**IJARCCE** ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14669

# INTELLIGENT CHATBOT FOR CYBERSECURITY INCIDENT RESPONSE

**Mrs. Nandini GR[1] , Lavanya HS[2], Likitha BN[3], Monika BN[4], Nayana K[5]**

Assistant Professor, Information Science and Engineering, SSIT, Tumakuru, India. [1]

Students, Information Science and Engineering, SSIT, Tumakuru, India.[2-5]

**Abstract**: In today's digital age, cybersecurity incidents are rising in frequency and sophistication, requiring intelligent, responsive, and proactive solutions. This paper presents the implementation of an AI-Driven Cybersecurity Chatbot for Incident Response, integrating OpenAI for natural language understanding and VirusTotal for real-time threat intelligence. The system assists users in detecting, analyzing, and responding to threats through a user-friendly conversational interface.A core feature is the secure user authentication system with login and logout tracking, where activity is logged and monitored across devices. If a login is detected from an unknown or suspicious device, the system sends an instant alert to the original device or email account, helping to prevent account takeovers. Furthermore, it provides actionable insights on how the email or device may have been targeted, such as brute-force attempts or phishing-based intrusions, enhancing transparency and user awareness.The system also includes MongoDB-backed chat history, a modern UI, and structured responses with contextual definitions and safety advice for AI and cybersecurity terms. By combining real-time intelligence with AI-powered guidance and proactive alerting, the chatbot empowers users to detect, understand, and mitigate cyber threats effectively.

**Keywords**: Artificial Intelligence (AI), Cybersecurity, Incident Response,Natural Language Processing (NLP), Chatbot, VirusTotal API, Threat Intelligence, OpenAI Integration,Login/Logout Tracking,Cross-Device Alert System

## 1. INTRODUCTION

In the modern digital era, the frequency and complexity of cyberattacks have escalated, making traditional manual incident response approaches insufficient. With the exponential growth of digital communication and cloud services, organizations are increasingly vulnerable to threats like malware, phishing, and unauthorized access. To address these challenges, there is a pressing need for intelligent and proactive security systems that can assist users and security teams in real-time.This project presents an AI-Driven Cybersecurity Chatbot integrated with OpenAI for intelligent natural language processing and VirusTotal API for real-time threat analysis. The system enables users to query the chatbot for definitions, threat assessments, and cybersecurity advice. Additionally, it incorporates a login/logout tracking module that detects cross-device access, logs IP addresses, and alerts users if suspicious activity is identified on their accounts. This mechanism enhances security awareness and helps mitigate risks related to compromised credentials.By combining Artificial Intelligence, Threat Intelligence, and User Behavior Monitoring, the chatbot not only educates users but also actively participates in protecting web applications from evolving threats.

## 11. LITRATURE SURVEY

1. Title: IntellBot: Retrieval Augmented LLM Chatbot for Cyber Threat Knowledge Delivery
   Authors: Dincy R. Arikkat, Abhinav M., Navya Binu, Parvathi M., Navya Biju, K. S. Arunima, Vinod P., Rafidha Rehiman K. A., Mauro Conti
   Published: November 2024
   Summary: This paper introduces IntellBot, a cybersecurity chatbot leveraging Large Language Models and Retrieval-Augmented Generation to deliver contextually relevant threat intelligence. The chatbot aggregates data from diverse sources to provide comprehensive cybersecurity insights, demonstrating high accuracy in evaluations.

2. Title: Cyber-All-Intel: An AI for Security related Threat Intelligence
   Authors: Sudip Mittal, Anupam Joshi, Tim Finin

DOI: 10.17148/IJARCCE.2025.14669

Published: May 2019
Summary: This study presents Cyber-All-Intel, an AI system designed to assist security analysts by extracting and analyzing threat intelligence from various sources. The system employs knowledge graphs and neural networks to provide actionable cybersecurity insights.

3. Title: Getting Started with VirusTotal API: No-Code Automation Guide
Author: Tines Security Team
Published: Date not specified
Summary: This guide provides a comprehensive overview of integrating VirusTotal's API for automating security analysis, including scanning files, URLs, and IP addresses for malicious activity, enhancing threat assessment capabilities.
4. Title: Build a Phishing Detection Bot With Gmail, VirusTotal, and GPT
Author: Corey Jones
Published: May 2025
Summary: This tutorial demonstrates how to combine Gmail, VirusTotal, and GPT to automate phishing detection, offering a practical application of integrating VirusTotal with AI-driven tools.

## 111. EXISTING SYSTEM

Traditional cybersecurity systems rely heavily on manual incident response processes, signature-based detection, and rulebased monitoring to identify and mitigate threats. These systems, while effective for known threats, often struggle to keep up with the dynamic and sophisticated nature of modern cyberattacks such as zero-day vulnerabilities, social engineering, and advanced persistent threats (APTs).In existing setups, threat detection is primarily managed by Security Information and Event Management (SIEM) tools and Intrusion Detection/Prevention Systems (IDS/IPS). These tools require continuous human monitoring, and their effectiveness is limited by predefined rules and static threat databases. While they generate alerts, analyzing and responding to them often demands significant time and effort from cybersecurity teams, leading to alert fatigue and delayed response.Some organizations have adopted chatbot-based systems for general IT support and basic user queries, but these systems typically lack integration with real-time threat intelligence services or AI-powered natural language processing (NLP). Furthermore, they do not offer personalized security insights or anomaly detection based on user behavior like login tracking or IP analysis.Moreover, the integration of VirusTotal or similar APIs in existing security tools is often limited to backend processes and not exposed in a conversational interface accessible to end users or non-technical staff.

DISADVANTAGES OF EXISTING SYSTEM

- Lacks real-time threat intelligence integration
- Depends heavily on manual incident response
- No user-friendly or conversational interface
- Does not support natural language processing (NLP)
- Causes alert fatigue due to excessive false positives
- Provides limited context for threat alerts
- No tracking of login/logout behavior or IP addresses

## IV. PROPOSED SYSTEM

The proposed system is an AI-driven cybersecurity chatbot designed to enhance threat detection, user interaction, and incident response capabilities. It leverages advanced natural language processing through OpenAI to allow users to interact with the chatbot using simple, conversational language. This makes cybersecurity knowledge and threat response accessible even to nontechnical users. The system is integrated with the VirusTotal API, enabling real-time analysis of URLs, IP addresses, and file hashes to assess potential threats instantly.To strengthen user account security, the chatbot includes a behavior monitoring module that logs login and logout activities along with the corresponding IP addresses. It actively monitors for cross-device login attempts and alerts users if suspicious activity is detected, helping to prevent unauthorized access and credential misuse. All chat interactions and activity logs are stored in a secure MongoDB database, supporting traceability and analysis.In addition to threat detection, the chatbot provides users with definitions

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

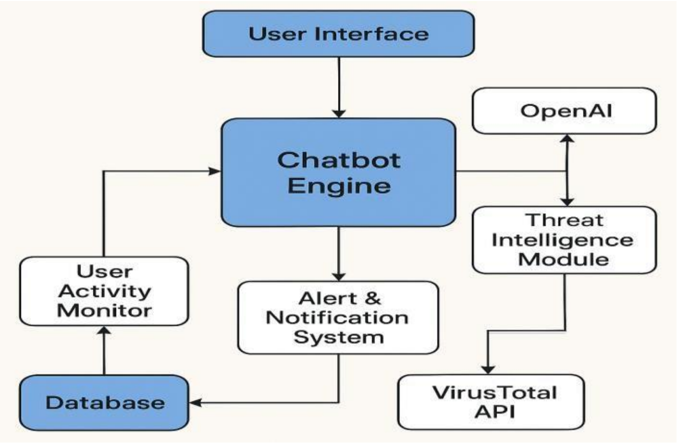
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14669

of cybersecurity terms, threat intelligence, and best practice advice. This educational feature promotes awareness and empowers users to recognize and respond to potential threats more effectively. The system also supports chat export and maintains a user-friendly web interface, ensuring a seamless experience across various platforms. Overall, this proposed solution automates incident response, improves detection speed, and bridges the gap between end-users and cybersecurity practices.

## V.SYSTEM ARCHITECTURE



1.User Interface

- They can ask queries, request threat scans, or seek cybersecurity advice.

2.Chatbot Engine

- The core of the system, built using Flask.
- Receives input from the user interface and routes requests accordingly.
- Coordinates with the OpenAI API and VirusTotal through other modules.

3.OpenAI (NLP Processing)

- The chatbot engine sends user questions to OpenAI's API.
- OpenAI processes the input and returns human-like responses related to cybersecurity concepts or advice.

4.Threat Intelligence Module

- If a user asks for a threat scan (e.g., URL or IP), the engine routes the data to this module.
- It prepares and formats requests to VirusTotal.

5.VirusTotal API

- The system uses VirusTotal’s API to analyze files, URLs, or IPs in real-time.
- The results are sent back to the chatbot engine for user feedback.

6.User Activity Monitor

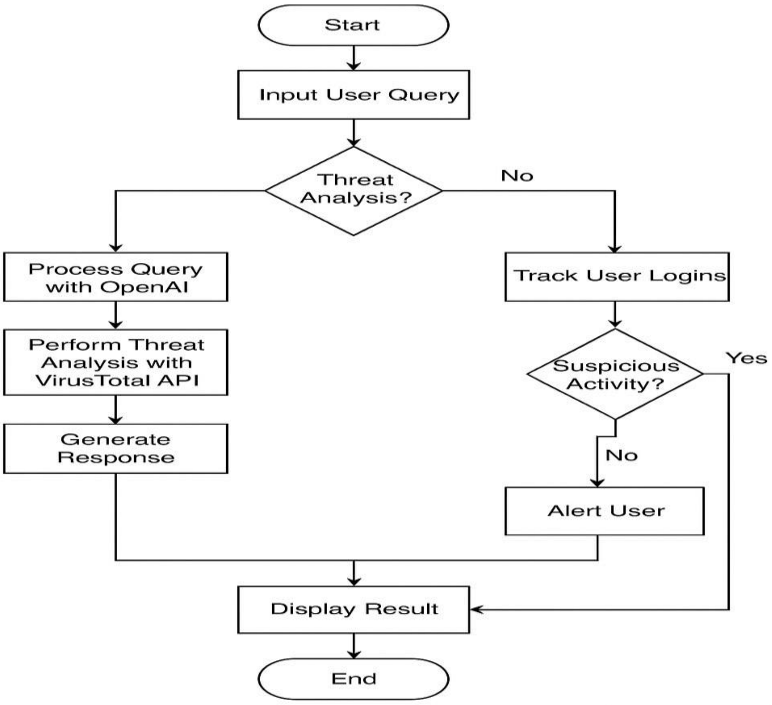
- Tracks login/logout actions and IP address details.
- Detects abnormal activity such as cross-device login attempts.

7.Alert & Notification System

- Generates and sends alerts to users when suspicious behavior is detected.
- It works in coordination with the chatbot engine and user activity monitor. 8.Database (MongoDB)
- Stores chat history, user logs, threat scan results, and activity data.
- Supports both audit trail and system intelligence.

DOI: 10.17148/IJARCCE.2025.14669

## VI. FLOW CHART DIAGRAM



In this diagram we will understand that how data will flow, how the system works.

## VII. IMPLEMENTATION

The implementation of the AI-Driven Cybersecurity Chatbot is structured across multiple modules, each handling specific tasks such as user interaction, threat analysis, authentication monitoring, and database management. The development is carried out using Python with Flask as the backend framework and HTML/CSS/JavaScript for the frontend interface.

1. Frontend Interface
   The user interface is built using HTML, CSS, and JavaScript to provide a responsive and interactive chatbot experience. It includes a chat window, input box, send button, and visual indicators (e.g., typing status). Users can ask cybersecurity-related questions, submit links for threat scans, and export chat history.

2. Backend and Flask Server
   The Flask backend acts as the core engine, handling all incoming user queries and routing them to appropriate services. Flask handles:

- OpenAI API calls for NLP-based responses
- VirusTotal API requests for threat scans
- MongoDB operations for storing chat and login data
- Login/logout tracking and IP logging

3. OpenAI Integration (NLP)
   The chatbot connects to OpenAI's GPT model to generate intelligent responses for cybersecurity terms, advice, and general queries. This enables a natural language interface for users who may not be technically proficient.
4. Threat Intelligence with VirusTotal
   For threat detection, the system integrates with the VirusTotal API. When a user submits a suspicious URL, file hash, or IP, the backend sends this data to VirusTotal and receives an analysis report, which is returned to the user.

DOI: 10.17148/IJARCCE.2025.14669

5. User Authentication and Monitoring
   The system implements Google OAuth for secure user login using the Authlib library. During login/logout, the user's email, timestamp, and IP address are recorded. If access is detected from an unfamiliar IP/device, the system flags it and sends an alert.

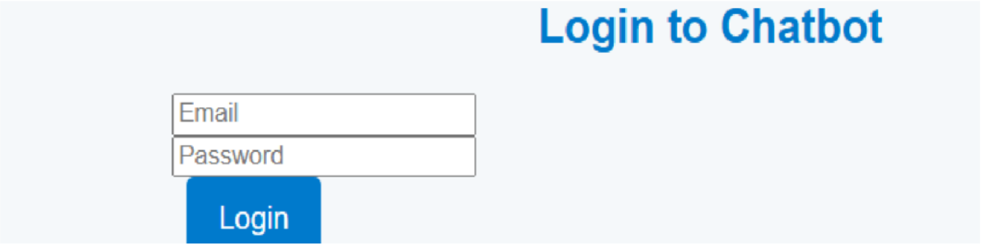
6. MongoDB Database MongoDB stores:

- User login/logout activity
- IP address logs
- Chat history and threat reports
  This allows for data persistence and audit trails, and supports features like chat export and history browsing.

7. Alerting System
   When suspicious login behavior is detected, the system immediately generates an alert and displays it to the user. This mechanism helps mitigate credential compromise.

8. Deployment
   The final system can be deployed on platforms like Render or Heroku. A .env file is used to manage API keys and sensitive configurations securely.

Result

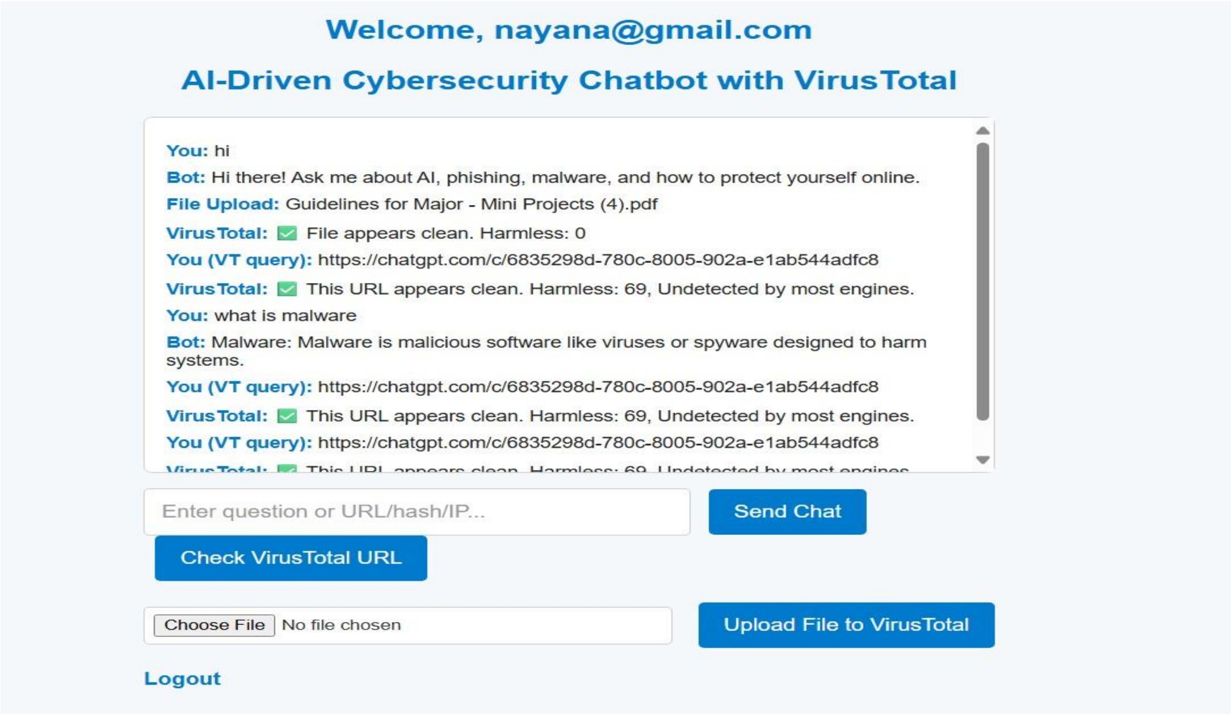


Login to Chatbot

Email

Password

Login page for the chatbot



Welcome, nayana@gmail.com

AI-Driven Cybersecurity Chatbot with VirusTotal

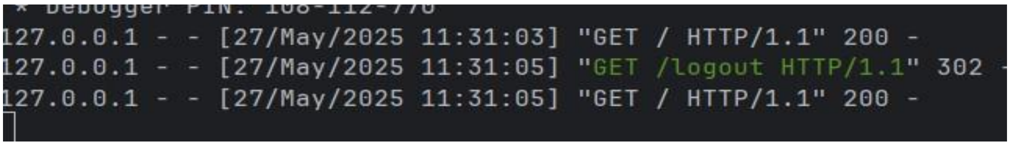
**You:** hi
**Bot:** Hi there! Ask me about AI, phishing, malware, and how to protect yourself online.
**File Upload:** Guidelines for Major - Mini Projects (4).pdf
**VirusTotal:** ✅ File appears clean. Harmless: 0
**You (VT query):** https://chatgpt.com/c/6835298d-780c-8005-902a-e1ab544adfc8
**VirusTotal:** ✅ This URL appears clean. Harmless: 69, Undetected by most engines.
**You:** what is malware
**Bot:** Malware: Malware is malicious software like viruses or spyware designed to harm systems.
**You (VT query):** https://chatgpt.com/c/6835298d-780c-8005-902a-e1ab544adfc8
**VirusTotal:** ✅ This URL appears clean. Harmless: 69, Undetected by most engines.
**You (VT query):** https://chatgpt.com/c/6835298d-780c-8005-902a-e1ab544adfc8
**VirusTotal:** ✅ This URL appears clean. Harmless: 69, Undetected by most engines.

Enter question or URL/hash/IP...

Choose File No file chosen

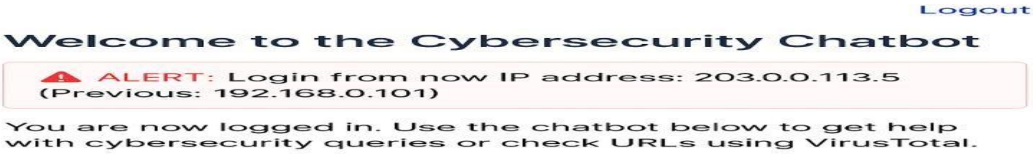
DOI: 10.17148/IJARCCE.2025.14669

Here we detect the file is harmful or not,and the given link is safe or not by using the virus total and also it will answer for the question for using the open ai



```
* Debugger PIN: 108-112-770
127.0.0.1 - - [27/May/2025 11:31:03] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [27/May/2025 11:31:05] "GET /logout HTTP/1.1" 302 -
127.0.0.1 - - [27/May/2025 11:31:05] "GET / HTTP/1.1" 200 -
```

Mongo DB for login and logout



Logout

Welcome to the Cybersecurity Chatbot

ALERT: Login from new IP address: 203.0.0.113.5 (Previous: 192.168.0.101)

You are now logged in. Use the chatbot below to get help with cybersecurity queries or check URLs using VirusTotal.

Gives the alert message if others are logged to the website that is linked to the particular email

## IX. CONCLUSION AND FUTURESCOPE

The AI-Driven Cybersecurity Chatbot presents a powerful and interactive solution for modern-day cyber threat detection and response. By combining OpenAI's natural language processing capabilities with VirusTotal's threat intelligence API, the system enables users to receive real-time insights, definitions, and recommendations related to cybersecurity threats. The integration of features such as login/logout activity tracking, IP address monitoring, and suspicious access alerts significantly enhances user account security. With a user-friendly interface and efficient backend architecture, the chatbot effectively bridges the gap between cybersecurity expertise and user accessibility, making it a valuable asset for both individuals and organizations.

Looking ahead, the system offers considerable scope for expansion and enhancement. Future developments can include training a domain-specific AI model tailored to cybersecurity queries, enabling more precise and contextual responses. Multi-language support can make the system globally accessible, while integration with SIEM tools can allow for deeper system-wide monitoring and automated incident responses. Voice-to-text and text-to-speech features can improve accessibility, and the development of mobile applications will ensure users can access the system from anywhere. Additionally, incorporating advanced analytics dashboards for administrators can help monitor system performance and user behavior. Implementing blockchain technology could further strengthen data integrity for critical security logs. These enhancements will collectively transform the chatbot into a more comprehensive cybersecurity assistant capable of both prevention and rapid response.

## REFERENCES

[1]. **Amit, A., & Sharma, R. (2023).** AI-based Cybersecurity Systems: A Review of Techniques and Applications. Journal of Cybersecurity and Information Systems, 11(2), 55-68.

[Discusses AI integration in cybersecurity tools and their impact on threat detection.]

**[2].Kumar, P., & Rathi, M. (2022).** Chatbot Applications in Security Awareness and Incident Handling. International Journal of Artificial Intelligence & Applications, 9(1), 23-30.

[Focuses on chatbots for user education and basic incident response in IT environments.]

**[3].OpenAI. (2023).** OpenAI API Documentation. Retrieved from https://platform.openai.com/docs [Provides guidelines and technical details for integrating GPT-based models.]

DOI: 10.17148/IJARCCE.2025.14669

**[4].VirusTotal. (2023).** VirusTotal Public API v3. Retrieved from https://docs.virustotal.com/reference [Documentation for real-time file, URL, and IP analysis.]

**[5].Mohammed, Z., & Lee, J. (2022).** Enhancing Threat Detection Using AI-Powered Chat Interfaces. Proceedings of the 2022 IEEE Conference on Cybersecurity, 112–119.

[Presents chatbot models integrated with threat intelligence for enterprise use.]

**[6].Garcia, M., & Singh, A. (2021).** User Behavior Analytics for Detecting Anomalies in Web Applications. CyberTech Journal, 18(4), 201–210.

[Describes behavior monitoring techniques including IP tracking and anomaly detection.]

**[7].MongoDB, Inc. (2023).** MongoDB Documentation. Retrieved from https://www.mongodb.com/docs [Explains storage architecture and implementation for logging and chat history.]

**[8].Authlib. (2023).** OAuth 2.0 and OpenID Connect with Flask. Retrieved from https://docs.authlib.org

[Used for implementing Google OAuth login in Flask applications.]