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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

AI DRIVEN CYBERSECURITY CHATBOT FOR INCIDENT RESPONSE

Ms. Pratyaksha S[1], Adeeb Sadiq[2], Aisiri K S[3], Deeksha K M[4], Kavya K[5]

[1]Assistant Professor, Dept. of ISE, East West Institute of Technology, Bengaluru

[2] Student, Dept. of ISE, East West Institute of Technology, Bengaluru

[3] Student, Dept. of ISE, East West Institute of Technology, Bengaluru

[4] Student, Dept. of ISE, East West Institute of Technology, Bengaluru

[5] Student, Dept. of ISE, East West Institute of Technology, Bengaluru

Abstract: In today's cybersecurity realm, combatting advanced threats requires innovative solutions for early detection and swift response. This system introduces a pioneering chatbot system tailored for cybersecurity, employing AI, ML, and NLP. It continuously monitors diverse data streams like network traffic and social media, using ML to pinpoint potential threats accurately, even zero-day vulnerabilities. Acting as a user-friendly interface, it allows real-time updates, incident report requests, and alerts, improving usability and decision-making. Integration capabilities enable seamless coordination across security platforms, maximizing current investments. Advanced automation features streamline incident response, with the chatbot autonomously initiating actions such as isolating compromised systems. This approach empowers organizations to protect vital assets in a dynamic digital landscape, leveraging AI, ML, and NLP to proactively tackle cyber threats.

Keywords: Cybersecurity, Chatbot system, AI, ML, NLP.

1. INTRODUCTION

In the modern digital realm, the rising complexity and frequency of cyber threats pose significant challenges to organizations globally. Traditional reactive cybersecurity approaches, which rely on manual analysis and response, are proving increasingly inadequate against the rapid evolution of attack methods and the dynamic landscape of threat actors. Therefore, there's a critical need for innovative solutions capable of proactively detecting threats and enabling swift incident response. This project explores a novel cybersecurity strategy by introducing a next-generation chatbot system specifically tailored to address these challenges. Leveraging advanced technologies such as artificial intelligence (AI), machine learning (ML), and natural language processing (NLP), this system represents a fundamental shift in how security incidents and threat intelligence are managed. At its core, the proposed chatbot system continuously monitors and analyzes vast streams of data from various sources, including network traffic, system logs, threat feeds, and social media platforms. Using advanced ML algorithms, the chatbot can accurately identify patterns indicative of potential security threats or anomalies. This proactive approach enables the system to detect both known and previously unseen threats, including zero-day vulnerabilities and emerging attack vectors, with exceptional precision. Furthermore, beyond its role as a detection tool, the chatbot serves as an intuitive interface, empowering users to seamlessly interact with the cybersecurity ecosystem through its natural language interaction capabilities. This user-centric design not only enhances usability but also expedites decision-making processes and facilitates rapid

incident response actions. Another key strength of the proposed system lies in its seamless integration with existing cybersecurity infrastructure and tools. This integration promotes synergy, enabling the chatbot to leverage data from diverse sources to provide comprehensive threat intelligence and coordinate incident response efforts across different security platforms. This interoperability ensures that organizations can optimize their existing investments while taking advantage of the enhanced capabilities offered by the chatbot system. Additionally, the chatbot system incorporates advanced automation features designed to streamline incident response processes. By leveraging contextual insights and historical data, the chatbot can autonomously trigger response actions such as isolating compromised systems, blocking malicious IP addresses, and orchestrating remediation procedures. This automation not only accelerates response times but also enhances the capabilities of human analysts, empowering organizations to respond more effectively to security incidents while minimizing potential damages. In summary, this project explores how the convergence of AI, ML, and NLP technologies within the framework of a next-generation chatbot system represents a transformative milestone in cybersecurity. By empowering organizations to proactively anticipate and swiftly counter evolving cyber threats, this

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

innovative solution is poised to safeguard critical assets and strengthen defenses in the face of an increasingly hostile digital landscape.

2. EXISTING SYSTEM

The existing system for "Al Chatbot Cybersecurity Next Gen Threat Intelligence and Real-time Incident Response" is a comprehensive integration of various technologies and components aimed at bolstering cybersecurity capabilities. At its core lies a chatbot interface powered by ChatGPT, an AI language model developed by OpenAI. This interface serves as the primary means for users to interact with the system, enabling them to access real-time threat intelligence updates, request incident reports, and receive proactive alerts. The system aggregates data from diverse sources such as network traffic, system logs, threat feeds, and social media platforms, leveraging ChatGPT's natural language processing capabilities to analyze unstructured data and extract meaningful insights for threat intelligence. Advanced machine learning algorithms are employed for real-time threat detection, with ChatGPT processing incoming data streams to identify patterns indicative of potential security threats or anomalies, including zero-day vulnerabilities and emerging attack vectors. Incident response actions are automated based on predefined rules and policies, with ChatGPT autonomously initiating response actions such as isolating compromised systems, blocking malicious IP addresses, and orchestrating remediation procedures. Moreover, the system seamlessly integrates with cybersecurity operations centers (COCs) or existing security infrastructure, facilitating collaborative incident response efforts and providing actionable insights. Mechanisms for performance monitoring and evaluation are included to assess threat detection accuracy, incident response efficiency, and usability, with continuous feedback loops enabling iterative improvements over time. Designed to be scalable and adaptable to evolving cybersecurity requirements, the system can accommodate changes in data sources, threat landscape, and organizational needs without significant disruption. Overall, the system leverages ChatGPT's advanced capabilities in natural language processing and generation to offer a comprehensive solution for addressing the dynamic and complex challenges of cybersecurity.

3. PROPOSED SYSTEM

The proposed system for "AI Chatbot Cybersecurity Next Gen Threat Intelligence and Real-time Incident Response" aims to redefine cybersecurity operations through the integration of cutting-edge technologies and novel methodologies. Here's an outline of its key features. The system will introduce a next-generation chatbot interface, powered by state-of-the-art AI technologies such as ChatGPT and other natural language processing (NLP) models, facilitating intuitive and efficient communication with the cybersecurity system. Enhanced threat intelligence gathering will be a cornerstone of the proposed system, aggregating data from diverse sources including network traffic, system logs, threat feeds, social media platforms, and open-source intelligence (OSINT). Advanced NLP algorithms will analyze unstructured data to extract relevant threat intelligence insights. Proactive threat detection will be enabled through machine learning and deep learning techniques, allowing real-time analysis of incoming data streams to detect security threats. Anomaly detection algorithms will identify suspicious activities and potential security breaches, including zero-day vulnerabilities and advanced persistent threats (APTs). Automated incident response capabilities will be integrated into the system to swiftly mitigate security incidents. Chatbot-driven automation workflows will orchestrate response actions such as containment, isolation, and remediation of compromised systems. Seamless integration with existing cybersecurity tools and platforms will be prioritized, facilitated by APIs and interoperability standards. This integration will enhance overall cybersecurity posture by leveraging existing security information and event management (SIEM) systems, threat intelligence platforms, and other security tools. Adaptive learning mechanisms will continuously improve the system's performance and effectiveness. Feedback loops and machine learning algorithms will analyze historical data and user interactions to refine threat detection models, automate response workflows, and optimize system behavior over time. A user-centric design approach will ensure seamless interaction and collaboration between human analysts and the cybersecurity system. Intuitive dashboards, natural language querying capabilities, and proactive alerting mechanisms will enhance usability and facilitate faster decision-making in incident response scenarios. Scalability and resilience will be inherent in the system's design, allowing it to accommodate growing data volumes, evolving threat landscapes, and organizational requirements. High availability, fault tolerance, and disaster recovery mechanisms will ensure resilience against cyber attacks and operational disruptions. Overall, the proposed system represents a comprehensive approach to cybersecurity, leveraging advanced AI technologies and innovative methodologies to enhance threat intelligence, enable real-time incident response, and empower organizations to stay ahead of emerging cyber threats in today's dynamic digital landscape.

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

4. IMPLEMENTATION

The implementation of the "AI Chatbot Cybersecurity Next Gen Threat Intelligence and Real-time Incident Response" system involves a meticulous process of translating its design into executable code and deploying it into a production environment. This process encompasses setting up development environments with the necessary tools and frameworks, developing the chatbot interface with natural language processing capabilities, and creating backend components for data collection, analysis, and incident response orchestration. Integration with existing cybersecurity infrastructure, including SIEM systems and threat intelligence feeds, is essential, as is the development of machine learning models for threat detection and anomaly detection. User interface design focuses on providing intuitive dashboards and visualization tools for system administration and monitoring. Rigorous testing and quality assurance procedures ensure the functionality, performance, and security of the system before deployment. Deployment and release management processes are implemented to ensure scalability, reliability, and security in production environments. Continuous monitoring and maintenance procedures are established to track system performance, detect anomalies, and apply updates and security fixes. User training sessions and ongoing technical support are provided to ensure users are familiar with the system and can effectively utilize its functionalities. Through this comprehensive approach, the implementation of the system aims to enhance cybersecurity capabilities and protect critical assets in today's dynamic digital landscape.

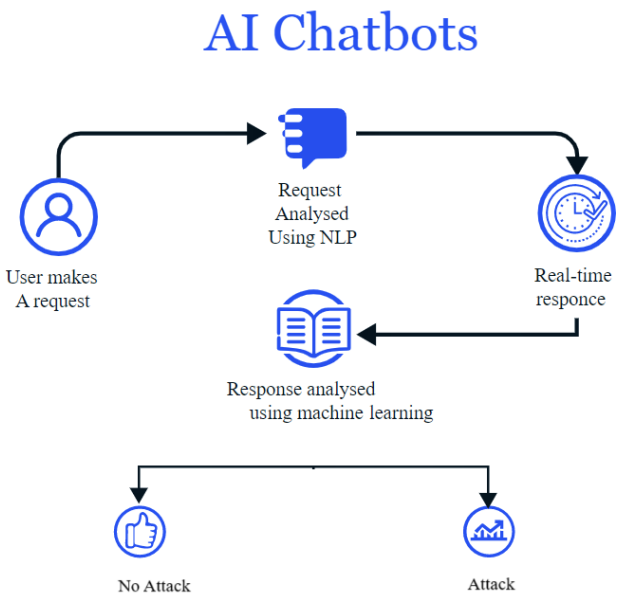

Fig 1. System Architecture

4.1 ALGORITHMS

1. NLP ALGORITHM

Tokenization involves breaking text into smaller units such as words, phrases, symbols, or other meaningful elements (tokens), serving as the initial step in numerous NLP tasks. Stemming reduces words to their root form, while lemmatization maps them to their base or dictionary form, aiding in normalization and vocabulary size reduction. Part-of-Speech (POS) Tagging assigns grammatical categories to words, crucial for parsing, named entity recognition (NER), and machine translation. NER identifies and classifies named entities like person names, organization names, and locations, aiding in information extraction. Syntax and parsing analyze sentence structure to understand word relationships, using techniques like constituency and dependency parsing. Word embeddings represent words as dense vectors, with similar words sharing similar representations, while sentence embeddings represent entire sentences or documents as vectors. Machine translation translates text between languages, employing statistical, rule-based, or neural models. Sentiment analysis determines expressed sentiment (positive, negative, or neutral) using supervised or deep learning techniques. Topic modeling identifies themes in documents using algorithms like Latent Dirichlet Allocation (LDA). Text generation produces contextually relevant text based on input, from n-gram models to sophisticated neural models like GPT. Question Answering (QA) systems automatically generate answers to natural language questions, involving understanding, information retrieval, and concise answer generation. These NLP techniques continue to evolve with machine learning and deep learning advancements, selected based on task and data characteristics.

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

2. LNN ALGORITHM

Light neural networks are favored in scenarios with limited computational resources, such as mobile or embedded systems, where memory and processing power are constrained. They offer faster inference speeds, vital for real-time applications, and enhance energy efficiency, crucial for battery-powered devices like smartphones or IoT gadgets. Their compact size facilitates easier deployment and distribution across diverse settings. To achieve lightness, various techniques can be applied. These include reducing model size by decreasing parameters through layer reduction, width reduction, or quantization. Pruning eliminates unnecessary connections or neurons, significantly cutting down computational requirements. Knowledge distillation trains a simpler model to mimic predictions of a larger one, resulting in comparable performance but lighter weight. Architectural design plays a key role, with strategies like depth-wise separable convolutions and smaller filter sizes contributing to a leaner network. Ultimately, the decision to use a light neural network hinges on the specific application requirements, considering factors like computational resources, performance needs, and deployment constraints.

5. RESULTS

Fig 2. Home Page

The above figure 2 represents the home page of the system where the user can click on the chatbot button to chat with the chatbot and the admin and can login into the system by clicking on the login button.

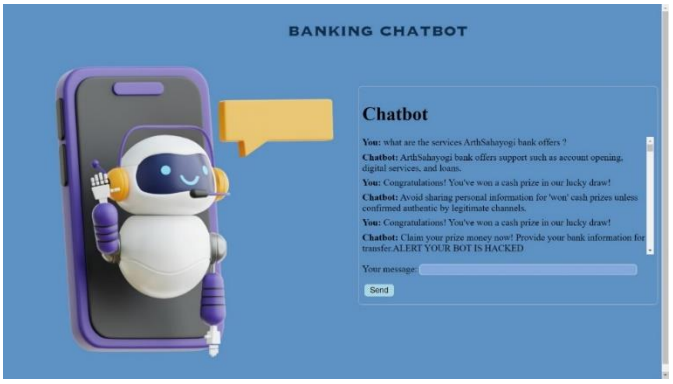

Fig 3. Chatbot

The above figure 3 represents the chatbot where the user can enquire about theirs queries and get the required responses, it also gives alert messages if the chatbot is hacked.

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

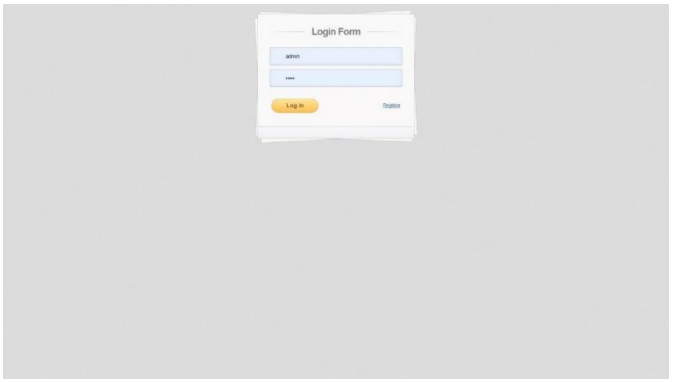

Fig 4. Login Page

The above figure 4 represents the login page where credentials like username and password are entered to login into the system, only if the entered credentials are correct.

Fig 5 Login Home Page

The above figure 5 represents the home page of the bank system where different details about the users and attacks can be viewed by the admin.

Fig 6. User Details

The above figure 6 represents the user details page where the admin will be able view different details about the user like their first name, last name, account number, phone number and email id.

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

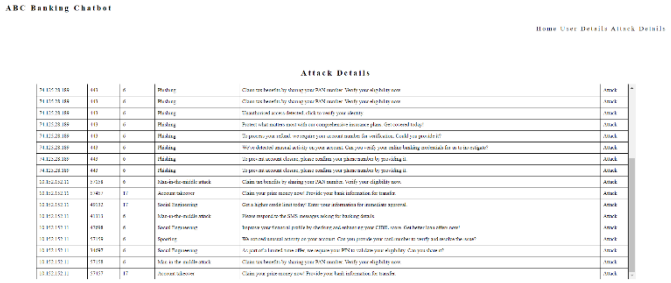

Fig 7. Attack Details

The above figure 7 represents the attack details where the admin can view different details like the type of attack that has taken place and in which port it has taken place.

6. CONCLUSION

The "AI Chatbot Cybersecurity Next Gen Threat Intelligence and Real-time Incident Response" system marks a pivotal advancement in cybersecurity. Utilizing state-of-the-art AI technologies like NLP and ML, it ensures proactive threat detection, real-time incident response, and seamless integration with existing infrastructure. Careful attention to modularity, scalability, security, and user experience underpins its design. The modular architecture ensures flexibility and maintainability, while robust security measures safeguard sensitive data. NLP-powered chatbot interface enables intuitive interaction, while ML algorithms drive accurate threat detection and automated incident response. Integration with existing tools enhances its utility, fostering seamless data exchange and coordinated incident response. Adaptive learning mechanisms continuously refine its performance, enabling it to effectively combat emerging threats. In essence, this system heralds a new era in cybersecurity, empowering organizations to navigate the evolving threat landscape with confidence and resilience.

ACKNOWLEDGEMENT

This project received support from the East West Institute of Technology. We express our sincere appreciation to our internal guide, **Ms. Pratyaksha S** , Assistant Professor in the Department of Information Science and Engineering (ISE), forher invaluable guidance and significant contributions in enhancing the manuscript. We also acknowledge **Dr. Suresh** MB, Prof & Head of ISE Department, for his continuous supportand mentorship throughout the project. Our sincere thanks go to Principal **Dr. Channakeshavalu** for his unwavering support and encouragement. We are indebted to classmates for their constructive feedback on earlier versions of the project. Any shortcomings in the manuscript remain our responsibility and should not reflect negatively on the esteemed professionals mentioned above.

REFERENCES

[1] Muhammad Usama, et al. "A Survey on AI in Cybersecurity" IEEE Access, 2019.
[2] "Artificial Intelligence for Cybersecurity: A Comprehensive Survey", Amir Houmansadr, et al. ACM Computing Surveys, 2021.
[3] "An Overview of the State of the Art in the Use of Machine Learning Techniques in the Automated Incident Response Lifecycle“, D. Zampunieris, et al., 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS).
[4] Arsh Arora, et al. "Machine Learning for Cybersecurity Incidents Detection and Response: A Survey “Journal of Network and Computer Applications, 2020.
[5] Hayajneh, Thair, et al. ,"Using AI to Augment Human Intelligence in Cybersecurity“, IEEE Security & Privacy, 2020
[6] Dey, S., Islam, M. R., & Saha, D. (2021). "A Review of Chatbots in Cybersecurity: Techniques, Applications, and Challenges." IEEE Access, 9, 36722-36740.
[7] Gokulakrishnan, P., & Saminathan, B. (2020). "AI-Based Cybersecurity Chatbot for Real-Time Incident Response." In Proceedings of the International Conference on Computing, Communication, and Cybersecurity (ICCCS 2020).
[8] Patil, A., & Patil, S. (2019). "Chatbots in Cybersecurity: A Comprehensive Review." In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI 2019).

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13509

[9] Sadasivam, S., & Prakash, V. (2018). "Real-Time Incident Response System Using AI Chatbots in Cybersecurity Operations." In Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2018).

[10] Schönberger, S., & Treubel, J. (2020). "Using Chatbots for Real-Time Threat Intelligence in Cybersecurity Operations." Journal of Cybersecurity, 3(1), 23-35.

[11] Sharma, N., & Jain, A. (2021). "Next-Generation Chatbots for Cybersecurity Incident Response: A Comprehensive Survey." Journal of Network and Computer Applications, 185, 102923.

[12] Wang, L., Wang, Y., & Zhao, D. (2019). "A Survey on Chatbots in Cybersecurity." In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2019).

[13] Zhang, Y., & Zhang, Y. (2018). "Application of Chatbots in Cybersecurity: Challenges and Opportunities." In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2018).

[14] Zhu, H., Wang, C., & Li, X. (2020). "A Novel Chatbot System for Real-Time Cyber Threat Intelligence." IEEE Access, 8, 101638-101648.

[15] Zhu, Y., & Chen, W. (2019). "AI-Driven Chatbots for Cybersecurity Incident Response: Opportunities and Challenges." In Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2019).

