

**Behaviorance-I Redefining Cyber Security with Secure Sense Behavioral Compliance**

**(Web Application Platform)**

**Final Year Project Report**

**Submitted by**

**Farwah Butt (1101-2021)**

**Emaan Nadeem (2438-2021)**

**Hafsa Khalid (2625-2021)**

**Supervisor**

**Sir Iqbal Uddin khan**

In partial fulfilment of the requirements for the degree of

**Bachelor of Science in Computer Science**

2024

Faculty of Engineering Sciences and Technology

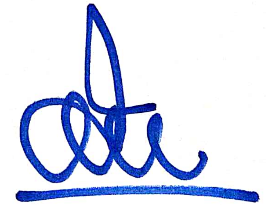
Hamdard University, Main Campus, Karachi, Pakistan

# Certificate of Approval

### Faculty of Engineering Sciences and Technology

Hamdard University, Karachi, Pakistan

This project “**Behaviorance-I”** is presented by **Farwah Butt / Emaan Nadeem / Hafsa Khalid** under the supervision of their project advisor and approved by the project examination committee and acknowledged by the Hamdard Institute of Engineering and Technology, in the fulfillment of the requirements for the Bachelor degree of **Computer Science**.



Sir Iqbal Uddin khan In-charge FYP-Committee

(Project Supervisor)

(Project Co-Supervisor) Chairman

(Department of Computing)

(Dean, FEST)

# Authors’ Declaration

We declare that this project report was carried out in accordance with the rules and regulations of Hamdard University. The work is original except where indicated by special references in the text and no part of the report has been submitted for any other degree. The report has not been presented to any other University for examination.

Dated:

Authors Signatures:



Farwah Butt



Emaan Nadeem

C:\Users\USer\Downloads\WhatsApp Image 2025-01-17 at 3.11.26 PM.jpeg

Hafsa Khalid

# Plagiarism Undertaking

We, Farwah Butt, Emaan Nadeem, and Hafsa Khalid, solemnly declare that the work presented in the Final Year Project Report titled Behaviorance-I has been carried out solely by ourselves with no significant help from any other person except few of those which are duly acknowledged. We confirm that no portion of our report has been plagiarized and any material used in the report from other sources is properly referenced.

Dated:

Authors Signatures:



Farwah Butt



Emaan Nadeem



Hafsa Khalid

# Acknowledgments

All praise and glory are due to Allah, the Almighty, for His endless guidance and blessings throughout this journey.

We extend our heartfelt gratitude to Mr. Iqbal Uddin Khan, our supervisor, whose expert guidance, invaluable insights, and unwavering support were instrumental in the successful completion of this project.

We are deeply thankful to our dedicated team members for their exceptional efforts, collaborative spirit, and commitment to excellence in the design, development, and testing phases of the project.

We also express our sincere appreciation to Hamdard University for providing the necessary resources, infrastructure, and support that enabled us to conduct effective research and development.

Our gratitude goes to the participants and users who contributed their time and valuable feedback during testing, allowing us to refine the platform to better meet user expectations and requirements.

Finally, we would like to thank our families, friends, and colleagues for their unwavering encouragement and support, which motivated us to overcome challenges and strive for innovation and success.

# Document Information

|  |  |
| --- | --- |
| **Project Title** | Behaviorance-I Redefining Cyber Security with Secure Sense Behavioral Compliance. (Web Application Platform) |
| **Project Code** | FYP-006/FL24 |
| **Document Name** | Software Requirements Specifications |
| **Document Version** | 1.0 |
| **Document Identifier** | FYP-006/FL24 - SRS |
| **Document Status** | Draft/ Final / etc. |
| **Author(s)** | Farwah Butt / Emaan Nadeem / Hafsa Khalid |
| **Approver(s)** | Sir Iqbal Uddin Khan |
| **Issue Date** | 17-1-2025 |

**Definition of Terms, Acronyms, and Abbreviations**

This section provides definitions for key terms, acronyms, and abbreviations used in the document to ensure clarity and proper interpretation.

|  |  |  |
| --- | --- | --- |
| **Term** | **Description** | |
| Cybersecurity | Measures and practices designed to protect networks, devices, programs, and data from attacks, damage, or unauthorized access. | |
| Behavioral Compliance | The adherence to security protocols and policies by individuals based on their actions and behavior patterns, rather than just the implementation of technical measures. | |
| Insider Threats | Security risks that come from individuals within an organization who may misuse their access to harm the organization's data or systems. | |
| Web Application Platform | A software application that is accessed and used through a web browser, often designed to perform a specific set of functions our solution. | |
| IDE Tool | Integrated Development Environment (IDE), a software application used by developers to write, test, and debug code (e.g., Visual Studio Code). | |
| Next Js | **Next.js** is a JavaScript framework used for the development of user interfaces, mainly SPA. Its base is React.js, and the feature added with it is server-side rendering, static site generation, and routing support. | |
| UI (User Interface) | The part of the system that the user interacts with directly, including the layout, design, and controls. | |
| UX (User Experience) | The overall experience a user has when interacting with the platform, including ease of use, accessibility, and efficiency. | |
| Dashboard | A user interface (UI) screen displaying key information, statistics, and alerts for either the employee or admin user. | |
| MFA (Multi-Factor  Authentication) | | A security process that requires more than one method of authentication to verify the user’s identity (e.g., password + OTP). |

# Abstract

The report proposes the development of the "Behaviorance-I" platform, designed to enhance cybersecurity by integrating behavioral compliance into security frameworks. The platform, called Secure Sense Behavioral Compliance (SSBC), leverages technologies like machine learning, real-time analytics, and behavioral monitoring to address the human factors that often contribute to security breaches.

The project aims to bridge the gap in traditional cybersecurity measures, which often overlook the human element, by predicting human behavior and potential vulnerabilities. The platform's focus is on real-time detection and mitigation of behavioral risks, thereby improving compliance and reducing security incidents.

It also discusses the potential impact of the platform on improving organizational security and fostering a culture of security awareness and compliance. The project is intended for sectors such as government, education, and corporate organizations, emphasizing the integration of psychological principles with cybersecurity measures.

# Keywords:

1. **Behavioral Compliance**: Ensuring adherence to cybersecurity protocols through human behavior analysis.
2. **Cybersecurity Awareness**: Enhancing knowledge and understanding of security practices among users.
3. **Insider Threat Mitigation**: Addressing security risks originating within the organization.
4. **Human-Centric Cybersecurity**: Focusing on the human element to strengthen security measures.
5. **Behavioral Patterns**: Analyzing actions to predict and prevent security breaches.
6. **Web-Based Platform**: A centralized application for behavioral analysis and compliance monitoring.
7. **Questionnaire Bank**: A repository of structured questions for evaluating user behavior.
8. **Risk Prediction**: Anticipating security vulnerabilities based on user behavior analysis.
9. **Secure Sense**: Creating a culture of proactive security awareness among users.
10. **Behavioral Threat Detection**: Identifying risky behaviors to prevent breaches.

# Table of Contents

|  |
| --- |
| Certificate of Approval **2** |
| Authors’ Declaration **1** |
| Acknowledgments **3** |
| Document Information **4** |
| Abstract **5** |
| CHAPTER 1 **7** |
| INTRODUCTION **7** |
| Motivation **7** |
| Problem Statement **7** |
| Goals and Objectives **8** |
| Project Scope **8** |
| CHAPTER 2 **9** |
| RELEVANT BACKGROUND & DEFINITIONS **9** |
| RELEVANT BACKGROUND **9** |
| Growing Importance of Cybersecurity Awareness: |
| Focus on human behaviour in cyber security **9** |
| Need For user Engagement **9** |
| DEFINATIONS **10** |
| **Behavioral Compliance Platform 10** |
| Human – Centric Cybersecurity **10** |
| Behavioral Compliance Monitoring **10** |
| User Engagment In cybersecurity **10** |
| User Experience (UX) in security platform **10** |
| CHAPTER 3 **11** |
| LITERATURE REVIEW & RELATED WORK **11** |
| Literature Review **11** |
| Abstract **11** |
| Introduction **11** |
| Literature Review **11** |
| Traditional Jewelry Customization Applications **11** |
| Limitations of Non-AI Customization Applications **12** |
| Related Work **13** |
| Gap Analysis **15** |
| REFERENCES **17** |

**CHAPTER 1 : INTRODUCTION**

The current landscape reveals a substantial gap in the cybersecurity market: the lack of comprehensive solutions that effectively address the human element of security. Traditional cybersecurity measures, while robust, often neglect the behavioral aspects that can undermine even the most advanced technological defenses. This gap leaves organizations vulnerable to insider threats, phishing attacks, and other security breaches that exploit human weaknesses.

In response to this pressing need, introduces the smart human behavioral analysis-based web application platform called “Behaviorance-I”, with the predictive assessment to forecast human behavior and potential vulnerable actions. It will be a groundbreaking software project designed to revolutionize cybersecurity. It represents a significant innovation in the field, seamlessly integrating behavioral compliance into the core of cybersecurity strategy

Cybersecurity is a major issue for organizations in this increasingly digitized world. Technology may advance, but the human factor is a significant weakness, which hackers often take advantage of. Human errors, violations of security policies, and insider threats are some of the leading causes of data breaches and security failures.

Behaviorance-I addresses this pressing issue by introducing a new approach to cybersecurity- one that integrates behavioral compliance into the core of organizational security strategies. This project bridges the gap between human behavior and cybersecurity by developing a smart, web-based platform that analyzes user behavior, predicts potential vulnerabilities, and fosters a culture of security compliance and awareness.

The current landscape reveals a substantial gap in the cybersecurity market: the lack of comprehensive solutions that effectively address the human element of security. Traditional cybersecurity measures, while robust, often neglect the behavioral aspects that can undermine even the most advanced technological defenses. This gap leaves organizations vulnerable to insider threats, phishing attacks, and other security breaches that exploit human weaknesses.

# Motivation

There is a mistake that security systems cannot guard against, and this mistake is the human error. Humans are the weakest link, and it is why there is a pressing need for organizations to reinforce the human factor in the security. High-end technologies shield systems and networks, vulnerabilities often arise from human errors insider threats and deficiency in adherence to rules. This project aims to revolutionize cybersecurity by integrating behavioral compliance into its core, fostering a culture of awareness and proactive security.

# Problem Statement

“Transforming the Weakest Link into the Strongest Defense”

Organizations struggle with ensuring that employees adhere to security protocols, leading to vulnerabilities that can be exploited by malicious actors. The lack of a comprehensive platform that combines behavioral compliance with cybersecurity measures exacerbates this issue. There is an urgent need for an innovative solution that not only enhances cybersecurity posture but also fosters a culture of security compliance and awareness among employees.

**Current Issues:**

* **Human Errors**: A large percentage of security breaches are caused by human mistakes, making them a weak link in cybersecurity.
* **Lack of Integration:** Existing cybersecurity measures do not effectively address the human behavioral aspect.

# Goals and Objectives

### Primary Goal:

To develop a smart, web-based platform, Behaviorance-I, that integrates behavioral analysis and predictive assessments with cybersecurity strategies to enhance organizational security and foster a culture of compliance and awareness.

The project objective is to develop the smart human behavioral analysis based web application platform “Behaviorance-I”, with the predictive assessment to forecast human behavior and potential vulnerable actions

### Objectives:

1. **Behavioral Compliance:**
   * Incorporate psychological principles to identify risky behaviors and reinforce adherence to security protocols.

### Questionnaire Bank:

* + Develop a comprehensive repository of structured questions to evaluate user awareness and compliance levels.

### User-Friendly Platform:

* + Provide an intuitive and efficient user interface for seamless interaction, data input, and compliance monitoring.

### Risk Mitigation:

* + Enable organizations to proactively address insider threats and human vulnerabilities using actionable insights derived from behavioral analysis.

### Cultural Shift:

* + Promote a culture of cybersecurity awareness within organizations by integrating behavior-based training and continuous compliance tracking.

## Project Scope

The Project Scope section defines the boundaries of the **Behaviorance-I** web application platform project.

The scope of project is limited to development of the **Behaviorance-I** web application platform with advanced integrated predictive cybersecurity and psychological assessment, build a comprehensive questionnaire bank, integration of cybersecurity and psychology principles into a unified framework.

**CHAPTER 2: RELEVANT BACKGROUND & DEFINITIONS**

## Project Background

The Project Background section gives relevant background information regarding the Behaviorance-I web application platform project.

Traditional measures of cyber security often miss the non-compliance of employees with protocols, thus leaving an organization vulnerable to risks. The Behaviorance-I platform overcomes this gap by combining human behavioral analysis with predictive cyber security to forecast and prevent actual risks that can further enhance security compliance in an organization.

## Growing Importance of Cybersecurity Awareness:

As cyberattacks increase, organizations are realizing the need for stronger employee awareness. The human factor remains a key vulnerability, highlighting the importance of integrating behavioral compliance to strengthen security protocols.

## Focus on Human Behavior in Cybersecurity:

Traditional cybersecurity measures often neglect human behavior, which is a significant source of risk. Behavioral analysis, using insights from psychology and machine learning, is emerging as a way to predict and reduce human-related security breaches.

## Need for Employee Engagement:

Employees should be involved in security practices. Behaviorance-I encourages employees to follow the security protocols and be alert so that a security-conscious culture can be developed, and errors leading to vulnerabilities are minimized.

# DEFINITIONS

## Behavioral Compliance Platform:

A behavioral compliance platform refers to an online solution that serves to ensure employees comply with security-related protocols through the introduction of behavioral analysis. It is a tool for monitoring, assessing, and influencing user behavior to further organizational security along the human dimensions of cyber-security.

## Human-Centric Cybersecurity:

Human-centric cybersecurity aims at the comprehension and reduction of risks stemming from human behavior, not only from the perspective of technical defenses. Behaviorance- Iinvolves incorporating human behavior analysis into security strategies to decrease vulnerabilities resulting from employee actions such as phishing or insider threats.

## Behavioral Compliance Monitoring:

It entails monitoring user compliance continuously, checking against cybersecurity protocols in place. In this process, there is always a detection of weak spots or behavioral anomalies likely to expose the organization to threats. Such situations necessitate remedial actions.

## User Engagement in Cybersecurity:

Engage: the active participation by user in implementing security best practice. This might comprise following security practices, attending some form of security awareness training and actively engaging tools such as Behaviorance-I, which also promotes compliance in addition to bringing about a cultural change of attitude towards security.

## User Experience (UX) in Security Platforms:

User experience (UX) in security platforms focuses on designing intuitive and user-friendly interfaces that encourage employees to adopt and adhere to security protocols. Behaviorance- I prioritizes seamless UX design to make cybersecurity tools accessible and engaging, ensuring higher adoption and compliance rates.

CHAPTER 3: LITERATURE REVIEW & RELATED WORK

# Literature Review Abstract

This literature review aims to trace the development of cybersecurity tools that could enhance behavioral compliance in organizations. Traditionally, most cybersecurity platforms emphasize technical defenses while leaving the human side of the matter unaddressed. This review will discuss some of the previous research and solutions on behavioral compliance, identify areas where current systems are lacking, and explore how advanced behavioral analysis and AI can fill these gaps. The purpose is to provide an overview of the current state of behavioral compliance platforms and the improvements AI can offer in terms of more proactive security strategies.

# Introduction

As cyber threats continue to evolve, enhancing cybersecurity based on the analysis of human behavior has become the essential of securing an organization. Traditional applications in cybersecurity focus on the technical aspects, including firewalls, encryption, and threat detection, but most ignore the role that people's actions play in security breaches. Behavioral compliance platforms, like Behaviorance-I, present a more human-centric approach to cybersecurity. This literature review explores existing solutions in behavioral compliance, identifies the shortcomings of those existing solutions, and discusses how AI-driven technologies might enhance security in analyzing and potentially influencing human behavior to prevent potential security vulnerabilities.

# Reference

Traditionally Computer Science (CS) researchers have investigated the technical aspects of cybersecurity [1]. The human aspect, although very important, is often neglected [2,3] Whereas human elements are the weakest link in cybersecurity chain [1-7]. 95% of security breaches are caused by human mistakes [1-3,5,7].

Without considering human behaviors, implementing these countermeasures will remain useless [1-7]. Because 90% of cyberattacks involve human based technique [6]. Cyberspace has transcended technological artifacts with importance given to the behavioral aspect of cybersecurity [3]. Behavioral cybersecurity, also known as the human factor, presents the social scientific perspective [1,3,4,6]. There is an urgent need to focus on social and behavioral issues can help deal with cybersecurity [1-7

# Related Work

## Qualtrics

URL: [https://www.qualtrics.com](https://www.qualtrics.com/)

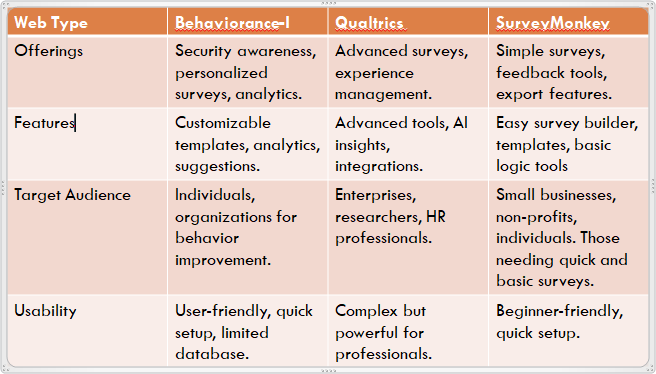
Qualtrics is a web-based platform that has been designed for creating surveys, collecting data, and analyzing insights. It offers an easy-to-use interface with customizable templates, advanced survey logic, and real-time analytics. It has been widely used for customer feedback, employee engagement, market research, and academic studies, and can be easily integrated with tools such as Salesforce and Tableau. Qualtrics ensures security and compliance with GDPR and HIPAA standards and provides automation features and robust reporting to help organizations improve experiences and make data-driven decisions.

### SurveyMonkey

URL: [https://www.surveymonkey.com](https://www.surveymonkey.com/)

SurveyMonkey is an online survey platform that helps users create, distribute, and analyze surveys easily. It provides customizable templates, multiple question types, and advanced logic for targeted responses. Used for customer feedback, market research, and employee engagement, it integrates with tools like Microsoft Teams and Salesforce.

# Competitive Analysis



1. **References**
2. Kannelønning, K. and Katsikas, S.K. (2023) ‘A systematic literature review of how cybersecurity-related behavior has been assessed’, Information & Computer Security, 31(4), pp. 463–477. Available at: https://doi.org/10.1108/ICS-08-2022-0139.
3. Almansoori, A., Al-Emran, M. and Shaalan, K. (2023) ‘Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories’, Applied Sciences, 13(9), p. 5700. Available at: <https://doi.org/10.3390/app13095700>.
4. Rohan, R. et al. (2023) ‘A systematic literature review of cybersecurity scales assessing information security awareness’, Heliyon, 9(3). Available at: <https://doi.org/10.1016/j.heliyon.2023.e14234>.
5. Khan, N.F. et al. (2022) ‘The cybersecurity behavioral research: A tertiary study’, Computers & Security, 120, p. 102826. Available at: <https://doi.org/10.1016/j.cose.2022.102826>.
6. Rohan, R. et al. (2021) ‘Understanding of Human Factors in Cybersecurity: A Systematic Literature Review’, in 2021 International Conference on Computational Performance Evaluation (ComPE). IEEE, pp. 133–140. Available at: <https://doi.org/10.1109/ComPE53109.2021.9752358>
7. Rahman, T. et al. (2021) ‘Human Factors in Cybersecurity: A Scoping Review’, ACM International Conference Proceeding Series [Preprint]. Available at: https://doi.org/10.1145/3468784.3468789.
8. Maalem, A. et al. (2020) ‘Review and insight on the behavioral aspects of cybersecurity’, Cybersecurity, 3(1), p. 10. Available at: https://doi.org/10.1186/s42400-020-00050-w.