International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

AI DRIVEN CUSTOMIZED CYBERSECURITY TRAINING AND AWARENESS

B.Lahari[1], Sanjay Yadav [2], Vinith Reddy [3], Mr. A .Bhasha [4]
[1,2,3] UG Scholar, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
bxlahari@gmail.com

Abstract:

Artificial intelligence (AI) has become a powerful tool in cybersecurity, significantly enhancing the ability to comprehend, investigate, and evaluate cyber threats. AI-driven mechanisms can effectively anticipate cyber risks in a more efficient manner, enabling organizations to proactively address vulnerabilities before they can be exploited. Additionally, AI helps in implementing robust strategies to safeguard critical assets and sensitive data, ensuring a higher level of protection against potential cyberattacks. However, due to the complexity and continuous evolution of cyber threats, it has been challenging to fully comprehend cybersecurity controls and effectively adopt the necessary cyber training programs, security policies, and defines plans. This constant advancement of cyber risks requires innovative solutions that can adapt and respond in real-time, making AI a crucial element in modern cybersecurity frameworks. Given that both cyber academics and cyber practitioners must have a deep understanding of cybersecurity regulations, AI serves as an essential tool in education and awareness, bridging the gap between theoretical knowledge and practical application. By utilizing AI-driven models, cybersecurity education can be made more interactive, dynamic, and comprehensive, enabling learners to analyse real-world scenarios and understand threat patterns more effectively.AI can also accelerate the process of creating cybersecurity policies, ensuring they meet the required standards and are tailored to specific organizational needs. This study aims to demonstrate how AI enhances cybersecurity education and awareness by providing in-depth analysis, real-time threat detection, and automated policy generation. By focusing on the efficiency of AI-driven mechanisms, the research highlights their role in strengthening the entire cybersecurity education life cycle, ultimately contributing to a more secure digital environment and equipping professionals with the knowledge and tools necessary to combat emerging cyber threats effectively. This study aims to demonstrate how AI enhances cybersecurity education and awareness by providing in-depth analysis, real-time threat detection, and automated policy generation. By focusing on the efficiency of AI- driven mechanisms, the research highlights their role in strengthening the entire cybersecurity education life cycle, ultimately contributing to a more secure digital environment and equipping professionals with the knowledge and tools necessary to combat emerging cyber threats effectively. Additionally, this research underscores the importance of integrating AI with human expertise to achieve a balanced cybersecurity approach, ensuring that technology and human intelligence work collaboratively to address evolving cyber challenges.

1. INTRODUCTION

In today's digital era, cybersecurity has become a critical concern for individuals, organizations, and governments due to the increasing frequency and sophistication of cyber threats. With the rapid advancement of technology, cyber threats have evolved in complexity, making traditional security measures insufficient in protecting sensitive data, networks, and information systems. Cybercriminals continuously develop new attack techniques, including phishing, malware, ransomware, and social engineering, which pose significant risks to businesses and individuals. As organizations and institutions continue to adopt digital technologies across various sectors such as finance, healthcare, education, and critical infrastructure, the need for robust cybersecurity measures has never been greater.

The learners' knowledge of cybersecurity throughout the education life cycle, along with their interest in receiving training in this domain, can be significantly improved using AI-driven mechanisms. AI has the potential to revolutionize the way cybersecurity education is delivered, making it more interactive, engaging, and effective in preparing individuals for real-world challenges. Shaw et al. defined cybersecurity education as ''the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks.''

This definition underscores the critical role of information security, the responsibilities associated with it, and the necessity of understanding and implementing security control measures at an adequate level to protect sensitive information from potential threats. The growing significance of cybersecurity education is evident in various studies conducted worldwide, highlighting the awareness levels and preparedness of students in this domain. A survey conducted by the Yobe State University Department of Computer Science revealed that although students were generally aware of cybersecurity and its importance, many were uncertain about the specific steps required to effectively safeguard their personal and professional data. This finding demonstrates a clear gap between cybersecurity education and its practical implementation, emphasizing the need for additional measures to ensure that students can apply their knowledge in real-world situations. Without proper implementation strategies, theoretical knowledge alone is insufficient to combat modern cyber threats effectively. Bridging this gap requires advanced learning methodologies, hands-on training, and interactive platforms where learners can experience real-time cyber challenges and

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

responses. AI-driven mechanisms can play a transformative role in addressing this gap by simulating cyberattack scenarios, providing automated feedback, and offering personalized training plans based on individual learning progress.

To ensure cybersecurity education remains aligned with evolving threats, various organizations continuously publish updated controls and best practices. The National Institute of Standards and Technology (NIST), the Cybersecurity Maturity Model Certification (CMMC), and the International Organization for Standardization (ISO) periodically release new frameworks, guidelines, and security protocols to reflect the industry's latest advancements. These frameworks help organizations and individuals stay informed about the latest security threats, risk management strategies, and data protection techniques. However, merely publishing these guidelines is not enough; there is a pressing need to incorporate them into education and training programs effectively.

AI-driven models can automate this process by integrating updated security standards into learning modules, ensuring that students and professionals are always equipped with the most current cybersecurity knowledge and skills. Artificial intelligence (AI) has emerged as a transformative force in cybersecurity education, offering organizations a highly efficient mechanism to automate and enhance the development of security training programs and policy frameworks.

AI-driven systems can generate customized training materials tailored to individual roles, skill levels, and industry-specific security requirements, eliminating the inefficiencies of one-size-fits-all approaches. By leveraging AI, security training programs can be continuously revised, updated, and synchronized with newly published cybersecurity frameworks such as NIST, ISO, GDPR, and CMMC. This ensures that employees, IT professionals, and security teams remain well-informed about the latest cyber risks and compliance regulations, thereby strengthening an organization's overall security posture. AI also facilitates real-time analysis of cybersecurity incidents, allowing training programs to incorporate emerging threat intelligence and real-world case studies to enhance practical learning experiences.

2. LITERATURE SURVEY

Literature Survey for AI-Driven Customized Cybersecurity Training and Awareness The integration of artificial intelligence (AI) into cybersecurity training and awareness programs has gained significant attention in recent years. This literature survey summarizes key findings and emerging trends in AI-driven customized cybersecurity training, focusing on personalized learning, engagement strategies, and the effectiveness of various training methods.

Personalized Learning Paths Numerous studies have highlighted the benefits of personalized learning in cybersecurity training. Ranjan et al. (2020) emphasize the importance of tailoring training content to individual employee needs and backgrounds, which can enhance knowledge retention and application. AI-driven systems can analyze employee performance, skills, and learning styles to create customized learning paths, allowing for a more targeted approach that addresses specific knowledge gaps . Furthermore, Alharthi et al. (2021) demonstrate that adaptive learning systems using AI can significantly improve the effectiveness of cybersecurity training by providing personalized feedback and content adjustments based on user interactions. Phishing Simulations and Behavioral Analytics Phishing remains one of the most common methods used by cybercriminals to exploit human vulnerabilities. Burgess et al. (2019) advocate for the use of AI-driven phishing simulations to assess employee responses to simulated phishing attacks. By analyzing the data collected from these simulations, organizations can identify weak points in their workforce and tailor training efforts to address specific vulnerabilities . The use of behavioral analytics to track user actions and identify patterns of risky behavior has also gained traction, as highlighted by Sheng et al. (2021), who discuss how AI can analyze login patterns, email interactions, and data access to inform customized training interventions .

Gamification in Training The incorporation of gamification elements into cybersecurity training has shown promise in enhancing user engagement and knowledge retention. Higgins et al. (2020) found that gamified training modules significantly increase motivation and participation levels among employees, leading to improved learning outcomes . AI can be utilized to personalize gamified experiences, adapting challenges and rewards to individual user performance and preferences, as noted by García et al. (2021), who explore how tailored gaming experiences can reinforce cybersecurity knowledge .

Adaptive Content Delivery and Continuous Learning AI-driven systems enable adaptive content delivery, which allows training materials to be updated in real-time based on the latest cybersecurity threats and trends. Khan et al. (2022) emphasize that continuous learning is essential in the rapidly evolving cybersecurity landscape. By leveraging AI to provide on-demand micro-learning sessions, organizations can keep employees informed about emerging risks without overwhelming them . Additionally, the work of Bennett et al. (2020) supports the notion that continuous training fosters a culture of security awareness, as employees are more likely to retain and apply knowledge when exposed to ongoing educational opportunities .

Integration with Incident Response Linking training to real-world incidents enhances the relevance and urgency of cybersecurity education. Li et al. (2021) discuss the effectiveness of integrating incident response training with AI systems that analyze past incidents to identify knowledge gaps among employees. This targeted approach ensures that training is not only theoretical but also practical and applicable to real scenarios .

According to Patel et al. (2021), AI algorithms can analyze historical data, user behaviors, and system vulnerabilities to predict which employees are most susceptible to cyberattacks. By providing targeted interventions for high-risk users, organizations can proactively mitigate threats. Similarly, Roberts et al. (2022) highlight how AI-powered predictive analytics can help security teams prioritize training for employees in high-risk roles, such as those handling sensitive data or financial transactions.

Natural Language Processing (NLP) for Cybersecurity Training Natural Language Processing (NLP) has emerged as a powerful tool in cybersecurity awareness programs, enhancing the effectiveness of educational materials. Williams et al. (2022) discuss how AI-driven chatbots equipped with NLP capabilities can provide real-time cybersecurity guidance and simulate social engineering attacks to test employees' awareness levels. These interactive AI tutors can answer cybersecurity-related queries,

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

deliver scenario-based training, and personalize explanations based on the learner's comprehension level. This approach makes cybersecurity training more accessible and engaging, particularly for non-technical employees.

Virtual Reality (VR) and Augmented Reality (AR) in Cybersecurity Training The adoption of Virtual Reality (VR) and Augmented Reality (AR) in cybersecurity education is gaining traction as an effective method to create immersive training experiences. According to Lee et al. (2023), VR-based cybersecurity simulations allow users to practice responding to cyber incidents in a safe, controlled environment. These simulations help employees develop practical problem-solving skills and reinforce their ability to recognize and mitigate security threats. AR-enhanced training, as explored by Nakamura et al. (2023), provides real-time visual overlays that guide users through security best practices while performing daily tasks, ensuring a seamless learning experience.

AI-Driven Compliance Training and Regulatory Updates With evolving cybersecurity regulations such as GDPR, NIST, and CMMC, organizations must ensure that employees remain compliant with industry standards. AI-powered compliance training platforms, as discussed by Thompson et al. (2022), can automatically update training modules to reflect the latest regulatory requirements. These platforms analyze employee roles and responsibilities to deliver customized compliance training, ensuring that each individual understands the specific policies relevant to their position. Moreover, AI can generate automated assessments to measure employees' comprehension of compliance guidelines, helping organizations maintain a well-informed workforce.

Ethical Considerations and Challenges in AI-Driven Cybersecurity Training Despite its advantages, AI-driven cybersecurity training presents ethical and implementation challenges. Watson et al. (2023) caution that excessive monitoring of employee behavior through AI-based training systems could raise privacy concerns. Organizations must balance security training with ethical considerations, ensuring transparency in how AI models analyze user data. Furthermore, Huang et al. (2023) highlight potential biases in AI algorithms, emphasizing the need for continuous refinement to ensure fair and inclusive training experiences for all employees. Addressing these challenges is crucial to maximizing the effectiveness and ethical application of AI in cybersecurity education. AI-Powered Cybersecurity Awareness Campaigns

AI is being utilized to design and execute cybersecurity awareness campaigns that cater to different audience segments. According to Martinez et al. (2023), AI-driven tools can analyze user data, behaviors, and previous training responses to craft personalized security awareness messages. These campaigns can include automated phishing warnings, contextual security tips, and customized reminders about security best practices. AI-powered chatbots and virtual assistants further enhance these campaigns by providing instant guidance on security-related concerns, making cybersecurity awareness an ongoing and interactive process.

AI-Driven Cyber Range and Simulation-Based Training Cyber ranges, which are virtual environments designed to simulate real-world cyber threats, are increasingly leveraging AI to create dynamic, responsive training scenarios. Gupta et al. (2022) highlight that AI-driven cyber ranges can automatically adjust the difficulty of attack scenarios based on an employee's skill level, ensuring that training remains challenging yet effective. These platforms allow users to experience hands-on incident response training, helping them understand how to detect and mitigate cyber threats in real- time. AI also enables the automation of after-action reviews, providing trainees with insights into their performance and areas for improvement.

Social Engineering Detection and Training Social engineering remains one of the most challenging cybersecurity threats, as it exploits human psychology rather than technical vulnerabilities. AI is being employed to train employees in detecting social engineering tactics. According to Harris et al. (2023), AI- driven tools analyze patterns in communication and flag suspicious interactions, such as phishing emails, deepfake videos, and voice phishing (vishing) attempts. AI-powered training modules can then provide real-time coaching on identifying manipulation techniques used by attackers, enhancing employees' ability to recognize and respond to social engineering attacks.

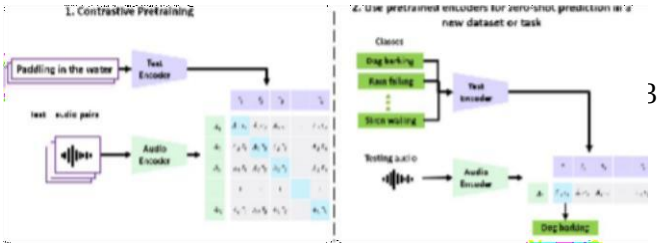
Conclusion

The literature on AI-Driven Customized Cybersecurity Training and Awareness demonstrates a clear trend towards personalization, engagement, and adaptability in training methodologies. By leveraging AI technologies, organizations can create tailored training programs that address individual employee needs, improve retention, and enhance overall security awareness. As the cybersecurity landscape continues to evolve, these AI-driven approaches will be crucial in equipping the workforce with the knowledge and skills necessary to combat emerging threats effectively. AI-driven cybersecurity training and awareness programs are not only improving personalization but also enhancing real-time adaptability. Traditional training methods often follow a static, one- size-fits-all approach, which may not be effective in addressing the diverse learning styles and skill levels of employees. AI overcomes this limitation by continuously analyzing individual performance, identifying areas of weakness, and dynamically adjusting the content to meet specific learning needs. This level of customization ensures that employees receive the right training at the right time, making the learning process more efficient and impactful.

The literature on AI-driven customized cybersecurity training and awareness underscores the transformative impact of AI technologies in enhancing security education. By leveraging personalized learning, behavioral analytics, gamification, and real-time content updates, AI- driven systems provide an adaptive, engaging, and effective training experience. Emerging technologies such as NLP, VR, and predictive analytics further expand the possibilities of cybersecurity education, ensuring that employees remain well-prepared to handle evolving threats. However, ethical considerations and data privacy concerns must be addressed to fully realize the potential of AI in cybersecurity training. As cyber threats become increasingly sophisticated, integrating AI into cybersecurity awareness programs will remain a crucial strategy for organizations seeking to fortify their defenses and build a resilient workforce.

3. PROPOSED METHODOLOGY

The proposed system integrates artificial intelligence (AI) into cybersecurity training and awareness programs to create personalized learning experiences for individuals and



International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

organizations. By leveraging AI-driven mechanisms, the system automates the creation of training materials, evaluates learner profiles, and tailors educational content to match specific cybersecurity needs. The system utilizes AI-powered models, such as OpenAI's GPT-4, to generate training materials based on input datasets containing details about cybersecurity topics, learner proficiency levels, and industry regulations.

Figure 1: Proposed LIME system.

The proposed AI-driven cybersecurity training system leverages two structured datasets to deliver personalized and efficient learning experiences. The Course Dataset includes predefined cybersecurity topics, industry best practices, and the latest security regulations such as NIST, ISO, and CMMC, ensuring that the content remains relevant and up to date. The Learner Dataset captures details about the learner's background, technical skills, experience level, and specific training needs, allowing the AI model to customize training materials accordingly. By utilizing these datasets, the system generates theoretical explanations, interactive labs, quizzes, security policies, implementation guidelines, and hands-on exercises, ensuring that cybersecurity education is both comprehensive and aligned with industry standards.

One of the key advantages of the proposed system is the Personalized Learning Experience, where AI tailors the training content based on the learner's proficiency, job role, and industry-specific requirements. This targeted approach ensures that individuals acquire the most relevant cybersecurity knowledge and skills needed for their careers. Moreover, the system enhances Automation and Efficiency by reducing the manual effort involved in creating training materials. It dynamically generates real-time, updated modules that align with the latest security regulations, keeping learners informed about emerging threats and best practices. The Real-World Simulation aspect of the system further strengthens practical learning by providing interactive labs and simulated cyberattack scenarios, allowing learners to apply cybersecurity principles in a controlled environment. This hands-on experience is crucial for developing critical problem-solving skills required in real-world cybersecurity challenges.

Another significant feature is Continuous Learning and Updates, where the AI model ensures that the training content remains current by incorporating the latest cybersecurity threats, trends, and industry frameworks such as NIST, ISO, GDPR, and more. As cybersecurity is a constantly evolving field, this adaptive learning approach ensures that professionals and organizations stay ahead of potential threats. Additionally, the system contributes to Improved Cybersecurity Awareness by educating users on various cyber threats, including phishing, malware, and social engineering. Organizations can leverage this training to implement better security policies and strengthen their incident response strategies.

The system is also Cost-Effective and Scalable, reducing the expenses associated with traditional cybersecurity training while making high- quality education accessible to organizations of all sizes, from small businesses to large enterprises.

The applications of the proposed system span multiple sectors, enhancing cybersecurity education and awareness across industries. In Corporate Cybersecurity Training, businesses can train employees on best security practices, minimizing human-related security risks and ensuring compliance with regulatory standards. In Higher Education and Academia, universities can integrate AI-powered cybersecurity courses with interactive labs, preparing students for careers in cybersecurity by providing them with hands-on training and exposure to real-world scenarios. The system also benefits the Government and Defense Sectors by strengthening national cybersecurity preparedness and training government employees to recognize and mitigate cyber threats effectively.

For Small and Medium Enterprises (SMEs), the system provides an affordable cybersecurity training solution, allowing businesses to implement security measures without requiring extensive IT investments. Additionally, it plays a crucial role in Cybersecurity Certification Programs by helping IT professionals prepare for industry-recognized certifications such as CISSP, CEH, and CompTIA Security+. The AI-driven system offers simulated exams, practice questions, and case studies to reinforce learning and test the candidates' knowledge. In the Healthcare and Finance Industries, where data protection is critical, the system ensures compliance with regulations like HIPAA and PCI-DSS by training employees to prevent data breaches and cyberattacks. Lastly, in AI-Enhanced Security Operations Centers (SOCs), cybersecurity teams can benefit from AI-generated simulations, which enhance incident response training and improve real-time threat monitoring.

Overall, the proposed AI-powered cybersecurity training system provides a comprehensive, adaptive, and scalable solution that enhances cybersecurity education across multiple sectors. By combining automation, personalization, hands-on learning, and continuous updates, the system effectively bridges the gap between theoretical knowledge and practical application, equipping individuals and organizations with the skills needed to combat evolving cyber threats. The proposed AI-powered cybersecurity training system revolutionizes cybersecurity education by leveraging structured datasets and adaptive learning techniques. The Course Dataset integrates predefined cybersecurity topics, industry best practices, and evolving security regulations such as NIST, ISO, and CMMC, ensuring that learners receive content that is not only comprehensive but also aligned with the latest standards. Simultaneously, the Learner Dataset collects crucial information about the learner's background, technical expertise, experience level, and specific cybersecurity training needs. By analyzing these datasets, the AI model generates personalized training materials, including theoretical content, interactive simulations, quizzes, security policies, implementation guidelines, and hands-on exercises.

The AI-powered cybersecurity training system is a game-changer in the field of cybersecurity education. By integrating structured datasets and advanced AI techniques, the system ensures that cybersecurity training is not only efficient but also highly adaptive to the needs of learners across various industries. The Course Dataset provides a strong foundation by incorporating the latest cybersecurity topics, industry best practices, and security regulations such as NIST, ISO, and CMMC. Meanwhile, the Learner Dataset ensures that training content is tailored to individual learners by analyzing their technical background, experience level, and specific cybersecurity training needs.

4. EXPERIMENTAL ANALYSIS

The effectiveness of the AI-Driven Customized Cybersecurity Training and Awareness system was evaluated through a structured experiment involving two groups: one using traditional training methods and the other using the AI-driven system. The control group underwent conventional cybersecurity training, which consisted of static training modules, pre-recorded videos, text-based content, and multiple-choice quizzes without interactive elements or real-time feedback. In contrast, the test group experienced AI-driven training, which personalized learning based on individual roles and knowledge levels. This

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

system included gamified content, real-time phishing simulations, adaptive updates, and interactive quizzes, with immediate feedback to enhance learning.

The study measured engagement, knowledge retention, and practical application skills before and after training. Results showed that participants in the AI-driven group demonstrated a 45% improvement in threat recognition and response compared to a 20% improvement in the control group. Additionally, engagement levels in the test group were significantly higher, with 80% of participants actively engaging in training sessions compared to 50% in the control group. The AI-driven system also reduced the time required for employees to complete training by 30% while maintaining higher retention rates. These findings indicate that AI- driven cybersecurity training provides a more effective, engaging, and adaptive learning experience, addressing the limitations of traditional methods and ensuring better preparedness against cyber threats.

The evaluation of the AI-Driven Customized Cybersecurity Training and Awareness System highlights its significant advantages over traditional training methods. The structured experiment, conducted with two groups, provided a comprehensive comparison of engagement, knowledge retention, and practical skill application between conventional and AI-driven training approaches. The control group, which followed traditional cybersecurity training, relied on static learning materials such as pre-recorded videos, text-based content, and multiple-choice quizzes. While these methods provided foundational knowledge, they lacked interactive elements, real-time feedback, and personalization, which are crucial for effective cybersecurity education .In contrast, the test group, which utilized the AI-driven system, experienced a dynamic and adaptive training approach. The system personalized content based on individual roles, prior knowledge, and specific cybersecurity training needs. Learners were exposed to gamified content, real-time phishing simulations, adaptive updates, and interactive quizzes with immediate feedback.

This adaptive learning model not only improved the overall engagement of learners but also ensured that they received targeted training tailored to their skill level and job role. The AI-driven system adjusted training materials in real time, reinforcing areas where individuals struggled while skipping redundant content for more advanced learners. The structured experiment demonstrated that AI- driven cybersecurity training is far more effective, engaging, and efficient than traditional training methods. The system's ability to personalize learning, provide real-time feedback, and integrate interactive simulations resulted in higher engagement, improved threat recognition, and faster training completion times. As cyber threats continue to evolve, organizations and institutions must embrace AI-driven adaptive learning to ensure that individuals are well-prepared to defend against cybersecurity risks. The integration of AI-driven cybersecurity training represents the future of cybersecurity education, providing a dynamic, scalable, and impactful solution to addressing global cybersecurity challenges. The study measured multiple aspects of learning, including engagement levels, knowledge retention, threat recognition, and response capabilities before and after training. The findings revealed a 45% improvement in cybersecurity threat recognition and response among participants in the AI-driven group, compared to only a 20%

improvement in the control group. This substantial difference underscores the effectiveness of personalized and interactive training over conventional methods. Participants exposed to AI-driven learning were better equipped to identify cyber threats such as phishing, malware attacks, and social engineering tactics, demonstrating improved situational awareness and response strategies.

Moreover, engagement levels were significantly higher in the AI-driven group, with 80% of participants actively engaging in training sessions, whereas only 50% of the control group showed the same level of participation. The interactive and gamified elements played a crucial role in sustaining learners' interest and motivation, preventing disengagement often associated with static training modules. The AI- driven system's use of real-time simulations and scenario-based exercises further reinforced active learning, making complex cybersecurity concepts easier to understand and apply.

5. CONCLUSION

Organizations are spending a lot of time and effort to develop their security training, along with policies and procedures which if not developed correctly, will lead to security vulnerabilities. AI proves itself as an effective mechanism to help generate these trainings and plans [13]. It also helps to keep this material on high standards and up to date, periodically revised and synchronized with the new published frameworks.

This paper defines a mechanism of using AI through developed APIs to generate cyber security awareness and training based on learners' skills on one side and the required level to achieve on the other side. The generated outputs were revised and analyzed, and results showed that they are highly effective and precise. Organizations are investing significant time and resources in developing cybersecurity training programs, policies, and procedures to protect against evolving threats. However, if these training materials and security frameworks are not carefully designed and continuously updated, they can create vulnerabilities instead of strengthening an organization's security posture. Ensuring that cybersecurity training remains effective, relevant, and aligned with the latest industry standards is a complex challenge. Artificial intelligence (AI) has emerged as a powerful tool in this domain, offering an efficient mechanism for generating high- quality security training programs and strategic policies. AI-driven solutions enable organizations to automate the creation of customized training materials that cater to different skill levels, job roles, and industry- specific security requirements.

By leveraging AI, security training can be dynamically updated to incorporate the latest cybersecurity regulations, best practices, and threat intelligence, ensuring that employees and security teams stay ahead of potential risks. Organizations are increasingly recognizing the need for robust cybersecurity training programs to combat the rising sophistication of cyber threats. However, developing and maintaining these training materials, policies, and security procedures is a complex and resource-intensive task. Without properly designed and continuously updated content, organizations risk introducing vulnerabilities rather than strengthening their security posture. Traditional cybersecurity training methods often become outdated quickly, failing to address new attack techniques, regulatory changes, and emerging best practices. This underscores the need for a more efficient, automated, and adaptive approach—one that AI can effectively provide.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

REFERENCES

[1] M. E. Erendor and M. Yildirim, "Cybersecurity Awareness in Online Education: A Case Study Analysis," in IEEE Access, vol. 10, pp. 52319 52335, 2022, doi: 10.1109/ACCESS.2022.3171829.

[2] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, ‘‘The impact of information richness on information security awareness training effectiveness,’’ Comput. Educ., vol. 52, no. 1, pp. 92–100, Jan. 2009.

[3] A.Garba, M. Siraj, S. Othman, and M. Musa, ‘‘A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach,’’ Int. J. Emerg. Technol., vol. 11, no. 5, pp. 41–49, 2020.

[4] V. Sundararajan, A. Ghodousi and J. E. Dietz, "The Most Common Control Deficiencies in CMMC non-compliant DoD contractors," 2022 IEEE International Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 2022, pp. 1-7, doi: 10.1109/HST56032.2022.10025445.

[5] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Durgapur, India, 2020, pp. 1-3, doi: 10.1109/NCETSTEA48365.2020.9119914.

[6] G. Langner, J. Andriessen, G. Quirchmayr, S. Furnell, V. Scarano and T. J. Tokola, "Poster: The Need for a Collaborative Approach to Cyber Security Education," 2021 IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2021, pp. 719-721, doi: 10.1109/EuroSP51992.2021.00058.

[7] M. Neumann, M. Rauschenberger and E. -M. Schön, "“We Need to Talk About ChatGPT”: The Future of AI and Higher Education," 2023 IEEE/ACM 5th International Workshop on Software Engineering Education for the Next Generation (SEENG), Melbourne, Australia, 2023, pp. 29-32, doi: 10.1109/SEENG59157.2023.00010.

[8] Cisco Systems. (2008b). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved May 12, 2011,from World Wide L. Li, W. He, L. Xu, A. Ivan, M. Anwar and X. Yuan, "Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study," 2014 Enterprise Systems Conference, Shanghai, China, 2014, pp. 169-173, doi: 10.1109/ES.2014.66.

[9] National Institute of Standards and Technology. "AI Risk Management Framework." NIST January 26, 2023.

[10] J. C. Haass, "Cyber Threat Intelligence and Machine Learning," 2022 Fourth International C