**Ministry of Education and Science of Republic of Kazakhstan**

****

**Department of Cybersecurity**

**Diploma thesis**

**Title:**

« Developing a cybersecurity strategy for Wi-Fi networks: vulnerability analysis and threat defense»

Team member: Mukhtarov Daniyal (30282)  
Mudegeev Rauan (30286)  
Zhanibek Temirlan (30289)

**Almaty 2025**

**MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN**

**INTERNATIONAL INFORMATION TECHNOLOGY UNIVERSITY**

**DEPARTMENT OF CYBERSECURITY**

**Approved**Head of Department   
Cand. tech. sc, assoc, professor  
 S.T. Amanzholova  
 **«\_\_\_» \_\_\_\_\_\_\_\_\_\_2025**

**DIPLOMA PROJECT**

Developing a cybersecurity strategy for Wi-Fi networks: vulnerability analysis and threat defense

**Educational program 6B06303 – Network Security**Done by:

Mukhtarov D. «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Mudegeev R. «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Zhanibek T. «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Research advisor:

«\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Reviewer:

«\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

International Information Technology University

Faculty of Computer Technology and Cybersecurity

Department of Cybersecurity   
Educational program 6B06303 – Network Security

Diploma Project

StudentsMukhtarov Daniyal  
Mudegeev Rauan  
Zhanibek Temirlan

Diploma project topic

Developing a cybersecurity strategy for Wi-Fi networks: vulnerability analysis and threat defense

Approved by IITU order №\_\_\_ dated «\_\_»\_\_\_\_2025

Diploma project submission date «\_\_»\_\_\_\_2025

Diploma project initial data

Details of computations and explanations (list of issues due to be addressed)

CD containing the digital version of diploma project and attachments

1. The source code and explanatory note;

2. Project presentation;

3. Electronic version of diploma project.

Consultations on Diploma Project (with related Project Chapters named)

|  |  |  |  |
| --- | --- | --- | --- |
| Consultant | Name | Signature, date | |
| Assignment given | Assignment received |
| Consultant on Economic effectiveness of the project |  |  |  |
| English language consultant |  |  |  |
| Compliance monitor |  |  |  |

Date «\_\_» \_\_\_\_\_\_\_\_2025

Research advisor  
 «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Assignment received by

Mukhtarov D. «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Mudegeev R. «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Zhanibek T. «\_\_\_» \_\_\_\_\_2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature)

Diploma Project Writing Schedule

Mukhtarov Daniyal , Mudegeev Rauan , Zhanibek Temirlan

Title: Developing a cybersecurity strategy for Wi-Fi networks: vulnerability analysis and threat defense

|  |  |  |
| --- | --- | --- |
| № | Assignment | Submission date |
| 1 | Creation of the graduation project writing schedule | October |
| 2 | Collection, study, processing, analyzing, and generalizing data | Novemberr |
| 3 | Drafting and submission to the Research advisor (Introduction, Chapter 1, Chapter 2, Chapter 3, Chapter 4, Conclusion) | January – February |
| 4 | Pre-defence | February |
| 5 | Submission of the chapter «Economic effectiveness of the project» to the consultant | February - March |
| 6 | Revision of the graduation project with due consideration of the advisor’s comments | March – April |
| 7 | Submission of the completed diploma project to the Research advisor | April |
| 8 | Submission of the completed diploma project to the English language consultant | April |
| 9 | Submission of the diploma project to the compliance monitor | April –May |
| 10 | Submission of the diploma project for the plagiarism check-up | May |
| 11 | Submission to the reviewer for approval | May |
| 12 | Diploma project defense | June |

**Аннотация**

В современном мире, где беспроводные сети становятся основой цифровой инфраструктуры, защита Wi-Fi сетей приобретает критическую важность для частных и корпоративных пользователей. Настоящий проект посвящен разработке комплексной стратегии кибербезопасности для Wi-Fi сетей, включающей анализ существующих уязвимостей и методов защиты от разнообразных угроз.

Основной задачей исследования является выявление и описание наиболее распространенных угроз для Wi-Fi сетей, таких как атаки типа «человек посередине» (MITM), создание поддельных точек доступа, атаки на пароли и эксплуатация слабых мест в протоколах шифрования. Проект анализирует недостатки стандартных протоколов безопасности, таких как WEP и WPA2, и подчеркивает преимущества современного стандарта WPA3, который значительно повышает защиту сетей от атак на повторную установку ключей и других сложных угроз.

Для реализации защиты предложен комплексный подход, включающий многофакторную аутентификацию, сегментацию сети с помощью виртуальных локальных сетей (VLAN) и использование VPN для защиты данных в корпоративных и общественных сетях. Также рассматривается использование систем обнаружения и предотвращения вторжений (IDS/IPS), шифрования трафика и фильтрации MAC-адресов. Дополнительно внедряются методы анализа аномалий и поведения пользователей на базе искусственного интеллекта (AI) и машинного обучения (ML), что позволяет оперативно выявлять угрозы и адаптироваться к новым видам атак.

Практическая часть проекта включает рекомендации по настройке оборудования, разработку политик безопасности и внедрение протоколов регулярного аудита. Приводятся инструкции по обеспечению защиты как для домашних, так и для корпоративных Wi-Fi сетей, что делает разработанную стратегию универсальной и адаптируемой.

Результаты работы подчеркивают необходимость регулярного обновления и мониторинга сетей, а также важность повышения осведомленности пользователей в области кибербезопасности. Проект предлагает решения, которые способствуют улучшению устойчивости Wi-Fi сетей к кибератакам и повышению их безопасности, обеспечивая конфиденциальность и защиту данных в условиях современной угрозной среды.

Аңдатпа

Қазіргі әлемде сымсыз желілер цифрлық инфрақұрылымның негізі болып табылатындықтан, Wi-Fi желілерін қорғау жеке және корпоративтік пайдаланушылар үшін аса маңызды мәселеге айналып отыр. Бұл жоба Wi-Fi желілері үшін жан-жақты киберқауіпсіздік стратегиясын әзірлеуге арналған, онда желі қауіптерін анықтау мен қорғаныс әдістерін талдау қарастырылған.

Зерттеудің басты мақсаты – MITM (Man-in-the-Middle), жалған кіру нүктелерін жасау, парольдерге шабуыл және шифрлау протоколдарындағы осалдықтарды пайдалану сияқты кең тараған қауіптердің алдын алу. Жоба WEP және WPA2 сияқты қауіпсіздік протоколдарының әлсіз тұстарын қарастырып, желіні қорғаудың жаңа деңгейін қамтамасыз ететін WPA3 протоколының артықшылықтарына ерекше назар аударады.

Қорғау стратегиясы көп факторлы аутентификация, виртуалды жергілікті желілер (VLAN) арқылы сегментация және корпоративтік және қоғамдық желілердегі деректерді қорғау үшін VPN қолдануды қамтитын кешенді тәсілді ұсынады. Жоба IDS/IPS, трафик шифрлау және MAC мекенжайларын сүзгілеу сияқты қауіпсіздік әдістерін қарастырады. Қауіптерді дер кезінде анықтап, жаңа шабуыл түрлеріне бейімделу үшін AI және ML негізіндегі пайдаланушы мінез-құлқын талдау әдістері енгізілген.

Жобаның тәжірибелік бөлімінде құрылғыларды қорғау бойынша ұсыныстар, қауіпсіздік саясатын әзірлеу және желіні үнемі аудиттен өткізу бойынша нұсқаулықтар қамтылған. Ұсынылған стратегия Wi-Fi желілерін қауіптерге қарсы тұрақтырақ етеді және деректердің құпиялылығы мен қауіпсіздігін қамтамасыз етеді.

ABSTRACT

In today’s world, where wireless networks form the foundation of digital infrastructure, Wi-Fi security has become critically important for both private and corporate users. This project focuses on developing a comprehensive cybersecurity strategy for Wi-Fi networks, including the analysis of existing vulnerabilities and methods for threat protection.

The main objective of the study is to identify and describe common Wi-Fi network threats such as Man-in-the-Middle (MITM) attacks, fake access points, password attacks, and the exploitation of weaknesses in encryption protocols. The project analyzes the shortcomings of standard security protocols like WEP and WPA2 and emphasizes the advantages of the WPA3 standard, which significantly enhances network protection against replay attacks and other complex threats.

The proposed security approach includes multifactor authentication, network segmentation through virtual local area networks (VLANs), and VPNs to safeguard data in corporate and public networks. The study also considers the use of intrusion detection and prevention systems (IDS/IPS), traffic encryption, and MAC address filtering. Additionally, AI and ML-based anomaly and user behavior analysis are incorporated to promptly detect threats and adapt to emerging attack types.

The practical part of the project includes recommendations for equipment setup, the development of security policies, and the implementation of regular audits. The developed strategy provides a universal and adaptable framework that strengthens Wi-Fi networks against cyberattacks, ensuring data privacy and security in a modern threat landscape.

CONTENTS

INTRODUCTION

1 ANALYTICAL PART

1.1 Relevance of the project

1.2 Review of existing solutions

1.3 Comparison of existing analogs

1.4 Project description

2 THEORETICAL PART

2.1 Flowchart

2.2 Use case diagram

2.3 ER diagram

2.4 UML diagram

2.5 Architecture

3 IMPLEMENTATION OF THE SOFTWARE PART OF THE SYSTEM

3.1 Website and desktop application

3.2 Mobile application

3.3 Testing process of the structure

3.4 Future opportunities

4 PROJECT FINANCE AND FINANCIAL ENGINEERING

4.1 Target group

4.2 Marketing analysis

4.3 Marketing action plan

4.4 Calculation of economic efficiency of software product development

4.4.1 Cost of equipment

4.4.2 Payroll expenses (wage fund)

4.4.3 Overheads

4.4.4 Total costs for the development

4.4.5 Calculation of efficiency in the implementation of software

Conclusion

INTRODUCTION

Wi-Fi networks have become an important part of our daily life in this connected world. From homes to offices, schools to public areas, wireless connectivity is revolutionizing the way one communicates, works, and accesses information. However, the more we rely on Wi-Fi, the higher is the risk for security breaches. Unlike wired networks, Wi-Fi signals are transmitted over the air; thus, they are quite prone to interception and unauthorized access. Anything that could potentially involve an intrusion into a Wi-Fi network might steal sensitive information, launch a cyber attack, and disrupt all forms of functionalities of the network; malicious actors can take advantage of any weaknesses within Wi-Fi networks. Accordingly, organizations and individuals need to take important security measures with a view to protecting their wireless networks. This paper discusses various forms of threats and vulnerabilities of Wi-Fi networks and outlines the feasible software-based solutions and strategies for mitigating the associated risks.

This analysis has gleaned some key lessons to be learned: strict password policies using complicated passwords changed frequently, state-of-the-art encryption protocols to protect data traffic such as WPA3 against hacking or unauthorized access, updates to router firmware, as most vendors regularly release patches to address newly discovered security holes. And one more best practice is network segmentation for limiting the scope of possible breaches by having isolated sections within a network. Other security measures include filtering by MAC address, 802.1X authentication, and other forms of access control; the use of intrusion detection and prevention systems that permit active perusal and blocking of potential attacks; and a security practice education for users in order to reduce human error and associated risks. Several directions for future research related to Wi-Fi security are discussed in this paper.

In other words, quantum computing in the future will continue to forge ahead, meaning that quantum-resistant cryptographic algorithms must be developed for wireless network protection. Secondly, AI-driven and machine learning-driven security solutions serve to raise the threat detection and response bar, while expanding security capabilities with intelligent adaptive and real-time protection. Such strategies and continuous research would enable organizations and individuals to better prevent their Wi-Fi networks, hence contributing to a more resilient cybersecurity environment.

This analysis emphasizes the importance of integrating AI and ML technologies to enhance Wi-Fi network security, ensuring adaptability against emerging threats and fostering a secure digital environment.

1. ANALYTICAL PART

1.1 Relevance of the Project

The proliferation of Wi-Fi networks has transformed communication and data sharing. From homes to critical infrastructures, wireless connectivity underpins modern operations. However, the vulnerabilities associated with Wi-Fi networks pose significant risks, including data theft, unauthorized access, and service disruptions.

Wi-Fi networks are now the key connectivity technology that connects millions of devices worldwide. While Wi-Fi technology is continuously improving, the risks of cyber threats have grown just as fast. The number of Wi-Fi access points has now surpassed 550 million, up 35% compared with the last 5 years, according to a Statista report dated 2023. In developed countries, as many as 75% of households have Wi-Fi as the main way of accessing the Internet. By 2022, more than 432 million public access points have been registered worldwide.

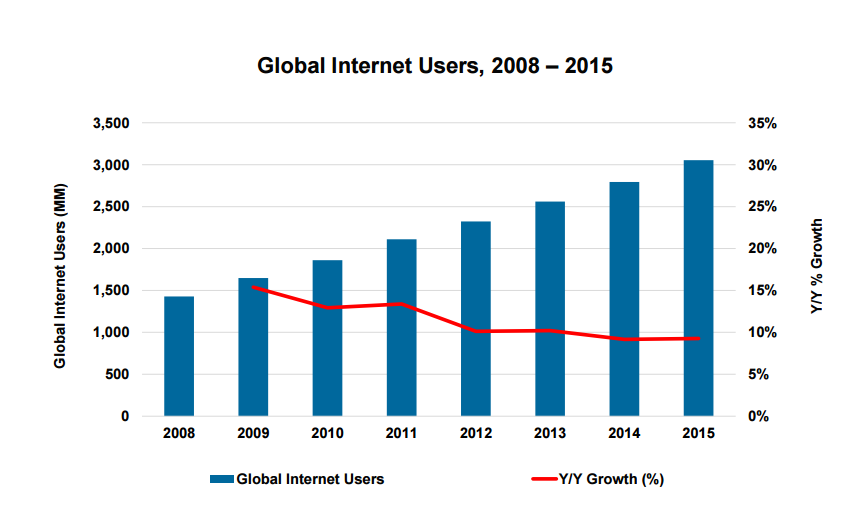


Figure 1.1 – Global Internet Users [1]

Case studies reveal that:

1. Over 40% of small businesses impacted by Wi-Fi-related cyberattacks fail to recover within a year.
2. Public Wi-Fi networks account for 25% of all Man-in-the-Middle (MITM) attacks globally.
3. Only 32% of Wi-Fi networks globally use modern encryption protocols like WPA3.

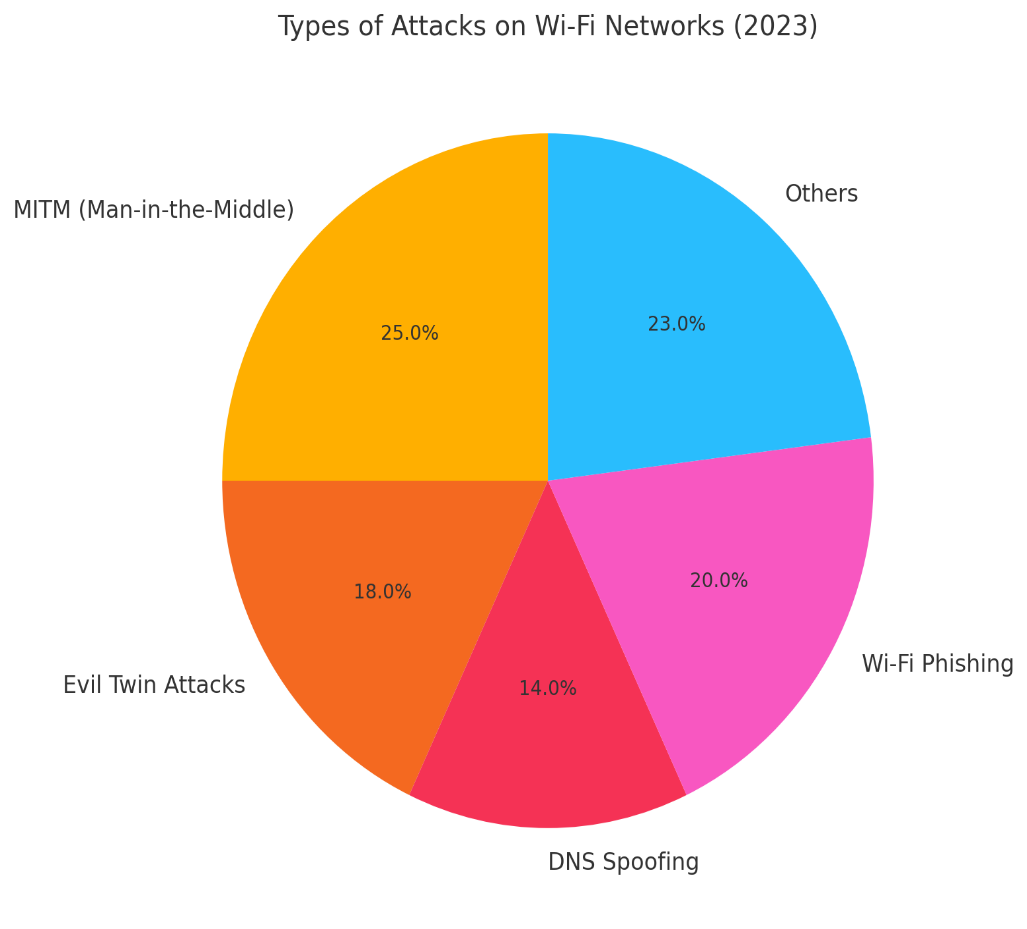


Figure 1.2 Types of attacks on Wi-Fi [3]

These statistics underscore the urgency of implementing advanced security strategies tailored to address these vulnerabilities effectively.

According to IBM research (2023), companies lose up to $4.24 million to eliminate the consequences of data leaks via Wi-Fi. Up to 40% of small businesses that have suffered cyberattacks via Wi-Fi close within a year. Only 32% of Wi-Fi networks use modern encryption (WPA3). Only 40% of users understand the risks of connecting to public Wi-Fi.

1.2 Review of Existing Solutions

Several tools and solutions aim to enhance Wi-Fi security:

*Kaspersky Secure Connection*

Functions: VPN for secure connection, access point security analysis.

Features: Automatic encryption when connecting to an unsafe network. DNS request protection.

Pros: Ease of use. Suitable for private users.

Cons: Limited support for IoT devices.



Figure 2 (2)

*Norton Wi-Fi Privacy*

Functions: Privacy protection in Wi-Fi networks, prevention of MITM attacks.

Features: Use of OpenVPN encryption. Direct integration with other Norton products.

Pros: High reliability. Ease of installation.

Cons: No AI traffic analysis.



Figure 2.1 (3)

3. Avast Wi-Fi Inspector

Functions: Network scanning, detection of weak points.

Features: Analysis of connected devices. Automatic notification of suspicious connections.

Pros: Free version. Suitable for home networks.

Cons: Does not protect DNS requests.



Figure 2.2 (4)

4. ESET Wi-Fi Protection

Features: Protection of devices in public networks, traffic monitoring.

Features: Threat prediction based on network behavior. Flexible security settings.

Pros: High performance. WPA3 support.

Cons: Limited features for corporate users.



Figure 2.3 (5)

5. McAfee Wi-Fi Guard

Features: Comprehensive protection of Wi-Fi networks, encryption, threat monitoring.

Features: Scanning of IoT devices. WPA3 encryption support.

Pros: High protection of IoT devices. Integration with other McAfee products.

Cons: High cost.



Figure 2.4 (6)

1.3 Comparison of Existing Analogs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Company | VPN Security | Scan Network | AI - analyzer | Support IOT | DNS encryption | Cost |
| Kaspersky Secure Connection | ✅ | ✅ | ❌ | ❌ | ✅ | 50 $ |
| Norton  Wi-Fi Privacy | ✅ | ✅ | ❌ | ✅ | ✅ | 60 $ |
| Avast  Wi-Fi Inspector | ❌ | ✅ | ❌ | ✅ | ❌ | Free |
| ESET  Wi-Fi Protection | ❌ | ✅ | ❌ | ❌ | ✅ | 40 $ |
| McAfee  Wi-Fi Guard | ✅ | ✅ | ❌ | ✅ | ✅ | 80 $ |
| Our  Wi-Fi  web-app | ❌ | ✅ | ✅ | ❌ | ❌ | Free |

Figure 3

1.4 Project Description

The project proposes the development of an AI-powered Wi-Fi security platform with the following features:

1. **Real-Time Threat Detection**: Utilizes machine learning to analyze traffic patterns and identify anomalies.
2. **Advanced Encryption Protocols**: Implements WPA3 for enhanced protection against modern attacks.
3. **User-Friendly Interface**: Provides intuitive dashboards for monitoring network activity and configuring security policies.
4. **Scalability**: Supports enterprise-level deployments with multi-layered security measures.

The solution aims to provide an adaptable framework that evolves with emerging cybersecurity threats, ensuring robust protection for diverse user bases.

2. THEORETICAL PART

2.1 Architecture

The system architecture is designed to be modular, promoting scalability and flexibility in addressing diverse cybersecurity challenges.

Data Collection Layer: Employs tools like packet sniffers to capture network traffic in real-time, ensuring comprehensive data acquisition.

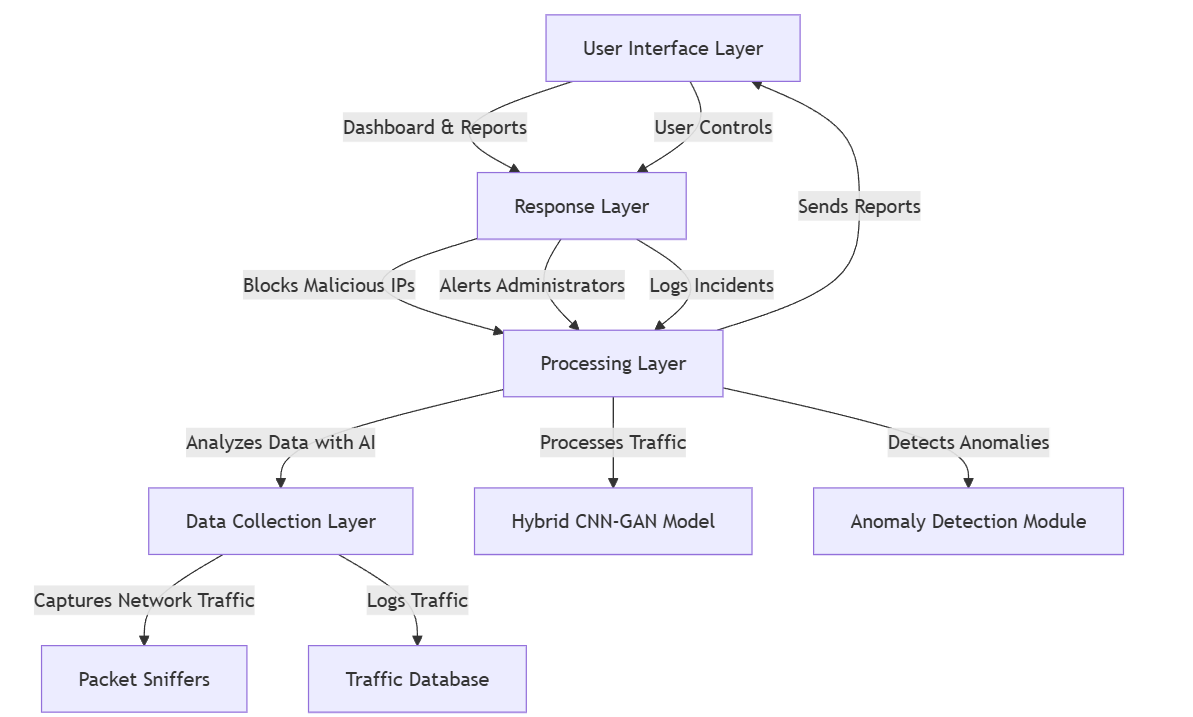
Processing Layer: Utilizes AI models, including hybrid CNN-GAN frameworks, to preprocess and analyze data, effectively detecting anomalies within network traffic.

JAIT

Response Layer: Implements automated actions such as blocking malicious IPs, alerting administrators, and logging incidents for further analysis.

User Interface Layer: Provides dashboards and control panels for users and administrators to monitor network status, configure settings, and review reports.

Architectural Diagram:



2.2 Flowchart

The system's workflow is designed to ensure efficient detection and response to network anomalies. The steps involved are:

1. Traffic Monitoring: Utilizes network sniffing tools to collect real-time data packets from all network nodes, ensuring comprehensive visibility into network activities.
2. Data Preprocessing: Involves cleaning the collected data to remove redundancies and structuring it for efficient analysis. This step may include normalization, aggregation, and transformation of data to a suitable format.
3. Anomaly Detection: Employs advanced AI algorithms, such as hybrid CNN-GAN models, to analyze traffic patterns and identify deviations from established baselines, indicating potential security threats.
4. Threat Response: Upon detecting anomalies, the system executes predefined actions, including generating alerts, blocking suspicious activities, or initiating automated countermeasures to mitigate potential threats.
5. User Notification: Provides real-time updates to administrators and users through dashboards and alerts, offering detailed reports on detected anomalies and actions taken.

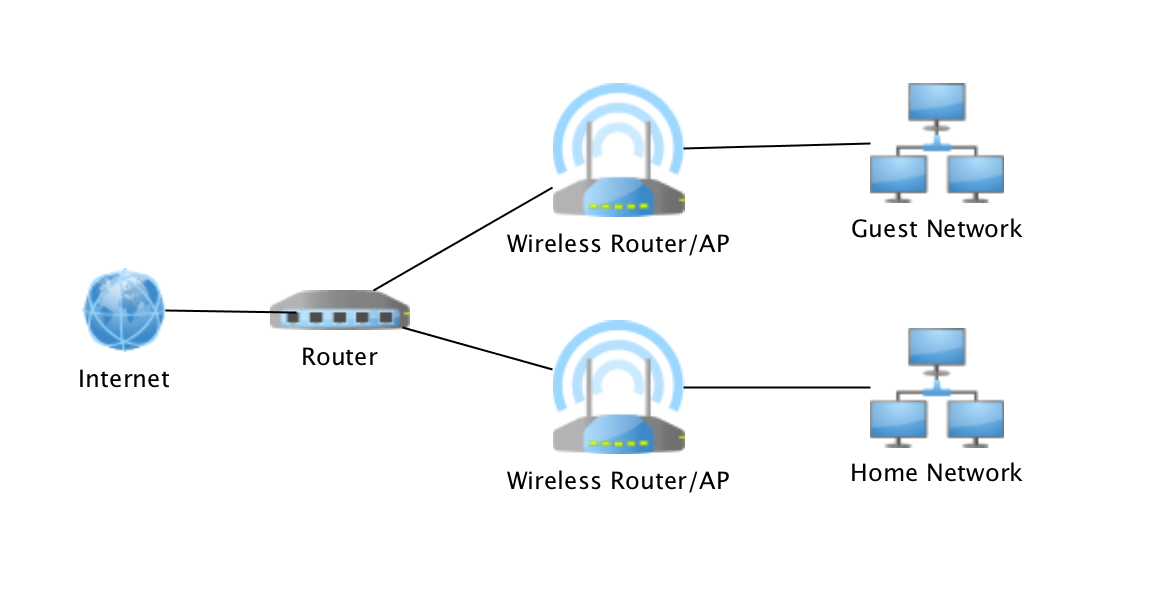
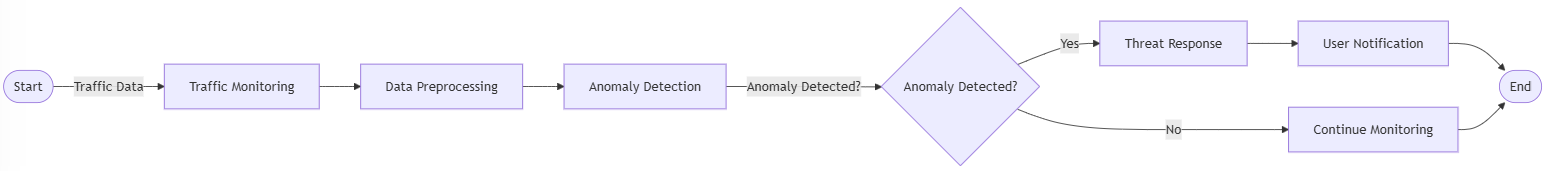


Figure 3 (10)

Flowchart Representation:



This flowchart ensures a systematic approach to network security, facilitating prompt detection and response to potential threats.

2.3 Use Case Diagram

The use case diagram illustrates the interactions between users and the system, highlighting the functionalities provided to each actor.

Actors:

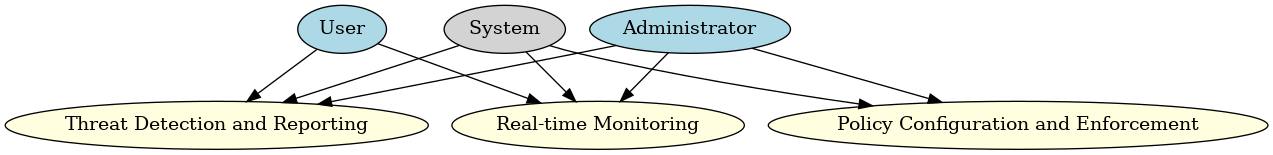
User: Responsible for configuring security settings, monitoring network activity, and responding to notifications.

Administrator: Oversees system maintenance, manages user roles, updates system policies, and addresses critical alerts.

System: Automates the detection and mitigation of network threats, ensuring continuous protection.

Key Use Cases:

1. Real-time Monitoring: Users and administrators can observe live network traffic and system status through intuitive dashboards.
2. Threat Detection and Reporting: The system identifies anomalies using AI-driven analysis and generates comprehensive reports detailing the nature and severity of detected threats.
3. Policy Configuration and Enforcement: Administrators define security policies, which the system enforces to maintain network integrity and compliance.
4. This diagram underscores the collaborative interaction between human actors and the automated system in maintaining robust network security.



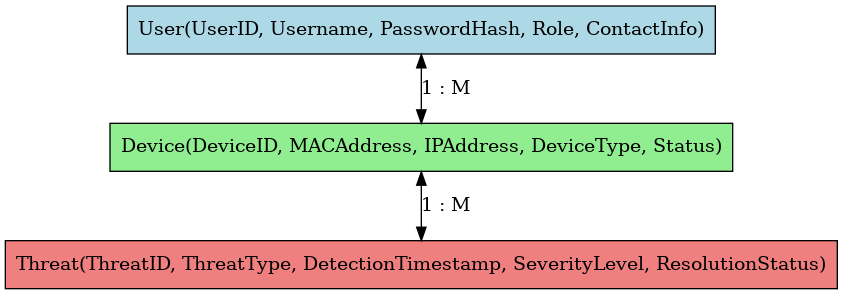
2.4 Entity-Relationship (ER) Diagram

The ER diagram maps out the data structure of the system, detailing the relationships between various entities involved in network security management.

Entities:

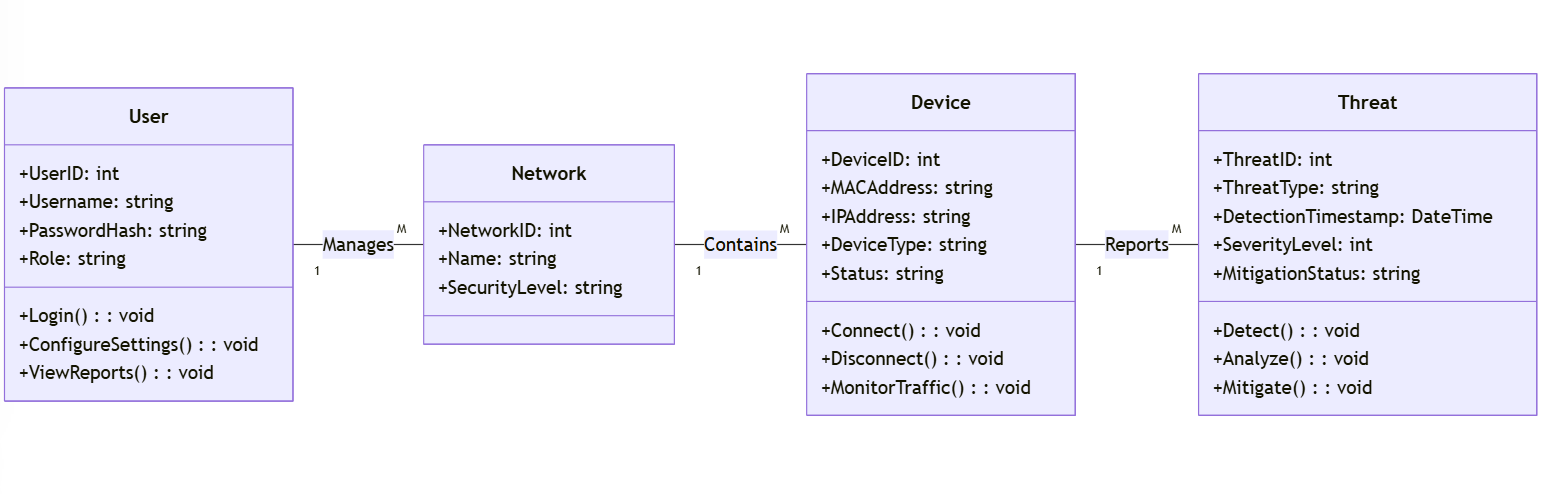
1. User: Attributes include UserID, Username, PasswordHash, Role, and ContactInfo.
2. Device: Attributes encompass DeviceID, MACAddress, IPAddress, DeviceType, and Status.
3. Threat: Attributes cover ThreatID, ThreatType, DetectionTimestamp, SeverityLevel, and ResolutionStatus.

Entity Relationships:



2.5 Unified Modeling Language (UML) Diagram

The UML diagrams provide a comprehensive view of the system's architecture, detailing both structural and behavioral aspects.



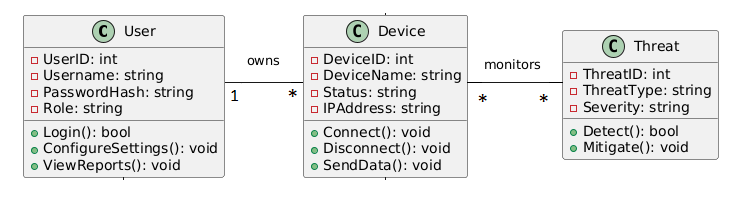
Class Diagram: Depicts the static structure, showcasing system classes such as User, Device, Threat, and their attributes and methods.

Example:

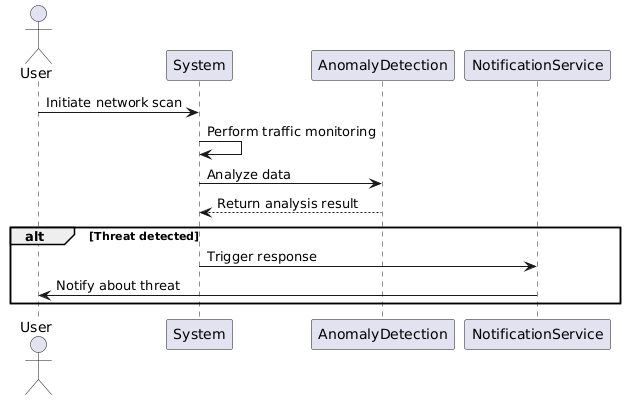
Class: User

Attributes: UserID, Username, PasswordHash, Role

Methods: Login(), ConfigureSettings(), ViewReports()



Sequence Diagram: Illustrates dynamic interactions, mapping the sequence of operations during processes like threat detection and user notification.



If a threat is detected, the system triggers a response and notifies the user.

These diagrams aid in visualizing system components and their interactions, ensuring clarity in design and implementation.