Towards Security Awareness Enhancement using Dynamic and Adaptive Behavior Learning Models

Preshika Basnet, Isha Nepal, Rasib Khan
School of Computing and Analytics, College of Informatics
Northern Kentucky University, KY, USA
basnetp1@mymail.nku.edu, nepali1@mymail.nku.edu, khanr2@nku.edu (*corresponding author*)

***Abstract*—As cyber threats continue to evolve alongside various forms of technological advancements, human behavior remains a critical vulnerability in modern security infrastructures. Understanding and addressing users' personalized behavioral traits is vital to strengthening an organization's overall security posture, as even well-designed technical defenses can be compromised by poor decision-making or lack of awareness. This paper proposes a dynamic, AI-driven cybersecurity framework that leverages User and Entity Behavior Analytics (UEBA), Machine Learning (ML), and Large Language Models (LLMs) to deliver personalized, real-time security awareness and training modules. Built on a feedback- and feedforward-enhanced Input-Process-Output (IPO) model, the system analyzes multi-modal behavioral data to detect anomalies, optimize policies, and adapt training content dynamically. The framework enhances engagement, improves long-term security behavior, and strengthens organizational resilience against emerging threats. Empirical evaluation demonstrates the model's scalability and effectiveness, while addressing challenges related to data privacy, integration complexity, and contextual adaptability.**

***Keywords*-Cybersecurity Awareness, User and Entity Behavior Analytics, Machine Learning, Large Language Models, Adaptive Training, Human-Centric Security.**

I. Introduction

In an era of unprecedented digital connectivity, cybersecurity vulnerabilities have grown significantly, with human factors becoming one of the most critical and frequently exploited security weaknesses [1–3]. Despite robust technical defenses, users often remain the weakest link due to varying levels of security awareness [4, 5]. Traditional cybersecurity training programs are mostly static and fail to adjust to individual user behaviors or evolving threats, thereby reducing their effectiveness over time [6, 7].

This paper presents a novel security-oriented awareness and training framework employing User and Entity Behavior Analytics (UEBA), Machine Learning (ML), and Large Language Models (LLMs). The concept overview is illustrated in Figure 1. Our adaptive model dynamically customizes security training based on real-time analysis of user behavior, continuously refining its approach to effectively enhance cybersecurity awareness.

The rest of the paper is organized as follows. Section II presents the background and motivation for the proposed work. Section III presents the details of the proposed framework. Detailed analysis of the proposed approach is presented in Section IV. The related work is presented in Section V, and finally, the conclusion and future work are presented in Section VI.

979-8-3315-2508-8/25/$31.00 ©2025 IEEE

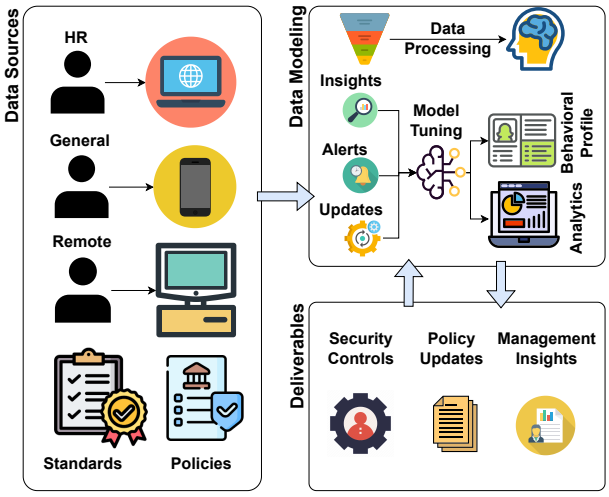

Fig. 1: System Concept Overview

II. Background and Motivation

Cyber threats have dramatically increased with advancements in Artificial Intelligence, highlighting vulnerabilities arising from human error or negligence [3, 8]. Existing cybersecurity training primarily utilizes static content, neglecting the varying levels of users' awareness and failing to adapt dynamically as threats evolve [2]. These static approaches lead to redundant training, wasted resources, and poor long-term retention. Empirical evidence suggests that personalized and adaptive training significantly enhances learning outcomes and behavior retention compared to generic training sessions [6]. Consequently, addressing the lack of dynamic adaptability and user-centric personalization in cybersecurity training has become a pressing research necessity.

Problem Statement: *Current cybersecurity training methodologies are generalized and insufficiently adaptive, resulting in inadequate engagement and ineffective defense against rapidly evolving cyber threats. A critical gap exists in developing training that dynamically learns and adapts to individual users' cybersecurity behaviors, leading to increased vulnerability due to human errors.*

As illustrated in Figure 1, our research addresses this gap by proposing a dynamic, adaptive, behavior-focused cybersecurity

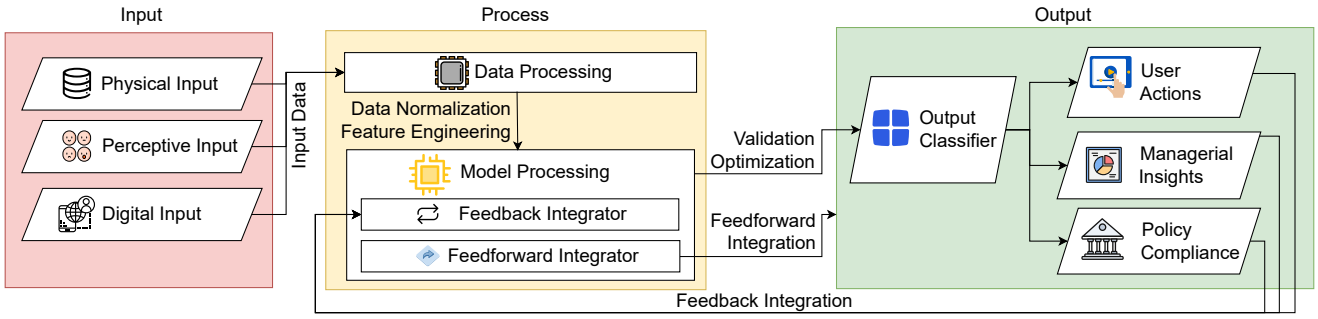

Fig. 2: System Model

training framework, integrating UEBA, ML, and LLM technologies to enhance real-time security awareness and mitigate human-driven vulnerabilities.

III. System Model

Our framework employs the Input-Process-Output (IPO) model with integrated feed-forward and feedback control loops to proactively address human behavior-driven security vulnerabilities and take effective countermeasures. By leveraging User and Entity Behavior Analytics (UEBA), Machine Learning (ML), and Large Language Models (LLMs), the system dynamically adapts to emerging threats, enhancing security scalability and resilience. The system model for the proposed approached is illustrated in Figure 2. The system aggregates security-related data from diverse sources, categorizing inputs into three key types:

- *Physical Inputs* include access logs, device usage patterns, and security infrastructure monitoring;
- *Perceptive Inputs* capture user behavior metrics, security training effectiveness, and phishing response data; and
- *Digital Inputs* consist of login patterns and anomalies, system activity logs, VPN usage patterns, and other network-based security signals.

Once collected, in the process layer, the data undergoes structured transformations, which include operations such as cleaning, aggregation, and feature vector engineering. Once prepared in useful formats, the data is then processed through the ML component to be analyzed towards generating behavioral analytics models. The core analytical components include the following elements:

- *Behavioral Anomaly Detection*, which identifies deviations in user interactions that indicate potential security risks;
- *Threat Detection and Risk Profiling*, which assesses deviations from security benchmarks to uncover emerging vulnerabilities; and
- *Adaptive Learning with Policy Optimization*, which employs feed-forward and feedback learning loops to refine risk models and dynamically adjust security policies based on new threat intelligence.

Beyond the process layer is the output later, which generates real-time security intelligence to inform users, managers, and policy enforcers, ensuring robust security operations. The elements of the output layer are as follows:

- *User Level* outputs include modules generated towards personalized security recommendations, adaptive training modules, and real-time feedback;
- *Management Level* outputs include documentation and reports on comprehensive risk assessments, security performance dashboards, and compliance tracking reports; and
- *Automated Policy Enforcement* outputs include functional components and updates for continuous monitoring of security protocols, adaptive access controls, and regulatory compliance adjustments.

By integrating a continuous feedback loop, the framework ensures ongoing threat detection, proactive risk mitigation, behavioral changes, and behavior-driven security awareness. The feed-forward loop reinforces policy adherence by preemptively aligning user actions with cybersecurity best practices and policy benchmarks, enabling a resilient and adaptive security posture across the organization.

IV. Model Analysis

The preliminary stature of the proposed model analysis suggests that the framework holds significant promises and identifies several key strengths and critical concerns, and are explained as follows:

A. User-Centric Strengths

Tailored cybersecurity interventions: The model utilizes analytical capabilities to offer highly personalized cybersecurity training interventions, targeting specific user vulnerabilities and improving overall cybersecurity awareness effectively.

Long-term retention and motivation: By employing continuous adaptation and iterative feedback mechanisms, the framework ensures sustained engagement and improved long-term retention of security practices.

B. Operational and Managerial Strengths

Scalability and customization: Our model is scalable and customizable to diverse organizational needs. Adaptive learning mechanisms ensure personalized feedback and tailored interventions based on user-specific behaviors and security awareness levels.

Measurable behavior and performance: The model generates quantitative metrics to measure and continuously improve

user security behaviors, training effectiveness, and adherence to security policies.

Data-driven decision-making for managers: The model provides detailed managerial insights through actionable risk reports, performance metrics, and decision logs, enabling informed and strategic decisions regarding cybersecurity policies and resource allocation.

C. Technical and Integration Strengths

Integrated and Interdisciplinary approach: The framework effectively combines technical aspects (AI, ML, UEBA, and LLM) with human factors, enabling comprehensive cybersecurity awareness through integrated multisource data collection.

Real-time adaptive security: The model continuously monitors user behavior using AI-driven analytics, dynamically adjusting security measures and training based on identified risks and threats, thus proactively reducing vulnerabilities.

D. Potential Concerns and Mitigation Strategies

Complexity of Implementation and Data Integration: Combining advanced technologies like UEBA, ML, and LLMs introduces significant complexity, requiring substantial resources. Mitigation involves modular architecture, phased deployment, and clearly defined integration standards.

Dependence on Data Quality: The accuracy of behavioral analysis and training effectiveness relies heavily on the quality of the input data. Enforcing rigorous validation of multi-modal data, continuous audits, and adaptive recalibration of analytical models is required to ensure effective continuity of operation.

Cultural and Contextual Sensitivity: Human behaviors related to cybersecurity are heavily influenced by cultural, organizational, and individual contexts. To address this, the framework integrates customizable training content and culturally-aware algorithms for enhanced relevance and effectiveness.

Resource Planning and Sustainability: Effective deployment and maintenance of the adaptive framework require careful planning of financial resources, infrastructure investments, skilled personnel, and ongoing operational costs. This can be addressed through detailed strategic planning and phased resource allocation.

Data Privacy and Security Concerns: Extensive collection and analysis of user data pose significant privacy and ethical challenges. The framework adheres strictly to data protection regulations (e.g., GDPR), enforces robust data governance practices, implements stringent security measures, and ensures transparency in data utilization.

V. Related Work

Traditional, non-targeted cybersecurity awareness methods are often ineffective because the level of awareness varies greatly among employees [6]. Recent research has extensively explored the use of AI, Machine Learning and UEBA to understand how advanced technologies can be leveraged to enhance human-centric cybersecurity [6, 9, 10]. Jawhar et al. highlights the use of AI, developed APIs to generate cybersecurity awareness training content tailored to learner's skills and required levels but lacks continuous real-time adaptation driven by human behavior [11]. Mashhour et al. proposed a machine-learning based model that analyzed user's online behavior by leveraging UEBA to classify them into different risk categories to provide targeted cybersecurity awareness training sessions [6]. While these works advance personalized training through static or risk-based customization, they do not integrate real-time behavioral adaptation or continuous feedback loops. Our framework addresses this gap by dynamically adjusting training content and security policies based on live UEBA-driven insights, ensuring interventions evolve alongside emerging threats and user behaviors.

Taherdoost introduced an Integrated Cybersecurity Awareness and Training (iCAT) model which leverages knowledge graphs and gamification to enhance user engagement and knowledge retention that offered more innovative training model going beyond traditional approaches [8]. Hatzivasilis et al. presented an educational methodology for the dynamic adaptation of cybersecurity training programees by combining pedagogical practices (like Bloom's taxonomy) and cybersecurity modelling (like STRIDE) within a cyber-range's platform [1]. Our framework extends these approaches by integrating LLMs for context-aware feedback and ML-driven anomaly detection, enabling immediate, personalized responses to behavioral deviations.

Frank et al. discussed the potential of AI for user-centric cybersecurity measures, including adaptive security awareness training, through a literature review and expert Delphi study which showed the AI's role in analyzing behavioral pattern pattens to identify at-risk groups to target them with specific security training [9]. Das et al. investigated how tailored learning experiences using AI affected academic achievement and engagement which demonstrated high potential of AI-driven personalization for improved learning outcomes [10]. While these studies underscore AI's role in personalization, they focus on periodic or group-level adaptations. Our framework uniquely combines UEBA, ML, and LLMs to deliver individualized, real-time feedback within a continuous learning loop, enhancing both engagement and threat responsiveness.

Greitzer et al. developed three different psychosocial models using ML and Neural networks to predict behavior relevant to security risks that identified the employees at risk of becoming insider threats based on behavioral insights and experts HR judgements [12]. Our research advances these foundations in a novel approach towards anomaly detection, and LLMs for personalized feedback. Unlike prior works, our model operates within a continuous learning loop, proactively refining training content and security policies based on live data. This approach transcends static or periodic adaptations, addressing the evolving nature of cyber threats and human vulnerabilities through seamless technical-human integration.

VI. Conclusion and Future Work

This study underscores the critical importance of adopting robust security practices to address the challenges posed by rapid technological advancements and digitization. The proposed framework prioritizes key aspects of organizational security, offering scalability and adaptive learning capabilities that enhance performance and provide valuable insights into behavioral security dynamics. However, its implementation faces limitations such as complexity, dependence on data quality, and concerns regarding data privacy and sensitive information.

Our future research will focus on overcoming these limitations by exploring direct applications of the framework in operational settings and refining its adaptability to diverse organizational contexts. Practical implementation strategies must align with organizational priorities while addressing emerging threats and compliance requirements. By maintaining equilibrium between innovation and existing constraints, subsequent studies can further enhance security practices, ensuring a proactive approach to safeguarding digital assets in an increasingly interconnected world.

References

[1] G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, and H. Koshutanski, "Modern aspects of cyber-security training and continuous adaptation of programmes to trainees," *Applied Sciences*, vol. 10, no. 16, p. 5702, 2020.

[2] M. F. Ansari, "A quantitative study of risk scores and the effectiveness of ai-based cybersecurity awareness training programs," *International Journal of Smart Sensor and Adhoc Network*, vol. 3, no. 3, pp. 1–8, 2022.

[3] R. Khan and R. Hasan, "The story of naive alice: Behavioral analysis of susceptible internet users," in *Proceedings of the IEEE 40th Annual Computer Software and Applications Conference*, ser. COMPSAC. Altanta, GA, USA: IEEE, 2016.

[4] A. AlQadheeb, S. Bhattacharyya, and S. Perl, "Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior," *Array*, vol. 14, p. 100124, 2022.

[5] R. Khan and R. Hasan, "Security-aware passwords and services usage in developing countries: A case study of bangladesh," in *In Proceedings of the 15th Services Computing International Conference (SCC), Held as Part of the Services Conference Federation (SCF)*, ser. SCC, SCF. Springer, 2018, pp. 67–84.

[6] A. Al-Mashhour and A. Alhogail, "Machine-learning-based user behavior classification for improving security awareness provision," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, 2023.

[7] C. Kallonas, A. Piki, and E. Stavrou, "Empowering professionals: A generative ai approach to personalized cybersecurity learning," in *2024 IEEE Global Engineering Education Conference (EDUCON)*, 2024, pp. 1–10.

[8] H. Taherdoost, "Towards an innovative model for cybersecurity awareness training," *Information*, vol. 15, no. 9, p. 512, 2024.

[9] M. Frank, M. Brennecke, P. Holzmer, N. Pocher, and G. Fridgen, "Potential of ai for user-centric cybersecurity in the financial sector," in *Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS)*, 2025.

[10] A. Das, S. Malaviya, and M. Singh, "The impact of ai-driven personalization on learners' performance," *International Journal of Computer Sciences and Engineering*, vol. 11, no. 8, pp. 15–22, 2023.

[11] S. Jawhar, J. Miller, and Z. Bitar, "Ai-driven customized cyber security training and awareness," in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, 2024, pp. 1–5.

[12] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, "Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats," in *2012 45th Hawaii International Conference on System Sciences*, 2012, pp. 2392–2401.