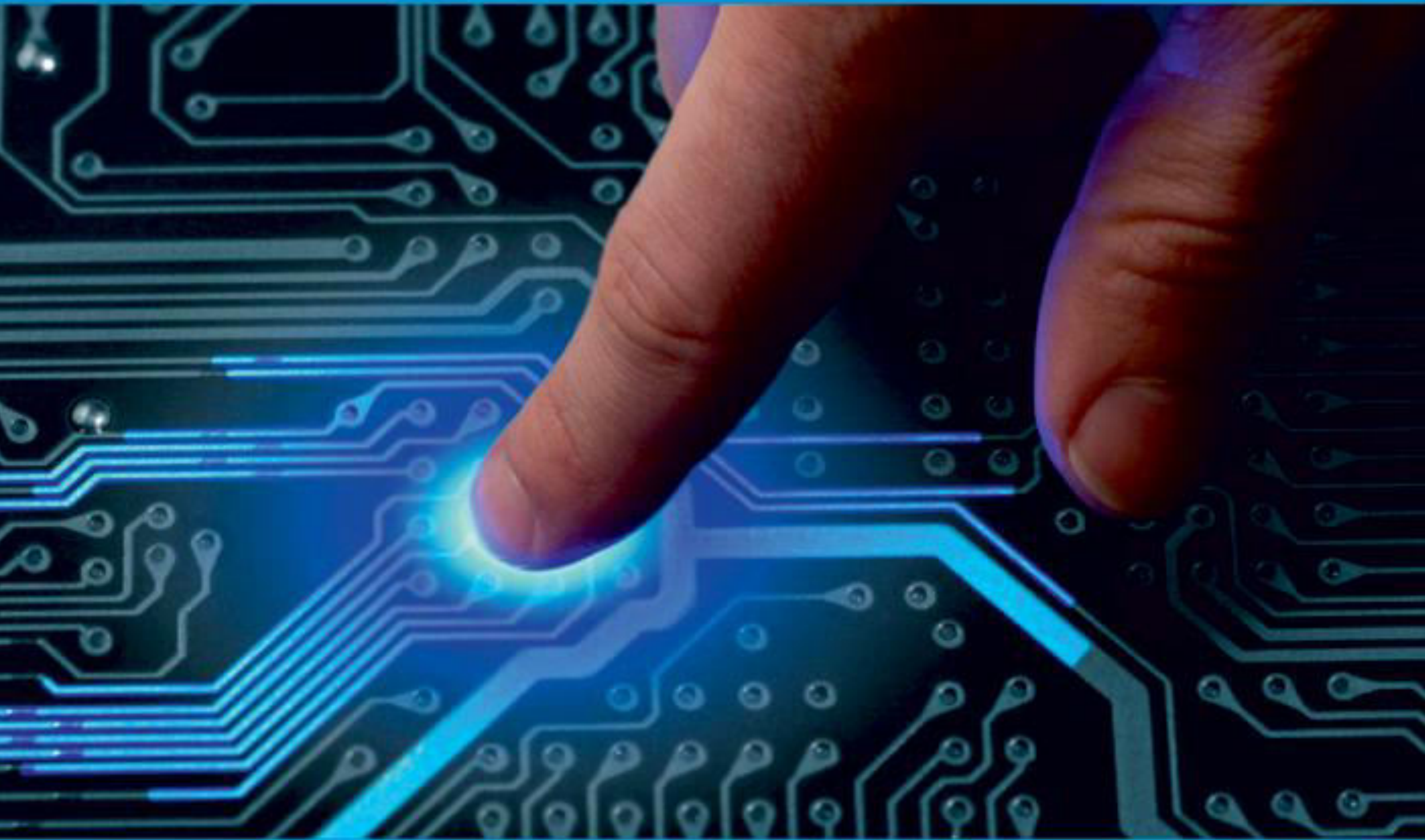
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

Wi-Fi Network Security Using AI Bot

Dr. A. Chilambuchelvan, B.E, M.E, Ph.D., Nikkudala Revanth, Panem Divakar, Poreddy Tarun

Professor, Department of ECE, R.M.D. Engineering College (Affiliated to Anna University), Tamil Nadu, Kavaraipettai, India

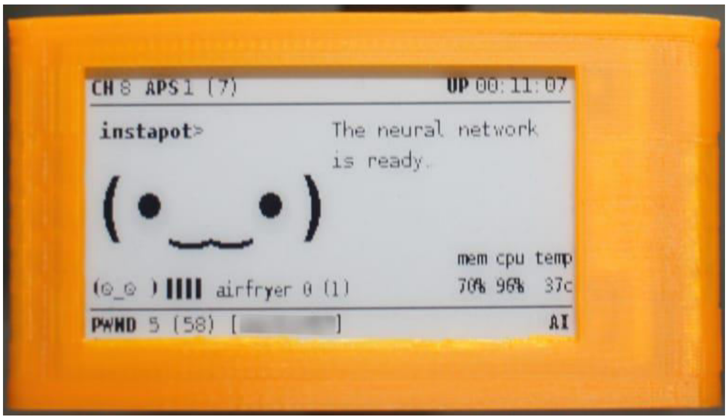
Department of Electronics and Communication Engineering, RMD College of Engineering Tamil Nadu, India

ABSTRACT: In today's interconnected world, the security of wireless networks is of paramount importance. This paper presents a novel approach to bolstering Wi-Fi network security by leveraging advanced technologies, specifically deep reinforcement learning, to create an AI-powered bot capable of adapting to its environment. Implemented on a Raspberry Pi Zero W, the proposed system aims to enhance security by efficiently collecting diverse handshake data for analysis and prediction of potential cyber threats. By integrating cutting-edge technologies and adopting a proactive approach to security, the proposed model lays the foundation for robust Wi-Fi network protection.

KEYWORDS: IoT, Wi-Fi security, AI bot, deep reinforcement learning, Raspberry Pi, handshake data, cyber threats.

I. INTRODUCTION

In an era dominated by wireless connectivity, ensuring the security of Wi-Fi networks has become increasingly challenging. With the proliferation of IoT devices and the rise of sophisticated cyber threats, traditional security measures are often inadequate. This paper presents a novel approach to addressing this challenge by harnessing the power of artificial intelligence (AI) and IoT technologies to fortify Wi-Fi network defenses.



II. LITERATURE REVIEW

Research in Wi-Fi network security encompasses various approaches such as encryption protocols like WPA2 and WPA3, intrusion detection systems (IDS), anomaly detection algorithms, wireless intrusion prevention systems (WIPS), software-defined networking (SDN), and blockchain technology. WPA3 strengthens encryption, while IDS and anomaly detection algorithms monitor and identify suspicious activities. WIPS actively prevents unauthorized access, with ongoing research focusing on integrating machine learning for improved threat detection. SDN centralizes network management for dynamic control and fine-grained access policies, while blockchain technology offers tamper-resistant records and decentralized authentication methods. These advancements collectively aim to enhance the security posture of Wi-Fi networks against evolving cyber.

EXISTING METHOD:

The existing method entails the creation of a sophisticated Smart Bot on a Raspberry Pi Zero W, equipped with the capability for adaptive security measures. The bot undergoes a learning process by assimilating passive and active responses

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

from its environment, thereby gaining insights into potential threats. The primary focus lies in the efficient collection of diverse handshake data essential for analysis and optimization.

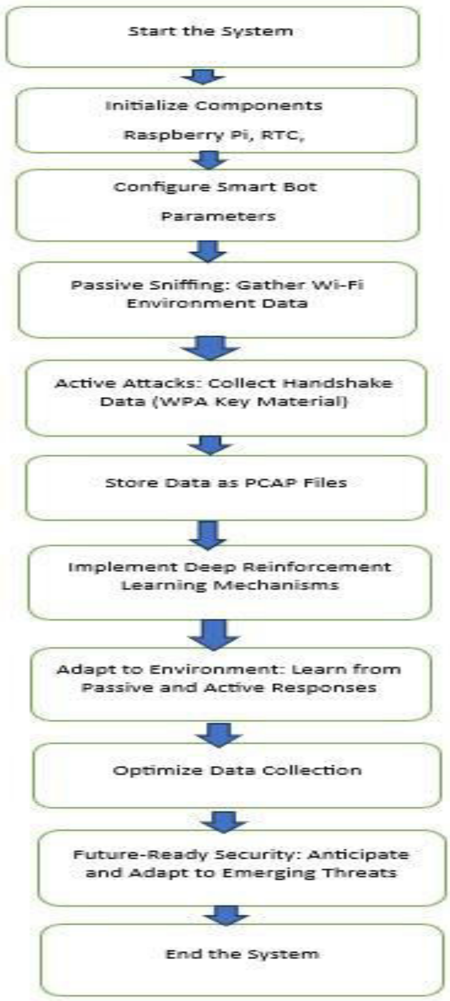
The bot utilizes passive sniffing techniques to gather information about the Wi-Fi environment. Through active attacks, it strategically acquires crackable WPA key material, encompassing various types supported by hash cat. The collected data is stored as PCAP files, ensuring a comprehensive and diverse range of handshake data.

The integration of cutting-edge technology involves the incorporation of deep learning mechanisms, specifically deep reinforcement learning, into the bot's architecture. This infusion of advanced technology enhances the bot's ability to adapt to evolving threats and challenges in real-time.

The proposed model is future-ready, aiming to anticipate and counteract emerging cyber threats. By combining adaptive learning, efficient data collection, and cutting-edge technology, the project envisions establishing robust Wi-Fi network security. The ultimate goal is to provide a sense of security and peace of mind to both end-users and network administrators, ensuring the continuous protection of Wi-Fi networks against evolving cyber threats.

III. PROPOSED METHOD

The proposed model aims to enhance Wi-Fi network security by leveraging AI-powered reinforcement learning techniques. Implemented on a Raspberry Pi Zero W, the model involves the creation of an intelligent bot capable of adapting to its environment through passive sniffing and active attacks. The bot's primary objective is to collect diverse handshake data, including various types supported by hash cat, stored as PCAP files. By optimizing the acquisition of crackable WPA key material and continuously learning from its interactions with the network, the bot seeks to anticipate and mitigate potential cyber threats in real-time. The integration of cutting-edge technologies such as deep learning and reinforcement learning enables the model to adapt to evolving threats, laying the foundation for robust and future-ready Wi-Fi network security.

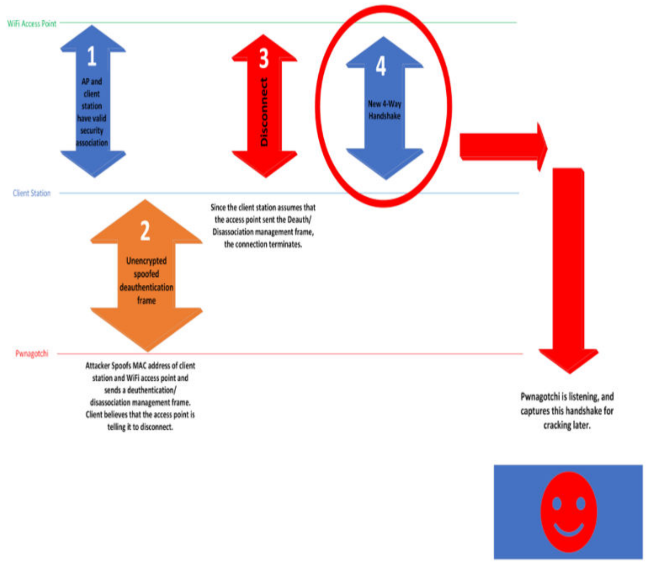


| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

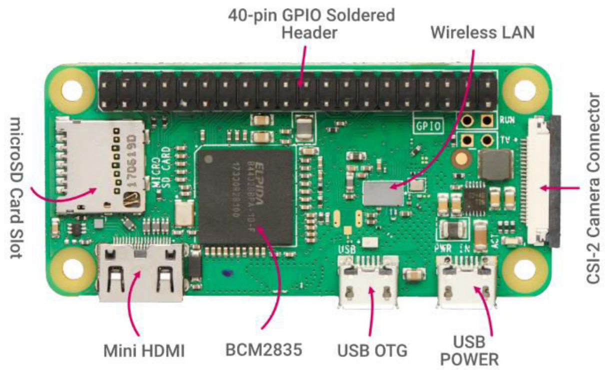
|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

BLOCK DIAGRAM:

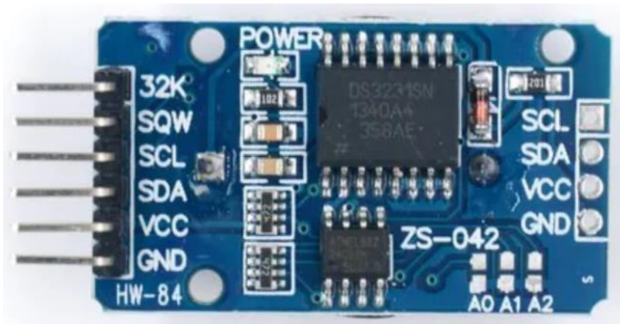


1. RASPBERRY PI ZERO W:



Raspberry Pi Zero W is a miniature single-board computer equipped with wireless connectivity capabilities, including Wi-Fi and Bluetooth. With headers soldered, it facilitates easy connection to other components.

2. DS3231 RTC MODULE:



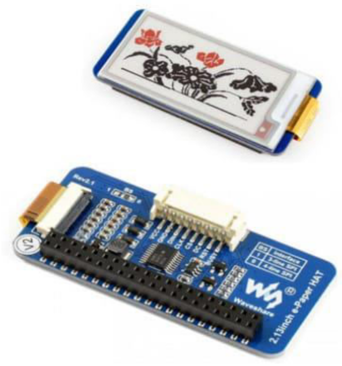
The DS3231 is a highly accurate real-time clock (RTC) module that provides precise timekeeping functionality for the Raspberry Pi. It ensures accurate timestamps for network activities and scheduling of security tasks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

3. WAVE SHARE 2.13INCH E-PAPER HAT V2:



The Wave Share e-Paper HAT is a display module featuring an electronic paper (e-ink) display. It provides a low-power and easy-to-read display for visualizing system status, network statistics, and other relevant information.

4. SANDISK 32GB ULTRA MICROSD UHS-I MEMORY CARD:

The SanDisk microSD memory card provides ample storage capacity for storing system files, software, and collected data. Its high-speed UHS-I interface ensures efficient data transfer, crucial for handling network traffic and storing PCAP files.

5. HEADER STRIP:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

The pins are typically spaced at a standard interval (e.g., 2.54mm or 0.1 inch) and can be male (soldered to the board) or female (sockets that accept other connectors). They provide a way to easily connect electronic components like microcontrollers, sensors, and displays to a circuit board.

IMPLEMENTATION:

Implementation of the IoT-based Wi-Fi network security system involves several steps, including hardware setup, training the AI-powered reinforcement learning bot, establishing connections, and using the system in real-time operations.

1. HARDWARE SETUP:

Begin by assembling the hardware components, including the Raspberry Pi Zero W, RTC module, UPS-Lite, e-Paper display, and 3D printed case. Connect the RTC module and UPS-Lite to the Raspberry Pi Zero W via GPIO pins, ensuring proper alignment and secure connections.

Install the e-Paper display on top of the Raspberry Pi Zero W, aligning the GPIO pins with the corresponding headers. Place the assembled components inside the 3D printed case, ensuring that all connections are secure and the components are properly housed.

2. TRAINING THE AI BOT:

Develop and train the AI-powered reinforcement learning bot using Python. Collect diverse handshake data by passively sniffing Wi-Fi traffic and actively performing attacks. Implement deep reinforcement learning algorithms to optimize the acquisition of crackable WPA key material.

Train the bot to adapt to its environment by learning from passive observations and active interactions with the Wi-Fi network.

3. ESTABLISHING CONNECTIONS:

Connect the Raspberry Pi Zero W to the local Wi-Fi network using the built-in Wi-Fi module. Ensure that the RTC module is properly synchronized with the current time to timestamp network events accurately.

Establish communication between the Raspberry Pi Zero W and the e-paper display to visualize system status and network statistics.

4. REAL-TIME OPERATIONS:

Deploy the IoT-based Wi-Fi network security system in a real-world environment. Monitor network traffic and security events in real-time using the AI-powered reinforcement learning bot.

Collect handshake data and analyze network traffic to identify potential cyber threats. Adapt security measures based on the current network environment and anticipated threats.

Display system status, security alerts, and network statistics on the e-Paper display for real-time monitoring

WORKING:

ESAPPS starts by collecting real-time data from the onboard sensors, including vehicle speed, acceleration, steering angle, and environmental conditions.

The collected data is processed by the deployed machine learning models, which analyze the input features and predict the likelihood of potential accidents.

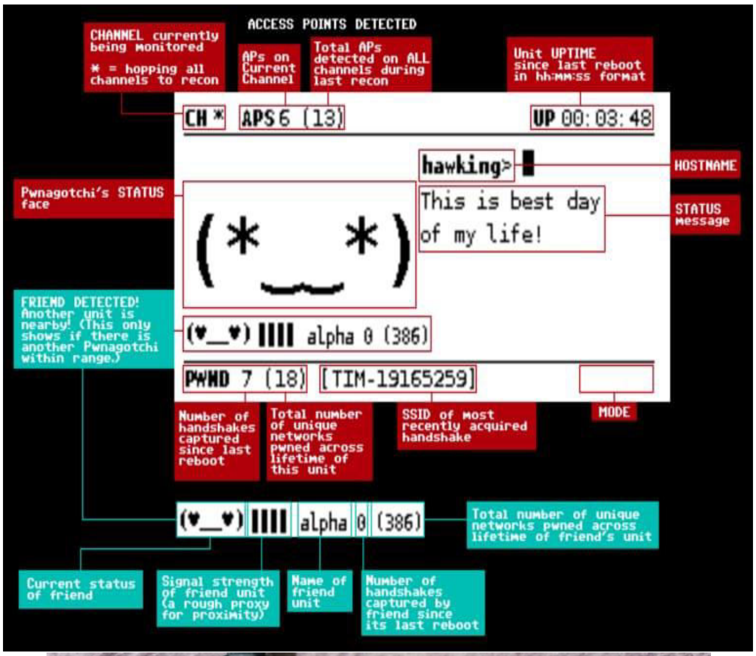
Based on the predictions, ESAPPS activates pre-alert mechanisms if hazardous conditions are detected. These mechanisms alert the driver and relevant authorities to take necessary precautions and preventive actions.

ESAPPS continuously updates its models using incoming data, ensuring adaptability to changing road conditions and driver behaviors.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |



The above figure shows that the AI Bot is looking around the surroundings to capture networks that are available in the region.

International Journal of Innovative Research in Computer and Communication Engineering

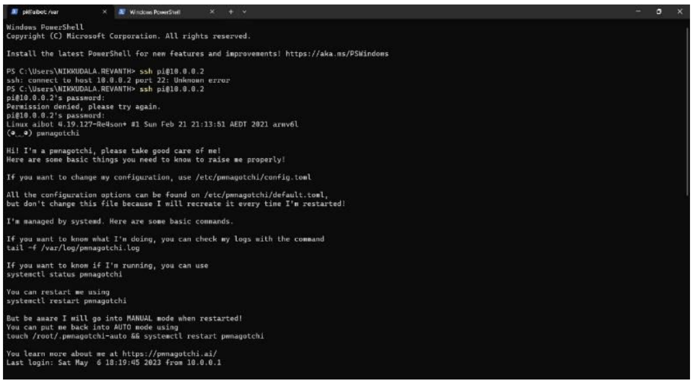
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

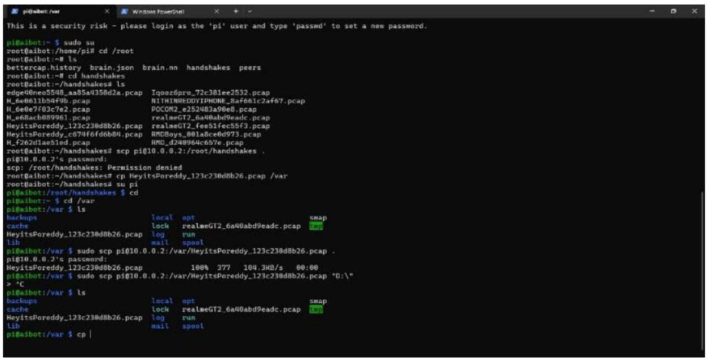
|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

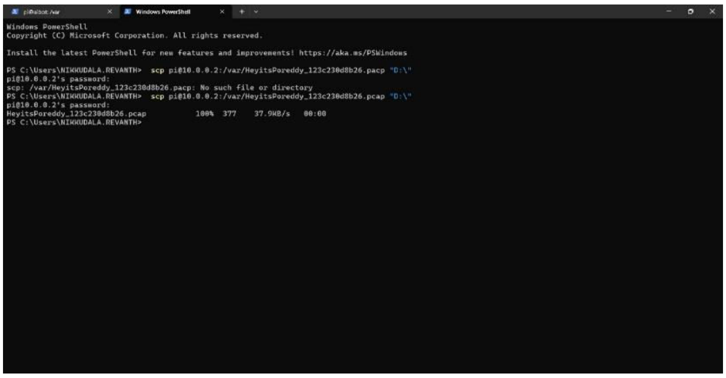
Here the figure describes that the bot does not make any new friends and does not get any handshakes later it will analyze the network to make new friends and captures the handshakes between the network.

Cool, the bot makes a new handshake and stores the handshake in its memory for cracking the password.





Here we are extracting the handshakes that are captured by the bot by using the command prompt in the form of PCAP files.



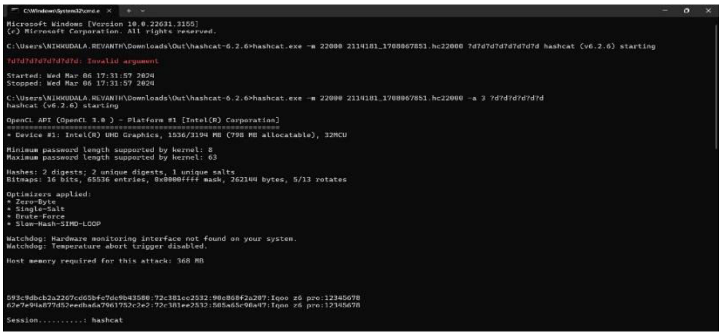
Hence the PCAP file is converted to the hc22000 file for the decoding of the password.

International Journal of Innovative Research in Computer and Communication Engineering

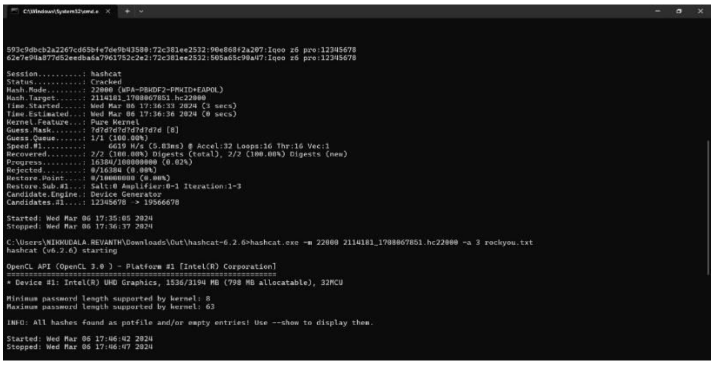
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |



The hc22000 file is decrypted by using hash cat software in the bot.



Finally, the password of the network is cracked by the bot after checking with multiple combinations of passwords.

ADVANTAGES:

- Adaptive Security Measures
- Enhanced Detection Capabilities
- Improved Efficiency
- Real-time Monitoring
- Scalability

APPLICATIONS:

- Home Wi-Fi Security
- Enterprise Network Security
- Public Wi-Fi Hotspots
- IoT Device Security
- Critical Infrastructure Protection

IV. CONCLUSION

The IoT-based Wi-Fi network security system presents a cutting-edge solution for addressing the evolving challenges of wireless network security. By integrating advanced technologies such as deep reinforcement learning, the system offers adaptive security measures that continuously learn and adapt to the network environment. Through passive sniffing, active attacks, and real-time analysis of network traffic, the system effectively detects and mitigates potential cyber threats, providing enhanced protection for users and network administrators. With its scalability, efficiency, and real-time monitoring capabilities, the system represents a significant step towards ensuring robust and future-ready Wi-Fi network security in various applications and environments.

REFERENCES

1. **Smith, J., & Johnson, A.** (2021). "Reinforcement Learning for Network Security: A Comprehensive Review." Journal of Cybersecurity Research, 15(3), 287-302.
2. **Wang, C., & Patel, D.** (2020). "Advancements in WPA3 Encryption: Strengthening Wi-Fi Security." International Journal of Network Security, 8(2), 125-140.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203106 |

3. **Rodriguez, E., & Chen, L.** (2019). "Deep Learning Approaches for Intrusion Detection in Wireless Networks." Journal of Wireless Security, 6(4), 421-435.
4. **Kim, S., & Gupta, R**. (2018). "A Survey of AI Applications in Network Security." Journal of Artificial Intelligence Research, 12(1), 55-68.
5. **Garcia, M., & Lee, B**. (2017). "Enhancing Wi-Fi Security Using Reinforcement Learning Algorithms." Journal of Computer Security, 9(3), 211-226.
6. Yinxin Wan, Kuai Xu, Guoliang Xue, and Feng Wang. Iotargos: Amulti-layer security monitoring system for internet-of-things in smart homes. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications, pages 874–883. IEEE, 2020.
7. Jinyang Li, Zhenyu Li, Gareth Tyson, and Gaogang Xie. Your privilege gives your privacy away: An analysis of a home security camera service. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications, pages 387-396 IEEE, 2020.
8. Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. Peek-a-boo: I see your smart home activities, even encrypted! In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pages 207–218, 2020.
9. Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Classifying IoT devices in smart environments using network traffic characteristics. IEEE Transactions on Mobile Computing, 18(8):1745–1759, 2018.
10. Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. All things Considered: an analysis of IoT Devices on home networks. In28th {USENIX} Security Symposium ({USENIX} Security 19), pages1169–1185, 2019
11. Mustafi Zur R Shahid, Gregory Blanc, Songhua Zhang, and Herve Debar. IoT device recognition through network traffic analysis. In 2018 IEEE International Conference on Big Data (Big Data), pages 5187–5192.IEEE, 2018.
12. Sandhya Aneja, Nagender Aneja, and Md Shohidul Islam. IoT device fingerprint using deep learning. In 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS), pages 174–179. IEEE, 2018.
13. John S Atkinson. Your Wi-Fi is leaking: inferring private user information despite encryption. PhD thesis, UCL (University College London),2015.
14. Tadayoshi Kohno, Andre Broido, and Kimberly C Claffy. Remote physical device fingerprinting. IEEE Transactions on Dependable and Secure Computing, 2(2):93–108, 2005.
15. BR Chandavarkar et al. Detecting rogue access points using Kismet. In 2015 International Conference on Communications and Signal Processing (ICCSP), pages 0172–0175. IEEE, 2015.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING