Retraction

Retracted: Construction and Management of Intelligent Campus Based on Student Privacy Protection under the Background of Artificial Intelligence and Internet of Things

Mobile Information Systems

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] P. Yi and Z. Li, "Construction and Management of Intelligent Campus Based on Student Privacy Protection under the Background of Artificial Intelligence and Internet of Things," *Mobile Information Systems*, vol. 2022, Article ID 2154577, 6 pages, 2022.

Research Article

Construction and Management of Intelligent Campus Based on Student Privacy Protection under the Background of Artificial Intelligence and Internet of Things

Pujin Yi [1,2] **and Zhongwu Li** [2]

¹*Guangxi Economic and Trade Vocational Institute, Nanning 530021, China*
²*National Institute of Development Administration, Bangkok 10700, Thailand*

Correspondence should be addressed to Pujin Yi; yi_pujin@outlook.com

With the coming of the era of artificial intelligence development and the mobile Internet of things, privacy security will become more and more prominent. As the contemporary college students have gradually developed into one of the main forces of the next generation of network information technology and intelligent terminals of Internet mobile communication, the problem of privacy and protection of college students in the era of artificial intelligence and the Internet of Things has naturally become a practical problem urgently solved by colleges and universities. This paper studies the application of "artificial intelligence + Internet of Things" (AIoT) in the construction and management of intelligent campus for student privacy protection. Firstly, some basic concepts and theories related to artificial intelligence and the Internet of Things are summarized, and the basic technical framework of "Artificial intelligence + Internet of Things" (AIoT) is preliminarily explained and analyzed. Secondly, relevant simulation experiments are carried out, and data support and help are provided for subsequent solutions and management methods by analyzing the simulation results. Through the investigation and analysis of the intelligent campus construction and management based on student privacy protection under the background of artificial intelligence and the Internet of Things, the final research results show that the background of artificial intelligence and the Internet of Things has a great role in promoting the function of student privacy protection, so this research has an important guiding role for student privacy protection in the context of artificial intelligence and the Internet of Things.

1. Introduction

With the development of artificial intelligence and the Internet of Things, the use of network technology will become more popular and convenient and there will be more and more users. As a new data technology, the Internet is rapidly infiltrating into various economic fields closely related to people's social life, and it is also closely integrated with the work and daily life of ordinary college students [1, 2]. In the Internet era, the rapid development of the Internet of Things has attracted worldwide attention. Many relevant institutions have made major breakthroughs in the field of IoT, such as IBM's "Smart Earth" strategy, the European Commission's "European Internet of Things Action Plan" [3, 4],

and so on. The Internet of Things is highly heterogeneous, and various networks and end entities differ greatly in processing and storage capabilities. To a certain extent, as one of the key technologies that has been widely used, the security of the Internet of Things has also been extensively studied [5, 6]. However, through in-depth research on the Internet of Things, many scholars found that there are still some security problems in the current Internet of Things system [7, 8]. The leak door of the network giant Facebook also shows that almost everyone can have no privacy in the network environment [9–12].

At present, the protection of user privacy in the Internet environment has been highly valued by governments and people around the world. In order to slow down and prevent

the occurrence of user privacy infringement, governments around the world have issued various laws, regulations, and corresponding policies. For example, the General Data Protection Regulation issued by the European Union on May 25, 2018, is considered to be the strictest and most comprehensive regulation to protect the privacy data of Internet users so far. However, even so, the security of user privacy data cannot be fully guaranteed. On the one hand, the definition of user privacy data in different application scenarios is not uniform, and the definition of privacy leakage behavior is flexible. On the other hand, attackers who violate user privacy data are usually service providers themselves or other relevant individual users, which makes it difficult for attackers to identify. Since the founding of the People's Republic of China in 1987, China has been making continuous efforts to establish and improve legal protection policies for various rights, including actively building a judicial protection system for individual privacy [13–16]. However, the legal protection of minors' privacy rights is still in the initial stage of development. Although the Internet of Things has been proved not to be a new technology a few years ago, special mandatory legislative protection is still slightly behind [3, 5, 7, 17, 18]. Through independent research, development, and operation, they have formed the application system of a personal network social platform. Most users need the third party to take the initiative to transfer part of their personal privacy and even take the initiative to grant some background data to the third party. At the same time, the artificial intelligence software and Internet products are behind another batch of the black industry chain, the company is the use of some of these industry legal blank, technical vulnerabilities, easily to the users' personal data resources, as the tool of making profit is a part of colleges and universities began trying to explore based on artificial intelligence methods and mobile Internet platform, innovate the original or traditional backward operation mode of college education innovation management in our school, and improve the management ability of big data innovation education service [19–23]. But it is in view of the current due to the domestic large-scale artificial intelligence network applications and world university biological information network technology high speed development and brings some disadvantages reality problem also let people neglected, huge amounts of reading Chinese college students' identity information, student information, and scientific research are also facing a lot of personal information leakage risk at any time. A famous domestic science and technology university due to the serious design vulnerability of its campus security application system platform and nearly led to the nation more than 70 ten thousand on college students' records all the important data privacy is leaked, the public and some domestic and foreign well-known university illegal release Chinese students personal physical health assessment report information and then extended to some foreign more top university of science and technology of China high difference transcripts, because a university management negligence leading to release. In terms of student privacy, the Internet and social big data can cause more serious privacy problems for students, forcing

major universities around the world to pay more attention to the privacy protection of college students in the era of artificial intelligence learning and the Internet of Things [24–28]. In recent years, as teachers and students of colleges and universities at all levels, as well as relevant discipline inspection and supervision departments around the province, reflect that privacy violations of college students are increasingly frequent, in order to strictly protect the privacy of college students, the website of the Ministry of Education of the People's Daily online has repeatedly issued a spot-check of the provincial law enforcement department staff and the school's network public opinion [29–31]. Verify the situation according to this spot check. In the process of privacy education management practice, colleges and universities must learn to time change the traditional concept of college students' privacy security education, make reasonable use of modern artificial intelligence knowledge, modern Internet of things tools, and social networks, and attach importance to the education protection of college students' personal privacy [32–34].

In this era of artificial intelligence society and the big Internet of Things, it is an extremely important task for our society to realize the advantages and avoid disadvantages, and to further protect the privacy information of Chinese college students while actively making good use of artificial intelligence technology and big Internet of things resources [35–38]. With modern artificial intelligence and iot research at home and abroad for academic background, and on the relevant expositions of college students' privacy protection is not much more special, so this question as far as possible in today's era background fit closely, hope it can continue to articles in the related fields of the current network security research in colleges and universities have the effect of icing on the cake.

2. Overview of Relevant Algorithms

2.1. Artificial Intelligence. Artificial Intelligence (Artificial Intelligence), abbreviated as AI, is a new technical science that researches and develops theories, methods, technologies, and application systems for simulating, extending, and expanding human Intelligence. From now, artificial intelligence discipline in many universities in the computer professional fine points out a professional artificial intelligence, he is the foundation of computer science, it is the core of the research is to explore a new kind of similar to human intelligence scientific method, designs the corresponding algorithm, research and development have similar to human thinking ability and the ability to respond to intelligent machines.

2.2. The Internet of Things. The application scenarios and application fields of the new technology integrating the Internet of Things and information technology extend from all walks of life to all aspects of people's work and life, making the limited information product resources of our industries, It will realize more efficient, optimized, reasonable use management and fair distribution, so as to greatly

improve labor productivity and promote the development of the efficiency and benefits of each major transportation industry. IoT technology and application has made good progress in solving the problem of student privacy protection in China. With the deepening of the Internet application in modern society, the problem of student privacy leakage will become a practical problem facing our country. The Internet of Things is a technology that directly transmits sensor signals to the cloud or other related devices through the network, realizing information communication and remote control between devices under a certain protocol.

2.3. Student Privacy Data Theft. One of the biggest problems for eavesdropping attacks is interference elimination. To solve this problem, under the assumption that the channel state information is transmitted in plain text, the eavesdropping attack should be based on the acquisition of the victim's channel state information. The relevant formulas for privacy data protection is

$$\begin{Bmatrix} \delta_1 \\ \delta_2 \end{Bmatrix} = \begin{Bmatrix} \mu_1 \\ \mu_2 \end{Bmatrix} \begin{Bmatrix} \gamma_1 \\ \theta_2 \end{Bmatrix} \begin{Bmatrix} \sqrt{\alpha_1} \, \varphi_1 \\ \sqrt{\alpha_2} \, \varphi_2 \end{Bmatrix},$$

$$\varphi_1^{MS_2} = \varphi_1 + \frac{\mu_{11}\theta_{22} - \theta_{21}\mu_{12}}{\sqrt{\alpha_1} \, (\mu_{21}\theta_{22} - \mu_{22}\theta_{21})}. \tag{1}$$

2.4. The Impact of AI and IoT Applications on Student Privacy Protection. To strengthen the privacy protection of students in the application of artificial intelligence, it is necessary to strengthen the risk analysis and prevention of artificial intelligence applications and integrate technologies such as innovation, ethics, and the legal degree to prevent "crazy growth" and ensure that the healthy development of artificial intelligence complies with morality. In terms of technology, the development and application of security and privacy technology should be accelerated, and the privacy protection needs of students should be incorporated into the design of artificial intelligence systems to maximize privacy protection. The ethical side requires research on the principles of student privacy protection. At the same time, experts must establish socialist core values, strengthen their own norms, standardize technology application standards, processes, and methods and respect and protect students' privacy. On the legal side, we must speed up legal development and strengthen privacy protection. China's privacy protector has not yet fully adapted to the needs of artificial intelligence development. Strengthen privacy protection in relevant laws and regulations, establish legal norms when conditions are ripe, protect the privacy of the public in artificial intelligence, protect citizens' rights and choices in artificial intelligence applications, and collect and memorize personal information in artificial intelligence applications. The handling and use must be strictly regulated. This program will be used for theft, forgery, exodus, and other illegal collection and use of student materials.

Table 1: Frequency of publishing privacy (multiple choice questions) ($N = 500$).

Category	Every day	Often	Once in a while	It depends	Never
Frequency	18	27	156	188	111
Percentage	3.6%	5.4%	31.2%	37.6%	22.2%

Table 2: Do you set the visible range of privacy (multiple choice questions) ($N = 500$).

Category	Shield strangers	Will not set	It depends	It does not matter
Frequency	251	68	159	22
Percentage	50.2%	13.6%	31.8%	4.4%

3. Experiments

Privacy protection includes the following aspects: data concerns: data concerns are individuals' concerns that their data will be illegally collected and used by others. Before visiting a specific platform, individuals can decide whether to continue to visit by understanding the privacy policy, laws, and regulations. Data collection risk: when an individual visits the platform online, various "traces" left on the web page will be recorded by the website or browser; that is, when individuals visit the website, they will face the possibility of data collection. College students' understanding of these contents is called data collection risk knowledge. Data supervision and protection: data supervision and protection is mainly at the level of laws and policies to regulate the processing of personal data, including the legal scope of data use, the reasonable time for data retention, and the preconditions for data sharing and transfer. College students' understanding of these laws and policies is called data supervision and protection knowledge. Seeking Rewards: individuals are willing to trade their data for more convenient services. For example, in order to access more content on the platform, register an account by filling in basic personal information. Social control: when individuals encounter their own data being collected, try to reduce the disclosure of more data, for example, using the wrong information or information that is not commonly used when registering. Social control primarily emphasizes personal control over the use of other platforms. Technical control: individuals use computers or certain management software to clear their personal data as much as possible to avoid misuse and misuse of data by others, resulting in serious data privacy disclosure problems. Technical control refers to a way in which individuals clear their own data. This paper uses a questionnaire to understand the current situation of college students' privacy protection in the context of artificial intelligence and the Internet of Things.

4. Experimental Analysis

4.1. Student Privacy Disclosure Degree. It can be seen from Tables 1 and 2 that college students' privacy is often ignored by colleges and universities, which can easily lead

TABLE 3: The degree of privacy concern.

Category	name (%)	Date of birth (%)	Id number (%)	Education (%)	Health status (%)	Personal photos (%)	Home address (%)
Very worried	6.5	8.2	53.1	5.1	20.3	33.1	63.7
Worried	7.7	9.5	28.7	6.9	21.7	30.9	22.1
General concern	32.0	35.1	13.2	27.4	34.3	21.8	11.8
Not too worried.	29.1	30.2	5.3	27.5	17.9	9.6	3.9
Do not worry	25.0	15.2	3.2	30.1	7.7	4.0	0.5

to college students' mental health problems. College students will establish their own identity files on the Internet during their usual learning process, and these files are not well protected. Colleges and universities should pay attention to this situation, and try not to disclose the private information of college students in their usual work unless they have the consent of the students themselves. College students themselves should also pay attention to privacy protection, do not easily disclose their privacy on the Internet, and have self-awareness of privacy protection.

4.2. Degree of Privacy Concern. The following is the assessment of the degree of concern about the disclosure of specific privacy content, as detailed in Table 3.

It can be seen from Table 3 that college students are more concerned about their own privacy disclosure, such as financial status and family situation. The private information of college students is often associated with the dignity of the college students themselves, which will aggravate the anxiety of college students.

4.3. Relevant Policies for Student Privacy Protection

4.3.1. Establishing the Awareness of Protecting Students' Privacy Rights. In the past few years when the Internet has flourished, it is not uncommon for students to violate the privacy rights of students. Therefore, it is necessary to fundamentally promote the protection of students' privacy rights. In practice, students' privacy rights are violated in the name of "responsibility for the benefit of students," and students' privacy rights are bound to be violated by using the materials obtained from student privacy review as the basis and means of student management. In this case, from the perspective of teachers, preventing students from playing games, and chatting online during the learning process affects their grades. Judging from the source of teacher authorization, parental authorization is obtained in the form of online parent-teacher conferences. Although the guidelines seem reasonable to protect students' right to education, it cannot be used as a reason for violating students' privacy rights. Teachers conduct activities in this way. It is also the cause of public criticism. Teachers have insufficient awareness of protecting students' privacy and lack of awareness of protecting privacy. Therefore, teachers should strengthen their awareness of protecting students' privacy in order to fully protect students' privacy.

4.3.2. Improving the School's System for Protecting Students' Privacy. Schools must fulfill the legal responsibility to protect students' privacy and improve the privacy protection system. Due to administrative needs, the school collects information on students' families. During the management process, travel information of family members can also be collected. In this case, it can be avoided if the school has a system in place to protect the privacy of students and teachers who are learning and following the rules. Therefore, it is necessary to improve the school education system and publicity and raise awareness of the privacy protection system. In practice, schools can abide by relevant laws and regulations enacted in China concerning the protection of student privacy. For example, the Law on the Protection of Minors has made some provisions to protect the privacy rights of minors and requires the principle of respecting the best interests of minors and protecting their personal data. In addition, the "Student Protection Regulations" have clear requirements for the protection of students' privacy in school education, schools shall not disclose the identity of students and their family information for the purpose of encouraging, funding and applying for poverty alleviation; schools shall, in accordance with these laws and regulations and in light of the actual situation, a school curriculum that explicitly protects student privacy in relevant laws and regulations.

4.3.3. Taking Responsibility for Violating Students' Privacy Rights. Student privacy is protected by the Constitution. If a student's right to privacy is violated at the school, the school or related personnel are responsible for violating that right. The Civil Code provides for civil liability, which can require the infringer to stop the infringement, eliminate the risk, and apologize and compensate in the event of a violation of student privacy rights and serious infringement. In addition, students or parents should not arbitrarily expand the scope of the Privacy Ordinance and deprive the school of the opportunity to conduct reasonable and necessary management.

5. Conclusions

In the era of "artificial intelligence and the Internet," the computer field is booming, and the mobile Internet, as a combination of wireless communication and computer networks, provides people with flexible and fast Internet access services. Many of the works introduced in this paper are carried out in the context of the Internet and artificial intelligence. On the other hand, when the mobile Internet

faces the challenges of emerging technologies such as big data and deep data mining, the privacy data of users is also particularly vulnerable. This paper conducts relevant investigations on the construction and management of smart campuses. The results of this paper show that the background of artificial intelligence and the Internet of Things has a great role in promoting the privacy protection function of students. Therefore, in the Internet era, in terms of personal privacy protection, artificial intelligence and Internet of Things technologies should be fully utilized to improve the degree of personal privacy protection. At the same time, because this paper only conducts experimental analysis on student groups and some aspects of privacy protection, the research on privacy protection is one-sided, and the research has shortcomings. In future research, the author will conduct research on privacy protection from different groups and levels to improve the deficiencies.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

References

[1] R. V. Dushkin and A. I. Mohov, "Distributed computing model for the organization of a software environment that provides management of intelligent building automation systems," *Computer Research and Modeling*, vol. 13, no. 3, pp. 557–570, 2021.

[2] R. N. Safiullin, A. S. Afanasyev, and V. V. Reznichenko, "The concept of development of monitoring systems and management of intelligent technical complexes," *Journal of Mining Institute*, vol. 237, no. 3, pp. 322–330, 2019.

[3] D. Tien Bui, T. A. Tuan, N. D. Hoang et al., "Spatial prediction of rainfall-induced landslides for the Lao Cai area (Vietnam) using a hybrid intelligent approach of least squares support vector machines inference model and artificial bee colony optimization," *Landslides*, vol. 14, no. 2, pp. 447–458, 2017.

[4] P. Qian and M. Wu, "Overview of privacy protection research and methods in the Internet of things," *Computer application research*, vol. 30, no. 1, p. 8, 2013.

[5] Z. Lv and S. Lv, "Clinical characteristics and analysis of risk factors for disease progression of COVID-19: a retrospective Cohort Study," *International Journal of Biological Sciences*, vol. 17, pp. 1–7, 2021.

[6] X. L. Dong, "Research Progress on privacy protection of Internet of things," *Computer research and development*, vol. 52, no. 10, pp. 2341–2352, 2015.

[7] D. Yu, Z. Ma, and R. Wang, "Efficient smart grid load balancing via fog and cloud computing," *Mathematical Problems in Engineering*, vol. 2022, Article ID 3151249, 11 pages, 2022.

[8] C. L. Li, "Introduction to privacy protection mechanism of Internet of things," *Fujian computer*, vol. 27, no. 4, p. 2, 2011.

[9] T. Naumovic, L. Baljak, L. Živojinović, and F. Filipovic, "Development of a software framework for real-time management of intelligent devices," *Proceedings of the Institute for System Programming of the RAS*, vol. 31, no. 3, pp. 35–46, 2019.

[10] M. Topolski, "Management of intelligent internal transport through computer-based probabilistic algorithms," *AUTOBUSY – Technika Eksploatacja Systemy Transportowe*, vol. 19, no. 6, pp. 968–972, 2018.

[11] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, "A secure and anonymous communicate scheme over the Internet of things," *ACM Transactions on Sensor Networks*, vol. 18, no. 3, pp. 1–21, 2022.

[12] H. Cheng, M. Shojafar, M. Alazab, R. Tafazolli, and Y. Liu, "PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2021.

[13] V. A. Tabakaeva, I. N. Karmanov, and V. R. An, "Features of intelligent information security management systems for critical information infrastructure objects," *Interexpo GEO-Siberia*, vol. 6, no. 2, pp. 99–104, 2020.

[14] O. Katerna, "Concept formulation of intelligent management in transport," *Modern Economics*, vol. 9, no. 1, pp. 30–42, 2018.

[15] J. Chen, Y. Liu, Y. Xiang, and K. Sood, "RPPTD: robust privacy-preserving truth discovery scheme," *IEEE Systems Journal*, pp. 1–8, 2021.

[16] P. Wang and Y. Liu, "SEMA: secure and efficient message authentication protocol for VANETs," *IEEE Systems Journal*, vol. 15, no. 1, pp. 846–855, 2021.

[17] Ł. Marzantowicz, "Changes in contemporary logistics management in the light of intelligent logistics," *Kwartalnik Nauk o Przedsiębiorstwie*, vol. 50, no. 1, pp. 62–71, 2019.

[18] D. Yu, J. Wu, W. Wang, and B. Gu, "Optimal performance of hybrid energy system in the presence of electrical and heat storage systems under uncertainties using stochastic p-robust optimization technique," *Sustainable Cities and Society*, vol. 83, Article ID 103935, 2022.

[19] M. Shakeri, M. Shayestegan, H. Abunima et al., "An intelligent system architecture in home energy management systems (HEMS) for efficient demand response in smart grid," *Energy and Buildings*, vol. 138, pp. 154–164, 2017.

[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[21] W. Zheng, L. Yin, X. Chen, Z. Ma, S. Liu, and B. Yang, "Knowledge base graph embedding module design for Visual question answering model," *Pattern Recognition*, vol. 120, Article ID 108153, 2021.

[22] W. Zheng, X. Liu, X. Ni, L. Yin, and B. Yang, "Improving visual reasoning through semantic representation," *IEEE Access*, vol. 9, pp. 91476–91486, 2021.

[23] W. Zheng, X. Liu, and L. Yin, "Sentence representation method based on multi-layer semantic network," *Applied Sciences*, vol. 11, no. 3, p. 1316, 2021.

[24] K. Mistry, L. Zhang, S. C. Neoh, C. P. Lim, and B. Fielding, "A Micro-GA Embedded PSO feature selection approach to

intelligent facial emotion recognition," *IEEE Transactions on Cybernetics*, vol. 47, no. 6, pp. 1496–1509, 2017.

[25] Y. He, G. J. Mendis, and J. Wei, "Real-Time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[26] Y. Choi, J. Wang, Y. Zhu, and W. F. Lai, "Students' perception and expectation towards pharmacy education: a qualitative study of pharmacy students in a developing country," *Indian Journal of Pharmaceutical Education and Research*, vol. 55, no. 1, pp. 63–69, 2021.

[27] L. Yao, X. Li, R. Zheng, and Y. Zhang, "The impact of air pollution perception on urban settlement intentions of young talent in China," *International Journal of Environmental Research and Public Health*, vol. 19, no. 3, p. 1080, 2022.

[28] L. Yao, J. Shen, F. Zhang, X. Gu, and S. Jiang, "Influence of environmental values on the typhoon risk perceptions of high school students: a case study in ningbo, China," *Sustainability*, vol. 13, no. 8, p. 4145, 2021.

[29] S. Zhao, F. Li, H. Li et al., "Smart and practical privacy-preserving data aggregation for fog-based smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 521–536, 2021.

[30] L. Zhao, Y. Zhang, and Y. Cui, "An attention encoder-decoder network based on generative adversarial network for remote sensing image dehazing," *IEEE Sensors Journal*, vol. 22, no. 11, pp. 10890–10900, 2022.

[31] Z. Wu, J. Cao, Y. Wang, Y. Wang, L. Zhang, and J. Wu, "hPSD: a hybrid PU-Learning-Based spammer detection model for product reviews," *IEEE Transactions on Cybernetics*, vol. 50, no. 4, pp. 1595–1606, 2020.

[32] Y. Y. Lu, *Research and Application of Internet of Things Privacy protection Strategy*, Nanjing University of Posts and telecommunications, Nanjing, China, 2013.

[33] J. Y. Wang, "Research on privacy protection of college students in the "Internet +" era," *Scientific and technological innovation and productivity*, no. 9, p. 4, 2020.

[34] Y. P. Liang, "Student privacy protection and thinking in the era of big data," *Quality and certification*, no. 7, p. 2, 2017.

[35] S. W. Chen, "Research on the protection of college students' privacy under the network environment," *Legal system and society*, 2013.

[36] K. L. Wu, "On the legal protection of students' privacy," *Journal of Minxi Vocational University*, vol. 42, p. 17862, 2001.

[37] Z. B. Gao, K. W. Jiang, and X. Yu, "Research and implementation of online grade announcement system based on student privacy protection," *Science and Technology Plaza*, no. 7, pp. 135–137, 2008.

[38] C. Chen, *Research on College Students' Privacy and its protection*, Xiamen University, Xiamen, China, 2012.