AI Personality-Driven Social Engineering Auto-Attack Simulator

*Note: Sub-titles are not captured for https://ieeexplore.ieee.org and should not be used

Raghad Lafe
College of Computer Science and Engineering
University of Jeddah
Jeddah, Saudia Arabia
2116345@uj.edu.sa

Atheer Alotaibi
College of Computer Science and Engineering
University of Jeddah
Jeddah, Saudia Arabia
2111266@uj.edu.sa

Sirin Akhamisi
College of Computer Science and Engineering
University of Jeddah
Jeddah, Saudia Arabia
2111517@uj.edu.sa

Joury Alshelwil
College of Computer Science and Engineering
University of Jeddah
Jeddah, Saudia Arabia
2110772@uj.edu.sa

Ghaidaa Alsultan
College of Computer Science and Engineering
University of Jeddah
Jeddah, Saudia Arabia
2116345@uj.edu.sa

Supervisor: Alaa Eshmawi
College of Computer Science and Engineering
University of Jeddah
Jeddah, Saudia Arabia

***Abstract*—In the fast-paced security environment of cyber protection, traditional training methods often fall short in preparing individuals to effectively recognize and counteract social engineering attacks. The AI Personality-Driven Social Engineering Auto-Attack Simulator introduces a novel approach to cybersecurity training by integrating artificial intelligence with the Big Five personality traits model. This project aims to enhance cybersecurity education by providing personalized training simulations that adapt to individual users' personality traits, thereby increasing engagement and effectiveness. Integrating sophisticated AI techniques, the platform simulates realistic social engineering attacks tailored to users' specific psychological profiles. This innovative method not only improves awareness and defensive strategies against social engineering tactics but also paves the way for future advancements in personalized cybersecurity training. The goal of this project is to transform cybersecurity training into a more adaptive, user-centric experience that effectively prepares individuals to navigate and respond to the complexities of real-world cyber threats.**

***Index Terms*—component, formatting, style, styling, insert.**

I. Introduction

A. Objectives

1) Enhancing Security Awareness: One of the crucial aspects of training learners to avoid phishing is to create awareness of the various social engineering attacks and how they take advantage of people's behavior.

Identify applicable funding agency here. If none, delete this.

2) Continuous AI Enhancement: The AI rules development and its periodic tuning will increase the competence and precision of the attack replicas over time.
3) Secure and Ethical Data Use: The security and ethical protocols of all data used will be strictly respected and the user's privacy will be protected.
4) Performance Tracking: Implementing monitoring and analysis solutions to provide users/IT employees with insights into their performance. Users and IT employees will be able to see their successes and failures on their dashboards, enabling them to track their progress and identify areas for improvement.
5) Realistic Simulations: Implementing the most realistic and useful simulation environments that are identical to real social engineering threat conditions

B. Motivation

With the spread of digital technologies in the world, the importance of cybersecurity awareness has become necessary. As social engineering attacks become more sophisticated, the need for specialized training solutions is greater than ever. Our project aims to address this high-priority problem and secure digital infrastructure safely by providing training solutions specifically designed depending on human personality using the best framework/model to enable individuals and organizations to effectively combat cyber threats.

C. Key Features

1) Customized learning path: Provides tailored learning experiences based on individual user profiles and performance.
2) Interactive training: engages users with interactive sessions that require active decision-making, helping to improve their reaction times and decision-making skills under pressure.
3) Personality Assessments: Conduct in-depth personality assessments to understand individual traits and behaviors.
4) Simulated Social Engineering Attacks: Offers realistic simulations of social engineering attacks, each scenario is designed to mirror real-world tactics used by cybercriminals, enhancing the training's practical relevance.

II. Background and State of the Art [1]

A. Understanding Social Engineering Attacks

Social engineering attempts are a broad range of unwelcome operations carried out through human relationships. They rely on psychological manipulation to manipulate users into committing security mistakes or disclosing sensitive data. Social engineering attacks are especially harmful since they are based on human error rather than software and operating system vulnerabilities.

Social engineering attacks have existed since the earliest days of human communication and manipulation techniques. It should be added that social engineering attacks were not common until the advent of the Internet and digital communication technologies. Thus, this type of information security threat cannot be dated. However, it is since the 1990s and the launch of the Internet that visiting the hole became more accessible from the technical side [2].

1) Historical background of the social engineering attacks: The first social engineering attacks in the digital era that are documented began in the 1970s and were associated with the activities of Kevin Mitnick, considered one of the most well-known hackers of all time. Kevin hacked computer networks primarily using social engineering, deceiving people into telling him passwords and confidential information. Its first hacking activities dates back to the late 1970s, and it extended into the 1980s. Such high-profile cases brought much attention to social engineering as a powerful weapon in a hacker's arsenal.

Social engineering decades thereafter, paralleled by technological developments, became more and more sophisticated in the utilization of certain individuals' and organizations' digital and social behavior. The COVID-19 pandemic has altered the way people operate, deploying solutions and technologies that have left them more exposed. Working remotely, the BYOD (bring your own device) policies and an increase in the use of video conferencing technologies provided additional potential vectors to exploit. As a result, knowledge workers have become more susceptible to spear-phishing attacks using zero-day exploits due to a lack of evidence that can confirm requests and limited trust in digital communication paths.

2) The Four Stages of a Social Engineering Attack: [3]:

1) Information gathering: as the name indicates the attacker collects as much information as possible on the target before the actual attack. For example, one may go through several online sites, such as LinkedIn, to discover the company's overall structure and find the most susceptible employee with high access rights. Many enterprises are unaware of the breadth of information an individual can acquire due to an individual's social activities and publications, including hobbies, employment positions, project details, company ties, acquaintances, and public event participation. Depending on the individual, this preparatory phase might take several weeks as the potential victim is carefully checked out [4].
2) Engagement: It is an attack stage when the potential attacker initiates contact with the victim. At this point, it is important that the initial connection does not seem unfriendly since detection can affect the entire operation. If the attempt fails, the attacker may continue for some time before trying another method or, if necessary, establishing contact with another individual. Phishing is frequently utilized during this stage to gain access to one's account [4].
3) Execution: After gaining access, the attacker will be able to control the victim party. Additional activities may be necessary at this level, as is evident from certain circumstances, such as the Uber data breach. When the scammer has accessed the network, terrorists can obtain information, send malware files, vandalize the system, or establish surveillance for later strikes [4].
4) Conclusion: This is the final stage. When contact is made with the individual, attackers must end contact and minimize the possible client's understanding of the incident. This level is characterized by a suspicious party's ability to properly recognize invasion and notify the competent authorities or organization members [4].

3) Social engineering attack vectors: There's a way to take advantage of human interaction and behavior to bypass security measures such as:

1) Tailgating: When attackers follow an authorized and legitimate person to enter a restricted area, and that is by asking them to hold the door or enter after them quickly. This method is becoming more effective since there are policies and regulations for certain activities

like smoking, which is an opportunity to blend with them [5].
2) Impersonating: When the attacker pretends to be someone else to gain access and privileges, and this includes piggybacking, which is similar to tailgating, but the attacker is getting explicit permission from the legitimate access holder by pretending to be a legitimate person who needs temporary access.
3) Eavesdropping: Listening in an open or public space to private conversations such as phone calls and emails in the intention of getting sensitive information [6].
4) Shoulder surfing: Watching from the back of someone to get sensitive information such as passwords.
5) Dumpster Diving: Searching in the trash for documents and papers and hardware such as USB that may contain important information. Reverse social engineering is when the attacker makes direct contact with the victim and creates a scenario that presents the attacker as a legitimate, trustworthy person and manipulates the victim into voluntarily providing information or access.

4) Examples of Social Engineering Mechanisms and Techniques [7], [8]: Social engineering uses many deceptive mechanisms that take advantage of human psychology. here are common mechanisms and techniques used:

1) **Exploitation of trust:** Building trust is at the very center of social engineering. Scammers apply this by gaining the trust of their victims, whom they then defraud by pretending to be a trusted colleague, an authoritative or respected person, a representative of a reliable company, or another type of trusted source.
2) **Fear and Urgency:** Technique that creates a sense of urgency, forcing the victim to respond right away without having time to question the request's validity. This might include alarming notifications on security breaches, legal action threats, or fictitious deadlines.
3) **Pretexting:** This is the act of making a false scenario (pretext) to engage the target in such a way that the target may willingly reveal information or perform certain acts. For instance, the attacker can pretend to be an IT staff member who requires access to certain data in the routine checks for security [2], [5].
4) **Phishing and Spear Phishing:** This is the practice through which cybercriminals send messages that seem to originate from known, trusted, or reputable sources with the intention of getting personal data, financial information, or login credentials from the recipient of the message. Spear phishing represents an even more individual attack targeting just a few specific individuals.
5) **Whaling:** This is the type of phishing targeting VIPs, such as C-level executives, politicians, or celebrities. Whaling attacks are more personalized with the appropriate scenario to the role or position of the victim and usually involve making it look like it has been communicated directly to them from the CEO or another high official.
6) **Baiting:** Similar to phishing, baiting is yet another trick that lures the victim with something attractive in return for his sensitive data or access credentials. This usually ranges from anything free, such as free music downloads, free movies, or USB sticks with a flashy title on them [2], [5].
7) **Quid pro quo:** Provides something in exchange for information. This could involve a gift given to a researcher to complete survey questions—those surveys designed to gather sensitive personal or organizational information [2], [5].

5) Targeting Individuals and Organizations: In social engineering attacks, attackers target both individuals and organizations with specific characteristics. Attackers focus on specific assets and information they aim to acquire.

Targeting Individuals

When targeting an individual, offenders are usually interested in getting direct access to one's financial assets, sensitive personal identification information, or credentials which can possibly give access to a system or service without permission. This can be done in several ways:

- Financial information: Attackers could try to get credit card and/or bank account numbers or other financial information to perform transactions and/or transfers without the owner's authorization.
- Personal Identification Information: Social security numbers, driver's license numbers, and identification numbers from personal identification can all be used in the theft of one's identity. These then may be reported as new accounts opened, credit obtained, or fraud committed in one's name.
- Access Credentials: The access credentials, such as passwords and usernames used during this issuance, may give attackers direct doors to private accounts, corporate systems, and secure networks, leading to further exploitation.

This might also be the case where the person is probably targeted due to his role in a company or perceived wealth or just to show that they were vulnerable and attacked in the past. Social media and public records give attackers everything they need to effectively tailor their attacks.

Targeting Organizations

Social engineering attacks are motivated by opportunities to extract money or any other advantage from humans,

organizations, or systems. The organizations that boast huge data repositories along with financial resources, get a gainful target for social engineering attacks. The goals here are often far-reaching from just short-term financial gain:

- Customer Information: Sensitive customer information including personal information, payment information, and purchase history, might be stolen.
- Intellectual Property: Theft of trade secrets, proprietary technology, and other intellectual assets for competitive advantage or ransom.
- Employee Vulnerability: Employees are often the weak point in a system or network and can easily fall victim to various entry points. Social engineering, such as phishing or pretexting, allows an attacker to use human fallibility against the technical security of a system. They are a target not only for the vast amount of exploitable data they hold but also for their potential as a gateway into even bigger networks. For example, in a supply chain attack, compromise at one single vendor may progress to spread to all connected organizations.

B. Understanding the Big Five Personality Traits Model [9]

The individual personality reflects what makes each person special and different. The Big Five personality trait framework is one of the most widely accepted and often studied personality models and it is used not only to understand the basic traits but also to evaluate various aspects of personality. This model proposes that human personality can be described in terms of five broad dimensions: The "Big 5" personality traits defined by the OCEAN model. There are some people who show more of this Big Five trait, while others show less of these characteristic traits [10].

- Openness is a characteristic of personality, which shows an intellectual curiosity, creativity, and readiness to do something new.
- Conscientiousness refers to a person's inclination to be organized, self-disciplined, and directed toward achieving their set goals.
- Extroverts demonstrate their talking and excited traits, and they are energetic and love to find themselves in the company of other people.
- Agreeableness is a person's tendency to be compassionate, cooperative, and friendly towards others. People high in agreeableness are willing to get along with others, collaborate, and trust others.
- Neuroticism refers to the tendency to experience negative emotions and emotional instability. People high in neuroticism are more likely to experience feelings such as anxiety, anger, frustration, and sadness.

There is a significant amount of research that has found that both genetic and environmental factors affect individual personalities. Realizing the Big Five framework helps to enrich the insight into how personality affects our thoughts, emotions, and behavior patterns across diverse fields of life.

1) Historical Background of the Big Five Personality Model: The beginning of the Big Five personality model can be traced back to the early 20th century. The claim that a human personality is a small number of broad dimensions is the result of the early works of trait theorists like Gordon Allport, Raymond Cattell, and Hans Eysenck among others [1].

In the 1930s, Allport and Odbert identified about 18,000 personality-reflected words in the English language, which only proves the variety of individual differences that determine human personality. Based on this, he later developed the model of 16 primary personality factors that became the foundation of the renowned Sixteen Personality Factor Questionnaire [3].

Whilst Eysenck's research in the 1950s and 1960s, was aimed at identifying the fundamental dimensions of personality, it resulted in a three-factor model consisting of Extraversion, Neuroticism, and Psychoticism [7]. The Modern Big Five model which features Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism, was proposed in the 1980s' by researchers, including Lewis Goldberg, Paul Costa, and Robert McCrae. These researchers used factor-analytic tools to conduct a regular analysis of a massive collection of personality traits and to reduce them into five broad, well-grounded, and empirically based traits [8], [11]. The consistency and cross-cultural replicability of the Big Five model have been proven to be high, and hence it became one of the most accepted and influential frameworks around personality psychology. The Big Five traits have been associated with biological underpinnings including appreciable heritability, brain regions, and neurotransmitter systems.

This integrative theory of personality has given a common vocabulary to personality research and has been utilized in a wide variety of fields. The ongoing improvement and application of the Big Five framework has significantly increased our understanding of the multifaceted and complex human personality.

2) Detailed Explanation of the Big Five Personality Model:

1) Openness to Experience: People who are highly open-minded typically find learning adventures, have a creative pursuit, and get pleasure from the arts as well as in meeting newcomers. For openness, the common traits include imagination, insight, originality as well as variety, inventiveness, preference for variety, cleverness, ingenuity, curiosity, insight, intellect, and complexity/depth [12].
2) Conscientiousness: Conscientious people often distin-

guish themselves at school and careers, can lead, exhibit perseverance, and prescribe thinking in whatever they do. Common traits include comprising persistence, sales drive, diligence, discipline, consistency, dependability, discipline, productivity, resourcefulness, diligence, and planning [12].

3) Extraversion: Extraversion concerns where an individual draws their energy from and how they interact with others (Leibowitz, 2016). Some of the traits that come with extraversion are sociability, eagerness, merriness, outward characteristics, energy, speaking a language properly, friendliness, affection, inclination, and confidence in social interactions [12].
4) Agreeableness: Those high in agreeableness usually are liked, trusted, and simply concerned with what other people are feeling and thinking. Such people are naturally very fond of and kind to others. The traits that come under Agreeableness include altruism, trust, modesty, humility, patience, tolerance, tact, politeness, kindness, loyalty, unselfishness, helpfulness, sensitivity, amicability, cheerfulness, and consideration [12].
5) Neuroticism: Individuals with neurotic personalities are most of the time afflicted by anxiety, sadness, worry, low self-esteem, and instability in emotions. They can easily be irritated or get angry very easily. Personality is usually perceived as exhibiting the following traits: awkwardness, sadness, bad mood, jealousy, quarrelsomeness, fear, nervousness, anxiety, timidness, wariness, self-blame, lack of confidence, insecurity, instability, and hypersensitivity [12].

3) The Big Five Personality Traits and Their Impact on Security Threats Susceptibility Susceptibility: The big five personality traits model (openness, conscientiousness, extraversion, agreeableness, neuroticism) has been shown in multiple studies to have an impact on how individuals will react or respond to a social engineering attack. Understanding the relationship between personality traits and their proneness to different social engineering patterns or attacks could provide a real benefit to cybersecurity training programs like our project.

1) Openness to Experience: People high on openness regularly feel the urge to look for something new, are artistic, vivid, and easily learn and accept new notions. This characteristic has been associated with the increased probability of being a social engineering victim. Openness enables people to trust and react positively to extraordinary and unconventional ideas, thus becoming natural victims of deceiving others [13]. Here the psychological principle of curiosity may be used by cybercriminals to introduce an unexpected scenario that would attract the victim's attention and make them respond by divulging their personal information.
2) Conscientiousness: Conscientious individuals usually have planned built-in habits, they are normally observant, and they tend to follow all the rules. It is because social engineering attacks are less probable for this type of people. People with a sense of duty are more inclined to observe security processes, verify the legitimacy of messages, and be cautious about disclosing sensitive information [10]. Cybercriminals could find it even more challenging to trick a person with high conscientiousness, who would be less likely to distract his/her mind from the norms and the principles he/she has established regarding cyber security.
3) Extraversion: Typically, extroverts can be described as sociable, bold, and highly involved in communication. It has been found that this tendency increases the chance of being the victim of social engineering scams. Extraverts could be those people who may be able to freely interact with strangers; hence, they may be susceptible to deceptive strategies by social engineers [13]. Cyber attackers can take advantage of this personality trait by appearing to be friendly and reliable persons and slowly establishing relationships with their victims.
4) Agreeableness: The agreeableness feature of personality usually leads to somebody being sincere, helpful, and ready to help. It involves the witty predators in their ability to manipulate others into fraudulent behaviors that may be tricked into revealing sensitive information, generating trust to steal bank details or even a friend's own heirloom. The agreeable individuals may even accede to the requests, although they seem to be odd or inconsistent [6]. Criminals could take advantage of this characteristic by sending emails with the aim of sending the victim into an emotional outburst of cooperation or help.
5) Neuroticism: Neurotic people usually tend to be nervous, emotionally, and financially unstable. Such a trait has been associated with a higher chance of becoming affected person of social engineering attacks. People having a high neuroticism score may be more susceptible to manipulation based on fear of negative consequences, urgency, and threats [13]. Cybercriminals are in a good position of power here as they can creatively use instigative trouble for people who depend on their judgmental skills and can cause them to react rashly in a situation that puts their security at risk.

In the final analysis, we can conclude that the Big Five personality traits play a major role in how people behave when confronted with social engineering attacks. The same personality traits, like openness, extraversion, agreeableness, and neuroticism increase your chance of getting caught

in a social engineering attack, while conscientiousness is linked to a lowered vulnerability to such tactics. Awareness and understanding of those personal characteristics make us stronger in fighting cybersecurity offenses, which are based on social engineering. That's our project aim.

III. Related Work (Literature Review)

Study 1: Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities, and Attack Methods [12]

The "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities, and Attack Methods" and our project the "AI Personality-Driven Social Engineering Auto-Attack Simulator" both concentrate on understanding and mitigating social engineering, with the first study focusing on exploring psychological social engineering in addition [14].

The first study goes into detail about the mechanisms that attackers use to exploit human vulnerabilities and explains human vulnerabilities, social influence, and methods of exploitation, as these mechanisms play an important role in emotions, trust, deception, and decision-making, while our project "Automatic attack simulator based on social engineering based on artificial intelligence" focuses on training and cybersecurity awareness through simulating attacks, analyzing user interactions, and providing solutions and suggestions to these characters to enhance defense capabilities [14].

The difference between our project and this study lies in how the user interacts, as the goal of the first study is to build the basics of social engineering attacks, while our project uses artificial intelligence to provide an interactive training experience to enhance users' education about social engineering attacks.

In our project, we are combining artificial intelligence and the Big Five traits with the art of social engineering from this study to generate an individual solution. Our contribution does not only include artificial intelligence to recommend attack scenarios that simulate attacks on the ground, but it also learns and adapts from human interactions and how people think and interact, which makes defense against attack more effective and intelligent. Integrating artificial intelligence and the Big Five traits makes it easier to understand, and implement these defenses, and make a significant improvement in how we prepare for and respond to SE cyber threats.

Study 2: Automated Recognition System for SE Attacks [12]

The paper presents an automated system for social engineering (SE) attack detection in chat communications of the enterprise. It elaborates on factors making such attacks possible and emanating from characteristics of personality, influence, deception, and patterns of communication. The present research aims at security professionals, enterprises, and academicians for defense against the social engineering (SE) threat to technologies, psychology, and linguistics [15].

The architecture integrates subsystems to recognize these elements in the bud and, in that way, become capable of fighting the ever-growing threat being caused by the misuse of electronic communication. Modernization allows for the best identification of these threats, and, consequently, potential SE threats are identified, making the cybersecurity defenses improve [15].

The system employs natural language processing, machine learning, and psychological analysis to automatically detect SE attackers in chat communications. This development has now led to the design of an automated detection system of SE threats that would help in further strengthening cybersecurity through the detection of such sophisticated tactics [15].

This paper challenge is that of the detection of SE attacks, whereby much focus is laid on the insufficient automated detection offered by the systems for the threats posed through chat. This then brings in the need for a system that would substantially reduce the success of the SE attacks by a bigger percentage, thus possibly altering the current framework for both secure communication and organizational cybersecurity in the field [15].

Our project contributes to understanding the role of the Big Five personality traits in determining susceptibility towards social engineering attacks. It brings into light how the openness, conscientiousness, extraversion, agreeableness, and neuroticism of the person add up to make the person more vulnerable to such attacks.

This project shall relate an interdisciplinary approach through this study in terms of integrating psychological insights into the analysis of the social engineering vulnerabilities, as a way of contributing toward an understanding in depth of the human factors that attribute to the effectiveness of the social engineering strategy.

Study 3: Impact of Personality Traits on SE Attacks [13]

This study by Brian Cusack and Kemi Adedokun. This study set an experiment to study the Big Five traits and figure out which traits are susceptible to social engineering attacks. The researchers found that users with high scores in agreeableness and extroversion traits are more susceptible to social engineering attacks than other traits. This paper also focused on attributes that affect user actions and identified moderating variables that included emotional state, the environment, and motivations. In our project, we used the impact of different types of social engineering attacks on different personality trait types. Our project is to identify types of personality traits that automatically simulate social engineering attacks tolerated to this type [16].

Study 4: The Social Engineering Personality Framework [6]

The Social Engineering Personality Framework (SEPF) investigated how personality traits influence vulnerability to

social engineering attacks and vulnerabilities in ICT security. In contrast to studies that focus solely on technical defenses, the social engineering personality framework integrates psychological and cognitive principles and emphasizes individuals' susceptibility to manipulation in the technological world. By linking individual characteristics and personal vulnerabilities to social engineering, the psychosocial personality framework provides theoretical insights and practical security measures to facilitate individual risk mitigation strategies in the technical community [9].

Overall, this research contributes to the development of knowledge in the field of social engineering by identifying complex relationships between personal traits and managerial capabilities, thus increasing the resilience of organizations to social attacks in a socio-technical environment. On other hand Our project aims to design a social engineering tool supported by artificial intelligence to simulate the behavior of attackers and hackers and improve technical capabilities in the real digital world. The tool provides insight into the evolution of human behavior through the generation and execution of realistic social threats and serves as a testing ground for security measures in different scenarios.

Study 5: Harnessing LLMs to Simulate Human Responses to SE Attacks [14]

"Harnessing Large Language Models to Simulate Realistic Human Responses to Social Engineering Attacks: A Case Study" published by Asfour and Murillo address the issue of exploiting human vulnerabilities in social engineering attacks. This work uses the capabilities of large language models (LLMs) to mimic human responses to simulated social engineering attacks. This study aims to use simulated human responses to social engineering attacks in order to understand human behavior and identify personality traits that are most vulnerable to these attacks based on the Big Five personality traits [17].

While our project is using artificial intelligence and the Big Five traits model to Recommend personalized attacks for each individual based on their traits. Our website application will Recommend the attacks automatically and periodically. And it aims to enhance cybersecurity training and awareness within organizations. The study proposed by Asfour and Murillo provides insights on common human traits that are most vulnerable to social engineering attacks and recommendations for mitigating risks. While our project created a website application that provides users with realistic training experiences tailored to individual behaviors to identify and safeguard against evolving cyber threats.

Study 6: Implementing a Real-World Phishing Ex world Phishing Exercise to Teach Social Engineering [15]

"Gophish: Implementing a Real-World Phishing Exercise" published by Luse and Burkman's worked on illustrating a practical educational approach to social engineering threats that expose human behavior to bypass traditional security measures. This paper describes a project where students executed a phishing exercise with a real-world company to understand the multifaceted aspects of social engineering. The study used GoPhish tool which is an open-source phishing framework that allows companies to manually create and execute phishing campaigns in a controlled environment, by manually simulating a real-world phishing attack [18].

While our project introduces a personalized automatic attack system that simulates social engineering attacks in a controlled environment utilizing artificial intelligence with the Five Big treats model. They both aim to test an organization's security awareness and readiness to withstand such attacks. Additionally, in our project, our software will provide education as well.

They both provide monitoring capabilities that allow Security Professionals to track various metrics related to their phishing attacks, such as email opens, link clicks, credential capture, attachment downloads, custom metrics, and reporting. Moreover, in our project, the attack details collected form the employees' devices and transfer to the IT department over the network to monitors employee responses identify the relationship between their responses and personalities and use these data to simulate a more precise social engineering attack.

* Real-world Application – In the table I refers to how the work can be directly applied or integrated into actual cybersecurity practices, training programs, and enterprise security measures & evaluates the degree to which the research, frameworks, or solutions can be directly leveraged by end-users, such as cybersecurity professionals, educators, and enterprise security teams, to enhance their security posture and improve user preparedness against social engineering attacks.

IV. Methodology

A. System Architecture and Platform Development

- System Overview
  - Developing a web-based platform that trains against SE attacks based on Personality Traits. First, the web application will assess the user's personality traits using the Big Five personality model through a specialized API. The results will then be saved in a database. Based on these results, advanced AI techniques will recommend the most suitable attack scenarios tailored to the user's personality traits to

TABLE I
COMPARISON OF STUDIES WITH OUR PROJECT (PART 1)

Study 6	Study 5	Study 4	Study 3	Study 2	Study 1	Our Project	Criteria
Practical, hands-on experience with phishing simulations.	Using LLMs to simulate human-based responses on SE attacks.	Theoretical model connecting Big 5 personality traits with susceptibility to SE.	Qualitative analysis of personality and SE vulnerability.	Automated system for detecting chat-based SE.	Theoretical, psychological analysis of SE.	AI-driven, user-personalized simulations to a different SE attacks.	**Approach**
GoPhish framework simulating real-world phishing attacks.	First to simulate human-based responses using LLMs.	Proposes a framework for understanding how personality traits influence SE attack susceptibility.	Links specific personality traits to SE susceptibility.	Focuses on automation in recognizing chat-based SE attacks.	Dives deep into psychological tactics used in SE.	Our auto-attack simulation is using AI and Big 5 model to create personalized SE attacks training path based on the personality.	**Creativity**
Engages users interactively in phishing attacks.	No user interaction, only using LLMs to imitate possible user's responses.	Provides a theoretical framework without direct user interaction.	No direct user interaction.	No direct user's interaction, Passive protection through automated detection.	Theoretical perspective with no direct user interaction.	Engages users interactively with personalized training in various security awareness & (SE) attacks.	**User Interaction**
Cybersecurity training providers, Corporate security awareness program managers, Cybersecurity students and entry-level professionals	Cybersecurity tool developers, Researchers in artificial intelligence and machine learning, Penetration testing and red team professionals	Security researchers and analysts, Cybersecurity consultants and advisors, Behavioral scientists	Cybersecurity trainers and educators, Human factors researchers, Security awareness program managers	Enterprise security teams, IT professionals responsible for implementing security solutions, Cybersecurity solution providers	Cybersecurity researchers, Behavioral psychologists, Security practitioners interested in psychological underpinnings of social engineering	Cybersecurity trainers, Everyone above age of 10, Cybersecurity researchers and practitioners, Policymakers and industry bodies	**Target Audience**

simulate personalized SE attacks. The web application will then display these tailored attack scenarios to the users. Finally, a dashboard will provide an overview of user interactions, performance metrics, and personalized feedback [19], [20].

- Backend Development:
  - Server Setup: The web application is hosted locally using a Node.js server, handling backend processes and AI-related computations.
  - Database Management: Using MySQL with MAMP for efficient and structured storage of user profiles, personality test results, simulation outcomes, and the predefined scenarios used in the training.
  - API Integration: Incorporating RESTful APIs for seamless communication between the frontend, the Sentino API, and the Gemini system. The Sentino API analyzes user personality traits using the Big Five model, providing psychological profiles that feed into the Gemini system, which generates personalized social engineering attack scenarios. Integration is achieved via Axios, with secure API key authentication and efficient data handling. Real-time interaction ensures an intuitive user experience, connecting front-end inputs with backend insights.
- Frontend Development:
  - Web Application Framework: We will Utilize frameworks like Angular or React to create a responsive user interface that adjusts to various devices and screen sizes.
  - User Interaction Design: Design interactive elements for users to easily take personality tests, view simulated attack scenarios, and receive personalized feedback.

TABLE II
COMPARISON OF STUDIES WITH OUR PROJECT (PART 2)

Study 6	Study 5	Study 4	Study 3	Study 2	Study 1	Our Project	Criteria
High: Tailors phishing simulations to organization-specific themes, industry-specific content, behavioral insights, varied attack vectors, interactive and dynamic content, as well as localized and cultural considerations.	Moderate: Simulates specific traits' responses.	Low: Theoretical framework offers general guidance without specific customization.	Moderate: Suggests custom strategies based on personality.	Low: Automated, with limited customization.	Low: Offers general psychological insights.	Extremely High: Our project incorporates AI and the Big 5 personality model in the process of creating highly personalized social engineering attack training path. Simulating the attacks in a manner that takes advantage of the particular vulnerabilities of the personality of the user.	**Customization**
Direct: implemented for training program.	Direct: help in enhance social engineering penetration testing, red team exercises, and security awareness training programs.	Indirect: Guides the development of detection, mitigation, and prevention strategies.	Indirect: Help in inform training content development.	Direct: Can be integrated into enterprise security systems.	Indirect: Enhances understanding for better defense strategies.	Direct: Continuously conduct attacks tailored to the individual's personality profile.	**Real-world Application**
High: enhancing individual learning experiences to influencing educational methodologies, professional practices, and ethical discussions in the wider field of cybersecurity.	High: increase the effectiveness of security testing by understanding each personality's potential response and use the data for training purposes.	Moderate: Helps in tailoring defense strategies but requires further empirical research for direct application.	Moderate: Offers insights for more effective training programs.	High: Could significantly lower enterprise vulnerability to SE.	Moderate: Improves theoretical understanding of SE defenses.	High: by providing highly personalized, adaptive simulations that significantly enhance individual and organizational resilience against a wide range of social engineering threats.	**Potential-benefit**

B. AI Mode Development Using Gemini AI

- Overview: The AI Personality-Driven Social Engineering Auto-Attack Simulator leverages Gemini AI to deliver personalized social engineering attack scenarios. This section of the methodology explains how Gemini AI dynamically generates and selects scenarios tailored to users' personality traits, based on their assessments and behavioral patterns, using advanced generative capabilities [19].
- Reason for Implementation:
  - Adaptability: Gemini AI's generative capabilities allow it to create and adapt scenarios dynamically based on users' profiles and performance, providing more personalized and realistic simulations.
  - Efficiency with Limited Datasets: Instead of relying on a predefined rule set, Gemini AI generates scenarios using its trained model, reducing dependency on large, detailed datasets.
  - Scalability: The AI can easily accommodate new traits, scenarios, and training strategies, making it flexible and scalable for future developments.
  - Dynamic Recommendations: Gemini AI uses personality assessment data and performance history to recommend scenarios that align with user vulnerabilities and training needs.
- Development Strategy:
  1) Personality Assessment and Data Storage:
     - Users complete the Big Five personality assessment via the Sentino API during signup [20].
     - Results, including scores for Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism, are stored in the database along-

side the scenarios.

2) Scenario Recommendation with Gemini AI:
   - Gemini AI uses a detailed prompt, incorporating user personality traits, performance history, and available scenarios from the database.]
   - The AI evaluates the user's highest-scoring traits and matches them with scenarios specifically designed to target vulnerabilities related to those traits.

- Integration with User Profiles:
  - Database-Driven Scenarios: All available training scenarios are pre-defined and stored in the database. Each scenario includes a description, objectives, and the vulnerabilities it targets.
  - AI-Based Matching: Gemini AI ensures scenarios are not repeated by tracking completed and failed scenarios in the database, adapting recommendations based on user progress.
- Enhanced AI functionality:
  - Adaptive Learning: Gemini AI adjusts recommendations based on user performance. If a user successfully completes scenarios targeting one vulnerability multiple times, the AI shifts focus to other vulnerabilities to ensure comprehensive training.
  - Feedback and Justification: After a recommendation, Gemini AI provides users with detailed feedback explaining why the scenario was chosen based on their personality profile and training needs.

C. Simulation Scenarios Development

- Overview of Scenario Development Methods:

1) Scenario-based Learning: We implement scenario-based learning where users engage with a collection of emails or messages and decide whether they are phishing attacks or genuine communications. This method helps users practice identifying potential phishing attacks through direct interaction with the simulated content.
2) Interactive Quizzes and Challenges: The training includes interactive elements where users act in roles that require them to decide on responses to simulated communications, such as an email purportedly from their bank asking for identification. This method enhances decision-making skills under scenarios that mimic real life.
3) Gamification: By incorporating elements such as timed quizzes, leaderboards, and rewards for correct answers, we transform the learning process into a more engaging and competitive experience. This approach motivates users to actively participate and improves their ability to quickly identify deceptive intentions.
4) Role-playing: Users engage in role-playing exercises where they must react to live interactions, such as phone calls (vishing) or direct messages, making critical decisions in real-time. This method is particularly effective in training users to handle direct social engineering attempts.
5) Simulated Environments: We will create controlled, immersive environments that replicate real-world settings, such as fake social networks or company intranets. These environments are designed with built-in indicators of simulation to maintain an educational focus while providing realistic practice scenarios.

- Alignment with Personality Traits: Understanding the influence of personality traits on susceptibility to social engineering is crucial for tailoring scenarios that are most effective for individual training needs:

1) **Openness**
   People high in openness are curious, have appreciation for art, imaginative, enjoy variety, and are open to new experiences and are more susceptible to attacks that offer access to exclusive or novel information or opportunities so the most effective attack for this personality is:
   Pretexting: Creating a fabricated scenario or identity to gain access to personal information. For example, pretending to be a researcher inviting users to join an exclusive study or beta test of a new, innovative product.
   Baiting: Offering something enticing to exploit someone's curiosity or desire for novelty. This could be a free download of "cutting-edge" software or access to a "leaked" innovative technology preview [21].
2) **Conscientiousness** People high in Conscientiousness are organized, detail-oriented, and cautious, demonstrating a strong commitment to order and due to their sense of duty and responsibility, these individuals are particularly susceptible to attacks that mimic business-related communications or urgent tasks that require immediate attention so the most effective attack for this personality is: **impersonation:** Taking on the identity of someone in authority or a position of trust, like a fake audit official or compliance officer, to extract sensitive information or prompt action that bypasses normal security procedures [21].
3) **Extraversion** outgoing, energetic, and sociable individuals who enjoy being around people. They might be more vulnerable to attacks that involve social interaction or events that promise networking opportunities so

the most effective attack for this personality is: Quid Pro Quo: Offering a service or assistance in exchange for information or access. For instance, an attacker might offer to connect extroverted individuals to a valuable network in return for confidential data [21].

4) **Agreeableness** People with high Agreeableness are cooperative, sympathetic, and caring. They are often very trusting, prefer to avoid conflict, are more susceptible to attacks that exploit individuals' willingness to help, as their trusting nature makes them easy targets so the most effective attack for this personality is:
   Charity Fraud: Misusing the trust and kind nature of agreeable individuals by soliciting contributions for fake charities, especially during times of crisis or after natural disasters.
   Consensus or Social Proof: Using fake endorsements and the apparent participation of many people ("Everyone is doing it") to convince agreeable individuals to partake in seemingly benign activities that compromise security [21].
5) **Neuroticism** People who are high in neuroticism tend to experience mood swings, anxiety, irritability, and sadness and they might react impulsively to certain stressful situations which makes them more vulnerable to attacks that create a sense of urgency or panic so the most effective attack for this personality is:
   Urgency Tactics: Utilizing messages that create a sense of panic or urgency, such as fake notices about locked accounts or legal actions, exploiting the neurotic trait's sensitivity to stress and potential overreaction.
   Scareware: Bombarding users with fake warnings and alerts to frighten them into believing their system is infected with malware, urging them to install fake security software [21].

V. Proposed solution overview

The AI Personality-Driven Social Engineering Auto-Attack Simulator takes an innovative approach to cybersecurity training. It combines the power of artificial intelligence with insights from personality psychology to provide a highly personalized and effective training experience.

The core idea is to leverage the famous "Big Five" personality model - openness, conscientiousness, extraversion, agreeableness, and neuroticism - to identify each individual's potential vulnerabilities to social engineering attacks. After all, we all have different personalities that may make us susceptible to different kinds of psychological manipulation tactics.

Here's how it works: When you first sign up for the training platform, you'll take a personality assessment that evaluates where you fall on the spectrum of those Big Five traits. The results from this assessment are then used to create a unique user profile for you.

Your personalized user profile gets fed into an AI system that has been programmed with rules mapping different personality profiles to specific types of social engineering attack scenarios stored in a database.

So if your profile shows you scoring high on neuroticism for example, indicating you're more prone to anxiety and emotional urgency, the AI might retrieve and serve up simulations from the database involving phishing scams trying to spark panic. Or if you're characterized as highly open and curious, it may pull baiting attack scenarios tempting you with exclusive access.

Using the distinct psychological fingerprint from your user profile, the AI essentially crafts a personalized curriculum of challenge scenarios tailored to your potential blind spots when it comes to social engineering threats. These simulations retrieved from the database are incredibly realistic and interactive - you'll respond to fake emails/calls/websites just as you would in the real world.

As you navigate the training, the system tracks your decisions and performance, providing helpful feedback along the way. And thanks to machine learning, it actually adapts and evolves the simulations over time based on your strengths and weaknesses, continually keeping you on your toes.

The key advantage is taking a style of training tailored not just to general principles, but to your unique psychological makeup. By experiencing hyper-customized attack simulations that apply maximum "psychological pressure" on your personal vulnerabilities, you become exponentially better prepared to identify and shut down social engineering in the real world before falling victim.

It's a highly innovative solution fusing cutting-edge AI with behavioral science - helping cybersecurity awareness training feel more personal, intuitive, and ultimately, effective in reducing risk across organizations.

VI. Implementation

Programming Language and Tools

1) Visual Studio code The development environment for the project, providing an integrated platform for writing and debugging code for both the frontend and backend components.
2) sentino API [20] The project leverages the Sentino API to process user responses from the Big Five personality test and generate personality trait scores. The following steps detail how the API is integrated into the system:
   - Selecting the Inventory The Big Five inventory is chosen as the framework for assessing personality traits, as it is widely recognized for its psychological validity.

- Sending User Responses After the user completes the personality test, their answers are compiled and sent to the Sentino API using the Score Text endpoint.
  - The API processes the responses by splitting the text into sentences.
  - Each sentence is labeled with a corresponding topic related to the Big Five traits.
- Processing and Results The Sentino API analyzes the data and returns detailed results for each of the Big Five personality traits. Each result includes:
  - **Quantile:** A percentile rank indicating the trait level compared to a reference group.
  - **Score:** A numerical score representing the trait's intensity, which is the primary value used in the project.
  - **Confidence and Confidence Text:** Indicators of the reliability of the analysis.
- Using the Results For this project, only the Score for each trait (e.g., openness, conscientiousness, extraversion, agreeableness, and neuroticism) is extracted from the API response. These scores are then used by the AI engine to simulate personalized social engineering attack scenarios tailored to the user's psychological profile.

3) **Gemini API [19]** In the project, the Gemini API is utilized to recommend cybersecurity training scenarios tailored to the user's personality profile. Here's how it works:
   a) Initializing the Gemini API
      - The Gemini API is initialized using the API key stored in environment variables (process.env.GEMINI_API_KEY.
      - A generative model, gemini-pro, is selected to handle the recommendation process.
   b) Filtering Scenarios
      - A predefined list of scenarios is created, each describing a specific social engineering attack.
      - The system filters out scenarios that the user has already completed by comparing them with a list of completed Scenarios.
   c) Creating a Prompt for the API
      i) A detailed prompt is dynamically generated based on:
         - The user's Big Five personality traits scores (e.g., Openness, Conscientiousness).
         - Insights about how these traits relate to specific vulnerabilities (e.g., high Openness is linked to susceptibility to phishing).
         - The user's performance history, including completed and failed scenarios.
      ii) The prompt includes instructions for the Gemini API to:
         - Recommend one scenario that matches the user's personality profile.
         - Provide a clear explanation linking the scenario to the user's traits and vulnerabilities.
   d) Calling the Gemini API
      - The generated prompt is sent to the gemini-pro model using the API's generateContent method.
      - The API processes the prompt and returns a response that includes the recommended scenario and an explanation.
   e) **Extracting and Validating the Recommendation**
      - The system parses the API response to extract the recommended scenario by matching it with the available scenarios list.
      - If no suitable scenario is found in the response, the system notifies the user that no matches are available.
   f) F**etching Scenario Details**
      - Once a scenario is identified, the system queries the database to retrieve the corresponding URL for the recommended scenario.
      - The scenario URL is sent to the frontend, along with the explanation provided by the API.
   g) **Output and Error Handling**
      - If the API fails to recommend a scenario or if no matching scenario is found, an appropriate error message is sent to the front end.
      - The system includes robust error handling to manage issues like missing database entries or API errors.
4) **mysql** The database solution for managing structured data such as: User profiles, Personality test results, Predefined social engineering scenarios and User performance history.
5) **MAMP** A local development environment used to host the MySQL database and the backend server during development.

Data Flow in a Node.js Application with Gemini API and MySQL Database

Flowchart Explanation:

This flowchart in Figure 1 represents the interaction between the client, Server.js server, MySQL database, and Gemini API in a personality profiling system:

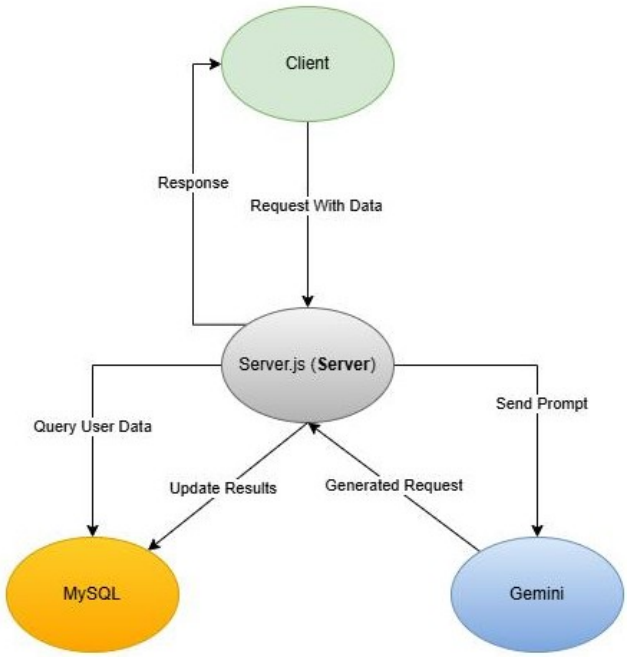

Fig. 1. System Architecture Diagram

- Client: Sends a request containing personality data (e.g., Big Five traits) to the Node.js server.
- Server.js Server:
  - Processes the client's request.
  - Queries the MySQL Database to retrieve or update user information.
  - Generates a prompt based on personality data and sends it to the Gemini API for text generation.
- Gemini API: Processes the prompt and returns a generated personality summary.
- server.js Server:
  - Receives the response from the Gemini API.
  - Updates the MySQL Database with the new summary or results.
  - Sends a final response back to the client.

6) **canva** Canva was used to create simulation videos for social engineering attack scenarios. Here's how it helped:
   - **Designing Visuals:** Canva's templates and tools were used to create engaging visuals and animations that represent phishing emails, fake login pages, and other attacks.
   - **Simulating Attacks:** Videos were designed to mimic real-world scenarios, showing how social engineering tricks work and how users might fall for them.
   - **Interactive Guides:** Text overlays and animations explained key attack methods and red flags to look out for.
   - **Exporting Videos:** The final videos were exported in high quality and integrated into the training platform.

VII. System Implementation

The system implementation focuses on providing a dynamic and personalized experience for users by assessing their personality traits and enhancing their cybersecurity awareness. It utilizes the Big Five personality model to evaluate traits, and based on the results, it recommends tailored training scenarios aimed at improving the user's weakest traits. The system integrates various components, including progress tracking, scenario recommendations, and real-time feedback, to ensure an adaptive learning journey. In the following section, we will outline the main components and pages of the project, explaining how each contributes to the overall functionality and user experience.

A. Personality Test Page

The Personality Test Page is designed to assess users' personality traits based on the Big Five Personality model. Upon signing in, users are directed to this page, where they are presented with a series of questions that relate to key traits such as Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness. Each question provides five response options, ranging from "Strongly Agree" to "Strongly Disagree," allowing users to select the statement that best reflects their personal views. The questions are displayed in sequence, and the page automatically scrolls to the next question after the user selects an answer, ensuring a smooth, uninterrupted experience.

Once the user completes the test, their answers are collected and sent to the backend via a request to the /api/calculate-personality endpoint. This request includes the user's responses and their userId, which is retrieved from the URL. The API processes the responses to calculate the user's Big Five personality traits and returns the results as percentage scores for each trait. These results are then displayed on the page, providing the user with a comprehensive overview of their personality. After finishing the test, users are redirected to their dashboard, where they can view further details or continue with their experience. This integration with the backend API ensures a seamless, real-time analysis of the user's personality traits based on their responses.

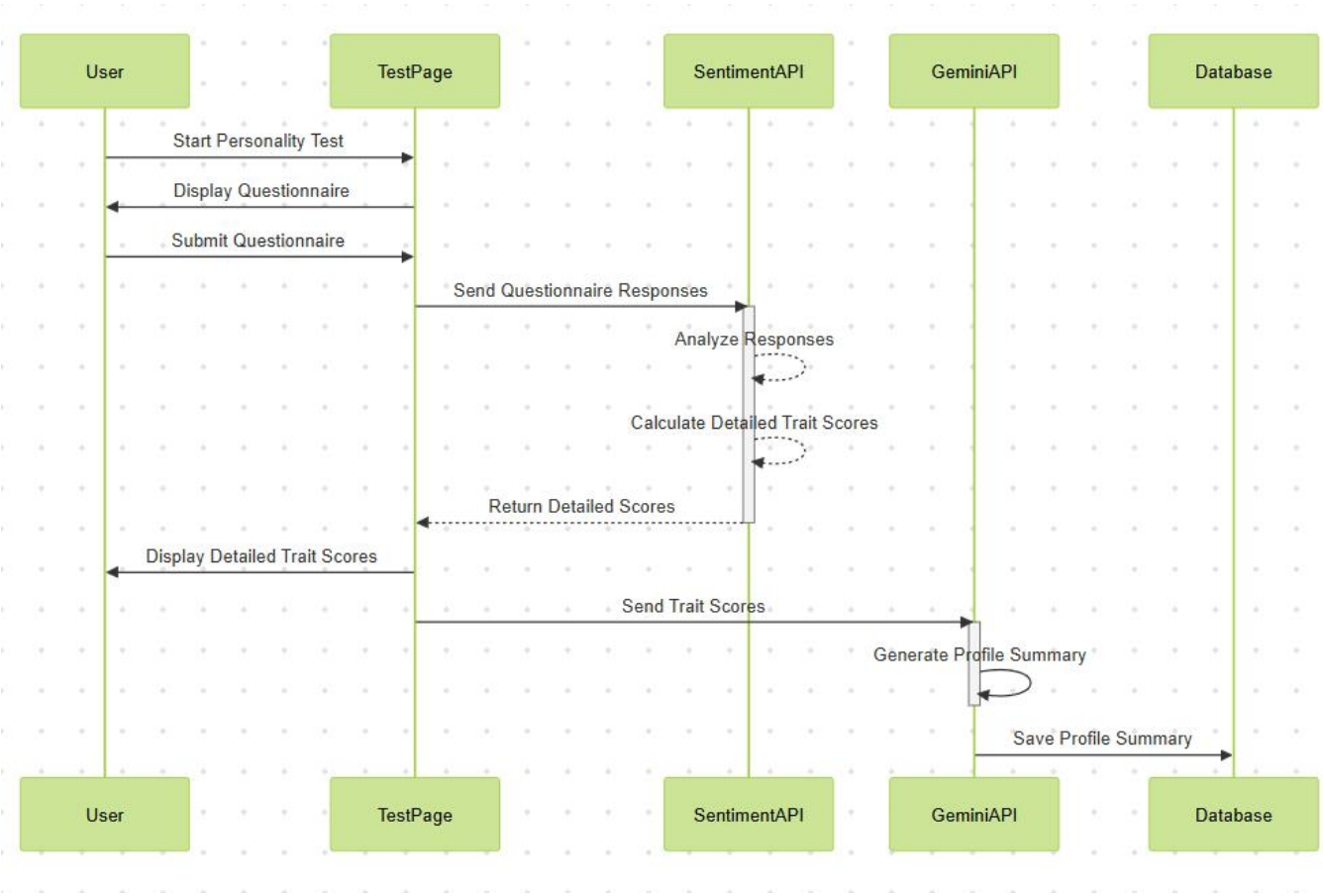

Fig. 2. Use Case Diagram for Personality Test Workflow in the Test Page

B. Dashboard page

The User Dashboard page provides a dynamic and personalized experience for users by displaying key information related to their personality traits, previous training sessions, and providing easy access to start new training challenges.

1) ***Personality Trait Results*** *:* After the user completes the personality test, their Big Five Personality Traits (Extraversion, Conscientiousness, Openness, Agreeableness, and Neuroticism) are displayed on the dashboard. Each trait is represented by a progress bar that visually indicates the user's score for that particular trait, as well as a numerical percentage next to each trait. These values are directly related to the results of the personality test. When the user completes the test, the results, including the percentage for each trait, are sent to the backend, where they are stored in the database. When the user visits the dashboard, this data is retrieved from the backend and displayed, ensuring the traits are dynamically updated to reflect the user's current personality profile.

2) ***Previous Session Data****:* Beneath the personality trait results, users can view a summary of their previous session scores, which includes indicators for Passed, Incomplete, and Failed sessions (displayed with colored indicators such as green, yellow, and red) and the overall score for previous sessions. This section helps users track their progress over time. The session data is stored in the database and retrieved when the user logs in and accesses the dashboard. This ensures that the user's previous progress is always visible and updated based on their past activities

3) ***Start Session Button****:* Located below the previous session summary, the Start Session button allows the user to begin a new training challenge based on their personality traits. When the user clicks on the Start Session button, the front end sends the user's personality trait data to the backend. The backend communicates with the Gemini AI system, which analyzes the trait data and determines which trait (typically the one with the lowest percentage) is the user's weakest. Gemini then selects a scenario tailored to

help the user improve that specific trait. The backend sends the appropriate scenario URL to the frontend, and the user is redirected to the selected training scenario [19]

*4) **Scenario Training and Session Completion**:* After the user clicks the Start Session button, they are redirected to a scenario designed to target their weakest personality trait, as identified by Gemini's AI. The AI selects the most appropriate scenario based on the user's personality data, focusing on areas that need improvement. [19]

Upon completing the scenario, the user answers questions related to the scenario content. The results, including whether the user passed or failed, are sent to the backend and stored in the database under the user's previous session scores. This allows the user to track their progress over time, with session scores and feedback updated accordingly to reflect their development in the targeted personality trait.

*5) **Profile Summary and AI Integration**:* After finishing a scenario, the Your Profile Summary section is updated with new information about the user's progress. The summary is populated with insights and recommendations based on the user's personality traits, including areas where they've shown improvement and areas that still need work. Gemini's AI plays a crucial role in providing personalized insights, analyzing the user's performance after completing scenarios, and offering suggestions for further growth. This updated information is stored in the backend and displayed in the Your Profile Summary section, ensuring the user has an up-to-date view of their personality and progress.

All user data, including personality test results, session scores, and profile updates, are stored in the database to ensure persistence across sessions. The database serves as the central storage, ensuring that the user's data is consistently available. The backend interacts with this database to save and retrieve information such as the user's personality trait percentages, session results, and profile updates. This ensures that the user's progress is continuously tracked and reflected in their dashboard.

C. Scenario Page

1) Scenario Selection Based on User's Personality: Once the user clicks the Start Session button, the Gemini AI uses the user's personality trait data to select the most appropriate scenario. The AI evaluates the user's personality scores (Extraversion, Conscientiousness, Openness, Agreeableness, Neuroticism) and identifies the weakest trait (the one with the lowest percentage). The selected scenario is designed to target this specific area of weakness [10], [19]

- Personality Trait Data: The user's personality trait scores are sent to the backend when the Start Session button is clicked.
- Gemini AI's Role: Based on these scores, Gemini determines the weakest trait and selects a scenario aimed at improving this trait.

2) User Interaction Within Scenarios: After Gemini AI selects the scenario, the user is redirected to the Scenario Page. The scenario is presented to the user in the following sequence:

1) **Video Description:** The scenario begins with a video that explains the situation the user will face. The video sets up the context for the scenario and introduces the challenges that will help improve the weakest trait.
2) **Answering Questions:** Following the video, the user is asked questions related to the scenario to assess their understanding. These questions help determine whether the user recognizes the risks involved and whether they can choose the correct response.
3) **Interactive Tasks:** Depending on the scenario, the user may also interact with the page by making choices or selecting responses, reinforcing their understanding of the situation.
4) **Pass or fail or incomplete:** Based on the user's answers, the system determines whether they pass or fail or incomplete the scenario.

3) Available Scenarios and Their Descriptions:

- **Scenario 1: Sara** o Prize phishing scenario showing risks of curiosity, targeting Openness to Experience. This scenario helps users recognize phishing attempts that exploit curiosity, encouraging them to think critically before engaging with unsolicited offers.
- **Scenario 2: RAwork** o Ransomware threat from suspicious attachments, targeting Conscientiousness. This scenario educates users on the dangers of opening attachments from unknown sources, aiming to improve caution and carefulness in handling emails.
- **Scenario 3: iPhone Ad** o Scam offers targeting entertainment enthusiasts, targeting Openness to Experience. This scenario focuses on identifying fraudulent offers that target users' interests, such as fake giveaways or promotions.
- **Scenario 4: Work** o Data breach from careless email handling, targeting Neuroticism. This scenario highlights the importance of cautious email management, focusing on how careless handling of emails can lead to data leaks.
- **Scenario 5: Tareq-Agree**
  o Social engineering through emotional manipulation, targeting Agreeableness. This scenario challenges users to recognize emotional manipulation techniques and teaches how to respond appropriately to such situations.
- **Scenario 6: Saud-Extra** o Phone scam targeting personal information, focusing on Extraversion. This

scenario educates users about common phone scams that attempt to steal personal details, emphasizing vigilance and caution in trusting unexpected calls.

- **Scenario 7: Internet Open** o Donation link phishing exploiting emotions, targeting Openness to Experience. This scenario focuses on charity-related phishing attacks, where scammers use emotional appeals to trick users into making donations to fraudulent causes.
- **Scenario 8: Charity-Agree** o Social media financial fraud, targeting Agreeableness. This scenario highlights how scammers exploit users' willingness to help by tricking them into giving away money via social media, teaching users to recognize fraudulent requests.
- **Scenario 9: InstagramDM-Help** o Phishing through fake login pages, targeting Agreeableness. This scenario teaches users to recognize fake login pages designed to steal account credentials, improving caution and mindfulness when dealing with suspicious login requests.

After completing the scenario, the results (pass/fail/incomplete status and responses) are sent back to the backend. The data is stored in the database, allowing the user to track their performance and progress. The backend updates the previous session scores in the database, and this data is used to provide feedback and recommendations for future training sessions.

VIII. User Interaction Flowchart

This Flowchart provides the user interaction flow for the web application, detailing how users interact with the system from login/signup to scenario recommendation.

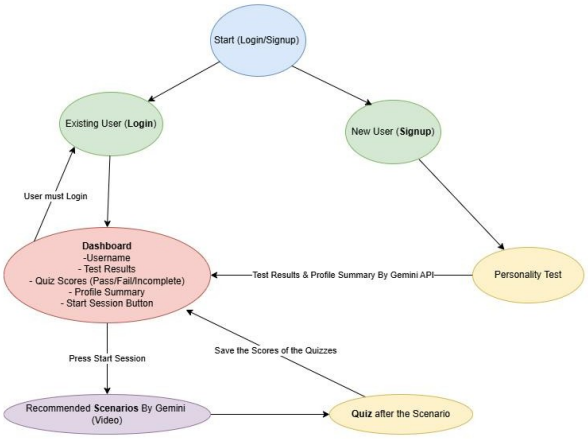

Fig. 3. User Interaction Flow for Personality-Based Recommendations System

Description of the Flowchart

1) **Start (Login/Signup):** - The user begins by either logging in as an existing user or signing up as a new user. New users must complete the personality test as part of the signup process.
2) **Login:** - Existing users can log in to the platform, and they are redirected to the dashboard.
3) **Signup and Personality Test:** - New users sign up and complete the personality test. The test results are displayed on the dashboard after login.
4) **Dashboard:** - The dashboard displays the user's personality test results and scenario scores. Users can initiate a session by pressing the 'Start Session' button.
5) **Start Session:** - The system loads a tailored scenario page for the user to engage with.
6) **Scenario Page:** - The scenario page contains a video and quiz provided by the Gemini API. The user interacts with this content and submits their quiz responses.
7) **Scenario Recommendation by Gemini:** - The Gemini API processes the user's personality data and past performance to recommend the most suitable training scenario. It explains why the scenario aligns with the user's traits and vulnerabilities.
8) **Updated Dashboard:** - The updated dashboard displays the final results and any new scenario scores. This concludes the session, and users can start a new session if desired.

A. Database

The database is designed for managing users, personality test results, scenarios, and their status in a system that analyzes and tracks user progress through predefined scenarios. The database was implemented using MAMP as a local server environment and MySQL as the relational database management system.

The database is structured to support the application's functionality and user flow. Below are the details of the tables:

- Users:
  o Purpose: Stores information about registered users, including their login
- $User personality\_Results$:
  o Purpose: Records the results of the Big Five Personality Test for each user, tracking their personality traits and the date the test was taken.
- **Scenarios:**
  o Purpose: Maintains the details of scenarios generated by the AI generative model, including their type and associated URLs.
- user_scenario_status:
  o Purpose: Tracks the progress and completion status

of users for each scenario, helping to monitor their performance and update statuses accordingly.
- user_profile_summaries:
  o Purpose: Stores personalized summaries for users, including a textual profile description and the timestamp of its creation.

Packaging

- @google/generative-ai: Used to interact with Google's generative AI models for generating content or recommendations.
- **axios:** Used to make HTTP requests to external APIs or backend services.
- **bcrypt:** Used to hash and compare passwords for secure user authentication.
- **body-parser:** Used to parse incoming request bodies (e.g., form data or JSON) in Express.js applications.
- **dotenv:** Used to load environment variables from a .env file, such as API keys or database credentials.
- **express-session:** Used to manage user sessions and persist login states across requests in Express.js applications.
- **express:** Used to set up the web server, define routes, and handle HTTP requests in a Node.js application.
- **mysql2:** Used to interact with a MySQL database, performing queries and operations.
- **node-fetch:** Used to make HTTP requests, similar to the fetch API, for accessing external data or services.

B. Testing

Testing is a critical phase in ensuring the reliability, functionality, and performance of a system. It evaluates all features to confirm that the system operates as intended. In our project, we primarily focused on unit testing, then user testing and feedback because the application is designed to align closely with user personalities and performance. After users tested the application, we documented the test cases and gathered feedback through surveys to refine the system.

Additionally, highlights the main functionalities of the system and outlines the correct procedures for executing its core features effectively.

1) Preparations:: The preparation phase began by setting the objectives of the web application and identifying the target users who would test the application. In addition, generating test cases and evaluate the system's performance and functionality

2) Goals::

- To verify the correctness and functionality of all features.
- To evaluate the user experience and identify usability issues through survey and direct feedback from participants.
- To ensure the system's continuous improvement.

3) Target Participants:: The primary target participants for testing are a small group from the public, as the simulator is designed to enhance cybersecurity awareness among all members of the community

4) Test Environment::

- MySQL Database
- Google Chrome Browser
- Visual Studio

5) Functionalities:: These are the main functionalities that we are going to test

TABLE III
FUNCTION DESCRIPTIONS

Function No.	Description
1	User Authentication (Sign-Up, Log-In)
2	Personality Assessment (Big Five Personality Test)
3	Scenario Recommendation
4	Performance Tracking and Analysis
5	Dashboard Features

Test methods:

1) **Unit testing** Unit testing is a software testing method that involves validating individual components or modules of a program to ensure they function as intended.
2) **System testing** This project was tested with a small group from the public, and the following test case scenarios illustrate the system's workflow.
   We requested users to evaluate the project, and the following figures present the results of the questionnaire. Below are the users' feedback after completing the app testing.

Fig. 4. : Database Schema Diagram

TABLE IV
FUNCTIONALITY TEST CASES

Function	Input	Expected Result	Actual Result
Sign-Up	• Username: Sara • Email: Sara@gmail.com • Password: Sara@Pa$$w0rd! • Confirm Password: Sarrapassword!	Error message: Passwords do not match.	Error message: Passwords do not match.
Sign-Up	• Username: Sara • Email: Sara@gmail.com • Password: Sara@Pa$$w0rd! • Confirm Password: Sara@Pa$$w0rd!	The web application creates an account with Sara@gmail.com and redirects the user to the test page.	Creates a new account and redirects the user to the test page.
Log-In	• Email: Sara@gmail.com • Password: Sarrapassword!	The email or the password is incorrect.	The email or the password is incorrect.
Log-In	• Email: Sara@gmail.com • Password: Sara@Pa$$w0rd!	Logs in successfully and redirects the user to the dashboard.	Logs in successfully and redirects the user to the dashboard.

TABLE V
PERSONALITY ASSESSMENT TEST CASES

Function	Input	Expected Result	Actual Result
Personality Assessment (Big Five Personality Test)	Answers all the test questions and clicks submit.	Display the personality results and provide a button to navigate to the dashboard page.	Display the personality results and provide a button to navigate to the dashboard page.
	Leaves some questions without an answer.	Cannot submit the test form until all the questions have been completed.	Cannot submit the test form until all the questions have been completed.
	Most of the selected answers are 'Agree' and 'Strongly Agree.'	Openness as a personality trait is above 90%.	Openness as a personality trait is above 97%.

IX. RESULTS AND DISCUSSION

A. Results

AI Personality-Driven Social Engineering Auto-Attack Simulator successfully integrates multiple components,

TABLE VI
SCENARIO RECOMMENDATION TEST CASES

Function	Input	Expected Result	Actual Result
Scenario Recommendation	The personality traits passed from the database into the Gemini API: • Openness: 97.90 • Conscientiousness: 24.40 • Extraversion: 63.55 • Agreeableness: 81.65 • Neuroticism: 72.30	Custom scenarios are recommended to match user vulnerabilities. Redirect to `sara_open.html` scenario.	Custom scenarios are recommended to match user vulnerabilities. Redirect to `sara_open.html` scenario.

TABLE VII
SCENARIO RECOMMENDATION TEST CASES

Function	Input	Expected result	Actual result
Performance Tracking and Analysis	Scenario completion status: Pass	System escalates to more advanced attacks.	System escalates to more advanced attacks.
	Scenario completion status: Fail	Users showing vulnerability are presented with simpler, educational scenarios.	Users showing vulnerability are presented with simpler, educational scenarios.

TABLE VIII
DASHBOARD FEATURES TEST CASES

Function	Input	Expected result	Actual result
Dashboard Features	Personality Trait Scores: User ID with a valid personality test record	Display personality trait scores	Display personality trait scores
	Previous sessions performance: Completed	Display performance metrics	Display performance metrics
	Previous sessions performance: Not yet	Display the score equal zero	Display the score equal zero
	Personalized Profile Summary: Percentage distribution of the Big Five personality traits	Openness as a personality trait is above 90%.	Openness as a personality trait is above 97%.

TABLE IX
TEST SCENARIOS AND RESULTS

Test Scenario	Result Status
Start page → Signup as a new user → Complete Personality Test → Test results displayed on Dashboard	Pass
Start page → Login as an existing user → Redirect to Dashboard → Dashboard displays past results	Pass
Dashboard → Click "Start Session" → System loads a tailored scenario page based on user data	Pass
Scenario Page → Video and quiz load successfully from the Gemini API → User interacts and submits responses	Pass
Updated Dashboard → Displays *final results* and new scenario scores → User can start a new session	Pass

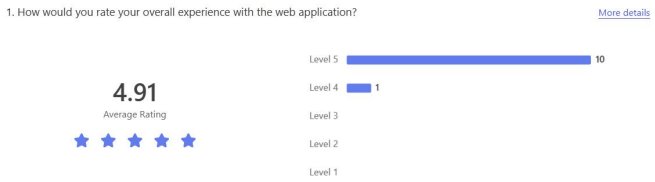

Fig. 5. User Experience with the System

each contributing to the overall system's goal of simulating and analyzing the intersection of AI, personality profiling, and behavioral scenarios. Below is a detailed account of the results and their implications:

a) **System Functionality and Performance**

- The system effectively personalized social engineering attack scenarios based on users' Big Five personality traits.
- Real-time recommendations using the Gemini

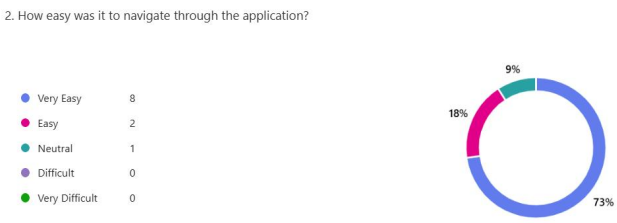

Fig. 6. Testing the system usability

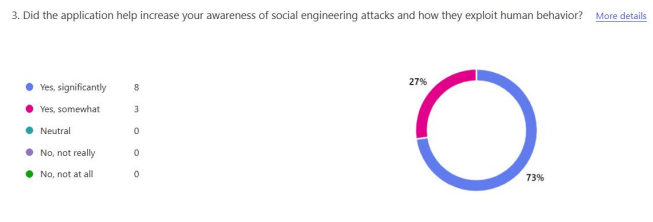

Fig. 7. The system's ability to raise awareness

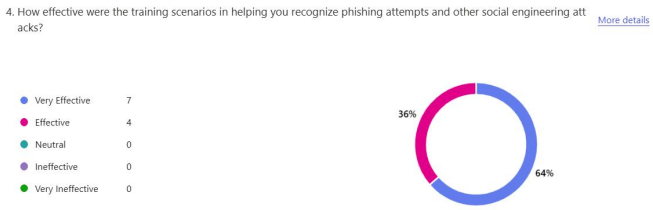

Fig. 8. System effectiveness in helping users with recognize phishing attacks.

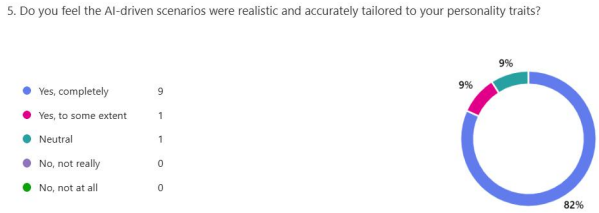

Fig. 9. Scenarios tailored to user's personality trait.

API provided tailored attack simulations that targeted user-specific vulnerabilities, such as phishing scenarios for high-openness individuals.

- The integration of Sentino API for personality assessments achieved high accuracy in reflecting users' psychological profiles, as verified by survey feedback during testing.

b) Big Five Personality Traits Test The Personality Test involves the user answering a series of questions designed to assess behaviors, feelings, and thoughts in different situations. Responses are collected on a five-point scale: Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree. The system analyzes the responses using the Big Five Personality Traits framework,

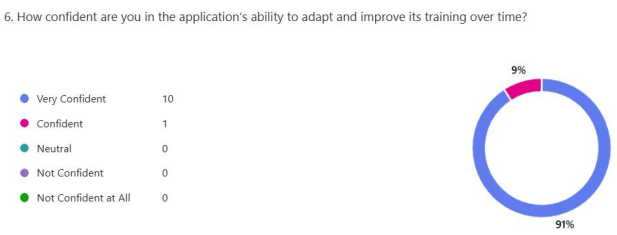

Fig. 10. System's adaptability.

Fig. 11. Dashboard's features.

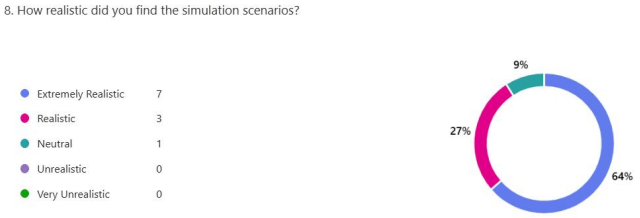

Fig. 12. Realism of scenarios

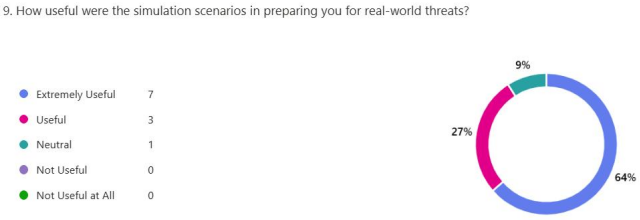

Fig. 13. The system's ability to prepare uses to real-world threats.

which includes Openness, Conscientiousness, Extraversion, Agreeableness, and Emotional Stability (Neuroticism). Algorithms calculate scores for each trait based on the weighted values of the responses. A comprehensive report is then generated, displaying the user's scores across the five traits. These results are visually presented in easy-to-understand graphs on the dashboard. Based on this test, a user profile summary is also displayed on the dashboard, providing an overview of the user's personality.

TABLE X
EXAMPLE OF PERSONALITY TRAIT SCORES OF USERS

Personality	**Openness(%)**	**Conscientiousness (%)**	**Extraversion (%)**	**Agreeableness (%)**	**Neuro - ticism (%)**
User 1	85	72	90	80	50
User 2	60	80	40	65	30
User 3	95	90	85	75	70

TABLE XI
USER PROFILE SUMMARY

Aspect	**Description**
Name	Hello, Sara,
Strengths	- Open to new experiences and ideas, helping to stay updated with the latest cybersecurity trends. - Agreeable and easy-going, making it easier to trust others and follow advice.
Weaknesses	- High neuroticism may increase susceptibility to phishing scams and other cyber threats.
Recommendations	- Improve cybersecurity awareness by staying updated on the latest threats and scams. - Be mindful of the information you share online. - Stay cautious of suspicious emails or messages.
Encouragement	Remember, it's okay to say no if something feels fishy.

3) **Personality-Based Scenario Customization** Scenarios are designed to align with individual personality traits, reflecting realistic and adaptive social engineering attacks. For instance, users with high extraversion traits might encounter scenarios involving social interactions, such as responding to phishing attempts posed as personal invitations. Similarly, users with high openness traits might face challenges centered around curiosity, such as links labeled "exclusive insights" or "confidential files." A personality test, implemented as a short quiz, provides scores for traits such as Extraversion, Openness, or Conscientiousness. These results are dynamically analyzed and stored in the personality_results database table. The scores then guide the recommendation engine to display scenarios tailored to the user's personality profile.
4) **Scenario Simulation** The scenario is presented as an interactive video simulating real-world situations, such as receiving a suspicious email or a message with a malicious link. The video is designed to feel realistic, immersing the user in the scenario as if it were happening in real life.
During the video, the user is prompted to make decisions, and all interactions are tracked to analyze behavior and determine susceptibility to potential threats.
5) **Outcome Analysis** After the video ends, a short quiz assesses the user's understanding of the scenario. The questions are straightforward, such as identifying phishing attack indicators. Examples of potential quiz questions include:
   - "The link is on a temporary server and a WordPress folder."
   - "No company logo in the message."
   - "Using a generic name like 'Digital World' instead of a well-known company name."

   Interactive options allow users to respond directly within the scenario interface by clicking buttons or selecting appropriate answers. The user's responses are analyzed to evaluate awareness of mistakes and provide personalized guidance for improvement. For example:
   • Correct answer! T***he link on the server is a sign of a phishing attack to direct you to the control panel.***
6) **Performance Report (Dashboard)** After completing the Big Five Personality Traits test, scenarios, and quizzes, the user receives a comprehensive performance report displayed on the dashboard. This report includes an analysis of the user's actions, highlighting mistakes and successes, along with clear recommendations to avoid similar mistakes in the future. Visual charts and graphs provide an intuitive representation of the user's strengths and weaknesses.
7) **User Dashboard Analysis** The dashboard provides essential information in a user-friendly layout, helping users monitor their performance and identify areas for improvement. Key features include:
   a) **Personality Summary:** The Big Five Personality Traits are prominently displayed, showing how each trait impacts decision-making. This information helps the system adjust scenario difficulty

TABLE XII
DASHBOARD FEATURES

Section	Details
Profile Summary	*"Hello Sara, Based on your personality profile, you have strengths to stay safe online. You're open to new ideas, agreeable, but high neuroticism may increase susceptibility to threats. Stay cautious."*
Profile Selection	User can choose between male or female for their profile avatar.
Personality Traits	• **Extraversion**: 48.15 • **Conscientiousness**: 49.90 • **Openness**: 42.45 • **Agreeableness**: 17.55 • **Neuroticism**: 31.65
Previous Sessions	• Passed: Green • Incomplete: Yellow • Failed: Red • **Score**: 100
Call to Action	Button: **"START SESSION"** with a motivational text: *"You're ready to conquer today's challenges!"*

and feedback. For instance:

- Users with high Conscientiousness might be assigned more complex scenarios.
- Users with high Neuroticism are encouraged to build confidence in their decision-making.

b) **Scenario Success Rates:** The dashboard visually tracks success rates for scenarios, categorized as (Passed, Failed , Incomplete)

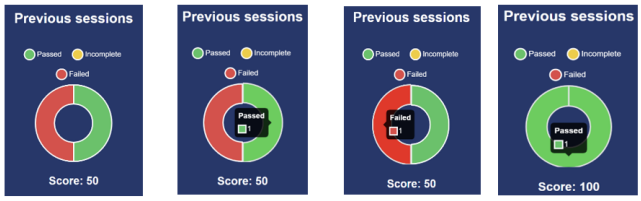

Fig. 14. Combined

Learning Recommendations:
Based on personality and performance, the system dynamically adjusts scenario difficulty. For example:

- A user excelling at identifying phishing attempts may receive advanced scenarios for further challenge.
- Recommendations for additional practice are provided to ensure continuous growth in cybersecurity awareness.

8) **Integration of AI Rules** The system incorporates AI-driven rules to dynamically adjust scenario difficulty and complexity based on the user's performance and personality data.
   - Adaptive Scenario Logic:
     - The AI evaluates user behavior and adapts accordingly. For instance:
       - If a user consistently demonstrates resilience in basic scenarios, the system escalates to more advanced attack types, such as spear-phishing or impersonation.
       - Users showing vulnerability are presented with simpler, educational scenarios designed to reinforce fundamental awareness

9) **Security Features**
   - Data Integrity:
     - User data, including personality quiz results and scenario performance, is securely stored in the backend database to ensure privacy and integrity.
     - Security measures, such as login mechanisms and data validation checks, protect against unauthorized access.
   - Dynamic Content Delivery: o Scenarios and quizzes are delivered in real-time through secure API calls, maintaining control over sensitive data flows while ensuring a fresh and engaging experience for users.

10) **Educational Component**
   - Awareness Training:
     - The project integrates an educational layer that explains the social engineering tactics encountered in scenarios.
     - Users gain access to curated resources, including articles, videos, and best practices, to enhance their understanding of cybersecurity principles.

11) **System Architecture**
   - **Frontend and Backend Collaboration:**
     - The user interface is designed with dynamic and responsive components, ensuring seamless interaction across a variety of devices.
     - Backend services handle essential operations, such as user authentication, scenario management, and analytics, ensuring both scalability and reliability for a smooth user experience.
   - **Database Integration:**

- A centralized $personality\_results$ table tracks user data, supporting personalized experiences and ensuring data integrity.
- The table schema is designed for scalability, allowing the integration of additional metrics or future features as the system evolves.

12) **Discussion** The project highlights the importance of integrating psychology, AI, and user-centered design to create an engaging and educational tool:
   a) **Improved User Engagement:**
      - The updated dashboard interface, with its congratulatory messages and visual summaries, enhances user motivation.
      - Personalized scenarios ensure users feel their experience is unique and relevant.
   b) **Impact of the Gemini Model:**
      - The generative model showcased its potential by creating scenarios tailored to psychological profiles, making training sessions both realistic and effective.

X. Future work

1) **Expand Scenario Diversity**
   - Increase the number and variety of social engineering scenarios to include emerging tactics such as deepfake phishing, vishing (voice phishing), and hybrid attack methods. This will provide users with comprehensive exposure to real-world threats.
2) **Implement an Admin Dashboard**
   - Develop an admin interface to monitor user progress, manage scenarios, and generate detailed reports. The admin can also oversee system performance and track trends in user behavior.
3) **Introducing Gamification Features**
   - Add elements like badges, leaderboards, and progress milestones to increase user engagement and motivation. These features can help sustain interest and encourage users to complete more training sessions.
4) **Mobile Application Development**
   - Create a mobile-friendly version of the platform to make the training accessible on smartphones and tablets, allowing users to learn anytime, anywhere.

XI. limitations

1) **Dependence on Gemini AI API** The platform's functionality is heavily reliant on the Gimine AI API for personality assessments and scenario customization. API downtime, rate limits, or inaccuracies in processing could impact user experience and training outcomes.
2) **Scenario Diversity** The current number of scenarios might not comprehensively cover all possible social engineering techniques, which may limit the platform's ability to prepare users for a broader range of real-world attacks.
3) **Limited Language Support** While the platform currently supports Arabic and English, extending support to other languages would require significant resource allocation, potentially delaying broader adoption in multilingual environments.

XII. Conclusion

This project successfully addresses the growing need for adaptive cybersecurity training by combining advanced AI technology with psychological frameworks. Through the integration of Gimine AI, the platform offers personalized and dynamic simulations that prepare users to recognize and counteract social engineering attacks effectively. The system's ability to tailor scenarios based on Big Five personality traits enhances user engagement and learning outcomes, as demonstrated by improved success rates and positive feedback.

Despite certain limitations, such as reliance on API performance and the need for greater scenario diversity, the project establishes a solid foundation for future advancements. Planned enhancements, including gamification and broader AI capabilities, will further elevate the platform's effectiveness and scalability. By leveraging innovative AI-driven methods and maintaining a strong focus on user privacy and ethical data handling, this platform not only contributes to individual cybersecurity awareness but also sets a benchmark for personalized, next-generation cybersecurity training solutions. This work serves as a stepping stone toward building resilient defenses against evolving social engineering threats.

References

[1] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Information Systems Security*, vol. 16, no. 6, pp. 315–331, 2007.

[2] P. T. Costa and R. R. McCrae, *Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual*. Psychological Assessment Resources, 1992.

[3] Fingerprint, "How social engineering works & prevention," 2023, [Accessed: May 18, 2024]. [Online]. Available: https://fingerprint.com/blog/how-social-engineering-works-prevention/

[4] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior*, vol. 24, no. 6, pp. 2799–2816, 2008.

[5] O. P. John and S. Srivastava, "The big five trait taxonomy: History, measurement, and theoretical perspectives," in *Handbook of Personality: Theory and Research*, 2nd ed., L. A. Pervin and O. P. John, Eds. Guilford Press, 1999, pp. 102–138.

[6] S. Uebelacker and S. Quiel, "The social engineering personality framework," in *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 2014, pp. 24–30.
[7] A. Silva, "Social engineering," https://www.linkedin.com/pulse/social-engineering-anjana-silva-xd48e?trk=article-ssr-frontend-pulse_more-articles_related-content-card, 2023, [Accessed: May 18, 2024].
[8] B. H. E. Hacking, "Social engineering," 2023, [Accessed: May 18, 2024]. [Online]. Available: https://www.blackhatethicalhacking.com/solutions/social-engineering/
[9] C. J. Soto, "Big five personality traits," in *The SAGE Encyclopedia of Lifespan Human Development*, M. H. Bornstein, M. E. Arterberry, K. L. Fingerman, and J. E. Lansford, Eds. Thousand Oaks, CA: SAGE, 2018, pp. 240–241.
[10] M. R. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. A. Butavicius, "Why do some people manage phishing e-mails better than others?" *Information Management & Computer Security*, vol. 20, no. 1, pp. 18–28, 2012.
[11] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015.
[12] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities, and attack methods," *IEEE Access*, vol. 9, pp. 11 895–11 908, 2021.
[13] B. Cusack and K. Adedokun, "The impact of personality traits on user's susceptibility to social engineering attacks," in *Proceedings of the 16th Australian Information Security Management Conference*, Perth, Australia, 2018, pp. 83–89. [Online]. Available: https://ro.ecu.edu.au/ism/228
[14] M. Asfour and J. C. Murillo, "Harnessing large language models to simulate realistic human responses to social engineering attacks: A case study," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 6, no. 2, pp. 21–49, 2023.
[15] A. Luse and J. Burkman, "Gophish: Implementing a real-world phishing exercise to teach social engineering," *Journal of Cybersecurity Education Research and Practice*, vol. 2020, no. 2, p. art. 5, 2021. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/5
[16] B. Rammstedt, D. Danner, C. J. Soto, and O. P. John, "Validation of the short and extra-short forms of the big five inventory-2 (bfi-2) and their german adaptations," *European Journal of Psychological Assessment*, vol. 36, no. 1, pp. 149–161, 2020.
[17] R. A. Power and M. Pluess, "Heritability estimates of the big five personality traits based on common genetic variants," *Translational Psychiatry*, vol. 5, p. e604, 2015.
[18] C. Ackerman, "Big five personality traits: The ocean model explained," https://positivepsychology.com/big-five-personality-theory, 2017.
[19] G. AI, "Google ai," 2024, [Accessed: Dec. 5, 2024]. [Online]. Available: https://ai.google.dev
[20] Sentino, "Sentino api," 2024, [Accessed: Dec. 5, 2024]. [Online]. Available: https://sentino.org/api/
[21] "Phishing and social engineering virtual awareness," The Cyphere, 2023. [Online]. Available: https://thecyphere.com