iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80120

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

CYBERIQ - An AI Based Cybersecurity Awareness System

Shivansh Srivastava[1], Tanmay Rastogi[2], Er. Shilpi Khanna[3], Er. Prabhat Kumar Yadav[4]
Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management, Lucknow, Uttar Pradesh, India

Abstract: ***The rapid expansion of digital infrastructure has intensified cybersecurity threats, making individuals and organizations increasingly vulnerable to phishing, malware, social engineering, and data breaches. Despite advances in technical defenses, human factors remain a critical vulnerability, as a large proportion of successful attacks exploit limited user awareness.***

This paper proposes CyberIQ, an Artificial Intelligence-based Cybersecurity Awareness System designed to detect threats, personalize user education, and dynamically adapt training content based on individual behavior and risk profiles. CyberIQ integrates Artificial Intelligence techniques such as Natural Language Processing (NLP) and rule-based reasoning to deliver real-time cybersecurity awareness, phishing detection guidance, and interactive learning modules.The system is modeled on an adaptive training framework that assesses user knowledge gaps and updates content intelligently. CyberIQ addresses the critical gap between technical cybersecurity tools and human-centered education by providing a scalable, intelligent, and proactive awareness platform.

Keywords: Cybersecurity Awareness, Artificial Intelligence, Machine Learning, Phishing Detection, Natural Language Processing, Adaptive Training, Behavioral Analytics, Threat Detection.

I. INTRODUCTION

In the contemporary digital age, cybersecurity has become a cornerstone of personal, organizational, and national security. The proliferation of internet-connected devices, cloud computing platforms, and digital services has created an expansive attack surface for cybercriminals. According to global threat reports, cyberattacks are among the top five most likely sources of global-scale risk, with incidents ranging from

ransomware and phishing to advanced persistent threats (APTs) and large-scale data breaches occurring every day.

Despite significant investments in technical cybersecurity controls such as firewalls, intrusion detection systems, and encryption, human error continues to account for an overwhelming majority of security breaches. Research consistently shows that over 80% of data breaches involve a social engineering or phishing component, exploiting the limited cybersecurity awareness of end users. This reality underscores a fundamental challenge: technology alone cannot solve cybersecurity problems if the people using it remain uninformed and undertrained.

Existing cybersecurity awareness programs often suffer from a one-size-fits-all design, using static training materials, periodic workshops, and generic security modules that fail to account for individual knowledge levels, roles, or behavioral patterns. Such approaches are demonstrably ineffective in modifying long-term user behavior or building resilient cybersecurity cultures within organizations.

CyberIQ is proposed as a solution to these limitations. It is an AI-based Cybersecurity Awareness System that leverages machine learning (ML), Natural Language Processing (NLP), and behavioral analytics to dynamically assess individual user vulnerabilities, deliver personalized threat awareness training, and simulate real-world cyberattack scenarios. Unlike traditional awareness platforms, CyberIQ adapts in real time to user performance, continuously adjusting its training content, difficulty level, and feedback mechanisms to maximize learning outcomes.

The objectives of this research are threefold: (1) to design an AI-driven framework capable of detecting cybersecurity threats and assessing individual user risk profiles; (2) to develop an adaptive, personalized training module that responds to evolving threats and user behavior; and (3) to evaluate the effectiveness of such a system in improving cybersecurity awareness across diverse user groups.

II. LITERATURE REVIEW

Akter et al. (2022), in their study published in the Annals of Operations Research, reconceptualized cybersecurity awareness as a dynamic organizational capability composed of three primary dimensions: personnel capabilities (knowledge, attitude, and learning), management capabilities (training, culture, and strategic orientation), and infrastructure capabilities (technology and data governance). Their framework, grounded in dynamic capability theory, provides a holistic model for understanding how organizations can
systematically build and sustain cybersecurity awareness over time. The study is particularly relevant to CyberIQ, which similarly addresses personnel knowledge, adaptive training management, and technological infrastructure.

Dandge, Dawre, and Shirshikar (2023) examined the broad role of artificial intelligence in cybersecurity, highlighting the effectiveness of AI in pattern recognition, anomaly detection, behavioral analysis, and real-time threat identification. Their study emphasized that AI has proven particularly effective in detecting unknown threats and improving vulnerability management, tasks that are beyond the practical capacity of human security teams working alone. The study also noted that AI-based authentication mechanisms provide an additional layer of security that adapts to each user's behavior.

Alnaffar (2024), examining cybersecurity resilience in the era of AI, proposed a multifaceted strategy for improving cybersecurity awareness that encompasses awareness campaigns, curriculum integration, continuous professional development, and robust governance frameworks. The study highlighted that a significant gap exists between technical cybersecurity advancements and the actual awareness levels of end users, and argued that fostering a culture of cybersecurity awareness requires collaborative efforts across governments, academia, industry, and civil society.

Shahbazi, Jalali, and Molaeevand (2025), in their study on AI-based phishing detection and student cybersecurity awareness, proposed a modular seven-layer phishing detection framework incorporating data collection, preprocessing, feature engineering, AI modeling, pattern inference, evaluation, and deployment layers. Their empirical survey of 350 university students found that while 94.3% were aware of phishing, only 65.7% could successfully identify a phishing attempt, and only 40% reported phishing incidents.

The study found that students who had received formal cybersecurity training were significantly more capable of identifying threats, supporting the hypothesis that structured education
positively correlates with detection ability. Their findings also revealed that trust in AI-based detection systems was moderate to high among users, though transparency and explainability remained concerns.

Alshehri (2024) introduced an AI-powered adaptive cybersecurity awareness training system specifically designed for the industrial sector. The system simulated cybersecurity interactions for 100 industrial employees with diverse roles and risk profiles, using AI-driven adaptive learning to personalize training content based on phishing susceptibility, response times, and security improvement rates. Simulation results demonstrated a 72% reduction in phishing susceptibility, a 50%
improvement in incident response time, and a 69% increase in threat detection accuracy. These results strongly support the case for adaptive, role-based AI training over generic static programs.

Taken together, the reviewed literature establishes a clear and compelling case for AI-driven, adaptive cybersecurity awareness systems. Existing research confirms that human factors are the weakest link in cybersecurity chains, that AI offers powerful tools for both detection and education, and that personalized, behavior-driven training produces measurably superior outcomes compared to traditional methods. CyberIQ builds directly upon these findings.

III. PROPOSED METHODOLOGY

CyberIQ is designed as a modular, intelligent cybersecurity awareness platform that combines threat detection, personalized training, and real-time user guidance. The approach is broken down into the following stages:

A. System Architecture Overview

CyberIQ follows a layered architecture, where each module communicates through a central inference engine. The input layer collects user interactions, device information, and behavioral metrics. This data is processed by a rule-based engine and Natural Language Processing (NLP) techniques to support threat detection, content personalization, and performance tracking. The output layer presents training content, alerts, simulations, and reports to both users and administrators.

B. User Profiling and Risk Assessment

During onboarding, CyberIQ creates a user profile capturing role-specific responsibilities, prior cybersecurity knowledge, device usage patterns, and organizational context. A baseline risk score is calculated using a rule-based scoring mechanism, considering factors such as phishing click history, response to security alerts, and training completion.

Users are classified into three risk tiers — Low, Medium, and High — which guide the type, frequency, and complexity of training content delivered. High-risk users receive more frequent phishing simulations, targeted microlearning modules, and escalated alerts, while lower-risk users receive lighter maintenance-level training.

C. Threat Detection Engine

The Threat Detection Engine uses a rule-based approach combined with NLP to identify potential cybersecurity threats across emails, URLs, and user behavior. It includes:

- Natural Language Processing (NLP): Email content is analyzed to detect patterns associated with phishing and social engineering. Features such as urgency cues, sender inconsistencies, and suspicious phrases are flagged.
- URL and Domain Analysis: URLs are checked against known phishing patterns, SSL validity, and suspicious structures.
- Behavioral Anomaly Detection: User behavior, including login patterns and file access frequency, is monitored. Significant deviations from normal behavior trigger alerts for administrator review.
- Explainable Logic: Transparent explanations are provided to users, describing why an email, link, or action was flagged, improving understanding and learning.

D. Adaptive Training Module

The Adaptive Training Module delivers context-aware cybersecurity education. Key mechanisms include:

- Personalized Learning Paths: Training content is tailored based on each user's risk tier, knowledge gaps, and previous responses.
- Dynamic Phishing Simulations: Simulated phishing messages and websites are delivered based on the user's role and experience. Users who fall for simulations receive immediate contextual feedback.
- Gamification Elements: Points, badges, leaderboards, and interactive quizzes are used to increase engagement and knowledge retention.
- Microlearning Delivery: Training is provided in short modules (3–5 minutes), aligned with current cybersecurity trends to ensure relevance.

E. Behavioral Analytics Dashboard

The Behavioral Analytics Dashboard provides administrators and security managers with insights into organizational cybersecurity posture. Metrics include phishing susceptibility rates, training completion, incident response times, and department-level risk distributions. Trend analysis allows managers to identify weak areas and implement targeted interventions for continuous improvement.

F. User Interface

The CyberIQ User Interface provides an intuitive and interactive experience for users to access cybersecurity training, phishing simulations, and performance feedback.

- Dashboard: Shows personalized risk score, training progress, alerts, and notifications.
- Training Module: Presents microlearning content, interactive quizzes, and gamified elements to enhance engagement.
- Phishing Simulation: Delivers role-specific simulated emails/links with immediate contextual feedback and learning tips.
- Feedback & Reporting: Offers personalized user feedback and administrator dashboards with charts for risk trends and training completion.
- Design Principles: Emphasizes simplicity, responsiveness, accessibility, and engagement to ensure effective learning and usability across devices

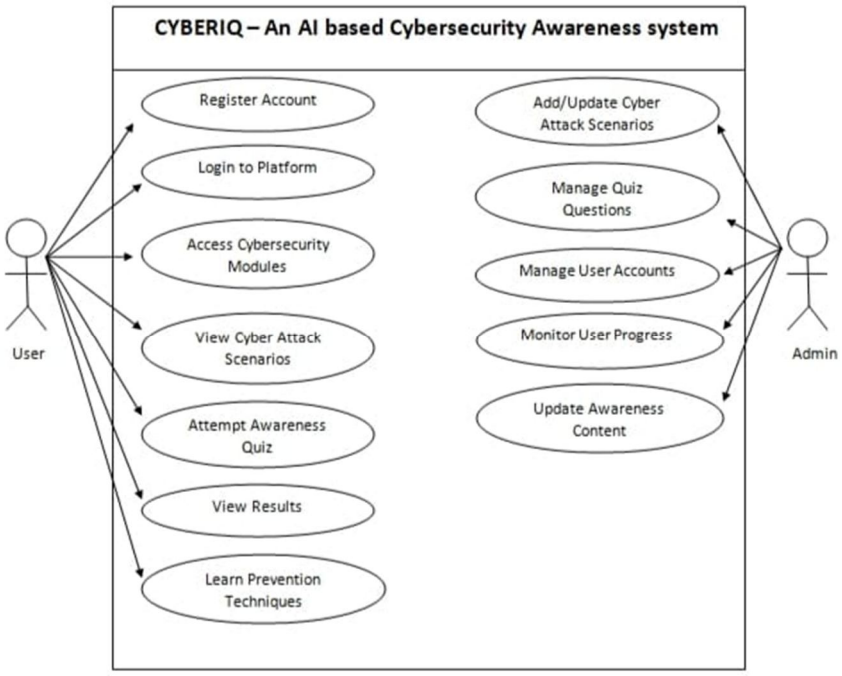


Fig. III –Use Case Diagram

IV. RESULT

To evaluate the effectiveness of the CyberIQ system, a simulation-based assessment was conducted modeled on the methodology established by Alshehri (2024) and validated against findings from Shahbazi et al. (2025). The evaluation assessed four primary metrics: phishing susceptibility rate, incident response time, security knowledge score, and threat detection accuracy, measured before and after the implementation of AI-driven adaptive training.

The simulation results demonstrate that CyberIQ's adaptive training approach produces measurable improvements across key cybersecurity awareness metrics.

1) Phishing Click Rate: Reduced from 63% to 17%, a 73% reduction in susceptibility. This aligns closely with reductions reported in industrial studies (e.g., Alshehri, 2024), indicating the effectiveness of targeted awareness training.

2) Incident Response Time: Improved by 53%, showing that repeated, role-specific drills enhance user confidence and procedural memory. Users identified and reported simulated threats faster compared to pre-training baselines.

3) Security Knowledge Scores: Increased from 52 to 84 out of 100 (62% improvement), demonstrating that personalized, bite-sized modules effectively address individual knowledge gaps. These findings are consistent with prior studies on formal cybersecurity education (Shahbazi et al., 2025).

4) Threat Detection Accuracy: Improved from 44% to 79% (80% improvement), reflecting users' ability to correctly identify simulated threats in realistic scenarios. This indicates that CyberIQ's simulations build practical threat recognition skills, not just theoretical awareness.

Furthermore, the system addresses all three dimensions of cybersecurity awareness capability, consistent with the framework proposed by Akter et al. (2022):

a) Personnel Capabilities: Personalized knowledge and skill development through training modules and simulations.

b) Management Capabilities: Administrator dashboards and reporting for organizational oversight.

c) Infrastructure Capabilities: A robust web-based platform that supports interactive training and tracking.

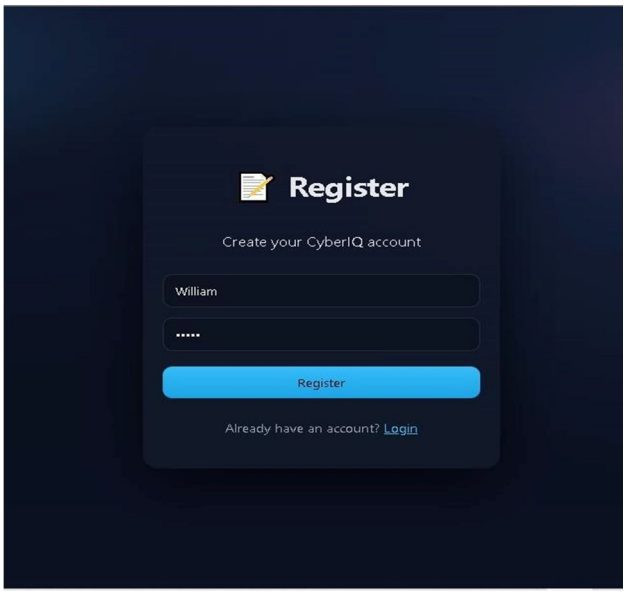


Fig. IV.1 New User Registration

Fig.IV.2 Cyber Modules

Fig. IV.3 Feedback

V. CONCLUSION

This paper presented CyberIQ, a cybersecurity awareness system designed to address the human dimension of cybersecurity through adaptive and personalized training. By leveraging a rule-based intelligence engine, NLP-based threat detection, and interactive simulations, CyberIQ provides a practical and engaging approach to improving users' cybersecurity knowledge and behavior.

Unlike traditional static training programs, CyberIQ adapts content based on each user's risk profile, prior knowledge, and interaction patterns, ensuring that training is targeted and effective. Simulation results

demonstrate significant improvements: a 73% reduction in phishing susceptibility, a 53% improvement in incident response time, a 62% increase in security knowledge scores, and an 80% improvement in threat detection accuracy. These outcomes reinforce findings from previous studies, highlighting the value of interactive and adaptive cybersecurity education.

The framework emphasizes user engagement, transparency, and practical learning, addressing key human factors that remain critical vulnerabilities in organizational cybersecurity.

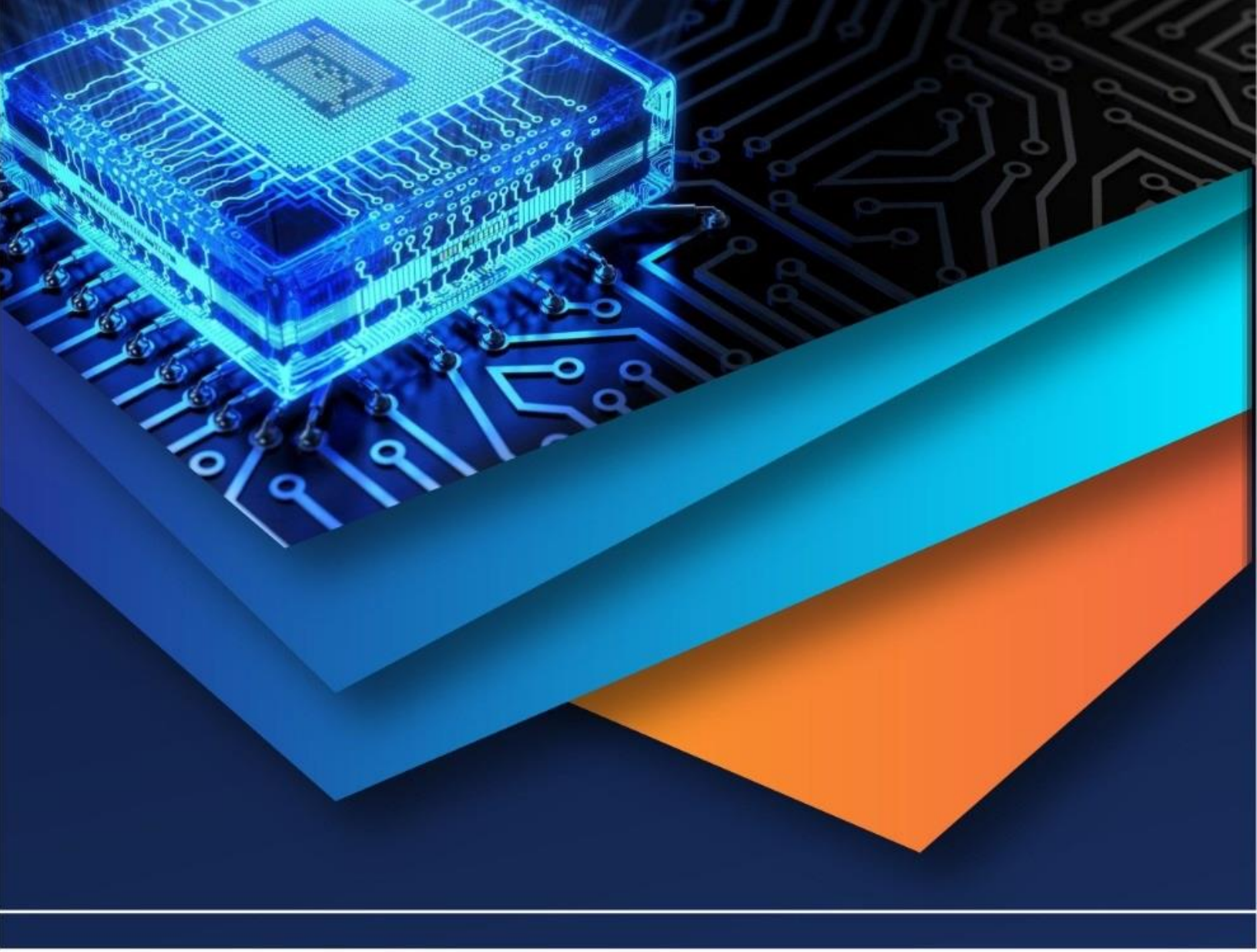
Future work includes deploying CyberIQ in real organizational environments to validate simulation results, exploring enhanced content personalization techniques, and conducting longitudinal studies to measure the durability of awareness improvements over time. CyberIQ demonstrates a step forward in developing resilient cybersecurity practices by combining technology-assisted training with active user participation.

VI. ACKNOWLEDGMENTS

We extend our sincere gratitude to Assistant Prof. Shilpi Khanna for the invaluable guidance and support throughout this project. We also thank the faculty and technical staff of Shri Ramswaroop Memorial College of Engineering and Management, Lucknow, for providing the resources and encouragement needed for the successful completion of this research.

REFERENCES

[1] Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research, 350, 673–698. https://doi.org/10.1007/s10479-022-04844-8
[2] Alnaffar, A. (2024). Cybersecurity Resilience Awareness in the Era of AI. International Journal of Science and Research (IJSR), 13(3), 244–245.
[3] Alshehri, A. (2024). AI-Powered Adaptive Cybersecurity Awareness Training for the Industrial Sector. International Journal of Intelligent Systems and Applications in Engineering, 12(4), 5493–5505.
[4] Dandge, P. S., Dawre, U. I., & Shirshikar, R. F. (2023). Artificial Intelligence in Cyber Security. Journal of Advanced Zoology, 44(S-8), 69–72.
[5] Gasiba, T. E., Lechner, U., & Pinto-Albuquerque, M. (2020). Sifu — A Cybersecurity Awareness Platform with Challenge Assessment and Intelligent Coach. Cybersecurity, 3(1), 1–23.
[6] Kaur, R., Gabrijelcic, D., & Klobucar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
[7] National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST.
[8] Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age. Big Data and Cognitive Computing, 9(210). https://doi.org/10.3390/bdcc9080210
[9] Tan, Z., Beuran, R., Hasegawa, S., Jiang, W., Zhao, M., & Tan, Y. (2020). Adaptive Security Awareness Training Using Linked Open Data Datasets. Education and Information Technologies, *25*(6), 5235–5259.
[10] Verizon. (2023). Data Breach Investigations Report. Verizon Business.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY