ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

Exploration and Practice of the 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model: A Case Study of Wuhu University

Ling Chen

Wuhu University, School of Computing Science, Wuhu, Anhui 241000, China

sherlyme2@163.com

Abstract

With the introduction of the “Double Thousand” Plan and the demand for talent in the context of artificial intelligence, the model for cultivating high-level, high-quality talent is undergoing transformation. Micro-majors have gradually extended from online MOOC platforms to university platforms, and as a new mode of education, they have received widespread attention. The AI context also imposes new requirements for talent development. Taking the construction of the Confidential Computing micro-major at Wuhu University as an example, this paper builds an AI innovative talent cultivation model of 'Majors and Micro-Majors Dual-Track'. Through the practice of micro-major development and the AI Innovation Class, it provides a new scheme for talent training. During the implementation of micro-majors and AI Innovation Class, talent is cultivated around the core competencies of micro-credential and AI talent. Owing to their short duration, specialized content, and strong practical orientation, they are widely recognized by students. This study holds certain significance for exploring and practicing pathways for talent cultivation.

Keywords

Talent cultivation model; Micro-major; Confidential computing; AI Innovation Class.

1. Introduction

Micro-majors are emerging talent training models formed by local application-oriented universities to better serve regional economic and social development under the background of new engineering concepts. In 2013, the concept of micro-majors was first proposed on the edX platform, jointly created by MIT and Harvard University. The earliest record of the effectiveness of micro-major construction in our country is the "entrepreneurship management" micro-major created by Zhejiang Gongshang University in 2014 [1]. The fundamental purpose of its education is to adapt to the development needs of new technologies, new formats, new models, and new industries in the era of digital intelligence, and to cultivate students' interdisciplinary knowledge, interdisciplinary thinking, and cross-border integration capabilities [2].

In the process of micro-major construction, our country continues to try new methods and paths, integrate multiple advantageous resources, and promote the construction of micro-majors. Among them, it is worth noting that the "AI+X" micro-majors training project built in 2021 is composed of a total of 6 universities, including Shanghai Jiao Tong University, Fudan University, University of Science and Technology of China, Tongji University, Zhejiang University, and Nanjing University, plus a number of companies including Huawei and Baidu to jointly establish the "New Generation of Artificial Intelligence Science and Education Consortium", which creates "AI+X" micro-majors through virtual teaching and research offices and industrial clusters to provide a way for non-computer students to learn artificial

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

intelligence knowledge. Cultivate interdisciplinary talents. The "AI+X" micro-major of the project realizes cross-school, interdisciplinary, and cross-professional teaching and management through co-construction and co-selection, mutual recognition of credits, and co-signing of certificates, and promotes the connection between education chains, talent chains, industrial chains, and innovation chains [3].

In addition to the universities in the "AI+X" micro-majors training program, universities in different regions and levels have also invested resources to apply for and open micro-majors that are in line with regional economic and social development and the foundation of university platforms, and implement micro-majors with their own characteristics. For example, Shanghai University of Engineering Technology offers a "blockchain" micro-major and adopts a six-dimensional teaching system of "teaching, supervision, learning, training, testing, and assistance" to carry out the construction and practice of micro-majors [4]. The micro-major of "Fine Chemical Manufacturing and Analysis" at Shanghai University of Applied Sciences cultivates nine key competencies: active learning and appreciation, independent learning ability, critical thinking ability, creative problem-solving ability, communication ability, teamwork ability, international vision ability, information literacy ability, applied technology ability, and professionalism [5].

Table 1. The Construction of Micro-Majors in Some Domestic Universities

School Name	College Name	Micro-Major Name	Curriculum	Total Credits	Duration of study
Jilin University	School of Mathematics	Intelligence and Data Computing	Scientific computing methods, machine learning and visual computing, numerical methods for optimization problems, Python data mining, mechanism and data fusion computing	10	1 year
University of Science and Technology Beijing	School of Mathematics and Physics	Intelligent Optimization and Data Computing	Mathematical Modeling, Optimization Methods, Machine Learning and Its Applications, Introduction to Scientific Computing, Statistical Computing, Python Data Analysis	13	1 year
Guangdong Polytechnic Normal University	School of Electronics and Information	Digital Twin Application Technology	IoT systems and software training, concepts and regulations of digital twins, 3D structural surveying, digital twin model construction training, overview of digital twin application scenarios, basic knowledge and training of structural design	15	1 year
Changsha University	School of Mechanical and Electrical Engineering	Intelligent Manufacturing and Digital Twin	Introduction to Digital Twins, Digital Twin Modeling and Simulation Technology, Mechatronics Design, Machine Vision, Intelligent Manufacturing Equipment and Systems, PLC Programming Technology, Industrial Big Data, Professional Integrated Practice	15~20	1 to 2 years

In addition, private undergraduate colleges and universities are also trying to open micro-majors. For example, Qingdao Binhai University has opened a micro-major of "information security" in accordance with the requirements of industry-education integration 2.0, and adopted the intelligent industry-education integration platform with "cloud-edge-end" collaboration to implement industry-education integration [6]. The School of Computing Science of Wuhu University also applied for the first batch of two micro-majors projects of "Confidential Computing" and "Digital Twin" in 2023, and was approved in May 2024. In order to better develop the introduction of the implementation process of the two micro-majors of Wuhu University, combined with the characteristics of these two micro-majors, the micro-majors of domestic universities are similar to the two micro-majors of "Confidential Computing" and "Digital Twin". The comparison is made from six dimensions: the name of the school, the name of the college, the name of the micro-major, the curriculum, the total number of credits, and the duration of study, see the table of the construction of micro-majors in some domestic universities in Table 1.

This paper mainly takes the construction of confidential computing micro-majors of Wuhu University as an example, and explains in detail from the basics of micro-majors, the

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

implementation of micro-majors and the challenges of micro-majors, and at the same time provides an in-depth introduction in combination with the implementation of the 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model.

2. The 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model

In the context of micro-majors and artificial intelligence, this study innovatively proposes a 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model. The core idea of this model is: first ensure the steady implementation of students' majors, then select some students to enter the micro-major study based on students' wishes, and finally combine students' wishes to enter the AI innovation class stage of learning. Thus, it constitutes a 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model for majors and micro-majors. The overall framework is shown in Figure 1.

The specific implementation plan of the 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model:

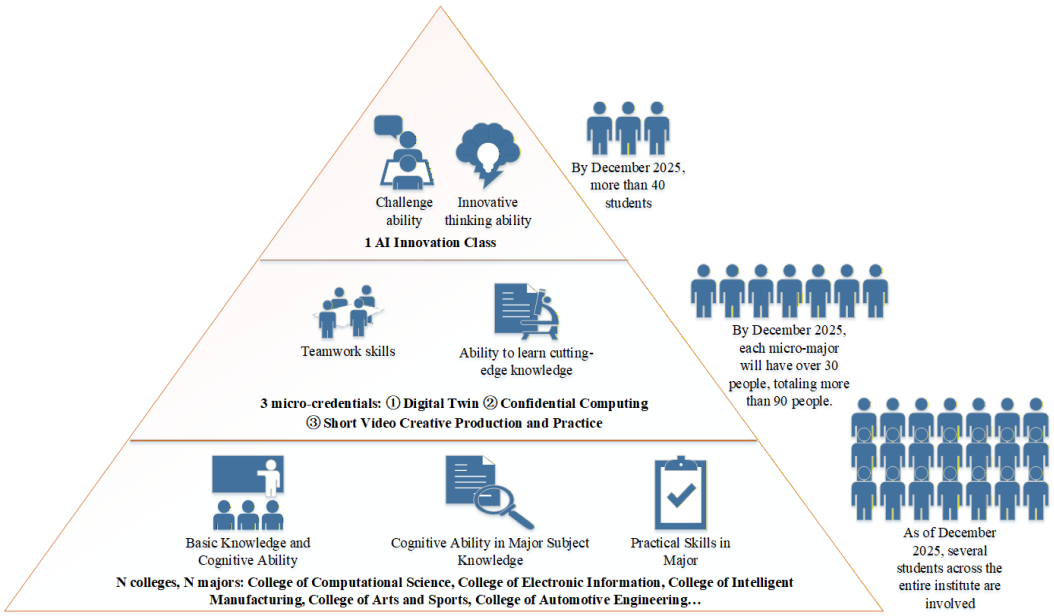

Figure 1. The 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model

2.1. Majors Build A Solid Foundation for Disciplines

Majors are cornerstones of talent training in colleges and universities, aiming to enable students to have a solid theoretical foundation in disciplines, systematic professional knowledge and practical skills, and cultivate students' cognitive ability of general basic knowledge, professional knowledge cognitive ability, and professional practice ability. Only by completing the study of the major can students build a solid foundation for disciplines, form basic professional qualities, and provide a solid guarantee for subsequent entry into society.

2.2. Micro-majors Focus on the Frontier of Society

Micro-majors offered by the school all belong to the direction of focusing on the frontier of society, and more deeply cultivate students' teamwork ability and cutting-edge knowledge learning ability. At present, three micro-majors have been opened: digital twin, confidential computing, and short video creation production and practice. Each micro-major enrolls about 30 students every year. Micro-major enrollment requirements: need to have a certain foundation in majors; On the premise that students have the ability to study their major majors, students voluntarily join; Pass the assessment of the college. Students who enter the micro-

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

major study need to pass the assessment of all courses in the micro-major talent training program within the specified time to obtain the micro-major certificate. During the micro-major training period, the course integrates rich practical teaching content, invites the school's industrial professors to jointly train students, and introduces actual industrial practice links to improve students' practical ability. Through the training of micro-major links, the participating students can better grasp the cutting-edge knowledge of society in a shorter period of time and better meet the requirements of social production practice.

2.3. AI Innovation Class Stimulates Students' Innovation Potential

AI innovation class is the top-level design of the training model of this research, aiming to cultivate outstanding students who can master and apply the knowledge and practical skills of certain subdivisions of artificial intelligence, and cultivate students' challenging ability and innovative thinking ability. At present, the members of the AI innovation class of our school are all selected from students from three micro-majors. The AI innovation class provides students with richer resources and platforms, holds lectures by experts in the field of artificial intelligence, conducts in-depth internships in enterprises, and teaches by corporate tutors. At the same time, students can obtain the certificate of the AI innovation class only if they have obtained at least one subject competition in the field of AI above class A or B under the premise of obtaining their micro-major certificate, and write a learning summary of the AI innovation class. This design provides a guarantee for cultivating students' cutting-edge artificial intelligence skills and stimulating students' innovation ability.

3. Take the Confidential Computing Micro-Major Construction + AI Innovation Class As An Example

3.1. Confidential Computing Micro-Major Setting Basis

With the continuous advancement and deepening of digital construction, artificial intelligence technology, big data technology, intelligent network technology, etc. have developed rapidly and continuously iterated, and people have gradually entered the era of networking, digitization, and intelligence [2]. At the same time, it also poses new challenges to the security of data storage, transmission and use, and Confidential Computing is the embodiment of a security technology in the process of data use. In order to further explain the necessity of establishing a Confidential Computing micro-major, the following is an explanation from two aspects: the policy basis and theoretical basis of the establishment of this major.

3.1.1. Policy Basis

In recent years, the construction of micro-majors in colleges and universities in Anhui Province has achieved fruitful results, and the earliest university in the province to open micro-majors is Anhui University of Technology, which opened the first "artificial intelligence" micro-major in 2020. In 2021, Anhui Province issued the "Opinions on Vigorously Developing the Top Ten Emerging Industries to Create Clusters of Emerging Industries with Important Influence", proposing to vigorously develop the top ten emerging industries during the "14th Five-Year Plan" period, including: a new generation of information technology industry, new energy vehicle and intelligent networked vehicle industry, digital creative industry, high-end equipment manufacturing industry, new energy and energy conservation and environmental protection industry, green food industry, life and health industry, smart home appliance industry, new material industry and artificial intelligence industry, see Figure 2. In 2022, the Anhui Provincial Government proposed the "Implementation Plan for Deepening the Reform of the Discipline and Professional Structure of Colleges and Universities and the Innovation and Development of the Service Industry (2022-2025)", and in March 2024, the "Notice of the Anhui Provincial Department of Education on Carrying out the Pilot Work of micro-majors in Colleges

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

and Universities", requiring the direction of serving the top ten emerging industry types, exploring and carrying out the reform of the talent training mode of "micro-disciplines", "micro-credentials" and "micro-courses", and supporting 104 universities and enterprises to jointly build 153 "micro-majors". Carry out pilot work on the construction of micro-majors in colleges and universities. In order to meet the needs of development, the School of Computing Science of Wuhu University applied for a Confidential computing micro-major, which meets the requirements of serving the new generation of information infrastructure industry and artificial intelligence industry in the top ten emerging industry types, and the project was successfully approved in 2024.

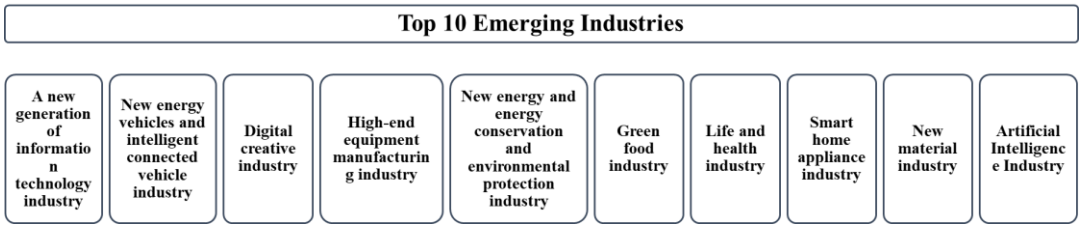

Figure 2. Top ten emerging industries in Anhui Province

3.1.2. Theoretical Basis

Data is a key production factor in the digital age, and data protection involves data in three different states: data at transit, data at rest, and data in use [7]. The Trusted Execution Environment (TEE) is a secure area in the CPU that is secured by embedded encryption keys [8]. With the increasing requirements of society for data security and privacy protection, Confidential Computing (CC) has attracted widespread attention as an emerging secure computing model.

Confidential computing is based on the calculations performed in the hardware TEE to protect the security of "in-use" data, involving scenarios such as cross-departmental data sharing in e-government, financial risk assessment, and IoT data aggregation analysis [9]. The development of confidential computing has gone through three stages: the TPM/TCM stage during 2003~2014, which is widely used in smartphones; The TEE stage from 2015~2018 has been applied in cloud platforms and other fields, and from 2019 to the present, the confidential computing stage has been further integrated with the CCC of the confidential computing Alliance established by the Linux Foundation in 2019 to further integrate confidential computing, machine learning, data security and other ecosystems [7]. The characteristics of confidential computing include data confidentiality, data integrity, code integrity, code confidentiality, authentication initiation, mutability, provability, and recoverability. The framework of confidential computing includes five parts: hardware layer, software layer, service layer, application layer and management layer. In October 2024, Asterinas, a "star bloom" containing confidential computing, was jointly released by Zhongguancun Laboratory, Ant Group, Peking University and other institutions, and the software stack of "Star Bloom" includes the Star Bloom operating system and Star Bloom confidential computing, of which the confidential computing software stack includes three components: HyperEnclave, Occlum, and TrustFlow, building a trusted technology ecosystem in computing scenarios such as cloud computing, trusted data circulation, and artificial intelligence [10].

The general framework for confidential computing is given by GB/T 45230-2025 "Data Security Technology-General Framework Standard for Confidential Computing", as shown in Figure 3. The framework is composed of ordinary computing environment and confidential computing environment, and is displayed from four levels: hardware layer, software layer, service layer and application layer of the two computing environments. In a confidential computing environment, the underlying hardware layer includes a trusted execution control unit, trusted firmware, isolated memory space, random number generator, hardware cryptographic engine,

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

hardware root key, and hardware root of trust. The software layer includes a confidential computing operating system, optional confidential computing virtualization software; The service layer includes confidential computing service interfaces and services in cryptographic applications, performance improvement, data protection, and basic security. The upper application layer is the application of confidential computing; In addition, optional security management is included, specifically key management, log management, resource management, and whitelist management [11].

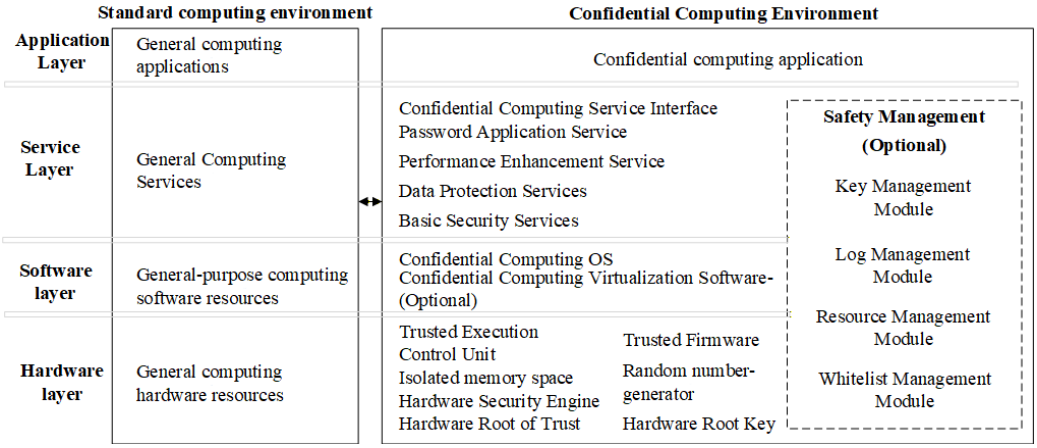

Figure 3. General framework for confidential computing

It is precisely because of the importance of confidential computing in data security, as well as the characteristics of the college and the advantages of disciplines and majors of the School of Computing Science, through the integration of school and enterprise resources, the construction of micro-majors is jointly carried out, and after full demonstration, Confidential Computing micro-majors are set up and recorded. Through the establishment of Confidential Computing micro-major, the exploration and practice of new models of compound talent training are realized. At the same time, we will cooperate with joint declaration enterprises to implement the integration of industry and education, support the registration and learning of micro-majors with spare energy, and improve students' comprehensive literacy.

3.2. Implementation of Confidential Computing Micro-Majors

3.2.1. Formulate a Training Plan for Confidential Computing Micro-major

According to the guiding ideology of serving the ten emerging industry types, the Confidential Computing micro-major meets the needs of two of them, one is the new generation of information infrastructure industry, and the other is the artificial intelligence industry. The formulation of micro-professional talent training programs should not only meet the four new requirements of new technologies, new formats, new models, and new industrial development, but also be based on the theory of confidential computing and maintaining "in-use" data security. After synthesizing all factors, the training objectives and curriculum system of the Confidential Computing micro-major are clarified to ensure that they meet the dual needs of discipline development and industrial development.

(1) Clarify the training objectives

The main purpose of carrying out the construction of Confidential Computing micro-majors is to meet the major strategic needs of the country, cultivate professionals who can adapt to the development of the digital economy and data security industry and the needs of the national data security strategy, firmly grasp the theoretical foundation of computers, systematically master the core technologies and principles of Confidential Computing, and be able to carry out efficient and safe computing processing and analysis under the premise of ensuring data security and privacy.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

Through systematic course learning and practical training, students can master cutting-edge knowledge in the field of confidential computing, and have the ability to independently carry out confidential computing technology research and development, system design, security evaluation and optimization. At the same time, focus on cultivating students' innovative thinking and practical ability to adapt to the changing information security environment and technological development trends. Through the construction of Confidential Computing micro-major, it provides knowledge and professional skills training for students to participate in subject competitions, and enhances the core competitiveness of students who have spare time to learn. The specific types of subject competitions that can be participated in include network security competitions, programming competitions, big data and artificial intelligence competitions, etc. The training goals of students majoring in Confidential Computing can be divided into the following points:

1) Knowledge and ability: master the basic principles, key technologies and application scenarios of confidential computing and privacy computing, and understand the development trends and cutting-edge technologies in the field of confidential computing at home and abroad; Solid basic knowledge of mathematics, computer and information security, and able to apply the knowledge learned to solve practical problems. It has the ability to solve actual data security problems, and can formulate and implement effective data security strategies and solutions according to different scenarios and needs.

2) Innovative thinking: have innovative consciousness and critical thinking, and be able to think independently, analyze problems and propose solutions; Able to pay attention to the development of new technologies and methods, and apply them to research and practice in the fields of confidential computing and data security.

3) Practical ability: cultivate students' practical ability and team spirit through course experiments, project practice, internship training, etc.; Enable students to familiarize themselves with the development process of confidential computing systems and have the ability to develop and implement actual projects.

4) Professional ethics and literacy: pay attention to cultivating students' professional ethics and literacy, so that they have a high sense of responsibility and mission; Comply with network security, data security laws and regulations, and industry standards to ensure data security and user privacy.

Through the cultivation of students' knowledge and ability in confidential computing, students can have professional knowledge; Through the cultivation of students' innovative thinking in confidential computing, guide students to participate in more subject competitions, apply for patents and precipitate achievement reports, and improve students' ability to think independently, summarize in depth, and innovate. Through the cultivation of students' practical ability in confidential computing, students' understanding of the industry can be improved, and the specific foothold of the practical ability of talents in confidential computing can be understood. Through the cultivation of students' professional ethics and literacy ability in confidential computing, students' correct values can be established, relevant network security and other standards can be established, professional norms and awareness can be strengthened, and students' future career direction and professional behavior can be correctly guided.

In order to ensure the quality of the confidential computing micro-major, certain requirements are also put forward for the registered students when enrolling micro-majors, which need to have a certain computer foundation, programming foundation and mathematical analysis foundation.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

(2) Establish a curriculum system

Through the establishment of the confidential computing micro-major curriculum system, it aims to cultivate professionals who can adapt to the development of the digital economy and data security industry and the needs of the national data security strategy, firmly grasp the theoretical foundation of computers, systematically master the core technologies and principles of confidential computing, and be able to carry out efficient and safe computing processing and analysis under the premise of ensuring data security and privacy. The establishment of the curriculum system needs to determine the number of courses, course names, course credits, weekly hours, total hours, theoretical and practical hours, etc.

Table 2. Confidential Computing micro-major Courses

Serial Number	Course Name	Credits
1	Data Protection and Cryptography Applications	4
2	Database Security Technology and Practice	4
3	Confidential Hardware and Software Product Design and Applications	2
4	Principles and Applications of Secure Computing	4
5	Confidential Software Engineering and Practice	3

In the process of establishing a confidential computing micro-major curriculum system, three main aspects are considered: first, through the interpretation of the "Notice of the Anhui Provincial Department of Education on Carrying out the Pilot Work of Micro-Major Construction in Colleges and Universities", the guidance on curriculum setting is refined: micro-majors need to be based on existing majors or specific industry fields, focus on core knowledge and ability training, support cooperation with the industry, build a curriculum system, and develop core courses; Micro-majors generally offer 3-5 courses, and in principle, they are taught in a project-based manner, and online and offline hybrid teaching is carried out. Second, the search, sorting and analysis of similar micro-majors in different schools are specifically referred to Table 1. From Table 1, it can be seen that the number of micro-majors in relevant colleges and universities ranges from 5-7 core courses, with a total credit of 10-20, and most of the study years are set in 1 year (between 1-2 years), thus reflecting the characteristics of short cycle and specialized content of micro-majors. Third, the curriculum system is designed based on the current professional situation and related courses offered by the college. Based on the three factors, the course system of confidential computing micro-majors was finally established, as shown in Table 2, including 5 compulsory courses: Data Protection and Cryptography Applications, Database Security Technology and Practice, Confidential Hardware and Software Product Design and Applications, Principles and Applications of Secure Computing, and Confidential Software Engineering and Practice, with a total of 17 credits.

Through systematic course learning and practical training, students can master cutting-edge knowledge in the field of confidential computing, and have the ability to independently carry out confidential computing technology research and development, system design, security evaluation and optimization. At the same time, focus on cultivating students' innovative thinking and practical ability to adapt to the changing information security environment and technological development trends. Before the micro-major certification, students must pass the course assessment and complete 10 credits to be issued a confidential computing micro-major certificate.

3.2.2. Implement the Mechanism for The Integration of Industry and Education

The implementation of the confidential computing micro major relies on the provincial "artificial intelligence and computing power platform" industrial college project of the School

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

of Computing Science and the two enterprise platforms jointly declared, and has professional corporate tutors and rich platform resources of the industrial college to provide support for the curriculum implementation and implementation quality assurance of the micro major.

The two companies jointly declared for confidential computing micro-majors have rich project implementation experience in data security and artificial intelligence: for example, they provide security products and services to government agencies, operators, finance, energy and other industries, and are in a leading position in the market in cloud security, big data security, Internet of Things security, smart city security and other fields; For example, the business covers digital government, smart transportation, intelligent networking, and industrial Internet, and is committed to creating core products and solutions using technologies such as big data, digital twins, artificial intelligence, and 5G applications.

Through the cooperation with the two joint reporting units, the school-enterprise cooperation and joint talent training of Confidential Computing micro-major provides a feasible curriculum implementation project-based teaching plan. Through the introduction, design and implementation of cutting-edge technical field solutions, students' hands-on practical ability and project implementation ability are exercised.

4. Achievements and Challenges of the Proposed Model

4.1. Results of Implementation

Based on the course "Database Security Technology and Practice" based on the confidential computing micro-major, the micro-course project of the provincial quality engineering project has been declared. The Confidential Computing micro-major has been implemented for two cycles, and the overall professional skills and subject competition results of students studying micro-majors are significantly higher than those who have not studied. In the process of micro-major construction, industrial professors are introduced to teach some courses in the course, and the actual work requirements and skill points in the enterprise are better and more deeply taught to students, so that students can master more practical work skills and improve their comprehensive competitiveness.

The results of discipline competitions have improved significantly, from the types of discipline competitions to the number of participants and the number and quality of awards, especially the results of category A and B and above competitions have been steadily advanced. The creation of AI innovation classes not only enriches the school's talent training model, but also improves the comprehensive quality of teachers, and obtains more opportunities for project funding and training.

4.2. Future Challenges

The implementation of the Confidential Computing micro-major is relatively stable, and there are many registered students, which has attracted widespread attention from the students of our school. Based on the support of the school's relevant policies, projects and platforms, the implementation of the course is generally smooth and meets the opening expectations. However, there are also some challenges faced in implementation, which are mainly illustrated from the following three dimensions.

First of all, the hardware platform is not perfect. In the first round of implementation of this micro-major, the hardware platform involved in confidential computing expertise is not perfect, and the platform construction needs to be further completed.

Secondly, the structure of the teaching staff needs to be optimized. At present, there are mainly young teachers participating in micro-major courses, and their teaching experience needs to be further improved. In the future, it is necessary to optimize the age structure and professional title structure of the teaching staff to further improve the teaching effect. The proportion of

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

corporate tutors is not high, so teachers with rich teaching experience can be further introduced to improve the effect of practical class teaching. Enterprise tutors and college teachers should strengthen teaching, research and communication, and jointly formulate teaching content and teaching plans.

Finally, the large difference in student base leads to an increase in teaching difficulty. Since micro-majors are open to the whole college, the student base is uneven, and the formulation of enrollment plans needs to be further optimized. In addition, during the implementation of the course, online resources are enriched, and students are provided with preview and review, so as to carry out systematic learning of knowledge and improve students' learning effect.

5. Conclusions and Prospects

This paper innovatively proposes the 'Majors and Micro-Majors Dual-Track' AI Innovation Talent Cultivation Model in the context of artificial intelligence, introduces the policy background of the establishment of micro-majors and the concept of micro-majors, analyzes the theory of confidential computing, and explains the practical process and achievements of the construction of confidential computing micro-majors in combination with Wuhu University. This paper interprets the connotation of the collaborative education model, and introduces the formulation of the talent training plan, the establishment of the curriculum system and the implementation of the integration mechanism of industry and education for confidential computing micro-majors, which provides an example for the establishment and implementation of micro-majors and AI innovation classes, which has good practical significance.

In the future, with the development of large language model LLM technology, many untrustworthy entities and complex software and hardware environments will emerge in the process of training and reasoning, and confidential AI will gradually become a new research field, which can be divided into three directions: partition execution (placing AI model partitions into TEEs for execution), heterogeneous TEE (GPU-enabled TEEs), and TEE-assisted AI computing [12]. Socialist successors with good confidential computing practice and excellent professionalism. At the same time, it is also hoped that through the setting of this talent training model, more outstanding top-notch talents can be cultivated in the field of artificial intelligence.

Acknowledgments

This work is supported by Anhui Provincial Quality Engineering Project, Project Number: 2023sdxx134.

References

[1] Liu Yuliang, Zhou Wenlong, Lian Xinze, et al. Construction Strategies of Engineering Micro-majors in Local Colleges and Universities: A Case Study of Wenzhou Institute of Technology [J]. Research on Higher Engineering Education, 2024, (04):88-93.

[2] Qin Leiyi, Chen Peng. Conceptual Characteristics, Purpose Value and Development Strategy of Micro-professional Education in Colleges and Universities [J]. Education Academic Monthly, 2023, (12):96-103.

[3] Yuan Jing, Zhai Xuesong, Wu Fei, et al. Construction of artificial intelligence majors (AI+X direction) in colleges and universities based on virtual teaching and research offices: A case study of Zhejiang University [J]. Modern Educational Technology, 2024, 34(05):123-133.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202602_9(2).0019

[4] Xia Chunming, Jin Xiaoyi, Wang Xiaojun, et al. Research and exploration of micro-major construction in local colleges and universities under the background of new engineering [J]. Research of Higher Engineering Education, 2023, (02):14-18.

[5] Ge Junyu, Jiang Chao, Wang Yuhong. Micro-professional construction based on "ASciT-ASP" teaching mode: a case study of fine chemical manufacturing and analysis [J]. Higher Engineering Education Research, 2025, (02):55-59.

[6] Diao Limei, Liu Chunqiang. Research on the training path of information security micro-majors based on the integration of industry and education [J]. Home Appliance Maintenance, 2025, (05):46-48.

[7] Feng Dengguo. Information Security Research, 2024, 10(01):2-5

[8] Li He. Protecting the Data Lifecycle through Confidential Computing [J]. Network Security and Informatization, 2022, (07):108-109.

[9] Comprehensive. 2024 Hot Words in the Field of Security and Confidentiality [J]. Confidentiality Work, 2024, (12):21-23.

[10] "Star Bloom" secure and trusted system software stack released for global developers open source [J]. China Information Security, 2024, (11): 85.

[11] National Network Security Standardization Technical Committee. GB/T 45230—2025 Data security technology—General framework standard for confidential computing [S]. 2025.

[12] Su Purui, Feng Dengguo. Review of cyberspace security technology hotspots in 2024 [J]. Science and Technology Review, 2025, 43(01):102-117.