ISSN 2663-8169 Vol. 7, Issue 7: 186-191, DOI: 10.25236/IJNDE.2025.070728

Research and Practice on the Teaching Reform of Internet of Things Security Technology Course

Weigang Guo

School of Computer Science and Artificial Intelligence, Foshan University, Foshan, Guangdong, China
wgguo@qq.com

Abstract: *This paper introduces the teaching reform practice of "Internet of Things Security Technology" from three aspects: teaching content, teaching methods and evaluation methods. The teaching content of the course mainly focuses on the perception layer, network layer and application layer of the Internet of Things. At the same time, experimental contents such as information encryption, security protocols and network security are also set up in the course, so that students can better grasp the relevant abilities of Internet of Things security and information security in practice. Flipped classroom and case study are adopted in classroom teaching. The course evaluation adopts multiple methods such as homework, experimental results and final examination, which can comprehensively investigate the whole learning process and learning effect of students. From the students' questionnaire survey and comprehensive evaluation results, the teaching goal has been achieved.*

Keywords: *Internet of Things Security, Teaching Content, Teaching Methods, Course Evaluation, Flipped Classroom*

1. Introduction

Internet of Things Security Technology is a required course for Internet of Things Engineering major. The purpose of this course is to enable students of this major to have a comprehensive and in-depth understanding of the relevant technologies and application fields of IOT security. The main task of the course is to learn and master the corresponding security theory and technology from all levels of the Internet of Things. This course plays an important role in the information security awareness and skills of students majoring in Internet of Things engineering, and lays a good foundation for the security application of the Internet of Things in future study and work.

Many scholars have carried out research on the teaching of Internet of Things security technology course. Literature [1] describes the teaching design of the Internet of Things information security technology course, including the selection of teaching materials, the revision of teaching syllabus, and the targeted setting of experimental types and projects. Literature [2] explores the effective path of the Internet of Things information security technology course construction for the Internet of vehicles, and solves the problems of lagging curriculum content, weak practical teaching, and single evaluation system in current colleges and universities. Literature [3] used sitcom deduction algorithm and virtual simulation teaching to improve students' learning interest and motivation in the teaching of Internet of Things security technology. Literature [4] puts forward the teaching method of the Internet of Things security technology course based on the results, so as to improve the teaching level of the Internet of Things security technology course. Literature [5] is guided by the concept of Outcome Based Education (OBE) and combined with the teaching practice of the course Internet of Things security technology, exploring a new student-centered and achievement oriented network teaching mode.

This paper introduces our practice and exploration from the aspects of teaching content, teaching methods and course evaluation methods.

2. Teaching Content Design

The teaching content of this course is divided into two parts: classroom teaching and practical teaching.

ISSN 2663-8169 Vol. 7, Issue 7: 186-191, DOI: 10.25236/IJNDE.2025.070728

2.1 Design of Classroom Teaching Content

According to the network structure of the Internet of Things, the main content of this course covers the security requirements analysis of the Internet of Things, the security technology architecture of the Internet of Things, password and identity authentication technology, RFID system security and privacy, WSN wireless sensor network security, wireless communication network security, Internet Network Security, information hiding technology principles, location information and privacy protection, the information security standards of the Internet of Things, and the planning and design of the security architecture.

Chapter 1: Security requirements analysis of the Internet of Things. The key contents include: the structure and level of the Internet of Things, the security requirements and security mechanisms of the perception and identification layer of the Internet of Things, the security requirements and security mechanisms of the network construction layer, the security requirements and security mechanisms of the management service layer, and the security requirements and security mechanisms of the integrated application layer.

Chapter 2: Security technology framework of Internet of Things. The key contents include: digital certificate and electronic visa authority, Internet of Things encryption authentication, key management mechanism, secure routing protocol, authentication and access control, intrusion detection and intrusion tolerance and fault tolerance technology.

Chapter 3: Password and identity authentication technology. The key contents include: RSA algorithm, symmetric password algorithm, identity authentication system, personal identity certification, electronic ID identification technology, IOT key management mechanism, IOT data processing and privacy.

Chapter 4: RFID system security and privacy. The key contents include: the basic characteristics of secure RFID system, the privacy issues in RFID technology, the implementation of RFID Security Mechanism and security protocol, the security design of RFID electronic tag in application, RFID chip attack technology and its prevention technology.

Chapter 5: Wireless sensor network security. The key contents include: security mechanism, security framework and key distribution of wireless sensor networks, routing security of wireless sensor networks, data fusion security, and security of wireless sensor networks based on ZigBee technology.

Chapter 6: Wireless communication network security. The key contents include: wireless application protocol application security, wireless LAN security technology, Bluetooth technology security mechanism.

Chapter 7: Internet network security. The key contents include: firewall technology, intrusion detection, IPSec Security Protocol, virtual private network.

Chapter 8: Middleware and cloud computing security. Key contents include: middleware technology security, Internet of Things cloud computing security, cloud computing application security system and key technologies, cloud computing application security protection, cloud security technology solutions.

Chapter 9: Principle of information hiding technology. The key contents include: three modes of information encryption and hiding, classification of information hiding technology, basic model and key technology, data steganography, copyright mark and digital watermark.

Chapter 10: Location information and privacy protection. The key contents include: location-based services and its technical principles, mobile GIS and positioning technology, network privacy protection technology, and privacy protection based on location-based services.

Chapter 11: Internet of Things information security standards. Key contents include: international information security management system, China's information security standard system, China's national Internet of Things standards organization, main contents of information security management system standards, and information security management system certification.

Chapter 12: Security architecture planning and design. Key contents include: Security Analysis of IOT system, objectives and protection principles of IOT security system, overall protection technology of IOT information security, and implementation technology of overall protection of IOT.

ISSN 2663-8169 Vol. 7, Issue 7: 186-191, DOI: 10.25236/IJNDE.2025.070728

2.2 Design of Practical Teaching Content

The practical teaching includes four experiments: data encryption technology experiment, network data integrity detection experiment, network security detection experiment, RFID Security Protocol experiment.

Experiment 1: Data encryption technology experiment. The main contents include: programming DES algorithm to encrypt and decrypt data; Write a program to realize the encryption and decryption of data by RSA algorithm; The characteristics and applications of the above two algorithms are summarized.

Experiment 2: Data integrity detection experiment in the network. The main contents include: using information extraction technology to achieve data integrity detection (MD5 algorithm, etc.); Digital signature technology is used to detect data integrity (DSA algorithm); The characteristics and applications of the two detection algorithms are compared.

Experiment 3: Network security detection experiment. The main content includes: review several common technologies of network attack; Learn to use network vulnerability scanning tools; Learn to use network sniffing tools.

Experiment 4: RFID Security Protocol experiment. The main contents include: using C language to implement hash lock protocol; C language is used to implement randomized hash lock protocol.

3. Teaching Methods

In teaching methods, the course uses the combination of theory and practice, students' independent topic selection, case study and discussion methods to fully cultivate and give full play to students' exploration spirit and research ability, so that students' training can meet social needs and cultivate real IOT information security talents.

3.1 Theoretical Teaching Framework

The teaching of IOT security theory is carried out around a three-tier architecture.

(1) Perception Layer Security: covering sensor network security, RFID Security and physical equipment protection, focusing on encryption communication and access control technology.

(2) Network layer security: including data encryption, secure routing, intrusion detection and other transmission security mechanisms.

(3) Application Layer Security: focus on application protection measures such as permission management, security audit and data privacy protection.

The teaching process adopts the three-stage mode of "concept introduction - principle analysis - technology implementation", and carries out systematic knowledge teaching with multimedia courseware and standard teaching materials.

3.2 Application of Flipped Classroom Model

Flipped classroom is a teaching mode that reverses the order of "classroom teaching+homework" in traditional teaching. In the course of Internet of Things security technology, the process we designed includes the following links:

(1) Pre class autonomous learning stage: teachers carefully design the learning task list and provide learning resources such as micro class videos, documents and online tests. Taking "Internet of Things encryption algorithm" as an example, teachers can produce 8-10 minutes of short video to explain the basic principles of AES, RSA and other encryption algorithms. The video adopts the structure of "1 minute import+6 minutes core explanation+1 minute summary" to ensure that the content is refined and focused. Students independently arrange the learning schedule according to the task list, and complete the preliminary mastery of knowledge points through the online platform. Students can watch the difficult part repeatedly until they fully understand it.

(2) In depth classroom interaction stage: classroom time is mainly used for discussion, question answering and practice. In the teaching of "RFID Security Protocol", the teacher designed the

ISSN 2663-8169 Vol. 7, Issue 7: 186-191, DOI: 10.25236/IJNDE.2025.070728

following activities: first, discuss the possible security threats faced by the RFID system in groups, then share the discussion results and summarize them into a security threat map, then the teacher demonstrated the man in the middle attack against RFID, and finally the students configured defense measures such as two-way authentication protocol. This method greatly improves students' participation and knowledge internalization.

(3) After class consolidation and expansion stage: students complete advanced tasks through the online experimental platform, such as analyzing the security vulnerabilities of real IOT devices. Teachers provide personalized feedback according to the learning data recorded on the platform. The teacher found the common problems of students through data analysis and explained them pertinently in the next class.

3.3 Case Studies and Discussions

Each student is required to select a topic related to Internet of Things security for research, write a research report, and report and discuss.

The main framework of the study includes the following contents:

(1) Background. This section mainly explains the reasons for choosing this topic.

(2) Introduce the technical architecture closely related to the topic. For example, the complete technical architecture and application mode in the fields of smart home, mobile payment, automatic driving, UAV security and so on, what kind of security mode is adopted, and what are the specific performance parameters.

(3) Existing security issues. According to the technical architecture, discuss and study which links may have security problems, what kind of attacks will be suffered, and what the reasons are, including the technical level, user use level, and management level. It is necessary to clearly describe the scenarios where security problems occur.

(4) Existing security solutions. Mainly from the authentication mechanism, password mechanism, secure communication mechanism, management mechanism (human factors) and other aspects of research and discussion.

(5) Students' own methods and suggestions. It is mainly researched and written from three aspects: technical level, application level (users) and management level.

(6) Summary.

4. Course Evaluation

4.1 Course Evaluation Methods

The assessment of this course adopts the combination of homework, experiment and closed book written examination. Students' scores are composed of three parts: usual scores, experimental scores and final exam scores. The usual scores account for 20% of the total scores, the experimental scores account for 25% of the total scores, and the final exam scores account for 55% of the total scores.

(1) Daily operation. Daily work shall be carried out in the form of individual work or group task. The homework questions are mainly comprehensive, designed and applied exercises, which are graded each time, and then the final homework score is obtained.

(2) Experimental assignments. For the four experiments, the experimental report should be written according to the content, process and results of the experiment. The instructor should grade the experimental report, and then synthesize it to get the final experimental results.

(3) Final exam. In the way of separate proposition, the teacher should formulate the corresponding reference answers and scoring standards according to the actual teaching situation.

4.2 Effectiveness Evaluation

According to the syllabus, this course has three objectives, namely:

Course objective 1: students need to understand the characteristics, development and future trends

ISSN 2663-8169 Vol. 7, Issue 7: 186-191, DOI: 10.25236/IJNDE.2025.070728

of Internet of Things security, master the architecture and key technologies of Internet of Things security, understand the security threats and security analysis, master the knowledge of password, the composition, working principle and security requirements of RFID and WSN, etc.

Course objective 2: students need to master the application of the Internet of Things in the security technology of perception layer, network layer, management service layer and application layer, the foundation of information security and the introduction of commonly used cryptography, learn the commonly used encryption technology and security protocol, and have a certain understanding of the security management of the Internet of Things.

Course objective 3: students have the awareness of autonomous learning, lifelong learning and self-improvement, and recognize the necessity of continuous exploration and learning.

4.2.1 Qualitative Evaluation (Subjective Evaluation)

After the completion of the course in summer of 2025, the teacher conducted a questionnaire survey on all students. The data analysis results of the questionnaire survey show that students' subjective achievement of the course objectives is high. See Table 1 for detailed data(1 means full score).

Table 1 Qualitative evaluation results of the degree of achievement of curriculum objectives

Curriculum Objectives	Teacher Evaluation	Student Evaluation
Course Objective 1	0.80	0.8231
Course Objective 2	0.80	0.8269
Course Objective 3	0.80	0.8192
Overall Course Objective	0.80	0.8242

4.2.2 Quantitative Evaluation

According to the usual homework, course experiments and final examination results, the degree of achievement of course objectives can be evaluated quantitatively. Table 2 shows the quantitative evaluation data of this course (1 means full score).

Table 2 Quantitative evaluation results of the degree of achievement of curriculum objectives

Curriculum Objectives	Evaluation Method 1: Usual Homework (weight: 20%)	Evaluation Method 2: Course Experiments (weight: 25%)	Evaluation Method 3: Final Examination (weight: 55%)	Evaluation Value of Course Objectives
Course Objective 1	0.8963	0.8231	0.7553	0.8047
Course Objective 2	0.8783	0.8269	0.8779	0.8643
Course Objective 3	0.8633	0.8192	0.8932	0.8783
Overall Course Objective	0.8492			

5. Conclusions

By setting up relevant teaching contents in the perception layer, network layer and application layer respectively, and conducting classroom teaching according to this framework, the overall content of the course is more comprehensive and reasonable. At the same time, experimental contents such as information encryption, security protocols and network security are also set up in the course, so that students can better grasp the relevant abilities of Internet of Things security and information security in practice. The flipped classroom and case study in classroom teaching have improved the efficiency of teaching and the ability of students' autonomous learning. The course evaluation adopts multiple methods such as homework, experimental results and final examination, which can comprehensively investigate the whole learning process and learning effect of students, and better achieve the teaching goal. In the future, new security technologies will be further integrated according to the development of the Internet of Things security field and new application scenarios, so that the course can keep up with the development of new technologies.

References

[1] Liu Hua. (2024) Instructional Design for the Course of Internet of Things Information Security

ISSN 2663-8169 Vol. 7, Issue 7: 186-191, DOI: 10.25236/IJNDE.2025.070728

Technology. Electronic Technology, 3, 416-419
[2] Liu Hua. (2024) Teaching Reform of Internet of Things Information Security Technology Course for Internet of Vehicles. Automotive Pictorial,(12:180-182.
[3] Li Wei, Chen Yuming. (2023) Exploration on Teaching Reform of "Internet of Things Security Technology" Course. Education and Teaching Forum, 24,56-60.
[4] Wusman Yushan. (2022) Research on Teaching Method of IOT Security Technology Course Based on Achievement Orientation. Computer Knowledge and Technology,34, 153-155
[5] Liu qingyu, Chen Lei, Chen Baoguo, et al. (2021) Research and Practice of Online Teaching Based on OBE Concept -- Taking the Course of "Internet of Things Security Technology" as an Example. Wireless Internet Technology, 8, 149-151