A Security-Oriented Awareness and Training Framework using Dynamic and Adaptive Behavior Learning Models

Preshika Basnet and Isha Nepal **Faculty Advisor: Rasib Khan, Ph.D.**

Motivation

Overview

This research presents a model unified framework model to enhance security awareness and reduce human-driven organizational and operational security vulnerabilities. By combining User and Entity Bhevior Analytics (UEBA), Machine Learning (ML), and Large Language Models (LLMs), the model adapts to user behaviors in real time, providing personalized feedback to strengthen cybersecurity practices.

Security Issues

- Lack of cybersecurity awareness
- Human error as a major risk factor
- Inconsistent security practices
- Lack of personalized security training
- Limited adaptive learning in security education

Research Gap

Current solutions focus mainly on technical defenses, neglecting the human aspect. While there are tools to track user behavior, most are static or lack the adaptability needed to address the diverse range of user behavior. Our approach bridges this gap by using dynamic learning to address diverse user behaviors and improve security awareness effectively.

Proposed Solution

The model leverages UEBA, ML, and LLMs to analyze and classify user behavior, offering real-time, personalized feedback through gamification, training, and documentation. By making security education scalable and adaptive, the framework helps organizations reduce human-related risks and build stronger cybersecurity practices.

System Model

Our holistic framework applies the Input-Process-Output (IPO) model with Feedforward and Feedback control-loops to proactively mitigate human behavior driven security vulnerabilities.

By leveraging User and Entity Behavior Analytics (UEBA), Machine Learning (ML), and Large Language Models (LLMs), the system continuously adapts to emerging threats and ensures scalable security enhancements.

***Input*: Multi-Source Data Collection**

The system aggregates security-related data from multiple variable-type sources. The framework gathers data from three key source categories:

- **Physical Input** – Access logs, device usage, and security infrastructure monitoring.
- **Perceptive Input** – User behavior, training effectiveness, and phishing response rates.
- **Digital Input** – Login patterns, system activity, VPN usage, and anomaly detection.

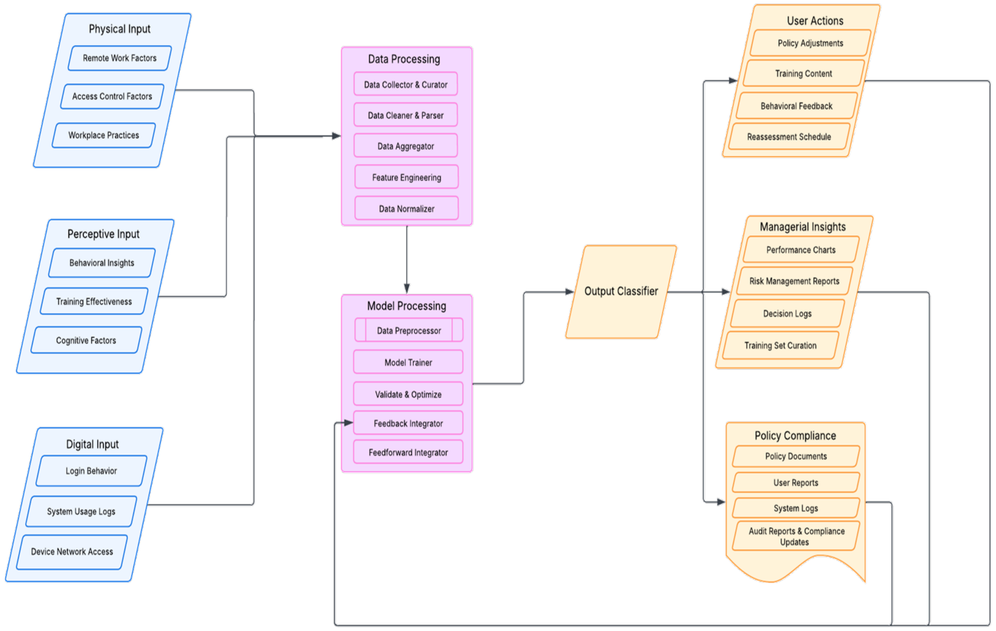

Fig: Input Processing Output (IPO) Model

***Output*: Actionable Security Insights**

The system generates real-time security intelligence to improve awareness, response strategies, and policy enforcement:

- **User Actions** – Personalized security training, behavior-based feedback, and reassessment schedules.
- **Managerial Insights** – Risk reports, performance metrics, and decision logs.
- **Policy Compliance** – Automated security policy adjustments, compliance tracking, and audit documentation.

By integrating a continuous feedback loop, the framework enhances threat detection, fosters security awareness, and ensures proactive risk mitigation across an organization.

***Process*: Intelligent Risk Analysis**

Once collected, data undergoes a series of transformations, including cleaning, aggregation, and feature engineering, before being analyzed through advanced ML models. The core analytical processes include:

- **Behavior Analysis** – Identifying anomalies in user interactions.
- **Threat Detection** – Detecting deviations from established security benchmarks.
- **Adaptive Learning** – Refining risk models based on feedforward and feedback loops for evolving threats.

Model Assessment

Benefits and Advantages

- Integrated and interdisciplinary approach
- Long-term retention and motivation
- Scalability and customization
- Measurable behavior and performance
- Tailored cybersecurity interventions
- Real-time adaptive security
- Personalization and user-centric approach
- Iterative learning through feedback loops
- Data-driven decision making for managers

Concerns and Pitfalls

- Complexity of implementation
- Dependence on data quality
- Cultural and contextual sensitivity
- Requires careful resource planning
- Data privacy and security concerns
- Complexity of data integration

Key References

1. Arwa AlQadheeb, Siddhartha Bhattacharyya, Samuel Perl, Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior Array, 14, https://doi.org/10.1016/j.array.2022.100146.
2. Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. Information, 15(9), 512. https://doi.org/10.3390/info15090512
3. Al-Mashhour, A., & Alhogail, A. (2023). Machine-learning-based user behavior classification for improving security awareness provision. International Journal of Advanced Computer Science and Applications, 14(8), https://doi.org/10.14569/IJACSA.2023.0140819