

Research on the "professional, ideological, and innovative" tri-integration reform of the "computer network security" course in the context of artificial intelligence

Li Liu*

Shandong Xiehe University, Yaoqiang town, Licheng district, Jinan city, China

Abstract. With the rapid development of information technology, artificial intelligence has become a significant force driving social transformation. In this context, the "Computer Network Security" course faces unprecedented challenges and opportunities. This paper explores how to integrate professional knowledge teaching, ideological education, and innovation and entrepreneurship training (referred to as "Professional, Ideological, and Innovative" or "PII") into the "Computer Network Security" course in the context of artificial intelligence, aiming to enhance students' comprehensive qualities and innovative capabilities. By reforming teaching content, methods, and evaluation systems, this paper seeks to construct a curriculum system that meets the demands of the new era, providing strong support for cultivating compound talents with cybersecurity awareness and innovation capabilities.

1 Introduction

With the widespread adoption of the internet and the advent of the digital age, cybersecurity issues have become increasingly prominent. From personal data breaches to attacks on national critical infrastructure, frequent cybersecurity incidents have caused significant losses to society and the economy. Therefore, the "Computer Network Security" course, as a crucial pathway for cultivating cybersecurity talents, urgently needs reforms in its teaching content, methods, and evaluation systems to adapt to the challenges of the new era. The rapid development of artificial intelligence technology has brought new solutions and ideas to the field of cybersecurity, offering new opportunities for the reform of the "Computer Network Security" course. This paper explores how to integrate professional knowledge teaching, ideological education, and innovation and entrepreneurship training into the "Computer Network Security" course in the context of artificial intelligence, aiming to enhance students' comprehensive qualities and innovative capabilities.

* Corresponding author: 9989037@163.com

2 Applications and challenges of artificial intelligence in cybersecurity

2.1 Applications of artificial intelligence in cybersecurity

Artificial intelligence is increasingly being applied in the field of cybersecurity, with its powerful data processing, pattern recognition, and self-learning capabilities providing strong support for cybersecurity protection. Specifically, the applications of artificial intelligence in cybersecurity mainly include the following aspects:

2.1.1 Intelligent threat detection and response

Using machine learning and deep learning technologies, artificial intelligence can automatically extract valuable information from massive datasets, identify potential threat patterns, and respond in real-time. For example, by monitoring network traffic characteristics, artificial intelligence can quickly detect DDoS attacks, malware, and other abnormal behaviors, and take corresponding defensive measures.

2.1.2 Intelligent firewalls and intrusion detection systems

Traditional firewalls and intrusion detection systems often rely on predefined rules for protection, making it difficult to counter new attack methods. In contrast, AI-based firewalls and intrusion detection systems can dynamically adjust protection strategies based on real-time data, improving defense effectiveness. Additionally, artificial intelligence can identify potential security vulnerabilities and attack paths through correlation analysis and behavioral analysis.

2.1.3 Intelligent security operations and management

Artificial intelligence can automate routine security operations tasks such as vulnerability scanning, patch management, and log auditing, reducing the workload of operations personnel. At the same time, AI can provide intelligent security decision support, helping operations personnel respond quickly to security incidents and reduce security risks.

2.2 Challenges of artificial intelligence in cybersecurity

Despite significant achievements in the application of artificial intelligence in cybersecurity, several challenges remain:

2.2.1 Data quality and privacy protection

The performance of AI systems largely depends on the quality and quantity of data. However, in practical applications, data often contains noise and missing values, which can affect the accuracy of models. Additionally, privacy protection is a critical consideration in the application of AI in cybersecurity. Balancing the protection of user privacy with the effective use of data for security purposes is an urgent issue that needs to be addressed.

2.2.2 Model interpretability and transparency

The decision-making processes of AI systems are often difficult to interpret, which can be problematic in scenarios requiring high decision-making transparency, such as finance and healthcare. Users need to understand the basis and rationale behind security decisions to ensure their legality and rationality. Therefore, improving the interpretability and transparency of AI models is an important research direction.

2.2.3 Adversarial attacks and defense

With the continuous development of AI technology, adversarial attacks have become a new threat in cybersecurity. Attackers can construct specific inputs to deceive AI systems, causing them to make incorrect decisions or leak sensitive information. Thus, building robust AI systems capable of resisting adversarial attacks is a current research hotspot and challenge.

3 The practice of "professional, ideological, and innovative" tri-integration in the "computer network security" course

3.1 The connotation and significance of "professional, ideological, and innovative" tri-integration

"Professional, Ideological, and Innovative" tri-integration refers to the close integration of professional knowledge teaching, ideological education, and innovation and entrepreneurship training, forming an organic whole. Practicing this tri-integration in the "Computer Network Security" course has the following significant implications:

3.1.1 Enhancing students' comprehensive qualities

By integrating professional knowledge teaching, ideological education, and innovation and entrepreneurship training, students' professional competence, ideological and political qualities, and innovation and entrepreneurship capabilities can be cultivated, thereby improving their overall competitiveness.

3.1.2 Promoting curriculum innovation and development

Integrating the "Professional, Ideological, and Innovative" tri-integration concept into the "Computer Network Security" course can drive innovation in course content, improve teaching methods, and refine evaluation systems, promoting the continuous development and optimization of the course.

3.1.3 Adapting to the needs of the new era

With the rapid development of AI technology and the constant changes in the cybersecurity field, the demand for cybersecurity talents is also evolving. Practicing the "Professional, Ideological, and Innovative" tri-integration can cultivate cybersecurity talents who meet the needs of the new era, providing strong support for social development.

3.2 Strategies for practicing "professional, ideological, and innovative" tri-integration in the "computer network security" course

To practice the "Professional, Ideological, and Innovative" tri-integration in the "Computer Network Security" course, the following strategies can be adopted:

3.2.1 Integrating course content

Integrate the content of professional knowledge teaching, ideological education, and innovation and entrepreneurship training into an organic whole. For example, incorporate ideological elements and innovation and entrepreneurship cases into professional knowledge teaching, enabling students to enhance their ideological and political qualities and innovation awareness while learning professional knowledge.

3.2.2 Innovating teaching methods

Adopt a combination of online and offline teaching, theory and practice, and project-based learning to stimulate students' interest and initiative. At the same time, use AI technology to assist teaching, improving teaching effectiveness and learning efficiency. For example, use intelligent teaching systems to provide personalized learning paths and resource recommendations for students; use virtual simulation technology to simulate cybersecurity attack and defense scenarios, enhancing students' practical and response capabilities.

3.2.3 Improving evaluation systems

Construct a diversified evaluation system that includes course exams, project practices, and innovation and entrepreneurship competitions. At the same time, focus on process evaluation and comprehensive evaluation, paying attention to students' learning processes, teamwork abilities, and innovation and entrepreneurship outcomes. By improving the evaluation system, students' learning situations and comprehensive qualities can be fully reflected.

4 Specific implementation of "professional, ideological, and innovative" tri-integration in the "computer network security" course in the context of artificial intelligence

4.1 Integration of professional knowledge teaching and artificial intelligence technology

In professional knowledge teaching, AI technology can be fully utilized to assist teaching and improve teaching effectiveness. Specifically, the following measures can be taken:

4.1.1 Using intelligent teaching systems for personalized teaching

Intelligent teaching systems can provide personalized learning paths and resource recommendations based on students' learning situations and interests. By intelligently analyzing students' learning data and behavioral characteristics, the system can offer customized learning plans and feedback suggestions, helping students better master cybersecurity knowledge and skills.

4.1.2 Using virtual simulation technology for practical teaching

Virtual simulation technology can simulate real cybersecurity attack and defense scenarios, allowing students to practice and drill in a virtual environment. Through virtual simulation technology, students can intuitively understand the principles of cybersecurity attacks and defense methods, improving their practical and response capabilities. At the same time, virtual simulation technology can reduce experimental costs and risks, improving experimental efficiency and safety.

4.1.3 Introducing AI cases and cutting-edge technologies

In professional knowledge teaching, AI cases and cutting-edge technologies in cybersecurity can be introduced to help students understand the applications and advantages of AI in cybersecurity protection. Through case analysis and technical explanations, students can gain a deeper understanding of the principles and implementation methods of AI technology, stimulating their interest in learning and innovation awareness.

4.2 Integration of ideological education and cybersecurity awareness

In ideological education, emphasis can be placed on cultivating students' cybersecurity awareness and ideological and political qualities. Specifically, the following measures can be taken:

4.2.1 Incorporating cybersecurity laws, regulations, and ethical morality

In ideological education, content related to cybersecurity laws, regulations, and ethical morality can be incorporated to help students understand the importance of cybersecurity and the requirements of laws and regulations. By explaining cybersecurity laws, regulations, and ethical cases, students can be guided to establish correct cybersecurity concepts and legal awareness, enhancing their self-protection awareness and capabilities.

4.2.2 Organizing cybersecurity-themed educational activities

Cybersecurity-themed educational activities, such as cybersecurity knowledge competitions and lectures, can be organized to help students learn cybersecurity knowledge and skills, enhancing their cybersecurity awareness and prevention capabilities. At the same time, these activities can cultivate students' teamwork spirit and innovation awareness.

4.2.3 Combining current events for ideological education

Ideological education can be combined with current events, such as analyzing and discussing cybersecurity incidents, to guide students to think deeply about cybersecurity issues and social responsibilities. Through current events education, students' sense of social responsibility and mission can be enhanced, inspiring them to contribute to the national cybersecurity cause.

5 Conclusion and outlook

This paper explores the "Professional, Ideological, and Innovative" tri-integration reform of the "Computer Network Security" course in the context of artificial intelligence. By integrating professional knowledge teaching, ideological education, and innovation and entrepreneurship training in terms of content and methods, this paper aims to construct a curriculum system that meets the demands of the new era. Practice has shown that the "Professional, Ideological, and Innovative" tri-integration can effectively enhance students' comprehensive qualities and innovation capabilities, providing strong support for cultivating compound talents with cybersecurity awareness and innovation abilities. In the future, we will continue to deepen the "Professional, Ideological, and Innovative" tri-integration reform, explore more innovative teaching methods and evaluation systems, and contribute to cultivating more outstanding cybersecurity talents. At the same time, we will also pay attention to the latest developments and application trends in AI technology, continuously integrating them into the "Computer Network Security" course to promote the continuous development and optimization of the curriculum.

Project source: The 2023 Shandong Xiehe University School-level Teaching Reform Project "Research and Practice on the Reform of Computer Network Security Classroom Teaching under the Background of ' Professional, Ideological, and Innovative ' Trinary Integration", Project Number: 2023XJ18

References

1. Huang X .The Application and Exploration of AI Technology in the Teaching of Marine Logistics Courses[J].Journal of Social Science Humanities and Literature,2025,8(2):
2. An Y ,Yu H J ,James S .Investigating the higher education institutions' guidelines and policies regarding the use of generative AI in teaching, learning, research, and administration[J].International Journal of Educational Technology in Higher Education,2025,22(1):10-10.
3. Ablass R K, Schliz K ,Schlick C , et al. Teaching opportunities for anamnesis interviews through AI based teaching role plays: a survey with online learning students from health study programs.[J].BMC medical education,2025,25(1):259.
4. Xin H .Research on the Reform Path of College English Teaching in the Era of Artificial Intelligence[J].Journal of Contemporary Educational Research,2025,9(1):135-139.
5. Li C .The integration and innovative practice of intelligent AI and local opera in college teaching [J].Frontiers in Psychology, 2025, 151521777-1521777.
6. Yu L ,Xiuping Z ,Jin C .Optimisation of Teaching Methods and Practical Exploration of Teachers' Teaching Methods in Vocational Education Based on AI Assistance[J].Applied Mathematics and Nonlinear Sciences,2025,10(1):