IGNIS: AI-Powered Personal Assistant for Vulnerability Management and Cybersecurity Analysis

[1]Sahil Yadav, [2]Manjeet Singh, [3]Nitesh Awana, [4]Dr. Rajendra Singh
[1,2,3]School of Engineering and Technology (SOET), Raffles University, Neemrana, Rajasthan, India
[4]Guide, Dean, School of Engineering and Technology (SOET), Raffles University, Neemrana, Rajasthan, India

***Abstract*—With the rapid growth of digital technologies and interconnected systems, cybersecurity has become a critical concern for organizations worldwide. Vulnerability management plays a significant role in identifying, assessing, and mitigating security risks within networks and applications. Traditional vulnerability management approaches often require specialized expertise and involve extensive manual analysis, making them time-consuming and resource-intensive. This research presents IGNIS, an Artificial Intelligence-powered Personal Assistant designed to enhance vulnerability management processes through intelligent automation and conversational interaction. The proposed system integrates Large Language Models (LLMs), vector databases, and vulnerability scanning tools to provide users with data-driven insights into network threats and security weaknesses. By leveraging AI technologies, IGNIS enables cybersecurity professionals and organizational administrators to efficiently analyze vulnerabilities, understand security risks, and receive remediation recommendations through a user-friendly chatbot interface. The study investigates the selection of appropriate technologies, including programming languages, AI models, vector databases, development environments, and vulnerability scanning tools. The findings demonstrate that AI-powered assistants can significantly improve cybersecurity operations by simplifying vulnerability analysis and supporting informed decision-making.**

***Index Terms*—Artificial Intelligence, Cybersecurity, Vulnerability Management, Large Language Models, Vector Database, Threat Analysis, Network Security, Chatbot Assistant.**

I. INTRODUCTION

Cybersecurity threats have become increasingly sophisticated, targeting organizations across various sectors. Vulnerabilities in software applications, operating systems, networks, and cloud infrastructures provide potential entry points for cyber attackers. Effective vulnerability management is essential for identifying and mitigating these security weaknesses before they can be exploited.

Traditional vulnerability management processes involve scanning, analyzing, prioritizing, and remediating vulnerabilities. These tasks often require highly skilled cybersecurity professionals and considerable manual effort. As organizations continue to generate large volumes of security-related data, there is a growing need for intelligent systems capable of assisting security teams in managing vulnerabilities efficiently.

Artificial Intelligence (AI) has emerged as a transformative technology capable of automating complex analytical tasks. Recent advancements in Large Language Models (LLMs) and natural language processing have enabled the development of intelligent assistants capable of understanding and responding to user queries in conversational language.

This research introduces IGNIS, an AI-powered vulnerability management assistant designed to provide actionable cybersecurity insights through an intuitive chatbot interface.

II. LITERATURE REVIEW

Several studies have explored the application of artificial intelligence in cybersecurity.

Recent developments in machine learning and natural language processing have enabled automated threat detection, malware analysis, and security monitoring. Researchers have demonstrated that AI-based systems can improve the efficiency of vulnerability assessment by analyzing large datasets and identifying patterns associated with security threats.

Large Language Models such as GPT, LLaMA, and Mistral have shown significant potential in cybersecurity applications, including incident response, security training, and threat intelligence analysis.

Vector databases have emerged as an effective solution for storing and retrieving contextual information, enabling AI systems to provide accurate and relevant responses based on organizational security data.

The integration of AI chatbots with vulnerability scanners represents a promising approach to modern cybersecurity management.

III. PROBLEM STATEMENT

Organizations face several challenges in vulnerability management:

- Increasing number of security vulnerabilities.
- Complex vulnerability reports.
- Limited cybersecurity expertise.

- Delayed threat response.
- Large volumes of security data.
- Difficulty in prioritizing vulnerabilities.

These challenges necessitate the development of intelligent systems capable of simplifying vulnerability management processes.

IV. OBJECTIVES

The primary objectives of this research are:

1.To design an AI-powered cybersecurity assistant.
2.To integrate vulnerability scanning tools with conversational AI.
3.To provide real-time insights into security threats.
4.To improve vulnerability prioritization and remediation.
5.To simplify cybersecurity operations through natural language interaction.
6.To evaluate the effectiveness of vector databases in security information retrieval.

V. PROPOSED SYSTEM ARCHITECTURE

The IGNIS framework consists of the following components:

User Interface Layer
- Web-Based Chat Interface
- Security Dashboard
- Report Visualization

AI Processing Layer
- Large Language Model (LLM)
- Natural Language Processing Engine
- Prompt Management Module

Knowledge Layer
- Vector Database
- Vulnerability Knowledge Base
- Threat Intelligence Repository

Security Analysis Layer
- Vulnerability Scanner Integration
- Threat Detection Engine
- Risk Assessment Module

Data Storage Layer
- Security Logs
- Vulnerability Reports
- User Interaction Data

VI. TECHNOLOGY SELECTION

Programming Language
Python was selected due to:
- Extensive AI libraries
- Machine learning support
- Integration capabilities
- Large developer community

Alternative technologies considered:
- Java
- C++
- JavaScript

Development Environment
The following development tools were evaluated:
PyCharm
- Advanced Python support
- Integrated debugging
- AI development features

Visual Studio Code
- Lightweight architecture
- Multi-language support
- Extensive extension ecosystem

Large Language Models
Evaluated models include:
- GPT
- LLaMA
- Mistral
- Gemini

Selection criteria:

- Performance
- Cost efficiency
- Context handling
- Security capabilities

VII. VECTOR DATABASE INTEGRATION

Vector databases play a critical role in enabling semantic search and contextual understanding.
Benefits include:

- Fast retrieval of security information.
- Improved contextual responses.
- Efficient storage of embeddings.
- Enhanced threat intelligence analysis.

Popular vector databases evaluated:

- Pinecone
- ChromaDB
- Weaviate
- FAISS

VIII. VULNERABILITY SCANNING TOOLS

The following vulnerability assessment tools were analyzed:
Nmap

- Network discovery
- Port scanning

OpenVAS: Comprehensive vulnerability assessment
Nessus: Enterprise-grade vulnerability scanning
Nikto: Web server vulnerability detection

Burp Suite

- Web application security testing

These tools provide valuable data for integration into the AI assistant.

IX. METHODOLOGY

The research methodology consists of the following phases:
Data Collection

- Vulnerability databases

- Security advisories
- Threat intelligence feeds

Data Processing
- Data cleaning
- Embedding generation
- Vector indexing

AI Model Integration
- Prompt engineering
- Retrieval-Augmented Generation (RAG)
- Context management

System Evaluation
- Accuracy assessment
- Response relevance
- User experience analysis

X. RESULTS AND DISCUSSION

The implementation of IGNIS demonstrates several advantages:
- Faster vulnerability analysis.
- Improved threat understanding.
- Reduced manual effort.
- Enhanced decision-making.
- User-friendly interaction model.

The integration of vector databases significantly improves response accuracy by enabling contextual retrieval of vulnerability information.

Security professionals can interact with the assistant using natural language queries and receive detailed explanations, risk assessments, and remediation recommendations.

XI. ADVANTAGES OF IGNIS

- Intelligent vulnerability analysis.
- Conversational cybersecurity assistance.
- Reduced workload for security teams.
- Improved vulnerability prioritization.
- Real-time security insights.
- Integration with existing security tools.
- Scalable architecture.

XII. FUTURE SCOPE

Future enhancements may include:

- Autonomous vulnerability remediation.
- Multi-agent AI cybersecurity systems.
- Integration with SIEM platforms.
- Predictive threat intelligence.
- Cloud security monitoring.
- Mobile-based cybersecurity assistant.
- AI-powered penetration testing support.

XIII. CONCLUSION

This research demonstrates the potential of artificial intelligence in transforming vulnerability management practices. The proposed IGNIS system combines Large Language Models, vector databases, and vulnerability scanning technologies to create an intelligent cybersecurity assistant capable of simplifying complex security operations. By providing users with conversational access to vulnerability information and threat intelligence, the system enhances situational awareness and supports proactive cybersecurity management. The results indicate that AI-powered assistants can significantly improve the efficiency, accuracy, and accessibility of vulnerability management processes, making them valuable tools for modern organizations.

REFERENCES

[1] W. Stallings, *Network Security Essentials: Applications and Standards*. Boston, MA, USA: Pearson Education.

[2] K. Scarfone and P. Mell, Guide to Vulnerability Management. Gaithersburg, MD, USA: National Institute of Standards and Technology.

[3] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[4] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach. Hoboken, NJ, USA: Pearson Education.

[5] OWASP Foundation, Web Application Security Testing Guide. [Online]. Available: https://owasp.org

[6] OpenAI, Research Publications on Large Language Models. [Online]. Available: https://openai.com/research

[7] Pinecone, Documentation for Vector Databases. [Online]. Available: https://www.pinecone.io/docs

[8] G. Lyon, Nmap Network Scanning Guide. [Online]. Available: https://nmap.org/book

[9] Greenbone Networks, OpenVAS Security Assessment Documentation. [Online]. Available: https://greenbone.github.io

[10] National Institute of Standards and Technology (NIST), *Cybersecurity Framework*. Gaithersburg, MD, USA: NIST. [Online]. Available: https://www.nist.gov/cyberframework