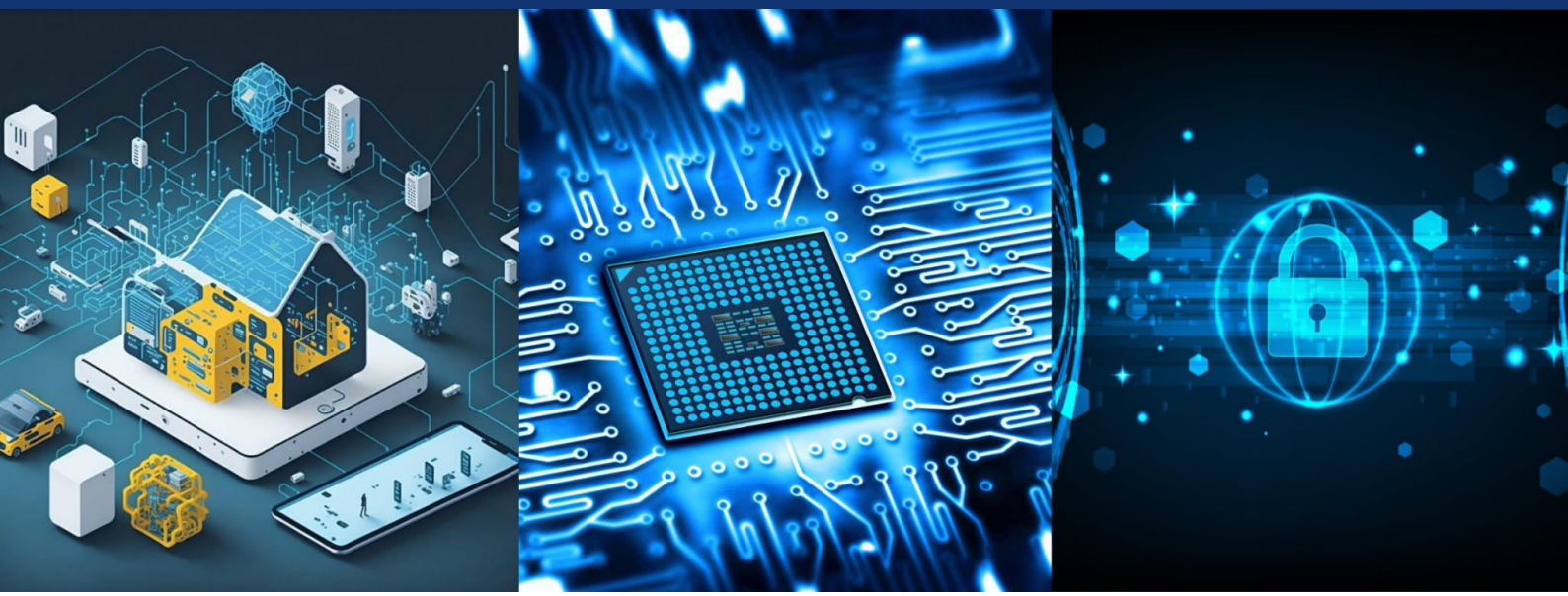
IJIRCCE

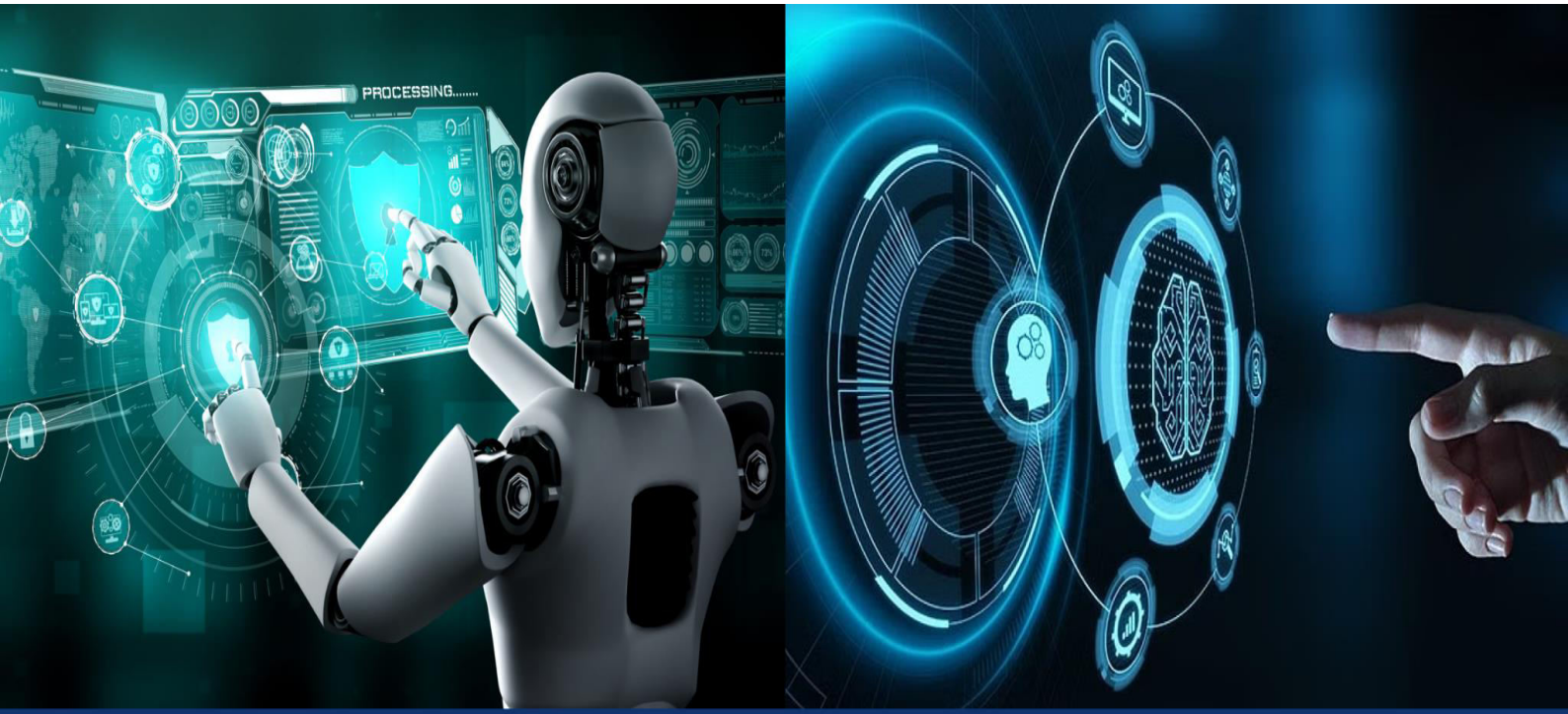
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CyberSafe: A Social Engineering Attack Simulation System

Netra Chandrakant Neman, Disha Ganesh Gawade, Samiksha Rakesh Patil,

Prof. Mansi Trivedi, Prof. Junaid Mandviwala

Department of Artificial Intelligence and Data Science, Rizvi College of Engineering, Bandra Mumbai, India

ABSTRACT: This paper presents an Interactive Cybersecurity Awareness and Training Platform designed to simulate real-world social engineering attacks such as phishing, smishing, pretexting, and scareware. The system enables users to engage in decision-based learning by interacting with realistic scenarios and receiving immediate feedback, scoring, and prevention guidance. A full-stack architecture using React, Node.js, and MongoDB ensures efficient user interaction, backend processing, and persistent data storage. The platform incorporates adaptive learning by analyzing user performance and identifying weak areas, thereby improving cybersecurity awareness and response capability. Experimental results show enhanced user understanding and decision-making accuracy after repeated interactions.

KEYWORDS: Social Engineering, Cybersecurity Awareness, Phishing, Smishing, Pretexting, Scareware, Attack Simulation, User Behavior, Adaptive Learning, Information Security.

I. INTRODUCTION

Social engineering attacks have become one of the most common and dangerous cybersecurity threats, targeting human behavior instead of technical vulnerabilities. Attackers use techniques such as phishing emails, fraudulent SMS messages (smishing), impersonation (pretexting), and fake security alerts (scareware) to manipulate individuals into revealing sensitive information. Due to a lack of awareness, many users fall victim to these attacks in their daily digital interactions.

With the increasing use of online platforms for communication, banking, and work, the risk of social engineering attacks has significantly increased. Traditional security systems focus mainly on protecting networks and software, but they often overlook the human factor, which remains the weakest link in cybersecurity. Therefore, there is a need for effective training systems that help users recognize and respond to such attacks in real-world situations.

The proposed Social Engineering Attack Simulator addresses this issue by providing an interactive and practical learning environment. It allows users to experience simulated attack scenarios, make decisions, and learn from their mistakes through feedback, prevention methods, and recovery steps. This approach helps improve user awareness and builds stronger resistance against social engineering attacks.

II. RELATED WORK

Existing cybersecurity training systems primarily rely on static content such as tutorials, videos, and quizzes, which provide basic awareness but lack interactivity and real-time decision-making practice. While some phishing simulation tools are available in enterprise environments, they are often limited in scope and do not offer adaptive learning or detailed feedback. Recent research emphasizes the importance of experiential learning and user behavior analysis in enhancing cybersecurity awareness. The proposed system addresses these limitations by integrating real-time simulation, adaptive learning, weak-area identification, and a scalable full-stack implementation.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROPOSED ALGORITHM

- The system begins with a secure login and authentication module to validate users and administrators.
- After authentication, role-based redirection is performed to either the User Dashboard or Admin Dashboard.
- The user selects an attack type such as Phishing, Smishing, Pretexting, or Scareware.
- The user then selects a difficulty level (Easy, Medium, Hard).
- Based on the selected parameters, the system retrieves scenarios from a predefined scenario pool (30–35 scenarios per category).
- A random selection mechanism generates a set of 5 scenarios for each simulation session:
- 3 attack scenarios
- 2 genuine scenarios
- The system ensures non-repetition of scenarios across multiple attempts using a tracking mechanism.
- Each scenario execution follows a structured flow:
- Scenario introduction
- Simulation display
- User decision input
- Result evaluation
- After completing all scenarios, the system calculates the total score and accuracy percentage.
- The system generates detailed feedback including:
- Identified weak areas
- Incorrect decisions
- Personalized recommendations
- Additionally, the system provides:
- Preventive measures against similar attacks
- Post-attack recovery steps
- An adaptive learning mechanism adjusts the difficulty level based on user performance.
- The admin module supports system management functionalities such as:
- Scenario creation and modification
- User performance analytics
- Feedback and rating analysis

IV. PSEUDO CODE

Step 1: Start
Step 2: Input user credentials Step 3: Authenticate user
If invalid → Exit
Step 4: Detect user role (User/Admin)
If Admin → Open Admin Dashboard Else → Continue
Step 5: User selects attack type and difficulty level
Step 6: Fetch scenarios from database
Step 7: Select 5 scenarios randomly
(3 attack + 2 genuine)
Step 8: Remove previously used scenarios (non-repetition)
Step 9: Initialize
score = 0 weak_areas = empty
Step 10: For each scenario:
- Display scenario
- Get user decision
- If decision is correct → score = score + 1
- Else → add to weak_areas

Step 11: Calculate accuracy accuracy = (score / 5) × 100
Step 12: Generate feedback
- Identify weak areas
- Give recommendations

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Step 13**:** Provide prevention and recovery steps Step 14**:** Apply adaptive logic
If score is low → suggest retry
If score is high → increase level Step 15**:** Store results in database Step 16**:** Display result and feedback
Step 17**:** End

V. SIMULATION RESULTS

The system was tested with multiple users across different attack types and difficulty levels to evaluate its effectiveness. The results showed that users improved their accuracy after repeated simulation attempts, indicating better understanding of social engineering attacks. The platform successfully identified weak areas such as phishing detection and provided targeted feedback to improve performance. The adaptive learning mechanism helped users progress gradually by adjusting difficulty levels based on their scores. Overall, the system demonstrated effective training capability by enhancing user awareness, decision-making skills, and response accuracy in handling cybersecurity threats.

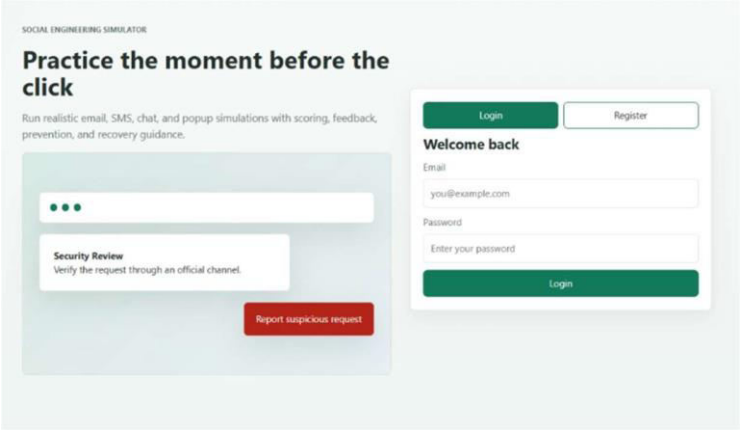


Fig1: Login User

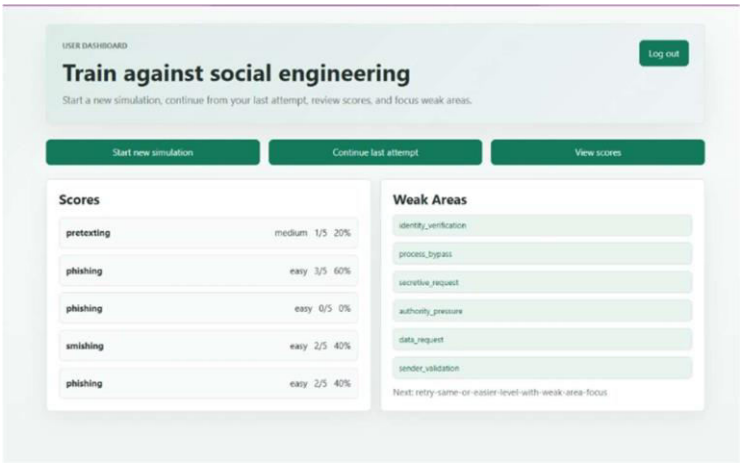


Fig 2: User Dashboards

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fig 3: Attack Selection Screen

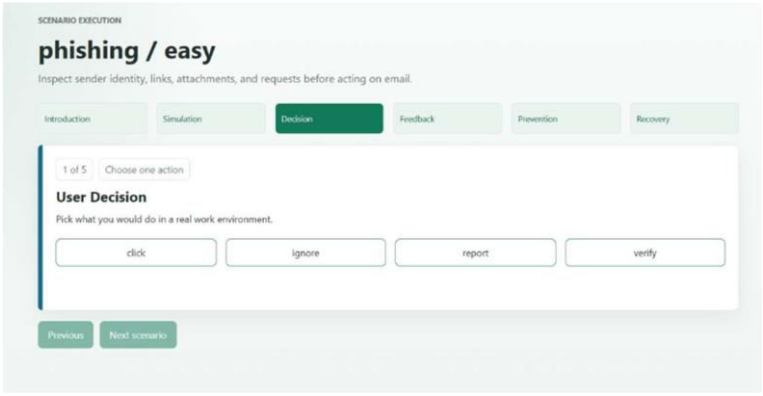


Fig 4: Decision Making Screen

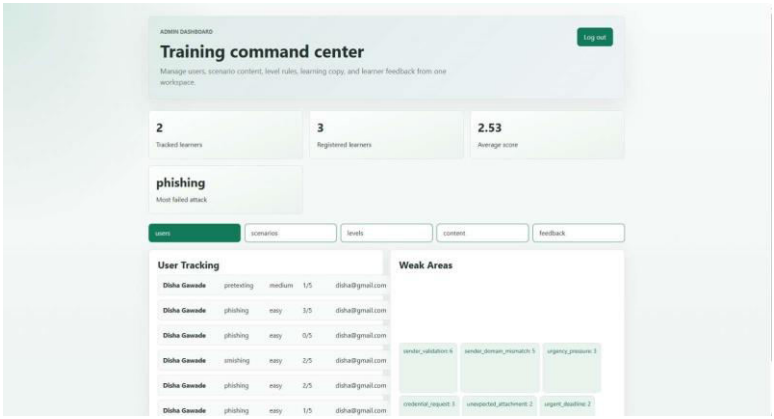


Fig 5: Admin dashboards

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

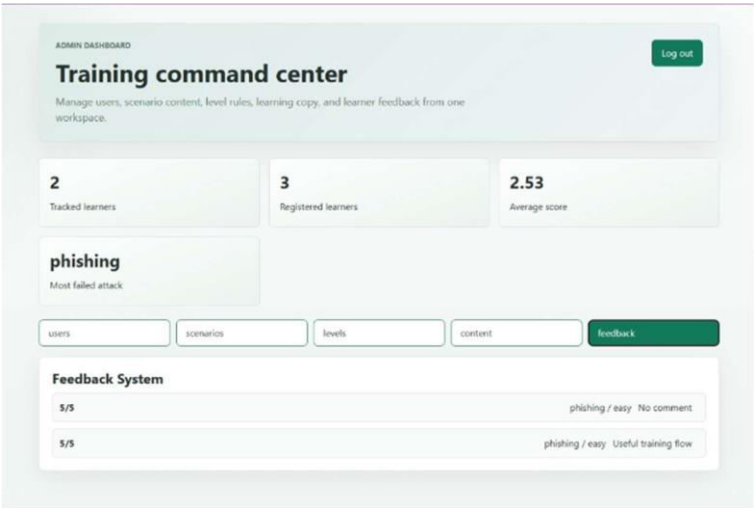


Fig 6: Tracking User Feedbacks

VI. CONCLUSION AND FUTURE WORK

The proposed Interactive Cybersecurity Awareness and Training Platform provides an effective solution for improving user awareness against social engineering attacks through realistic simulations and adaptive learning. By combining scenario-based training, performance analysis, and feedback mechanisms, the system enhances users' decision-making skills and ability to handle cyber threats. The full-stack architecture ensures efficient operation and scalability. In future, the system can be enhanced by integrating AI-based scenario generation, developing a mobile application, adding gamification features such as leaderboards and badges, and deploying it on cloud platforms for large-scale usage and real-time analytics.

REFERENCES

1. H. Gil, J. Yoo and J. Lee, "An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks," in Proc. 2nd Int. Conf. Human Society and Internet (HSI'03), pp. 302–311, 2003.
2. S. K. Dhurandher, S. Misra, M. S. Obaidat, V. Basal, P. Singh and V. Punia, "An Energy-Efficient On Demand Routing Algorithm for Mobile Ad-Hoc Networks," in Proc. Int. Conf. Electronics, Circuits and Systems, pp. 958–961, 2008.
3. D. Kumar S. M. and B. P. Vijaya Kumar, "Energy-Aware Multicast Routing in MANETs: A Genetic Algorithm Approach," Int. Journal of Computer Science and Information Security (IJCSIS), vol. 2, 2009.
4. M. AlGabri, C. Li, Z. Yang, N. Hasan and X. Zhang, "Improved the Energy of Ad hoc On-Demand Distance Vector Routing Protocol," in Int. Conf. Future Computer Supported Education, Elsevier IERI, pp. 355–361, 2012.
5. D. Shama and A. Kush, "GPS Enabled Energy Efficient Routing for MANET," International Journal of Computer Networks (IJCN), vol. 3, no. 3, pp. 159–166, 2011.
6. S. Jain and S. Jain, "Energy Efficient Maximum Lifetime Ad-Hoc Routing (EEMLAR)," International Journal of Computer Networks and Wireless Communications, vol. 2, no. 4, pp. 450–455, 2012.
7. R. Vadivel and V. Murali Bhaskaran, "Energy Efficient with Secured Reliable Routing Protocol (EESRRP) for Mobile Ad-Hoc Networks," Procedia Technology, vol. 4, pp. 703–707, 2012.
8. N. Ezaki, M. Bulacu and L. Schomaker, "Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons," in Proc. 17th Int. Conf. Pattern Recognition (ICPR), IEEE, pp. 683–686, 2004.
9. R. H. Davda and N. Mohammed, "Text Detection, Removal and Region Filling Using Image Inpainting," International Journal of Futuristic Science Engineering and Technology, vol. 1, no. 2, ISSN 2320–4486, 2013.
10. U. Modha and P. Dave, "Image Inpainting: Automatic Detection and Removal of Text From Images," International Journal of Engineering Research and Applications (IJERA), vol. 2, no. 2, 2012.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details