Curriculum and Teaching Methodology (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/curtm.2024.070812
ISSN 2616-2261 Vol. 7 Num. 8

Exploration into the Teaching Reform of Introducing the Internet of Things Security Course Project

Cui Dong

Guangdong University of Science and Technology, Dongguan City, Guangdong Province, China
877437617@qq.com

Keywords: Internet of Things, information security, smart home, project introduction method

Abstract: With the rapid development of Internet of Things technology, its application in various fields of society is becoming increasingly widespread, but it also brings unprecedented security challenges. To address these challenges, it is imperative to cultivate high-quality talents with IoT security skills. This article analyzes the problems existing in the current teaching of Internet of Things security technology courses, and proposes a curriculum reform plan based on project introduction method. The introduction of smart home projects elaborates on the implementation process of specific Internet of Things security projects, in order to enhance students' practical ability and ability to solve practical problems. Through this reform, students can not only deeply understand the theoretical knowledge of Internet of Things security technology, but also master key skills in practice, laying a solid foundation for future career development.

1. Introduction

As an important part of the new generation of information technology, the Internet of Things (IoT) is profoundly changing the way of human production and life[1]. However, with the widespread use of IoT devices, their security issues have become increasingly prominent, such as data leakage, privacy infringement, and cyber attacks, which pose significant risks to society and individuals. Therefore, it is particularly important to cultivate professionals with the ability to use IoT security technology. Currently, there are problems in the Internet of Things security technology courses in universities, such as the disconnect between theory and practice, and the lack of students' innovative application ability, which are difficult to meet the industry's demand for talents. With the rapid development of Internet of Things technology, smart home systems[2] have become an indispensable part of modern homes. These systems realize intelligent control and management of the home environment by integrating sensors, controllers, network communication technology, and artificial intelligence algorithms. The widespread use of smart home systems has also brought serious information security challenges. Hackers use system vulnerabilities to conduct illegal intrusion, data theft, privacy leakage, and other activities, which seriously threatens users' family security and privacy rights. Therefore, it is particularly important to build a sound smart home security protection system. This article uses the case of smart home security protection system as an introduction project for the Internet of Things security course, and explores a teaching reform plan centered on project

introduction methods, with a view to improving the quality of the course and the overall quality of students.[1]

2. Analysis of the current situation of the Internet of Things security technology course

2.1 The course content is lagging behind

At present, the content of IoT security technology courses often focuses on the teaching of theoretical knowledge, such as encryption algorithms, security protocols, intrusion detection, etc., and does not involve the application of emerging technologies such as blockchain and artificial intelligence in IoT security. This has led to a disconnect between the course content and the development of the industry, making it difficult to adapt to market demand[3].

2.2 The teaching method is single

Traditional teaching methods have been applied in IoT security technology courses for many years, such as:

Classroom teaching: The traditional teaching method is mainly based on classroom teaching, and teachers impart knowledge to students through explanations, board books, PPT and other methods.

Focus on theory: The traditional teaching method focuses on the teaching of theoretical knowledge and emphasizes the mastery and understanding of theoretical knowledge, but lacks the cultivation of students' innovation and practical ability, resulting in students' lack of ability to solve practical problems. Students lack the opportunity to practice and combine theoretical knowledge with practice, resulting in students' lack of ability to solve practical problems and apply the knowledge they have learned to practical work.

Less teacher-student interaction: In the traditional teaching method, the teacher is generally in the dominant position, and the student belongs to the passive acceptance of knowledge, lacking the opportunity to actively think and explore, and the teacher's interaction.

In the course of IoT security technology, the disadvantages of traditional teaching methods are gradually revealed.[2]

3. Reform plan of the project practice method

In order to overcome the disadvantages of traditional teaching methods, new teaching methods have emerged. One of the applications of the new teaching method in the IoT security technology course is to introduce project practice and conduct case analysis. By analyzing real-world IoT security cases, students can understand the types, sources, and preventive measures of IoT security threats, and improve security awareness and prevention capabilities. This method focuses on the combination of theory and practice, and allows students to combine theoretical knowledge with practice and improve their practical ability and problem-solving ability through experimental teaching and case analysis[4].

3.1 Reform objectives

Through the introduction of the reform of the project practice method, the following goals are achieved: first, to enhance students' practical ability and innovation ability; the second is to improve students' understanding and application ability of IoT security technology; the third is to promote the deep integration of theory and practice; The fourth is to cultivate students' teamwork spirit and professional quality.

3.2 The content of the reform

3.2.1 Restructuring of course content

According to the development trend of IoT security technology and industry needs, the course content is reconstructed. On the basis of retaining traditional theoretical knowledge, the application content of emerging technologies such as blockchain such as artificial intelligence in the security of the Internet of Things is added. At the same time, it pays attention to the combination of case analysis and practical operation, so that students can better understand and master the knowledge they have learned.

3.2.2 The project introduction method is used as the main teaching method

Using the project-in-practice approach as the primary teaching method, the project is divided into several sub-projects after selecting the appropriate project, each of which is designed around one or more IoT security issues. In the process of group discussion, the interactive way of group discussion is used to allow students to communicate and share their ideas and opinions with each other, promote the collision of ideas and inspiration, and at the same time, in the process of group discussion, teachers can keep abreast of students' learning situation and problems, and provide targeted guidance and help to help students deepen their understanding of knowledge points. In the process of project practice, students can complete the project tasks through teamwork under the guidance of teachers, and at the same time, students need to use the knowledge they have learned to carry out problem analysis, scheme design, experimental verification and result analysis. This teaching method can stimulate students' interest and initiative in learning, and improve the teaching effect.[3]

4. Implementation of specific IoT security projects

4.1 Project background

This project takes the smart home system that uses emerging technologies such as artificial intelligence as an example, and the design concept of the smart home security protection system is "comprehensive protection, active defense, and intelligent response", which means that the system needs to fully consider all possible security threats, including cyber attacks, physical attacks, data leaks, etc. Proactive defense means that the system needs to take proactive measures such as real-time monitoring, anomaly detection, proactive defense strategies, etc. The system includes multiple subsystems such as smart door locks[5], smart lighting, smart security, and smart home appliances. These subsystems are connected to the home network through wireless communication protocols such as Wi-Fi and ZigBee for remote control and data sharing. The goal of the project is to build a comprehensive teaching system integrating theoretical teaching, practical operation, and innovation ability training, so that students can master the core technology of smart home security protection, have the ability to design, implement and maintain smart home security protection systems, and improve the security and stability of smart home systems through the implementation of a series of security measures, so as to ensure user privacy and data security.[4]

4.2 Integration of curriculum design and project content

In terms of curriculum design, it is necessary to pay attention to the cutting-edge and practical nature of the content. First of all, the basic courses cover key areas such as computer basics, network fundamentals, sensor principles, etc., to lay a solid theoretical foundation for students. The professional course will deeply discuss the application of multi-sensor data fusion technology,

communication network architecture, mainstream wireless communication technology and artificial intelligence technology in smart home security systems. In the project practice, it includes data query and collection, project demand analysis, laboratory operation, project practice and other forms to enhance students' practical ability.[5]

Example of course plan design:

First, the architecture of IoT security is determined, which is generally divided into three layers, namely perception layer security, network layer security and application layer security. The technologies contained in each layer of the three-layer network structure are the precursors of this course. Then, take the smart home project as an example, which corresponds to the IoT security architecture hierarchy, as shown in the following figure 1:

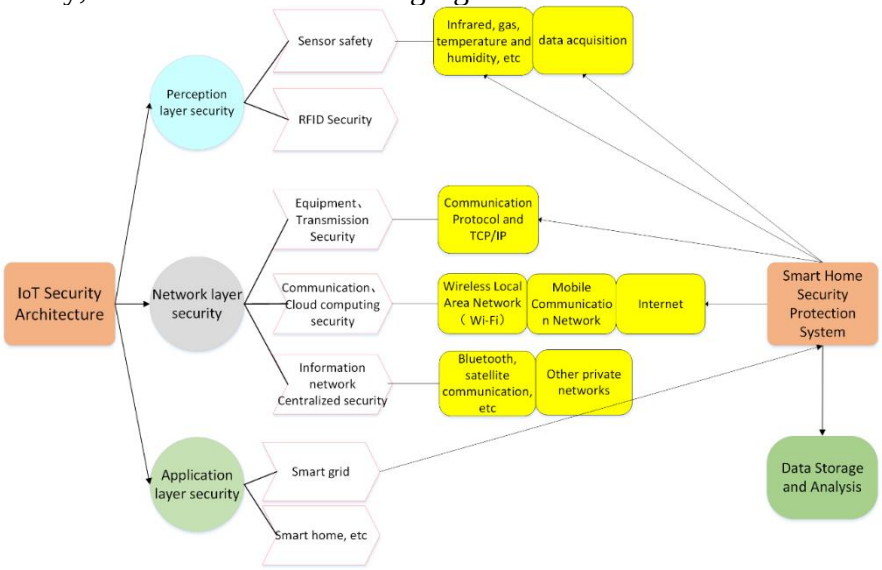

Figure 1: Schematic diagram of IoT security system and main technologies of smart home

The project contains a number of sub-projects, and the security requirements of the project need to be analyzed in the early stage, and before class, students are asked to collect the security requirements of the project through data query, offline observation and other methods, and organize these problems into documents, and through the analysis, the possible security problems of the project are obtained, such as the smart door lock may be cracked, resulting in illegal incursion; The cameras of the smart security system can be controlled by hackers for remote surveillance; The remote control function of smart home appliances can be exploited for malicious operations or data theft. When explaining the security architecture of the Internet of Things, such as the security of the perception layer, what is the role of the perception layer, and arouse students' discussion about what are the Internet of Things technologies involved in the perception layer. During the teaching process, students are first guided to review the knowledge points, and then grouped for group discussions to discuss which technologies are involved in the security system hierarchy and their application in the sub projects of the project. The security issues encountered in this project and the corresponding security protection methods. After the group discussion is completed, the teacher is responsible for collecting the questions and results of each group, summarizing and generalizing them, selecting non repetitive knowledge points and methods for presentation, supplementing and summarizing the incomplete areas, and finally organizing the results into a document for display on the online learning platform. For example, Chaoxing Learning Pass is displayed to facilitate students to review after class.

The perceptual layer is used as an example, and the rest of the hierarchy is taught according to the pattern of that layer. Firstly, the teacher will explain the basic knowledge related to the perception layer in the security architecture. The perception layer is located at the bottom layer and is the

fundamental layer of the Internet of Things. Its main function is to identify objects through various sensors, RFID tags, cameras, and other devices, collect information, and transmit this information to the upper layer for processing and analysis. The performance and application of perception layer technology directly affect the overall efficiency and application scope of the Internet of Things. After the teacher explains the basic knowledge, guide students to recall the technologies of the sensing layer, such as sensor technology, recognition technology, short-range wireless transmission technology, etc.The teacher explains the principles of these technologies to the students and then initiates discussions on topics such as their applications in real life.Finally, the teacher assigns group tasks to the students in each group, with each group responsible for explaining and summarizing one or two technologies. The teacher provides feedback on which technologies have been applied in the smart home project and what roles these technologies play in the project.

For example, the technologies applied in the application of smart door locks in sub-projects are as follows:

Sensing technology converts various physical quantities (such as temperature, humidity, pressure, etc.) into electrical signals through sensors, and then realizes data collection and transmission. In smart door locks, sensors are usually used to detect the status of the door lock (such as whether it is locked, whether it is picked, etc.), and transmit this information to the control system for further processing and judgment.

RFID non-contact automatic identification technology, which can identify specific targets through radio signals and read and write relevant data. In smart door locks, RFID technology is often used to achieve keyless unlocking. For example, a user can bring a card or bracelet containing an RFID chip close to the door lock, and the door lock verifies the user's identity by reading the information in the RFID chip, so as to realize the unlocking operation.

Biometrics technology identifies individuals by identifying their biometrics (such as fingerprints, faces, iris, etc.) for identity verification. In smart door locks, biometric technology has to be applied. For example, fingerprint recognition technology can verify identity by reading a user's fingerprint information; Facial recognition technology can realize unlocking by recognizing the user's facial features. These technologies not only improve the security of the door lock, but also provide users with a more convenient way to unlock the lock.

Other technologies, smart door locks may be used in the perception layer of other related technologies, such as: QR code recognition: by scanning the QR code to verify the user's identity or enter the unlocking code. Infrared sensing: It is used to detect if there is a person or object approaching around the door lock, thus triggering certain functions of the door lock.

Through these technologies, students are guided to think about what are the security risks and how to protect them, and how to protect them from password locks and password cracking, prevent password theft, and design passwords to strengthen data encryption and permission management to ensure user privacy and data security. This leads to the next knowledge point, cryptography. Through discussing these technical topics, the teacher will introduce the next knowledge point, cryptography. The teacher will then elaborate on cryptography-related knowledge, covering its origin and development, as well as the entire evolutionary journey from ancient to modern cryptography. In this process, the evolution of password types and changes in password design principles are discussed. After explaining the basic knowledge points, questions are raised on how to design a good password, which prompts students to think. After the student discussion is concluded, the teacher instructs the students to design their own passwords. Once the design is finalized, they proceed to conduct experimental verification. The students utilize programming tools, such as Java, C language, and other code design languages pertinent to the Internet of Things, to validate the accuracy and practicality of the designed passwords. Throughout the entire process, teachers must remind students to keep meticulous records of the process, encompassing any issues encountered during the

experiment as well as the methodologies and steps taken to resolve them. Simultaneously, teachers must remind students to prioritize team communication and collaborative problem-solving. This approach enables students to acquire a deeper comprehension of knowledge through practical experience.

4.3 Teaching Resource Construction

The adoption of project-based practice as the main teaching method requires support from other resources, such as strengthening the construction of teaching resources to provide strong support for project-based practice. On the one hand, it is necessary to actively seek support from schools and increase investment in experimental equipment and teaching resources; On the other hand, it is necessary to utilize online and social resources to expand practical teaching channels. For instance, schools can forge partnerships with pertinent enterprises to collaboratively develop IoT security practice projects and integrate them into teaching practices. In daily teaching scenarios, teachers can utilize online course platforms to furnish students with abundant teaching resources and facilitate case sharing.The curriculum reform based on this foundation can enable students to learn more practical knowledge to the greatest extent possible and provide greater assistance for their future career development.

5. Conclusions

In the teaching reform of Internet of Things information security introduced by the smart home project, we pay attention to the combination of theory and practice, so that students can think, analyze, and participate in practical design, and understand the importance of Internet of Things information security. Through project-based learning and group discussions, students can not only master theoretical knowledge, but also learn how to solve safety problems in practical applications. The education reform is expected to achieve good results, which can improve students' security skills and teamwork ability, in order to cultivate more outstanding talents in the field of IoT security in the future.

Acknowledgement

This work is supported by the Internet of Things Engineering Course Ideological and Political Demonstration Professional Project, with project number GKZLGC2022278.

References

[1] Tian Jingxi, Li Haiyan, Lu Xia, et al. Introduction to the Internet of Things [M]. Nanjing Southeast University Press: 202108.338

[2] Lv Liewei. Design and Implementation of a New Generation Information Technology Smart Home System [J]. Home Appliance Maintenance, 2024, (09): 68-70.

[3] Huang Wanni. Exploration of Teaching Reform in Network Virtualization and Information Security Technology Course in the New Era [J]. Chinese Journal of Multimedia and Network Teaching (Volume One), 2023, (03): 74-77.

[4] Fu Lai, Bing Zhigang. Research on the Practice and Optimization of "Project Introduction Task Driven" Teaching Method in Vocational Education: Taking PLC Technology and Application Course as an Example [J]. Vocational Education Research, 2019, (12): 63-69.

[5] Li Ming, Wang Chaoyang. Research on the Design of Smart Home Security Early Warning System Based on Internet of Things Technology [J]. Journal of Anyang Normal University, 2023, (05): 46-49+111.