Social Engineering Simulator: Enhancing Cybersecurity Awareness Through Realistic Simulation

Modadugu Sai Yaswanth
Assistant Professor
Department of Cyber Security
Narasaraopeta Engineering College
Narasaraopet, Palnadu, India
yaswanthsai225@gmail.com

Devu Bala Brahmaji
Department of Cyber Security
Narasaraopeta Engineering College
Narasaraopet, Palnadu, India
balabrahmajid@gmail.com

Ramavath Lekhya
Department of Cyber Security
Narasaraopeta Engineering College
Narasaraopet, Palnadu, India
lekhyaramavath@gmail.com

Vankayalapati Rahul Babu
Department of Cyber Security
Narasaraopeta Engineering College
Narasaraopet, Palnadu, India
Rahulbabuvankayalapati4@gmail.com

G. Ramesh
Department of CSE,
GRIET, Hyderabad,
Telangana, India.
ramesh680@gmail.com

Jyothi Uppari
Department of Information Technoldgy,
GNITS(for women)
Shaikpet,Hyderabad,
Telangana, India
Jyothi.uppari@gnits.ac.in

***Abstract*— Social engineering attacks continue to pose a serious threat to modern organizational security by exploiting human behavior rather than technical weaknesses. This paper presents the design and implementation of a Social Engineering Simulator developed to enhance cybersecurity awareness through realistic and controlled attack simulations. The proposed system replicates common attack vectors including phishing, vishing, smishing, impersonation, and baiting to evaluate user responses and improve decision-making skills in high-risk situations. The simulator integrates automated campaign management, behavioral analytics, real-time monitoring, and feedback mechanisms to strengthen organizational resilience against human-centric threats. A modular architecture consisting of frontend, backend, database, and detection layers supports scalability and efficient data processing. Machine learning–based analysis enables identification of risky patterns and supports adaptive training strategies tailored to user performance. Experimental evaluation demonstrates improvements in user awareness, reduced response time to suspicious activities, and measurable decline in unsafe interactions during repeated simulations. The findings indicate that immersive simulation-based training enhances preparedness compared to traditional awareness programs. The system provides a practical, scalable, proactive approach for organizations seeking to minimize human-factor vulnerabilities and build a strong security culture against evolving social engineering threats.**

Keywords—Social Engineering, Cybersecurity Awareness Training, Phishing Simulation, Human-Centric Security, Behavioral Security Analytics, Insider Threat Detection, Cyber Attack Simulation, Security Awareness Systems.

I. INTRODUCTION

Social engineering has become one of the most critical challenges in modern cybersecurity

because attackers increasingly exploit human psychology rather than technical system vulnerabilities. Techniques such as phishing, vishing, smishing, impersonation, and physical intrusion attacks manipulate trust, urgency, fear, and authority to deceive users into disclosing sensitive information or performing unsafe actions. These attacks frequently bypass conventional technical defenses and continue to cause significant financial losses, operational disruption, and reputational damage across organizations worldwide [13], [14]. Reports consistently indicate that human error remains a dominant factor in successful cyber incidents, emphasizing the importance of strengthening user awareness alongside technological protection mechanisms [3], [18].

Traditional awareness programs typically rely on theoretical instruction or periodic training modules, which often fail to produce lasting behavioral change due to limited engagement and lack of realistic exposure [20]. As attackers employ increasingly sophisticated and context-aware strategies, organizations require training approaches that simulate real-world threats and measure user responses in practical environments. Simulation-based learning platforms have emerged as effective tools for improving decision-making skills by exposing individuals to controlled but realistic attack scenarios, enabling continuous evaluation of behavioral patterns and vulnerabilities [16].

The development of a Social Engineering Simulator addresses this need by integrating realistic attack simulations with behavioral analytics and automated performance assessment. By combining immersive training with data-driven insights, organizations can identify high-risk behaviors, deliver targeted awareness programs, and build a proactive cybersecurity culture capable of defending against evolving social engineering threats [1], [8].

II. Literature Survey

Social engineering attacks have been widely studied due to their increasing effectiveness in bypassing technical security controls by exploiting human behavior. Early research primarily focused on phishing detection techniques using rule-based filters and traditional machine learning approaches to analyze email content, metadata, and structural patterns [1], [2]. Surveys on phishing detection emphasized the importance of combining textual analysis with behavioral indicators to improve detection accuracy and reduce false positives [8], [9]. These studies demonstrated that attackers continually adapt communication strategies, making static detection models insufficient for long-term protection [3].

With the advancement of deep learning and natural language processing, researchers began developing intelligent detection systems capable of understanding contextual and semantic relationships within malicious messages. Transformer-based architectures and neural network models significantly improved the detection of sophisticated phishing attempts by capturing subtle linguistic patterns and user interaction behaviors [11], [16]. Word embedding techniques and representation learning further enhanced the performance of automated classification systems by enabling deeper semantic analysis of communication data [10], [12].

In addition to technical detection mechanisms, awareness-based cybersecurity training has received significant attention as a critical component of defense strategies. Studies have shown that immersive and simulation-driven training programs increase user vigilance, reduce susceptibility to attacks, and improve reporting behavior compared to traditional theoretical learning methods [18], [20]. Organizational reports also confirm that repeated simulations and real-world scenario exposure significantly lower click-through rates and strengthen incident response readiness [13], [15]. However, many existing solutions address detection and training separately, creating a gap in integrated systems that combine behavioral analytics, adaptive simulations, and continuous risk evaluation. The proposed Social Engineering Simulator addresses this limitation by merging intelligent detection with interactive simulation-based awareness training.

III. Proposed System

The proposed Social Engineering Simulator is designed to enhance cybersecurity awareness by providing a realistic and interactive training environment that evaluates human behavior under simulated attack conditions. The system enables organizations to conduct controlled simulations of phishing, smishing, vishing, impersonation, and other social engineering techniques to assess user responses and identify vulnerabilities. Unlike traditional awareness programs that rely on theoretical instruction, the proposed system emphasizes experiential learning through practical exposure to real-world attack scenarios [18], [20].

The platform allows administrators to design customized simulation campaigns based on current threat trends and organizational requirements. Simulated communications are delivered through multiple channels such as email, messaging platforms, or web interfaces to replicate authentic user experiences. During each campaign, the system monitors user actions including link clicks, credential submissions, reporting behavior, and response time, generating measurable performance metrics that reflect awareness levels [13].

A multi-layer analytical framework enhances the system's effectiveness. The first analytical layer applies natural language processing and classification models to evaluate communication content and identify phishing-like patterns [11]. The second layer analyzes behavioral patterns and interaction history to detect risky decision-making and potential insider threat indicators over time [19]. Automated feedback mechanisms provide immediate educational guidance following each simulation, reinforcing learning outcomes and encouraging improved future performance [20].

Additionally, the system features centralized dashboards and reporting tools that present risk scores, awareness trends, and organizational performance summaries. These analytics enable management to identify high-risk users, measure training effectiveness, and develop targeted awareness strategies. By combining realistic simulations with intelligent behavioral analysis, the proposed system offers a scalable and proactive solution for strengthening human-centric cybersecurity defenses and reducing susceptibility to evolving social engineering threats [16], [1], [8].

IV. METHODOLOGY

The methodology of the proposed Social Engineering Simulator focuses on delivering realistic attack simulations while collecting structured behavioral data to evaluate user awareness and improve cybersecurity readiness. The process begins with the development of attack scenarios based on real-world threat intelligence and commonly observed social engineering techniques such as phishing, smishing, impersonation, and pretexting. These scenarios are carefully designed to replicate authentic communication patterns, psychological triggers, and contextual elements used by attackers, ensuring realistic user interaction and accurate behavioral assessment [17], [18].

Once scenarios are prepared, simulation campaigns are executed by delivering crafted messages or prompts to target users through email interfaces, web portals, or messaging platforms. Users interact with these simulated communications without prior disclosure to replicate real-world decision-making conditions. During each simulation, the system captures detailed interaction data including link clicks, credential submissions, reporting behavior, and response time. This data is then passed through preprocessing modules that remove redundant entries, standardize textual inputs, and organize behavioral logs into structured datasets suitable for analysis [11].

Feature extraction techniques convert raw communication content and user activity into measurable indicators such as linguistic patterns, metadata characteristics, and interaction frequency. Machine learning models analyze message content to evaluate phishing probability using the following formulation:

$$P = \sigma(WX + b)$$

where X represents extracted feature vectors and W and b are learned model parameters. In parallel, a behavioral risk score is calculated to assess user susceptibility:

$$RiskScore = \frac{W_c \times Click + W_s \times Submission + W_r \times ResponseTime}{TotalInteractions}$$

This scoring mechanism enables identification of high-risk users and patterns requiring additional training.

Algorithm: Simulation Evaluation and Risk Analysis

Initialization Phase: The process begins by defining simulation objectives, selecting appropriate social engineering scenarios, and configuring campaign parameters such as attack type, difficulty level, and delivery channels. Target users are identified, and the simulation environment is prepared for execution.

Simulation Execution Phase: Simulated communications are delivered to users through predefined interfaces such as email or web

platforms. During the interaction, the system monitors and records user activities including clicks, credential submissions, reporting behavior, and response time to evaluate real-time decision-making patterns.

Data Processing Phase: The collected interaction data undergo preprocessing to remove redundant entries and normalize textual content. Feature extraction techniques are then applied to derive linguistic attributes from messages and behavioral indicators from user actions, converting raw logs into structured analytical data.

Risk Analysis Phase: Extracted features are processed using classification models to estimate phishing probability, while behavioral metrics are used to compute individual risk scores through weighted evaluation parameters. This stage identifies patterns indicating susceptibility to social engineering attacks.

Feedback and Storage Phase: Based on the analysis results, the system generates automated awareness feedback and training recommendations tailored to user performance. Finally, all processed data, risk scores, and interaction records are securely stored in the analytics database to support reporting, future simulations, and continuous improvement of awareness programs.

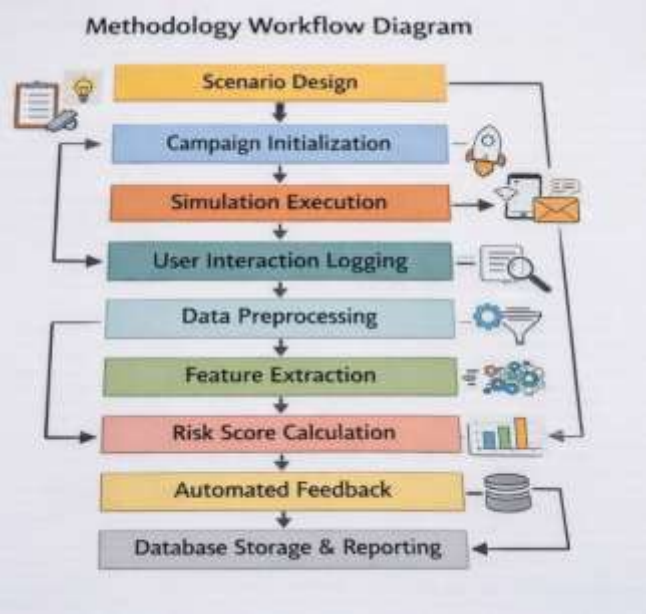

Fig. 1: Methodology Workflow Diagram

Table 1: Dataset Description.

Parameter	Description
Number of Users	100–500 (example)
Simulation Types	Phishing, Smishing, Vishing, Impersonation
Features Extracted	Linguistic, Metadata, Click Behavior, Response Time
Total Campaigns Conducted	5–10
Behavioral Metrics	Click Rate, Report Rate, Credential Submission
Output Labels	Safe / Risky / High Risk
Storage Type	Encrypted SQL Database

V. SYSTEM ARCHITECTURE

The proposed Social Engineering Simulator is developed using a modular and scalable architecture designed to support realistic attack simulations, behavioral monitoring, and intelligent threat analysis. The system is organized into multiple layers, including the frontend interface, backend processing engine, analytical detection layer, database storage, and external integration components. This layered architecture ensures flexibility, efficient data processing, and seamless integration with existing organizational infrastructure [10], [11].

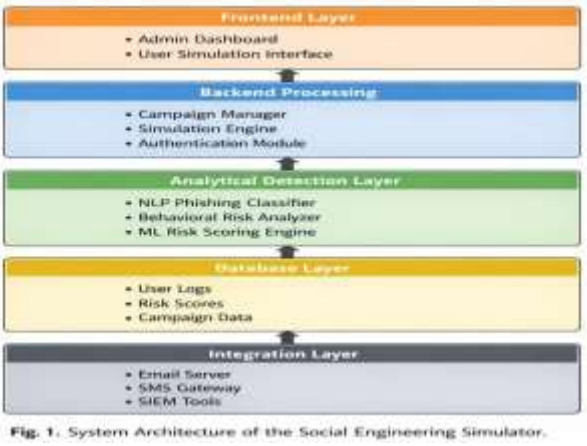

Fig. 2: System Architecture Diagram illustrating layered simulator components.

The **frontend layer** provides an interactive web-based interface through which administrators create simulation campaigns, configure attack scenarios, and monitor user performance through analytical dashboards. End users interact with simulated communications that closely resemble real-world emails, messages, or system prompts, enabling accurate behavioral evaluation [10].

The **backend processing layer** manages core system operations such as simulation scheduling, campaign execution, user authentication, and data handling. It

processes user interactions in real time and coordinates communication between system components to ensure efficient workflow execution [11].

The **analytical detection layer** integrates machine learning models and behavioral analytics modules. Content analysis models evaluate simulated communications for phishing characteristics, while behavioral analysis modules monitor user activity patterns and calculate risk scores based on interaction history [16], [19].

The **database layer** securely stores simulation logs, user interaction records, training metrics, and system configurations using encrypted storage mechanisms to maintain data confidentiality and integrity [13]. Efficient indexing enables rapid data retrieval for reporting and analytics.

Finally, the **integration layer** connects the simulator with external systems such as email servers, SMS gateways, HR platforms, and Security Information and Event Management (SIEM) tools. These integrations enable automated campaign delivery, centralized monitoring, and comprehensive incident tracking across organizational environments [2], [19].

Table 2:. Comparison Between Existing Two-Layer Detection Systems and the Proposed Multi-Layer Intelligent Detection Framework(MIDF).

Feature	Existing Two-Layer Systems	Proposed MIDF
Content Detection	Yes	Yes
Behavioral Analysis	Limited	Advanced Multi-Session
Risk Scoring	Basic	Weighted Behavioral + ML
Simulation Capability	No	Yes
Adaptive Training	No	Yes
Real-Time Monitoring	Partial	Yes
Insider Threat Indicators	No	Yes
Feedback Automation	No	Yes

VI. RESULTS AND ANALYSIS

The effectiveness of the proposed Social Engineering Simulator was evaluated through multiple simulation campaigns designed to measure user awareness, behavioral responses, and susceptibility to social engineering attacks. Simulations included phishing emails, smishing messages, and impersonation scenarios delivered to participants in controlled environments. During each campaign, the system recorded interaction metrics such as click rates, reporting behavior, credential submission attempts, and response time. These metrics were analyzed to assess awareness improvement and the impact of repeated simulation-based training.

Initial simulation results indicated higher click-through rates and delayed reporting behavior, reflecting limited awareness among users during early stages. However, after receiving automated feedback and targeted training recommendations, subsequent campaigns showed significant reductions in unsafe interactions and faster incident reporting. The system's analytical modules successfully identified high-risk users and behavioral patterns, enabling administrators to implement personalized awareness programs and monitor organizational security posture over time [13], [18].

Machine learning–based content analysis achieved high classification performance in detecting phishing-like communication patterns, contributing to accurate behavioral evaluation and adaptive training strategies [16]. Visual analytics dashboards allowed administrators to track progress through awareness improvement graphs and risk score trends. Comparative analysis of campaign results demonstrated that repeated exposure to realistic simulations led to measurable improvements in user decision-making and increased vigilance when interacting with suspicious communications.

Fig 3 : Test Interface of the Social Engineering Awareness

Fig : 4. Phishing scenario interface showing timed decision options and user awareness ranking.

VII. FUTURE WORK

Future enhancements of the Social Engineering Simulator will focus on improving realism, adaptability, and analytical capabilities to address evolving cyber threats. Advanced artificial intelligence techniques can be incorporated to generate adaptive and context-aware attack scenarios that dynamically adjust difficulty levels based on individual user behavior and historical performance [16]. The inclusion of voice-based simulations, mobile-oriented attack modeling, and social media threat scenarios will expand coverage of emerging attack vectors [14]. Integration with real-time threat intelligence platforms and organizational security systems such as SIEM solutions can enable automated risk alerts and continuous monitoring capabilities [19]. Additionally, gamified training approaches and personalized learning pathways may enhance user engagement and long-term retention of cybersecurity practices [20]. Future research can also explore predictive behavioral analytics models capable of identifying high-risk patterns and potential insider threats before incidents occur [13], thereby strengthening proactive defense strategies and ensuring long-term effectiveness of the simulation platform.

REFERENCES

[1] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg and E. Almomani, "A survey of phishing email filtering techniques," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2070–2090, 2013.

[2] M. Aburrous, M. A. Hossain, K. Dahal and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," Expert Systems with Applications, vol. 37, no. 12, pp. 7913–7921, 2010.

[3] J. Hong, "The state of phishing attacks," Communications of the ACM, vol. 55, no. 1, pp. 74–81, 2012.

[4] K. Thomas et al., "Data breaches, phishing, or malware? Understanding the risks of credential exposure on the web," in Proc. ACM Internet Measurement Conf. (IMC), pp. 125–136, 2017.

[5] T. Abdelhamid, A. Ayesh and F. Thabtah, "Phishing detection based associative classification data mining," Expert Systems with Applications, vol. 41, pp. 5948–5959, 2014.

[6] S. Garera, N. Provos, M. Chew and A. D. Rubin, "A framework for detection and measurement of phishing attacks," in Proc. ACM Workshop on Recurring Malcode (WORM), pp. 1–8, 2007.

[7] S. Abu-Nimeh, D. Nappa, X. Wang and S. Nair, "A comparison of machine learning techniques for phishing detection," in Proc. Anti-Phishing Working Groups eCrime Researchers Summit, pp. 60–69, 2008.

[8] M. Khonji, Y. Iraqi and A. Jones, "Phishing detection: A literature survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091–2121, 2013.

[9] G. Kim, S. Yang and H. Park, "Email phishing detection using machine learning techniques," Information Systems Security, vol. 23, no. 2, pp. 103–114, 2014.

[10] T. Mikolov et al., "Efficient estimation of word representations in vector space," arXiv:1301.3781, 2013.

[11] J. Devlin, M.-W. Chang, K. Lee and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," in Proc. NAACL-HLT, 2019.

[12] Y. Goldberg, Neural Network Methods for Natural Language Processing. Morgan & Claypool, 2017.

[13] Verizon, "Data Breach Investigations Report," 2023.

[14] ENISA, "Phishing Threat Landscape," European Union Agency for Cybersecurity, 2022.

[15] SANS Institute, "Why phishing awareness training works," 2019.

[16] M. Alazab et al., "Machine learning applications for social engineering attack detection," IEEE Access, vol. 9, pp. 121387–121399, 2021.

[17] D. Cooper and M. Edge, "Tailgating in physical security: Risks and mitigations," Security Management Journal, vol. 45, no. 3, pp. 21–30, 2020.

[18] W. Alasmary et al., "Awareness-based solutions for social engineering attacks," Computers & Security, vol. 77, pp. 94–109, 2018.

[19] CERT Insider Threat Center, Common Sense Guide to Mitigating Insider Threats, Software Engineering Institute, 2017.

[20] A. Ferreira et al., "Awareness-based security education: A strategy for reducing social engineering attacks," International Journal of Information Security Science, vol. 4, no. 1, pp. 1–14, 2015.