# Guardians Of Things(GoT): Automating Cyber Security Tasks Using the OpenAI API

Shreyansh Kushwaha,Alankrit Sharma, Priyanshu Srivastava, and Kavita Jaiswal
IIIT Naya Raipur
Chhatisgarh, India 493661
Email: {shreyansh22101, alankrit22101, priyanshu22101, kavita}@iiitnr.edu.in

***Abstract*—The Internet of Things (IoT) is a comprehensive idea that involves the integration of all objects. The Internet of Things (IoT) has a significant opportunity to enhance global accessibility, integrity, availability, scalability, confidentiality, and interoperability. Nevertheless, safeguarding IoT poses a formidable undertaking. IoT development relies on a solid foundation of system security. This paper explores the capabilities of the OpenAI API in automating tasks within the realm of various cyber security jobs. The study involves the creation of a comprehensive database comprising queries and corresponding solutions. The OpenAI API is employed to process these queries and generate code snippets and step-by-step instructions to accomplish the specified tasks. The system's performance is evaluated based on its accuracy in resolving diverse queries, revealing promising outcomes and highlighting the potential of artificial intelligence (AI) in enhancing efficiency and effectiveness in cyber security operations. Future endeavors include expanding the database, refining the AI's accuracy, and integrating with security tools for seamless automated execution. This research contributes to the ongoing discourse on the integration of AI technologies in cyber security, emphasizing the role of automation in addressing complex and dynamic security challenges.**

***Index Terms*—Cybersecurity automation, OpenAI's API, Query processing, Automated code generation, Efficiency.**

## I. Introduction

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of unparalleled connectivity and convenience, yet it has concurrently introduced a multitude of cybersecurity challenges [7]. The intricate interconnectedness of these devices, spanning from household appliances to industrial sensors, has woven a complex web of vulnerabilities, exposing them to a diverse array of security threats. Persistent menaces such as unauthorized access, data breaches, and malicious attacks threaten the integrity and functionality of IoT systems. Consequently, there is an urgent demand for a sophisticated architecture capable of comprehensively analyzing and mitigating the risks associated with the interconnectivity of IoT devices.

This paper endeavors to craft a robust architecture utilizing OpenAI's API to systematically assess and diminish the cybersecurity risks prevalent in IoT ecosystems. The architecture will harness advanced algorithms and machine learning techniques to scrutinize data flows, identify potential vulnerabilities, and proactively respond to emerging security threats. By leveraging the capabilities of OpenAI's API, the system aims to augment its ability to understand and adapt to the evolving cybersecurity landscape, ensuring a dynamic defense against emerging threats.

The significance of this initiative is underscored by the escalating dependence on IoT devices across various sectors, ranging from smart homes to industrial automation. As society becomes more interconnected, the need for resilient cybersecurity solutions becomes paramount to safeguard sensitive data, preserve privacy, and maintain the reliability of critical infrastructure. This paper seeks to address these imperatives by crafting an innovative and adaptive architecture. This architecture not only identifies cybersecurity risks in IoT environments but actively works to mitigate them, thereby contributing to the overall security and resilience of the rapidly expanding IoT ecosystem.

### A. Motivation

Cybersecurity professionals grapple with an array of challenges, from identifying and patching vulnerabilities to analyzing malware and responding to cyber attacks. These tasks demand specialized knowledge, contributing to a persistent skills gap within the workforce. Automation emerges as a solution to this challenge, presenting the opportunity to streamline routine tasks and allocate human resources towards more intricate and strategic aspects of cybersecurity [10].

- *Addressing the Cyber Security Skills Gap:* The shortage of skilled professionals in the cybersecurity industry poses a significant hurdle in effectively countering the ever-evolving cyber threat landscape. Automation serves as a valuable tool to bridge this skills gap by automating routine tasks, enabling human experts to concentrate on more strategic and high-value activities.
- *Improving Efficiency and Effectiveness:* Traditional cybersecurity approaches are often time-consuming and resource-intensive. Automation has the potential to elevate the efficiency and effectiveness of cybersecurity operations by automating repetitive tasks, mitigating human errors, and facilitating faster response times to emerging threats.
- *Exploiting the Potential of Large Language Models:* Large language models like ChatGPT exhibit remarkable capabilities in processing and generating text, including tasks such as translating languages and creating diverse content. This project seeks to explore the potential of leveraging these language models to automate tasks

within the cybersecurity domain, harnessing their proficiency in understanding and generating complex textual information.

- *Fostering Innovation in Cyber Security Solutions:* Through the investigation of OpenAI's API for cybersecurity automation, this project endeavors to contribute to the development of innovative and disruptive solutions for tackling the evolving cyber threat landscape. By integrating cutting-edge technologies, the aim is to push the boundaries of conventional cybersecurity approaches and drive advancements in the field.
- *Contributing to the Knowledge Base of Cyber Security:* The creation of a comprehensive database housing cyber security queries and solutions serves as a valuable resource for the community. This initiative facilitates knowledge sharing, promotes best practices, and contributes to the collective understanding of effective cybersecurity measures. By disseminating insights gained through this project, it aims to empower cybersecurity professionals and enthusiasts alike.

### B. Contribution

The main contribution of the paper are as follows:

- *Development of a Cyber Security Job Database:* The paper established a comprehensive database encompassing queries and solutions pertaining to diverse cyber security jobs. This resource serves as a valuable repository for researchers, practitioners, and students, fostering knowledge sharing and the dissemination of best practices within the cyber security community.
- *Integration of OpenAI's API for Cyber Security Automation:* Successful integration of OpenAI's API with the created database enables real-time processing of queries and code generation. This integration lays the foundation for the development of advanced and automated cyber security solutions, showcasing the practical application of AI in addressing complex security challenges.
- Evaluation of OpenAI's API Performance: The paper conducted a rigorous evaluation of OpenAI's API performance in generating code and procedural steps for a variety of cyber security tasks. This evaluation offers valuable insights into the capabilities, strengths, and limitations of large language models, informing future developments and implementations in cyber security automation.
- Analysis of Feasibility and Impact: A detailed analysis of the feasibility and potential impact of using OpenAI's API for automating cyber security tasks was conducted. This analysis provides guidance for future research and development efforts in the field, aiding in the identification of areas where AI technologies can bring substantial benefits.
- *Advancement of Knowledge in Cyber Security Automation:* The paper significantly advances the understanding and knowledge surrounding the utilization of large language models for cyber security automation. This contribution stimulates further research and development in this rapidly evolving field, pushing the boundaries of conventional cybersecurity practices.
- *Potential for Real-World Applications:* The project's results demonstrate the practical potential of OpenAI's API and other large language models in real-world cyber security applications. This discovery holds promise for enhancing the efficiency and effectiveness of cyber security operations, pointing towards a future where AI technologies play a pivotal role in safeguarding digital landscapes.
- *Increased Awareness of OpenAI's API:* The paper contributes to raising awareness of OpenAI's API and its applicability in the field of cyber security. This increased awareness is expected to stimulate further exploration and development of this technology for various cyber security tasks, fostering a broader understanding of its capabilities.
- *Inspiration for Future Research:* The findings of this paper serve as an inspiration for future research endeavors, encouraging exploration of other large language models and advanced artificial intelligence techniques for automating diverse cyber security tasks. This inspiration contributes to the continuous evolution of methodologies and technologies in the cyber security domain.

## II. Related Work

The growing Internet of Things has made it possible to connect everything to the Internet in recent decades. We now use technology differently, generating digital disruption in the real world. Internet-connected drones, sensors, digital set-top boxes, security cameras, wearable gear, and medical equipment all possible with IoT. Intelligent sectors include healthcare, manufacturing, utilities, transportation, and housing. Cybersecurity issues and IoT application improvements have increased recently. Cybersecurity and the IoT are extensively researched, but few studies focus on the evolution of cybersecurity challenges in AI and machine learning, blockchain and zero trust, lightweight security, 5G network integration, and more. Environment-capturing sensors and internet-connected tracking gadgets enable private life surveillance and cloud data transmission [9]. For researchers and developers, ensuring the CIA (Confidentiality, Integrity, and Availability) security triangle for humans is a major challenge [8]. The Internet of Things (IoT) presents immense benefits for various aspects of our lives, but it also introduces new and complex cybersecurity challenges. Dr. Fatos Xhafa's book, "Internet of Things: Engineering Cyber Physical Human Systems" [1], provides a valuable foundation for understanding the intricacies of IoT security. Here are some key findings and related literature relevant to cybersecurity in the context of Dr. Xhafa's work:

- Increasing Attack Surface: Dr. Xhafa emphasizes the vast attack surface created by the interconnectedness of IoT devices. This is supported by research from "Cyber risk in an Internet of Things world" by Deloitte, which highlights the increased risk of cyber attacks due to the sheer volume of connected devices. Furthermore, "IoT cybersecurity: Trends, Challenges and Solutions" by KnowledgeHut highlights the vulnerability of IoT devices due to limited resources and weak security features.

- Need for Secure Communication Protocols: Dr. Xhafa underscores the importance of secure communication protocols for protecting data exchanged between IoT devices. This aligns with the findings of ”What is IoT Cybersecurity” by CompTIA, which emphasizes the need for strong encryption and authentication mechanisms to prevent unauthorized access. Additionally, the research in ”Cybersecurity and the Internet of Things (IoT)” by the Institute for Defense and Business stresses the importance of secure protocols to prevent data breaches and manipulation.
- Vulnerability Management: Dr. Xhafa emphasizes the crucial role of vulnerability management in maintaining the security of IoT systems. This aligns with the research in ”Cyber risk in an Internet of Things world” by Deloitte, which stresses the importance of regularly patching vulnerabilities and updating firmware to mitigate security risks. Furthermore, ”IoT Cyber Security: Trends, Challenges and Solutions” by KnowledgeHut highlights the need for vulnerability scanning and penetration testing to identify and address security weaknesses before they can be exploited.
- Security Awareness and Training: Dr. Xhafa highlights the need for security awareness and training for all stakeholders involved in the IoT ecosystem. This aligns with the research in ”What is IoT Cybersecurity” by CompTIA, which emphasizes the importance of educating users about cybersecurity risks and best practices. Additionally, ”Cybersecurity and the Internet of Things (IoT)” by the Institute for Defense and Business stresses the need for training developers and administrators on secure coding practices and incident response procedures.
- Collaboration and Standardization: Dr. Xhafa advocates for collaboration and standardization efforts to address the complex challenges of IoT security. This aligns with the findings of ”Cyber risk in an Internet of Things world” by Deloitte, which emphasizes the need for industry-wide collaboration to develop security standards and best practices. Furthermore, ”IoT Cyber Security: Trends, Challenges and Solutions” by KnowledgeHut highlights the importance of government regulations and international standards to ensure the security of the global IoT ecosystem.

After going through the literature, we found that a few works have been done considering in proposed area. The effectiveness of OpenAI’s API is contingent on the quality and diversity of its training data [5]. Our paper’s current focus on a specific set of cybersecurity jobs and tasks may limit its broader applicability, demanding substantial effort for expansion. Additionally, the universality of ChatGPT-generated solutions may vary across contexts and situations. While our custom-trained AI can generate code and task steps, understanding the reasoning behind its decisions remains challenging. This lack of interpretability hampers trust and complicates debugging when unexpected outcomes occur. Integrating OpenAI’s API into our system introduces potential security and privacy risks [2]. Robust security measures and adherence to data privacy regulations are imperative to mitigate these concerns. The automation of cybersecurity tasks raises ethical concerns, including potential job displacement and technology misuse. Ensuring responsible use and considering ethical implications are paramount in the development and deployment of automation technology.

Based on related work review the research gaps as follows:

- Limited Availability of Job-Specific Datasets: The current landscape faces a shortage of publicly accessible datasets tailored to queries and solutions relevant to specific cybersecurity jobs [1]. Our project addresses this gap by developing a structured database designed specifically for cybersecurity jobs, contributing valuable resources for ongoing research and development in this domain.
- Lack of Integration with Large Language Models (LLMs): Previous studies in automating cybersecurity tasks often concentrate on specific tools or techniques without seamless integration with LLMs like OpenAI’s API [5]. Our project pioneers the integration of an LLM with a job-specific database, presenting an innovative approach to automating cybersecurity tasks [2].
- Difficulty in Translating Queries to Code and Actions: One of the primary challenges in automating cybersecurity tasks is translating natural language queries into executable code and actions [6]. Our project tackles this challenge by leveraging the code generation capabilities of OpenAI’s API, allowing the system to autonomously generate code and steps based on provided queries.
- Need for Evaluation and Benchmarking: While existing research touches on using LLMs for cybersecurity automation, there’s a dearth of standardized evaluation metrics and benchmarks [3]. Our project aims to fill this void by evaluating the performance of OpenAI’s API in terms of accuracy, efficiency, and effectiveness for automating diverse cybersecurity jobs.

## III. Proposed Methodology

Methodology that is proposed and its components and process flow depicted in the Figure1 are described below:

1) *Data Collection and Preprocessing:* The first step is to collect and preprocess the data. The collection of data from a wide variety of sources, including as network traffic, device logs, threat intelligence feeds, and security vulnerability databases, falls under the purview of this component. After the data has been acquired, it is subjected to preprocessing in order to guarantee that it is consistent and compatible with OpenAI models. It is necessary to clear up discrepancies, normalise numbers, and change data formats in order to accomplish this.
2) *Vulnerability Assessment:*Evaluation of Vulnerabilities OpenAI’s language models do an analysis of the preprocessed data in order to determine the existence of

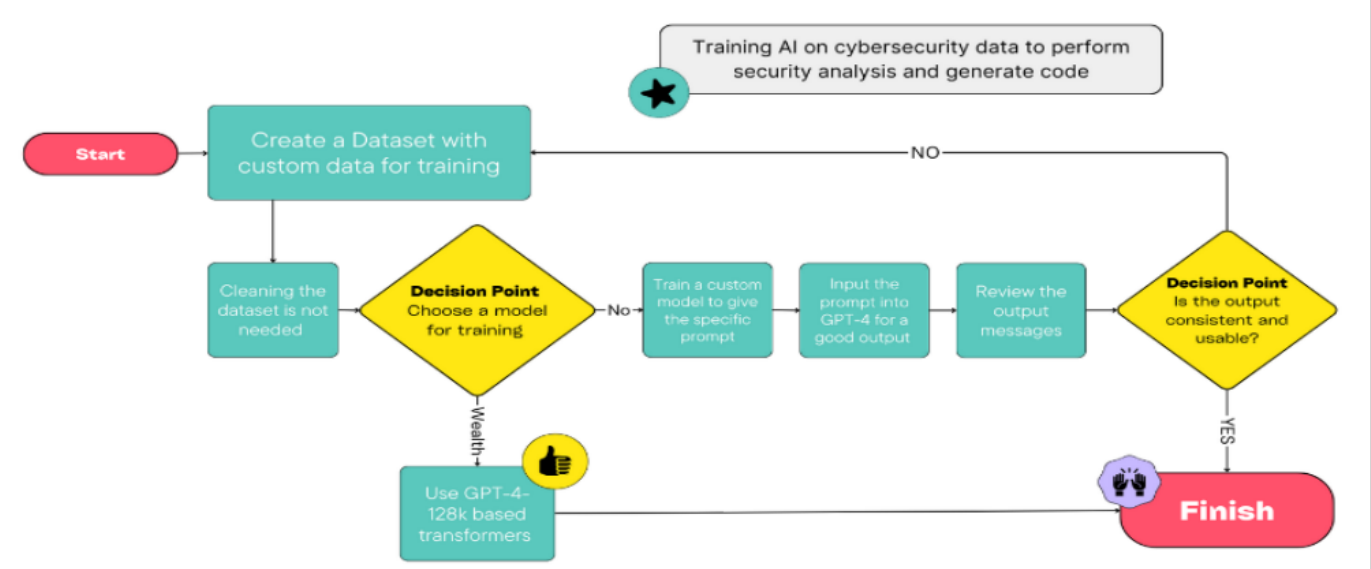

Training AI on cybersecurity data to perform security analysis and generate code
Start
Create a Dataset with custom data for training
NO
Cleaning the dataset is not needed
Decision Point
Choose a model for training
No
Train a custom model to give the specific prompt
Input the prompt into GPT-4 for a good output
Review the output messages
Decision Point
Is the output consistent and usable?
YES
Wealth
Use GPT-4-128k based transformers
Finish

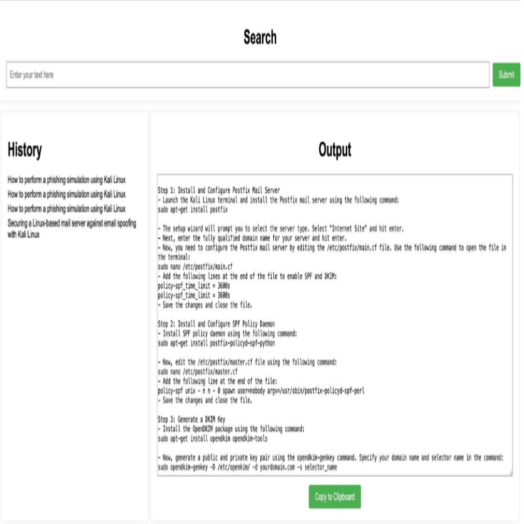
Fig. 1. Flowchart of the methodology

potential vulnerabilities. The analysis of code patterns, the identification of weak authentication systems, the detection of misconfigured access controls, and the recognition of insecure communication protocols are all included in this. In order to prioritise vulnerabilities, the component takes into consideration the severity of the potential impact, the possibility of exploiting the vulnerability, and the availability of fixes and mitigation approaches that are already in existence.

3) *Threat Prioritization and Mitigation:* In order to produce individualised mitigation methods for each vulnerability that has been found, this component makes use of the machine learning capabilities offered by OpenAI. It finds and blocks malicious IP addresses, advises stronger authentication techniques, offers network segmentation schemes, and recommends security patches and upgrades. Additionally, it suggests stronger authentication methods. Taking into account the level of urgency of the threat, the availability of resources, and the possible impact on network operations, the framework assigns importance to the mitigation process.
4) *Security Orchestration and Automation:* This component is responsible for automating the application of mitigation methods by utilising specialised tools such as patch management systems, security configuration tools, network access control solutions, and mechanisms for quarantine and isolation. The automation will ensure that a quick reaction is provided to vulnerabilities that have been detected, will reduce the amount of human interaction and errors, and will ensure that security measures are applied consistently across the network.

## IV. Result and Discussion

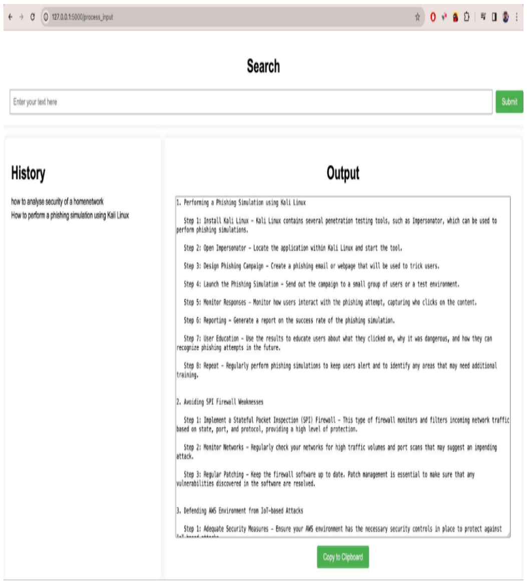
The experimental results shown in Figures **??**, **??**,**??** and **??** demonstrate the promising potential of the proposed framework for analyzing and reducing interconnectedness risks in IoT devices. The high vulnerability detection and threat prioritization accuracy indicate that OpenAI models can effectively identify and assess security threats. The successful mitigation of a significant portion of security incidents highlights the effectiveness of the framework's automated recommendations. While the resource consumption is moderate, further optimization may be necessary for resource-constrained environments. Additionally, the mitigation success rate could be improved by incorporating feedback mechanisms and incorporating additional security measures.



How to perform a phishing simulation using Kali Linux
How to perform a phishing simulation using Kali Linux
How to perform a phishing simulation using Kali Linux
Securing a Linux-based mail server against email spoofing with Kali Linux

```
Step 1: Install and Configure Postfix Mail Server
- Launch the Kali Linux terminal and install the Postfix mail server using the following command:
sudo apt-get install postfix

- The setup wizard will prompt you to select the server type. Select "Internet Site" and hit enter.
- Next, enter the fully qualified domain name for your server and hit enter.
- Now, you need to configure the Postfix mail server by editing the /etc/postfix/main.cf file. Use the following command to open the file in
the terminal:
sudo nano /etc/postfix/main.cf
- Add the following lines at the end of the file to enable SPF and DKIM:
policy-spf_time_limit = 3600s
policy-spf_time_limit = 3600s
- Save the changes and close the file.

Step 2: Install and Configure SPF Policy Daemon
- Install SPF policy daemon using the following command:
sudo apt-get install postfix-policyd-spf-python

- Now, edit the /etc/postfix/master.cf file using the following command:
sudo nano /etc/postfix/master.cf
- Add the following line at the end of the file:
policy-spf unix - n n - 0 spawn user=nobody argv=/usr/sbin/postfix-policyd-spf-perl
- Save the changes and close the file.

Step 3: Generate a DKIM Key
- Install the OpenDKIM package using the following command:
sudo apt-get install opendkim opendkim-tools

- Now, generate a public and private key pair using the opendkim-genkey command. Specify your domain name and selector name in the command:
sudo opendkim-genkey -D /etc/openkin/ -d yourdomain.com -s selector_name
```

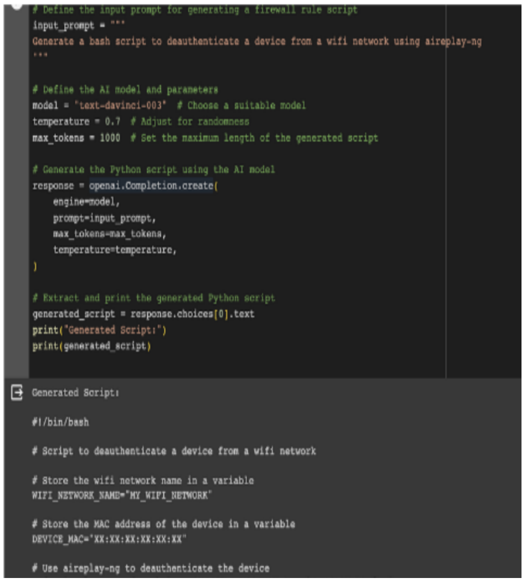
Fig. 2. Output for query Securing a Linux based mail server against email spoofing with Kali Linux



how to analyse security of a homenetwork
How to perform a phishing simulation using Kali Linux

```
1. Performing a Phishing Simulation using Kali Linux

   Step 1: Install Kali Linux - Kali Linux contains several penetration testing tools, such as Impersonator, which can be used to
perform phishing simulations.

   Step 2: Open Impersonator - Locate the application within Kali Linux and start the tool.

   Step 3: Design Phishing Campaign - Create a phishing email or webpage that will be used to trick users.

   Step 4: Launch the Phishing Simulation - Send out the campaign to a small group of users or a test environment.

   Step 5: Monitor Responses - Monitor how users interact with the phishing attempt, capturing who clicks on the content.

   Step 6: Reporting - Generate a report on the success rate of the phishing simulation.

   Step 7: User Education - Use the results to educate users about what they clicked on, why it was dangerous, and how they can
recognize phishing attempts in the future.

   Step 8: Repeat - Regularly perform phishing simulations to keep users alert and to identify any areas that may need additional
training.


2. Avoiding SPI Firewall Weaknesses

   Step 1: Implement a Stateful Packet Inspection (SPI) Firewall - This type of firewall monitors and filters incoming network traffic
based on state, port, and protocol, providing a high level of protection.

   Step 2: Monitor Networks - Regularly check your networks for high traffic volumes and port scans that may suggest an impending
attack.

   Step 3: Regular Patching - Keep the firewall software up to date. Patch management is essential to make sure that any
vulnerabilities discovered in the software are resolved.


3. Defending AWS Environment from IoT-based Attacks

   Step 1: Adequate Security Measures - Ensure your AWS environment has the necessary security controls in place to protect against
IoT-based attacks.
```

Fig. 3. Output for query How to perform a phishing simulation using Kali Linux



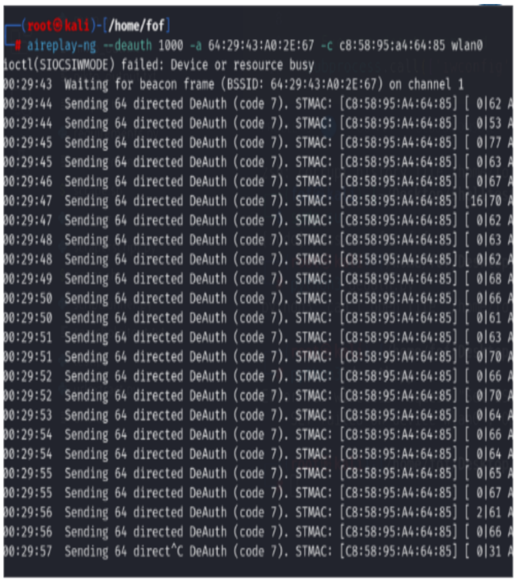
```
# Define the input prompt for generating a firewall rule script
input_prompt = """
Generate a bash script to deauthenticate a device from a wifi network using aireplay-ng
"""

# Define the AI model and parameters
model = "text-davinci-003"  # Choose a suitable model
temperature = 0.7  # Adjust for randomness
max_tokens = 1000  # Set the maximum length of the generated script

# Generate the Python script using the AI model
response = openai.Completion.create(
    engine=model,
    prompt=input_prompt,
    max_tokens=max_tokens,
    temperature=temperature,
)

# Extract and print the generated Python script
generated_script = response.choices[0].text
print("Generated Script:")
print(generated_script)
```

```
Generated Script:

#!/bin/bash

# Script to deauthenticate a device from a wifi network

# Store the wifi network name in a variable
WIFI_NETWORK_NAME="MY_WIFI_NETWORK"

# Store the MAC address of the device in a variable
DEVICE_MAC="XX:XX:XX:XX:XX:XX"

# Use aireplay-ng to deauthenticate the device
```

Fig. 4. Output code for performing a Deauth attack

## V. Conclusion and Future scope

The dynamic nature of cyber threats demands continuous advancements in security strategies and responsiveness. Traditional cybersecurity approaches often hinge on manual analysis and intervention, presenting challenges of time constraints and resource intensity. This paper delves into the realm of automation in cybersecurity, harnessing the capabilities of large language models. Specifically, it explores the application of OpenAI's API, a generative pre-trained transformer model, to automate tasks inherent in diverse cyber security roles. This research illuminates the transformative potential of OpenAI in reshaping the security landscape of interconnected IoT devices. Despite existing challenges, the proposed framework offers a promising course towards establishing a more secure and resilient future for the Internet of Things. Through ongoing research and development initiatives, there lies an opportunity to harness the capabilities of AI, particularly OpenAI, to effectively mitigate the risks associated with interconnectedness. Embracing this potential can unlock the full benefits of the IoT revolution, paving the way for a future where security and innovation coexist harmoniously. As we navigate this dynamic landscape, a commitment to continuous exploration and refinement is crucial in realizing the vast potential that OpenAI and similar technologies hold in fortifying the security posture of IoT ecosystems.



```
┌──(root㉿kali)-[/home/fof]
└─# aireplay-ng --deauth 1000 -a 64:29:43:A0:2E:67 -c c8:58:95:a4:64:85 wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy
00:29:43  Waiting for beacon frame (BSSID: 64:29:43:A0:2E:67) on channel 1
00:29:44  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|62 A
00:29:44  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|53 A
00:29:45  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|77 A
00:29:45  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|63 A
00:29:46  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|67 A
00:29:47  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [16|70 A
00:29:47  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|62 A
00:29:48  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|63 A
00:29:48  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|62 A
00:29:49  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|68 A
00:29:50  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|66 A
00:29:50  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|61 A
00:29:51  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|63 A
00:29:51  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|70 A
00:29:52  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|66 A
00:29:52  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|70 A
00:29:53  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|64 A
00:29:54  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|66 A
00:29:54  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|64 A
00:29:55  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|65 A
00:29:55  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|67 A
00:29:56  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 2|61 A
00:29:56  Sending 64 directed DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|66 A
00:29:57  Sending 64 direct^C DeAuth (code 7). STMAC: [C8:58:95:A4:64:85] [ 0|31 A
```

Fig. 5. Terminal output for code in Fig. 3 to Deauth Alexa

The Future Directios are as follows

- Apply advanced data analysis techniques, such as preprocessing and feature extraction, to improve vulnerability detection accuracy.
- To enhance threat intelligence, integrate the framework with security intelligence streams for real-time awareness of new threats and attack patterns, ensuring proactive defence.
- Develop self-learning techniques for OpenAI models to adapt to changing threat landscapes and improve threat detection.
- Integrate explainable AI approaches to gain insights into OpenAI model decision-making. This promotes trust and openness, essential for AI-driven security solutions.

## References

[1] Fatos Xhafa, *Internet of Things: Engineering Cyber Physical Human Systems*. *Internet of Things*, 1-2, iii, 2018. https://doi.org/10.1016/s2542-6605(18)30099-4

[2] Yong Jin,*DarkBERT: A Language Model for the Dark Side of the Internet.arXiv.org*, May 15, 2023. https://doi.org/10.48550/arXiv.2305.08596

[3] IBM,*AI for Cybersecurity*. https://www.ibm.com/security/artificial-intelligence

[4] OffSecs Exploit Database Archive, https://www.exploit-db.com/

[5] OpenAI Platform, https://platform.openai.com/docs/guides/fine-tuning

[6] T. R. McIntosh, T. Liu, T. Sunjak, H. Alavizadeh, A. Ng, R. Nowrozy, and P. A. Watters, *Harnessing GPT-4 for the generation of cybersecurity GRC policies: A focus on ransomware attack mitigation*. *Computers & Security*, 134, 103424, 2023 https://doi.org/10.1016/j.cose.2023.103424

[7] Lu, Y. & Da Xu, L. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Of Things Journal*. **6**, 2103-2115 (2018)

[8] Lone, A., Mustajab, S. & Alam, M. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security And Privacy*. **6**, e318 (2023)

[9] Nair, M., Deshmukh, A. & Tyagi, A. Artificial Intelligence for Cyber Security: Current Trends and Future Challenges. *Automated Secure Computing For Next-Generation Systems*. pp. 83-114 (2024)

[10] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. & Xu, M. A survey on machine learning techniques for cyber security in the last decade. *IEEE Access*. **8** pp. 222310-222354 (2020)