SS2012

**Technical and Business Writing**

**Project Proposal**

**DefendAI:** An AI-Powered Cybersecurity Assistant for Digital Footprint Protection

**Submitted by:** Fatima Naeem, Rumaisah Haroon, Amna Ali, Sarita Sangrez

**Roll number:** 23i-2046,23i-2106,23i-2067,23i-2088

**Date:** 6th May 2025

**Table of Contents**

[**DefendAI: An AI-Powered Cybersecurity Assistant for Digital Footprint Protection** 4](#_Toc197032221)

[**Executive Summary** 4](#_Toc197032222)

[**Problem Statement** 4](#_Toc197032223)

[**Solution Overview** 5](#_Toc197032224)

[Core Functionalities 5](#_Toc197032225)

[1. Digital Footprint Scanner 5](#_Toc197032226)

[2. Dark Web Threat Detection: 5](#_Toc197032227)

[3. Real-time alerts 5](#_Toc197032228)

[4. Protection tips 6](#_Toc197032229)

[5. Phishing Detection 6](#_Toc197032230)

[6. Password Strength Recommendations 6](#_Toc197032231)

[Addressing the Issues with Functionalities 6](#_Toc197032232)

[1. Proactive Threat Detection 6](#_Toc197032233)

[2. Digital Footprint Visualization 6](#_Toc197032234)

[3. Dark Web Scanning: 6](#_Toc197032235)

[4. Real-Time Alerts: 6](#_Toc197032236)

[5. Security Awareness and Strengthening Recommendations: 6](#_Toc197032237)

[User experience 6](#_Toc197032238)

[1. Non-technical users: 6](#_Toc197032239)

[2. Technical users: 6](#_Toc197032240)

[**Target Audience** 7](#_Toc197032241)

[IT professionals: 7](#_Toc197032242)

[Small business owners: 7](#_Toc197032243)

[How DefendAI Helps: 7](#_Toc197032244)

[General users with low cyber security knowledge: 7](#_Toc197032245)

[USER NEEDS AND CHALLENGES 8](#_Toc197032246)

[**Key Features** 8](#_Toc197032247)

[1. Phishing Detection 8](#_Toc197032248)

[2. Malware Scanning 8](#_Toc197032249)

[3. Dark Web Monitoring 8](#_Toc197032250)

[4. Real-Time Alerts 9](#_Toc197032251)

[5. Digital Footprint Visualization 9](#_Toc197032252)

[6. Security Recommendations 9](#_Toc197032253)

[7. AI Learning and Adaptability 9](#_Toc197032254)

[8. User Profile Customization 9](#_Toc197032255)

[9. Non-Technical User Support 9](#_Toc197032256)

[**Market Potential** 9](#_Toc197032257)

[Gaps in Existing Tools 10](#_Toc197032258)

[DefendAI Potential 10](#_Toc197032259)

[**Implementation Plan** 11](#_Toc197032260)

[Tools and Technologies 11](#_Toc197032261)

[Development Timeline 11](#_Toc197032262)

[Team Structure: 12](#_Toc197032263)

[**Ethical Considerations** 12](#_Toc197032264)

[User Privacy and Data Protection: 12](#_Toc197032265)

[AI Transparency and Explainability: 12](#_Toc197032266)

[Bias Mitigation and Inclusivity: 12](#_Toc197032267)

[**References** 12](#_Toc197032268)

# **DefendAI: An AI-Powered Cybersecurity Assistant for Digital Footprint Protection**

# **Executive Summary**

DefendAI is an AI-powered cyber security assistant which is designed to empower individuals and organizations on managing their digital footprint. It achieves this by by monitoring, alerting, and guiding users on potential online risks. In today’s digital era where there is an increase in online exposure and rise in data breaches, DefendAI proactively helps users understand and reduce their cyber security risks instantaneously. It has a user-friendly interface and easy-to-understand language which makes it especially valuable for users who lack deep technical expertise.

This project addresses a specific cyber security issue which is the growing threat of digital footprint exposure. Digital footprint refers to the trail of personal and sensitive data users leave online which can be exploited by online criminals. Flashpoint's 2024 Global Threat Intelligence Report [6] reported a 34.5% increase in data breaches and over 17 billion personal records compromised in 2023, which shows how urgent it is to address this problem. Current solutions are often focused on just enterprises, which leaves individual users vulnerable because of limited accessibility.

DefendAI is designed specifically with students, instructors, and non-expert users in mind. Our aim is to provide personalized risk analysis, privacy tips, and dark web alerts through a dynamic AI assistant. Its ability to simplify technical threats and offer clear insights makes it both innovative and essential.

The project offers a unique value proposition by filling an essential gap in the cybersecurity space: making digital safety accessible, proactive, and comprehensible for the everyday user. DefendAI not only strengthens online defense but also fosters a culture of awareness and digital responsibility.

# **Problem Statement**

In the modern digital landscapes, the exposure of digital footprints is one of the most pressing cyber security concerns. Digital footprints are the collection of personal, behavioral, and possibly sensitive data individuals leave behind through their online interactions. This information includes social media activity, search history, shared files, IP addresses, location check ins, and so on. Although much of this data is passively collected, it can be aggregated and exploited by criminals to conduct phishing attacks, impersonation, identity theft, and targeted scams.

The significance of this issue lies in how easily users, especially those with limited cyber security awareness, expose themselves unintentionally. A well-known real life example is the 2019 Facebook data breach [7], where the personal information of over 533 million users from 106 countries (including phone numbers, full names, and email addresses) was leaked and made available on online platforms. This trend continues to grow with increased online engagement across age groups.

To validate this concern, we conducted a survey among 26 individuals, undergraduate Students, IT Professionals and common people with varying levels of cyber security awareness. The analysis revealed the following:

* 50% (13 out of 26) had never checked if their data had been leaked; 4 users were completely unaware such checks were even possible. This highlights a significant awareness gap regarding digital footprint monitoring.
* Major concerns included identity theft, unauthorized access to social media, and financial fraud, with many respondents selecting multiple threats, recognizing their interconnected nature.
* 8 users rarely changed passwords, and another 8 only did so when forced to. Just 4 practiced regular updates—indicating a clear vulnerability to brute-force attacks or credential stuffing.
* Half the respondents (13) had acquaintances who were victims of cybercrime, and 7 had personally been affected, confirming the real-life consequences of poor cyber hygiene.

These findings highlight the clear need of awareness and protection tools, especially those that are easy to understand and accessible for everyday users. Large enterprises invest in complex cyber security systems, but individuals and small organizations lack personalized solutions that effectively monitor and secure their online presence. The problem is widespread and requires an AI-powered assistant that can educate and alert users by continuously tracking their digital footprint and guiding them with useful advice.

# **Solution Overview**

DefendAI provides a user-friendly dashboard that addresses all the mentioned risks associated with digital footprint exposure. It uses its main functionalities like digital footprint tracker, real time alerts, dark web detection and personalized recommendations to bridge the gap between cyber security awareness and practical action, especially for users without technical background.

## Core Functionalities

1. Digital Footprint Scanner: Continuously monitors a user’s digital footprint across online platform and tracks user data like credentials across websites, dark web and social media platforms.
2. Dark Web Threat Detection: It identifies unauthorized usage of credentials, emails or personal details on underground marketplace.
3. Real-time alerts: It also provides an alert as soon as any suspicious activity is detected.
4. Protection tips: It gives tips and Advices to remove and protect data online.
5. Phishing Detection: Moreover, detects any mail or message that attempts to steal information.
6. Password Strength Recommendations: Notifies to provide a strengthened password and suggests improvement for better protection.

## Addressing the Issues with Functionalities

These features help solve the problems by directly addressing all the issues discussed.

1. Proactive Threat Detection**:** Users are unaware of ongoing threats which lead to delayed responses and damage. Proactive monitoring and tracking data across platforms will allow to identify those threats or vulnerabilities, notifying user before they lead to more serious issues like fraud.
2. Digital Footprint Visualization**:** DefendAI tracks and visualizes the digital footprint in an easy-to-understand format making all threats and hidden risks visible.
3. Dark Web Scanning: Stolen data is often traded on underground marketplace and users often don’t have any information about it until it’s too late. Dark web scanning identifies exposed data and clearly explains what actions should be taken.
4. Real-Time Alerts: This AI provides real time alerts to users in plain language by presenting insights and recommendations without any technical knowledge.
5. Security Awareness and Strengthening Recommendations: Many users don’t understand how weak security can lead to risks like hacking, phishing or data theft. Recommendations suggest how security can be strengthened to enhance overall online security and reduce the likelihood of future cyberattacks.

Rather than reactive measures, DefendAI takes a proactive approach by providing constant tracking and delivering preventive guidance before damage occurs.

## User experience

DefendAI is made for all including all technical and non-technical users.

1. Non-technical users: The AI dashboard is clean and user friendly providing color coded alerts in simple language and explanations. This makes it easier for people with less cyber related knowledge to understand risks and take actions accordingly.
2. Technical users: For users with greater knowledge or people belonging to IT backgrounds, DefendAI can provide deeper insights and access to detailed information about risks and threats for them to analyze the situation with granularity.

Overall, DefendAI aims to provide a simple dashboard that simplifies all the complexities of cyber security and helps everyone to take action to secure their data.

# **Target Audience**

DefendAI aims to cover a wide range of users from beginners to experienced people. It ensures accessibility for all by providing a friendly interface. Below are the key audience DefendAI targets using user personas:

## IT professionals:

**Persona:** IT Manager in Telecom Company

**Needs:** Real-time alerts for breaches, advanced reporting, integration with existing security workflows.

**Challenges**: Needs quick detection to act fast, requires actionable logs and minimal false positives, and demands compatibility with other tools.

**How DefendAI Helps:**

* Provides system-level insights, data breach metadata, and threat classifications.
* Provides detailed reports, system alerts and integrates with existing tools.
* Speeds up incident response with summarized recommendations and full traceability.

## Small business owners:

**Persona:** Retail Shop Owner (Clothing Business)

**Needs:** Secure customer information, prevent phishing attacks, and ensure smooth online operations.

**Challenges:** No dedicated IT staff, limited time to learn security protocols, overwhelmed by managing multiple accounts and platforms.

## How DefendAI Helps:

* Automates monitoring of business credentials and data breaches.
* Sends real-time alerts for unusual activity.
* Recommends actions in simple terms (e.g., when to change a password, or recognize a phishing email).
* Reduces the burden of manual security checks.

## General users with low cyber security knowledge:

**Persona:** Administrative Secretary in Education

**Needs:** Protection of personal information and work-related credentials.

**Challenges:** Limited awareness of cyber security threats, lacks technical vocabulary, unaware of data exposure or how to check for it.

**How DefendAI Helps:**

* Provides simple alerts with non-technical explanations.
* Visualizes digital footprint clearly (e.g., what is exposed and why it matters).
* Offers basic tips like password improvements, phishing warning signs, and privacy recommendations.

## USER NEEDS AND CHALLENGES

|  |  |  |
| --- | --- | --- |
| **Users** | **Needs** | **Challenges** |
| General | Privacy tips, risk alerts | Less awareness, no knowledge of tech terms |
| Small business owners | Account protection, phishing detection | No IT staff, less security management |
| IT professionals | Advanced insights, fast breach detection | Needs speed, accuracy and integration options |

# **Key Features**

DefendAI has powerful and Ai-driven tools and have made them in such a way that even a person with no technical background can know hoe to use them. Some of the main features integrated into DefendAI are:

## Phishing Detection

This AI uses already made algorithms to run every email and message the customer gets to detect phishing. It uses AI to spot already known pattern of phishing and scans attached links and downloadable documents in the mails. Users are warned in simple language, with actionable steps to avoid compromise.

## Malware Scanning

It does real-time scanning of links and any downloadable attachments or even currently downloading files through signature-based detection and looks for new patterns as well. This ensures even new or modified malwares can be identified. When a malware detected or even suspected, alerts are issued instantly, with clear and easy to understand next steps to stop this.

## Dark Web Monitoring

This AI regularly scans forums, breacjs, and black-market listings for any leaked PII (Personally Identifiable Information). If personal data (emails, usernames, passwords,address etc) is found, DefendAI notifies the user and also provides the user with a guide on how to reduce such events in the future.

## Real-Time Alerts

All kind of threat detections alerts are given promptly and the user is notified immediately. These alerts are in easy and plain English and no technical words are used. These alerts include risk level, affected data, and recommended actions. This ensures that every user can understand and respond effectively to these threats timely.

## Digital Footprint Visualization

Shows a clear visual dashboard of user data that shows the exposure of the user online. It also displays which data is publicly visible and is in the danger of being compromised. This makes complex security measures and statistics easy to read and understand.

## Security Recommendations

Based on daily activity and regular scans, DefendAI provides suggestions that are tailored to the users requirement. It gives tips like update passwords, remove your exposed data, and how to avoide malicious links.

## AI Learning and Adaptability

This system improves by daily user interactions and also by reading and studying threat trends in the market. Feedback allows it to learn what alerts are useful, and how to tailor itself on user requirements. This reduces false positives and also improves accuracy over time.

## User Profile Customization

This AI additionally allows users to set threat sensitivity levels, preferred alert modes, tell which data is priority and can also tell which websites user trusts. This makes the experience more personal and aligned with user needs.

## Non-Technical User Support

This system introduces features like color-coded risk levels, glossary tooltips, and interactive guides to ensure usability for those unfamiliar with cybersecurity concepts.

# **Market Potential**

The cybersecurity market is currently dominated and rules by enterprise level solutions and this leaves a huge gap for intuition and creative alternatives. This allows the birth of such AI-powered cybersecurity assistants that are tailored specifically for individuals and small scale businesses. An in-depth evaluation of three key competitors — **Norton Genie [1], IBM Watson for Cybersecurity [2], and Microsoft Defender + Copilot [3]** — further reveals that DefendAI stands out in several areas, including innovation, accessibility, and functionality.

**Norton Genie** is software offered by NortonLifeLock. It is a simple, free tool designed for individuals and small businesses. Its main strength are detecting phishing attempts through AI-powered analysis of emails and screenshots**. However**, it is very limited in scope and focuses solely on phishing and lackes essential features like dark web scanning, digital footprint tracking, or real-time alerts [1]. In comparison**, DefendAI** provides continuous real-time protection, including real-time alerts, dark web scanning, and personalized recommendations. This makes DefendAI far more comprehensive and dynamic than Norton Genie's model.

**IBM Watson for Cybersecurity is** an enterprise-focused tool that uses advanced AI for threat intelligence, natural language processing, and automated incident response [2]. While it is a powerful solution, its **complexity** makes it impractical and difficult to use for non-professional users and this also requires a dedicated security team to operate and manage. This makes it financially and technically unfeasible for individuals or small businesses. In contrast, **DefendAI** makes cybersecurity easy by offering an easy-to-use interface, educational insights, and AI-driven assistance that empower everyday users, effectively removing the need for specialized technical knowledge or infrastructure.

**Microsoft Defender + Copilot** integrates well with the Microsoft made systems and supports IT teams with threat analytics on which action can be taken [3]. While useful for IT admins, it is **not suitable** for personal users or non-technical audiences and users due to its reliance on the Microsoft environment and its lack of simple, user-friendly guidance. On the other hand, **DefendAI** is and over-all platform which integrates well with every environment and also offers cross-platform support, clear alerts, and visualizations that cater to both personal users and small businesses, regardless of their technical expertise.

## Gaps in Existing Tools

Many existing cybersecurity tools, including **Norton Genie [1], IBM Watson for Cybersecurity [2], and Microsoft Defender + Copilot [3]**, have some limitations and gaps that leave holes in the market:

* Complex and hard to read interfaces that are often not suitable for average users.
* A lack of educational and personalized guidance with alerts and leavs users uncertain on how to respond responsibly.
* Minimal or no digital footprint map and this makes it difficult for users to understand their exposure across different platforms.
* Dark web content is often hidden and only accessible if you pay. This prevent individuals and small businesses from accessing essential protections.
* Alerts are often too confusing or technical and that makes it harder for regular users to understand and respond accordingly.

In contrast, **DefendAI** addresses these gaps by offering a simple, user-friendly interface with educational insights and real-time alerts. It ensures that individuals and small businesses have access to essential cybersecurity features, such as dark web scanning, digital footprint visualization, and proactive protection, all without the need for technical expertise.

## DefendAI Potential

The demand for effective, user-friendly cybersecurity solutions has been rapidly increasing, particularly among individuals and small businesses. In fact, over **60%** of data breach victims in **2023** were individuals or small businesses without dedicated IT staff [4], highlighting a significant market for easy-to-use, proactive cybersecurity tools. Additionally, cybercrime is predicted to cost **$10.5 trillion** annually by 2025 [5] (Cybersecurity Ventures), further emphasizing the need for accessible cybersecurity solutions.

**DefendAI** stands out in this growing market by catering specifically to individuals and small businesses, sectors that are often underserved by existing solutions. The increasing demand for automated, easy-to-use personal security tools, especially in the **EdTech** (Education tecjnology) and freelance sectors, creates a strong opportunity for **DefendAI** to establish a significant user base. The remote work and the growing attack surfaces for everyday users further underscore the need for personal cybersecurity tools like DefendAI, which empowers individuals to take control of their digital safety.

Moreover, DefendAI’s free model with affordable upgrades ensures wide-scale user onboarding while maintaining sustainability. Its cross-platform support and integration potential with browsers, email platforms, and learning systems increase its reach, making it an ideal solution for mass adoption. The focus on usability, automation, and education positions DefendAI as a powerful, accessible tool that will appeal to non-technical users and small teams, further solidifying its potential for widespread adoption.

# **Implementation Plan**

## Tools and Technologies

* **Frontend:** React.js for building the user interface, with CSS for neat and mobile-friendly design.
* **Backend:** Java Scripting to handle user requests and connect everything behind the scenes.
* **AI/ML Engine:** Python with easy AI libraries like TensorFlow and Scikit-learn for detecting threats and giving suggestions.
* **Database:** MongoDB, a simple and flexible tool to store user data and alerts.
* **APIs:** Services like HaveIBeenPwned, VirusTotal, and Flashpoint to check for leaked info and online threats.
* **Deployment & DevOps:** Docker to package everything neatly, GitHub Actions to automate updates, and AWS/Azure to run the system online.

## Development Timeline

|  |  |  |
| --- | --- | --- |
| **Phase** | **TimeFrame** | **Description** |
| Planning and Design | Weeks 1–2 | Finalize outlook , create architecture diagrams and UI mockups |
| |  | | --- | | Core Feature Development |  |  | | --- | |  | | |  | | --- | | Weeks 3–6 |  |  | | --- | |  | | Develop digital footprint tracker, real-time alerts, dashboard UI. |
| AI Model Integration | Weeks 7–8 | Train and test AI for phishing, anomaly detection, recommendations |
| Testing and User Feedback | Week 9 | Perform QA, gather user feedback, refine UI/UX |
| Deployment and Documentation | Week 10 | Launch beta version, complete user manuals and integration guides |

## Team Structure:

* **Project Coordinator:** Fatima Naeem – oversees documentation, progress, and communication.
* **Backend Developer:** Rumaisah Haroon – manages APIs, database, and integration services.
* **AI Developer:** Amna Ali – implements and tests machine learning models.
* **Frontend Designer:** Sarita Sangrez – designs and develops the user interface.

# **Ethical Considerations**

User Privacy and Data Protection:  
DefendAI follows strict privacy principles. All collected data is encrypted using **AES-256 an encryption technique** , and users must provide direct consent for any form of tracking. No sensitive data is stored permanently unless authorized by the users . The system complies with **GDPR**-inspired standards, offering complete transparency and user data control.

AI Transparency and Explainability:  
To promote trust, DefendAI includes short explanations for all alerts. For example, a user will be told, “Your email was found in a known data breach,” with a link to learn more. This approach supports **explainable AI (XAI)**, which is a growing ethical requirement in machine learning systems.[8].

Bias Mitigation and Inclusivity:  
DefendAI is tested on large group of user cases to avoid biased results. It does not use personal attributes such as gender, race, or location in any predictions or alerts. Additionally, the platform includes color-coded alerts, tooltips, and non-technical language to ensure accessibility for all users, regardless of background or education level.

# **References**

[1] NortonLifeLock, *Norton Genie*, [Online]. Available: <https://lifelock.norton.com>/. [Accessed: Apr. 30, 2025].

[2] IBM, *Watson for Cybersecurity*, [Online]. Available: <https://www.ibm.com/security/watson>. [Accessed: Apr. 30, 2025].

[3] Microsoft, *Microsoft Defender and Security Copilot*, [Online]. Available: <https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot> . [Accessed: Apr. 30, 2025].

[4] Verizon,” Data Breach Investigations Report,” 2023. [Online]. Available: <https://www.verizon.com/dbir>. [Accessed: Apr. 30, 2025].

[5] S. Morgan, “Cybercrime to cost the world $10.5 trillion annually by 2025 – Special report: Cyberwarfare in the C-suite,” *Cybersecurity Ventures*, Nov. 13, 2020. [Online]. Available: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/> . [Accessed: Apr. 30, 2025].

[6] Flashpoint, “A Global Pulse on Threat Intelligence: What You Need to Know As 2024 Unfolds,” *Flashpoint*, Mar. 27, 2024. [Online]. Available <https://flashpoint.io/blog/threat-intelligence-report-2024/> . [Accessed: Apr. 30, 2025].

[7] A. Holmes, “A hacker published phone numbers and personal data of 533 million Facebook users online for free,” *Business Insider*, Apr. 3, 2021. [Online]. Available: <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>. [Accessed: Apr. 30, 2025].

[8] DARPA, “Explainable Artificial Intelligence (XAI),” [Online]. Available: https://www.darpa.mil/program/explainable-artificial-intelligence