A cartoon of a egyptian god

Description automatically generatedA computer network diagram with a globe and arrows

Description automatically generated with medium confidence

**Cairo University**

**Faculty of Computers and Artificial Intelligence**

**Department of Networks and cybersecurity**

**Safe Net**: The Security Shield

A logo of a security shield

AI-generated content may be incorrect.

Supervised by

Dr. Nour-ElDeen Mahmoud

Implemented by

|  |  |
| --- | --- |
| *20225085* | *Mostafa Hesham Sherif* |
| *20216011* | *Ahmed Mohamed Talaat* |
| *20216038* | *Radwa Khaled Fathy* |
| *20216138* | *Karim Wael Marwan* |
| *20215044* | *Yousef Yasser El-Kady* |
| *20216078* | *Farida Mohammed Seleem* |

Graduation Project

Academic Year 2024-2025

Mid-year Short Documentation

**TABLE OF CONTENTS**

[LIST OF ACRONYMS/ABBREVIATIONS 2](#listOfABB)

[LIST OF FIGURES 3](#listOfFgures)

[LIST OF TABLES 4](#ListOfTables)

[1.Abstract 4](#Abstract)

[2.Background 7](#_Toc190284644)

[3.Problem definition 8](#Problem_def)

[4.Related work 10](#relatedwork)

[5.Project specifaction 11](#_Toc190284647)

* **5.1: SYSTEM ARCHITECTURE DIAGRAM …………………………..9**
* [5.2 Stakeholders 11](#_Toc190284648)
* [5.3 functional requirments 12](#_Toc190284649)
* [5.4 non-functional requirements 13](#_Toc190284668)
* **5.5 USE-CASE DIAGRAM……………………………………...………..11**
* **5.6 CLASS DIAGRAM……………………………………...…………… 12**
* **5.7 SEQUENCE DIAGRAM……………………………………...……... 13**
* **5.8 ENTITY RELATIONSHIP DIAGRAM(ERD)……….…………… 15**

[**6.WORK PLAN DIAGRAM ……………………………………………………18**](#workplan)

[**7.REFRENCES……………..……………………………………………………20**](#refrence)

# LIST OF FIGURES

**[Figure 5.1: System Architecture Diagram …………………………………………………...9](#systemarch)**

[**Figure 5.5: Use-case Diagram………………………………………………………………..**](#_5.5_Use-case_diagram) **13**

[**Figure 5.6: Class Diagram …………………………………………………………………..**](#_5.6_class_diagram)  **14**

[**Figure 5.7: Sequence Diagram ……………………………………………………………...**](#_5.7_sequence_diagram) **15**

* **Figure 5.7.1: Signup Sequence Diagram …………………………………………... 15**
* **Figure 5.7.2: Login Sequence Diagram ……………………………………………. 15**
* **Figure 5.7.3: Scan Sequence Diagram ……………………………………………... 16**
* **Figure 5.7.4: Report Sequence Diagram …………………………………………... 16**

**[Figure 5.8: Entity Relationship Diagram(ERD) ………………………………………….. 17](#_5.8_Entity_Relationship)**

[**Figure 6: Work Plan Diagram ……………………………………………………………...****.19**](#ganntchart)

# LIST OF TABLES

# [Table 4.1: Related work……………………………….…………….……………. 5](#_4.Related_work)

# [Table 6.1:work plan ………………………………………………...……………… 18](#workplan)

# LIST OF ACRONYMS/ABBREVIATIONS

|  |  |  |
| --- | --- | --- |
| **Acronym** | **Definition of Acronym** | **Page** |
| URLs | Uniform Resource Locators | 6 |
| API | Application Programming Interface | 6 |
| AI | Artificial Intelligence | 6 |
| SQL | Structured Query Language | 6 |
| SPF | Sender Policy Framework | 7 |
| DKIM | DomainKeys Identified Mail | 7 |
| DMARC | Domain-based Message Authentication,  Reporting, and conformance | 7 |
| IDE | Integrated Development Environment | 7 |
| IT | Information Technology | 11 |
| ERD | Entity-Relationship Diagram | 17 |

Abstract

With the rise of cyber threats, phishing attacks have become a major security risk, leading to

financial losses and data breaches. Attackers continuously refine their tactics, using malicious

websites and phishing emails to deceive users. Traditional detection methods often struggle

to keep up, highlighting the need for a real-time, efficient, and accessible phishing detection

system.

SafeNet: The Security Shield addresses this challenge by providing a website-based plat-

form that scans URLs and email files for potential threats. The Standard Plan utilizes the

VirusTotal API for basic detection, while the Premium Plan integrates multiple APIs, such as

IPQualityScore, for enhanced security. SafeNet also employs heuristic analysis and WHOIS

lookup to improve detection accuracy, along with an awareness module that educates users

when phishing threats are detected. Additionally, the system features a chatbot for communi-

cation platforms, leveraging AI-API to provide real-time security guidance.

Built with JavaScript for the backend, React for the frontend, and MongoDB for database

management, SafeNet seamlessly integrates external APIs for real-time detection. GitHub is

used for version control, ensuring a structured development process. By combining API-driven

detection, heuristic analysis, and real-time user awareness, SafeNet offers a scalable and user-

friendly cybersecurity solution.

Chapter 1

Introduction

1.1 Motivation

The motivation for this project is rooted around the escalating and pervasive threat of phishing

attacks, which represent a significant challenge to modern cybersecurity. These attacks are no

longer rudimentary scams; they have evolved into highly sophisticated operations that leverage

social engineering to steal sensitive credentials, financial information, and personal data. The

consequences for individuals and organizations are severe, ranging from direct monetary loss

and identity theft to widespread data breaches that can cripple a company’s operations and its

reputation.

A critical vulnerability in this digital ecosystem is the human factor. Many users, regardless

of their technical proficiency, lack the specialized tools and, more importantly, the situational

awareness needed to detect these deceptive emails and links. Existing security solutions often

fall short of addressing this gap. They can be overly complex for the average user, requiring

technical configuration that creates a barrier to entry. Furthermore, many tools are platform-

specific—such as desktop antivirus software or browser extensions—leaving users unprotected

across the multitude of devices they use daily.

This creates a clear and urgent need for an accessible, intuitive, and centralized tool. Safe

Net is designed to fill this void. Our motivation is not merely to create another layer of defense,

but to empower the user directly.We do that by providing a platform that combines immediate

phishing detection, a simple mechanism for reporting malicious URLs, and integrated edu-

cational resources, we aim to enhance overall online security from the ground up while also

educating users about potential threats. The goal is to transform the user from a potential vic-

tim into an informed and proactive participant in their own digital safety, thereby fostering a

more resilient and secure online environment for everyone.