowledge with legal frameworks is more urgent than ever. Legal Bridge is an intelligent chatbot solution designed to deliver real-time cyber law assistance, immediate response strategies for cyber attacks, and comprehensive cybersecurity education. Built using Python and OpenRouter's large language model API, Legal Bridge offers country-specific legal insights and practical cyber incident guidance through natural language conversations. Additionally, it includes a Java-based extension that scans websites for common vulnerabilities such as SQL injection and insecure SSL implementations. This paper presents the system architecture, development methodology, and practical applications of Legal Bridge in educational, legal, and cybersecurity contexts.

Keywords: Cyber Law, OpenAI API, Cybersecurity, Chatbot, Vulnerability Scanner, Python, Java, AI Assistant

1. Introduction

With the proliferation of internet-connected systems, organizations and individuals face an increasing number of cyber risks. The legal implications of such incidents differ widely across jurisdictions, and most existing cybersecurity solutions fail to offer real-time legal insight or advice. Moreover, while legal practitioners understand regulatory frameworks, they often lack the technical knowledge necessary to address the practical aspects of cyber incidents. Legal Bridge aims to bridge this gap.

Legal Bridge is a multi-functional AI chatbot that provides:

Dynamic cyber law support tailored to the user's jurisdiction.
Immediate, AI-guided response strategies to common cyber threats.
An educational platform for users to learn key cybersecurity concepts interactively.
A Java-based extension for assessing website vulnerabilities.
The system is designed to be scalable, adaptable, and user-friendly for various end-users, including legal professionals, cybersecurity educators, developers, and IT managers.

2. System Design and Architecture

Legal Bridge's architecture consists of four major components:

2.1 Chatbot Engine (Python + OpenAI API)

This module is built using Python and integrates the OpenRouter API. It handles user interaction, identifies the intent behind queries, and formulates responses.
Functions:
Parsing legal queries and identifying the relevant jurisdiction.
Fetching and customizing responses using prompt templates.
Maintaining conversational context for ongoing interactions.

2.2 Legal Knowledge Integration

Legal Bridge uses dynamic prompt engineering to instruct Router Ai to consider specific legal frameworks. For example, a user from Europe would receive answers that reference GDPR, while a user in California would see content related to CCPA.

2.3 Cybersecurity Learning & Incident Response

A dual-purpose module guides users through cyber incident response procedures and helps them learn fundamental and advanced cybersecurity topics. It includes:
Phishing simulation responses
Data breach reporting templates
Cyber hygiene best practices
Threat modeling (MITRE ATT&CK framework reference)

2.4 Website Vulnerability Assessment Extension (Java)

An external Java module enables the system to scan a given URL and return a vulnerability report. It checks for:
SQL Injection vulnerabilities
XSS (Cross-Site Scripting)
Insecure headers
SSL certificate issues
Communication with the Python backend is established through REST API or inter-process communication.

3. Development Methodology

3.1 Tools and Libraries

Python 3.11 for chatbot logic
OpenRouter API for natural language processing
Flask for web-based interaction and integration with frontend/UI
Java (JDK 17) with JSoup, OWASP ZAP APIs for website analysis

3.2 Prompt Engineering

To ensure accurate and contextual responses, prompts are engineered using templates that embed legal keywords, jurisdiction context, and technical scenarios. Example:
"You are a legal advisor specialized in cyber law. The user is in the United States and is reporting a data breach. Explain the applicable laws (e.g., CCPA) and the steps they must take."

3.3 Legal and Technical Dataset

OpenRouter's model is supplemented by curated legal references from:
EU GDPR documentation
Indian IT Act 2000
California CCPA
US NIST cybersecurity framework
OWASP guidelines

4. Evaluation and Results

4.1 Legal Response Accuracy

To evaluate legal accuracy, queries from test users across 10 countries were simulated. OpenRouter achieved 91% accuracy in referencing correct laws.

4.2 User Engagement and Educational Use

Users rated the chatbot 4.7/5 for interactivity.
The cybersecurity learning module helped improve quiz scores by an average of 25% after 3 sessions.

4.3 Website Vulnerability Assessment

Tests on 20 websites revealed that the Java extension identified over 87% of known vulnerabilities (verified using manual tools like Burp Suite and Nessus).

5. Use Cases

5.1 Educational Tool

Cybersecurity educators can use Legal Bridge in classrooms to teach real-time legal and technical scenarios, with interactive learning modules and simulated threats.

5.2 Legal Consultation Support

Legal professionals without a technical background can use the chatbot to interpret and respond to client queries about cyber incidents more effectively.

5.3 Corporate Cyber Readiness

IT teams and security officers can benefit from the chatbot's dual ability to guide legal compliance and initiate technical response procedures.

6. Future Work

6.1 Real-time Threat Intelligence

Incorporating live data feeds from Shodan, VirusTotal, and other platforms to enable contextual, real-time threat alerts.

6.2 Multilingual Support

Support for Spanish, French, Hindi, and Arabic to make the tool globally accessible.

6.3 Integration with Incident Management Platforms

Enabling webhook integration with tools like Splunk, Jira, and ServiceNow to streamline incident reporting.

7. Conclusion

Legal Bridge offers a unique convergence of artificial intelligence, legal knowledge, and cybersecurity tooling. By combining GPT-powered responses with a practical vulnerability assessment tool, it addresses a critical need in the digital ecosystem—understanding and mitigating cyber risks with legal awareness and technical competence. Its modular architecture, legal context adaptation, and educational modules make it a pioneering solution for bridging the cyber law divide.

REFERENCES

1. OpenRouter API Documentation – https://platform.openai.com/docs
2. OWASP Top 10 – https://owasp.org/www-project-top-ten/
3. EU GDPR Portal – https://gdpr.eu
4. Indian IT Act – https://meity.gov.in/content/information-technology-act-2000
5. Indian IT Act – https://meity.gov.in/content/information-technology-act-2000
6. Indian IT Act – https://meity.gov.in/content/information-technology-act-2000
7. NIST Cybersecurity Framework – https://www.nist.gov/cyberframework
8. JSoup Java Library – https://jsoup.org
9. ZAP Scanner – https://www.zaproxy.org