**Journal of Global Information Management**
Volume 30 • Issue 7 • January-December 2022

# Data Privacy Protection in News Crowdfunding in the Era of Artificial Intelligence

Zhiqiang Xu, School of Film and Animation, China-ASEAN Art College of Chengdu University & School of Digital Media and Creative Design, Sichuan College of the Communication, China & The Education University of Hong Kong, China

Dong Xiang, School of Digital Media and Creative Design, Sichuan College of Communication, China

Jialiang He, School of Information and Communication Engineering, Dalian Nationalities University, China

## ABSTRACT

This paper aims to study the protection of data privacy in news crowdfunding in the era of artificial intelligence. This paper respectively quotes the encryption algorithm of artificial intelligence data protection and the BP neural network prediction model to analyze the data privacy protection in news crowdfunding in the artificial intelligence era. Finally, this paper also combines the questionnaire survey method to understand the public's awareness of privacy. The results of this paper show that artificial intelligence can promote personal data awareness and privacy, improve personal data and privacy measures and methods, and improve the effectiveness and level of privacy and privacy. In the analysis, the survey found that male college students only have 81.1% of the cognition of personal trait information, only 78.5% of network trace information, and only 78.3% of female college students' cognition of personal credit.

## KEYWORDS

Artificial Intelligence Era, News Crowdfunding, Personal Data, Privacy Protection

## 1. INTRODUCTION

### 1.1 Background of Topic Selection

With the rapid development of social economy, artificial intelligence has also developed rapidly, and now it mainly presents the characteristics of the era of artificial intelligence development. In the era of artificial intelligence, people can learn and communicate online, as well as shop and entertain online. Artificial intelligence has become an important part of people's daily life, and artificial intelligence has gradually changed the way people live and work. The convenience of artificial intelligence puts people in a free, open and transparent space, which to a certain extent also threatens people personal privacy, and even causes great damage to people's personal and personal safety. Nowadays, as artificial intelligence increasingly penetrates into people's daily life and work, effective data privacy protection has become the focus of attention of all parties, and effective data privacy protection is also an important issue that needs to be solved urgently.

DOI: 10.4018/JGIM.286760

### 1.2 Significance of the Research

Privacy and protection include training, encryption, network communication technology and laws. Foreign research and practice in the protection of personal data and privacy have achieved certain development results. However, domestic research and the practice of privacy and privacy started late, with little success. The protection of personal data and privacy depends to a large extent on the individual's self-protection awareness and is also affected by all social protection measures. The protection of personal data and confidentiality cannot only be based on the correctness and integrity of the law, but also requires sound laws. The protection of personal data and privacy in this article can increase personal awareness of data and privacy, improve the measures and methods of personal data and privacy, and increase the effectiveness and level of personal data and privacy. In this case, it is necessary to learn from domestic and foreign experience and various measures and methods of network platforms to understand relevant personal data and privacy technologies.

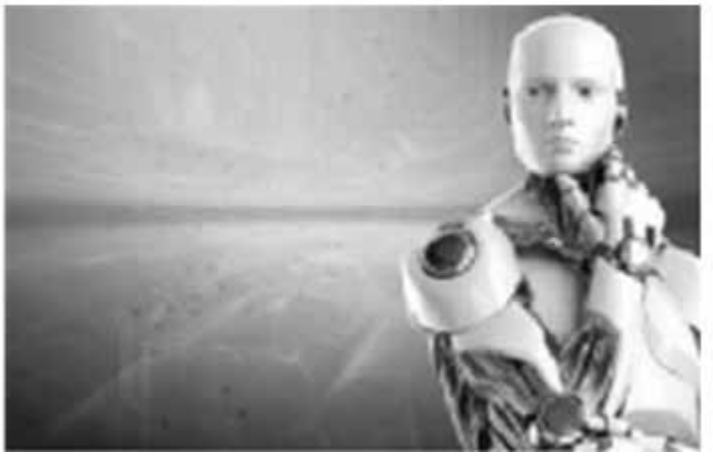
### 1.3 Data Privacy Protection in News Crowdfunding in the Era of Artificial Intelligence

Artificial intelligence will become the focus of scientific and technological development in the next ten years or more, and will change the world in more detail and bring human society into a new era. In the development of artificial intelligence, there are many hidden dangers in data security and privacy. Balthazar P pointed out that surveillance mainly includes psychological surveillance, physical surveillance and data surveillance, among which data is closely related to personal privacy. With the development of the social economic environment and the development of information technology, personal privacy mainly presents the differentiated characteristics of different stages of social development (Kotsenas et al. 2021). Gwb B pointed out that artificial intelligence is a discipline of knowledge, a discipline that studies how to express, acquire, and use knowledge. The definition is defined by artificial intelligence simulation objects. In addition, from the perspective of the purpose of research and development of artificial intelligence, artificial intelligence is the study of the ability of computers to complete tasks that could only be done by humans in the past (Dblm et al. 2019). However, artificial intelligence is a tool that serves humans by simulating human intelligence and inputting human instructions in the form of data. Boulay B D believes that "artificial intelligence without reasoning" and "artificial intelligence without expression". There is also a diametrically opposed view in the academic community that the continuous development of artificial intelligence will bring disasters to mankind (Boulay, 2016). For example, Hawking once delivered a speech in Beijing, claiming to be alert to the threat of artificial intelligence to mankind. However, human society will not cause the collapse of the entire society because of any technological revolution. Artificial intelligence may bring a series of problems to society.

### 1.4 Innovation Points of This Research

(1) Combine the latest relevant cases in society with the research on the latest technology of personal data and privacy protection in artificial intelligence to improve the ability of argumentation.
(2) The questionnaire survey method used in this article is mainly carried out on campus. The campus is used to promote the safety of artificial intelligence personal information to improve the awareness and privacy of personal data.
(3) It is more convenient, safe and reliable to use artificial intelligence in news crowdfunding applications.

**Figure 1. Artificial Intelligence Robot (Source: www.baidu.com)**



## 2. RESEARCH METHODS OF DATA PRIVACY PROTECTION IN NEWS CROWDFUNDING IN THE ERA OF ARTIFICIAL INTELLIGENCE

### 2.1 Overview of Artificial Intelligence

(1) Definition of artificial intelligence

Artificial intelligence can be explained in two ways: On the one hand, artificial intelligence comes from the continuous development and development of human beings, and is the crystallization of human wisdom and culture (Lu et al. 2017). On the other hand, artificial intelligence is the imitation of certain people by computers, or other electronic devices, functions and behaviors. Artificial intelligence is about how to use computers to simulate certain human thought processes and intelligent behaviors. In short, artificial intelligence is the theory and application of computer systems (Bundy, 2017). This is the development of artificially constructed human consciousness and way of thinking, which can replace humans to complete certain tasks (Jha et al. 2016).

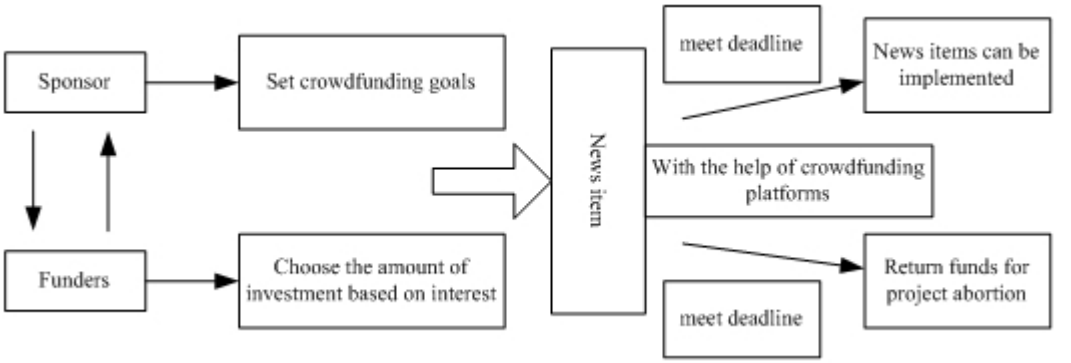
(2) Artificial intelligence research content

Artificial intelligence research is very technical and professional. Each branch is deep and offline, covering a wide range. The research content of artificial intelligence mainly includes: knowledge representation and automatic reasoning, knowledge search and processing methods, machine learning and knowledge acquisition, computer vision and natural language understanding, automatic programming and intelligent robots, etc. (Raedt et al. 2016). As shown in Figure 1:

### 2.2 Concept and Process of News Crowdfunding

The news crowdfunding platform is a kind of crowdfunding application in the news industry, that is, the sponsor announces its news report plan and requires the sponsor to obtain its funds within a certain period of time and obtain corresponding financial support from the sponsor to complete the news report. And get rewards from sponsors (Pigozzi et al. 2016). The milestone for the crowdfunding model to enter the press in my country was the official introduction of spot.us in the United States in 2008. It is a typical crowdfunding news website that supports “community power to promote news

**Figure 2. Flow chart of news crowdfunding.**




coverage" and actively stimulates the general public to actively participate in news production (Li et al. 2017).

This approach has narrowed the relationship between the two parties and changed the relationship between the media and the public; public participation has changed the way news reports; it has broadened the channels for collecting money and changed the way the media operates. In short, the new crowdfunding activities provide new impetus for the decline of the news industry, and provide new ideas for the reform and innovation of the media (Glauner et al. 2017). The specific process of news crowdfunding is shown in Figure 2:

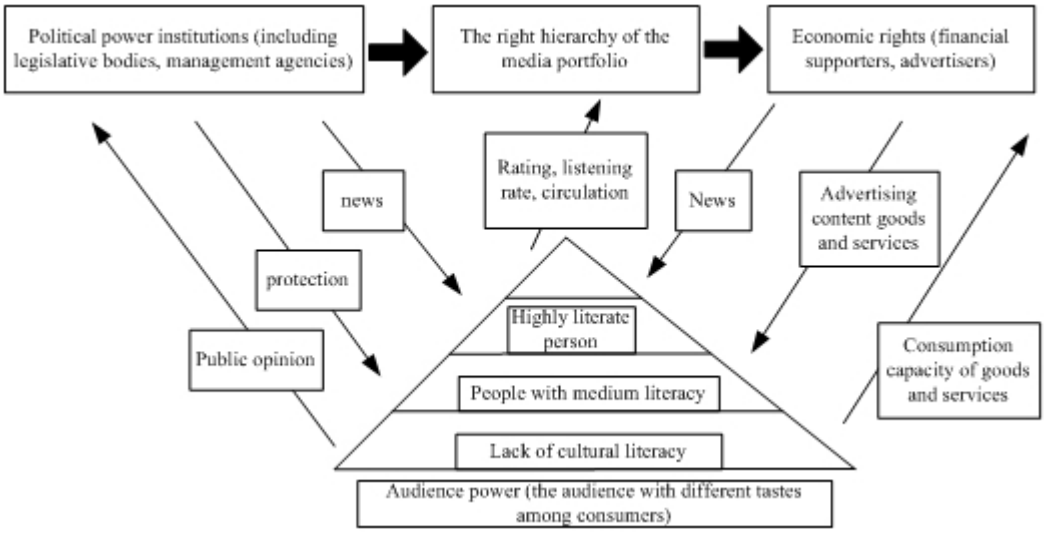
In the flow chart, we can see that the project sponsors put forward their own news topics or research projects, and introduced the report plan, research steps, report content, and the specific use of funds required through crowdfunding or personal social networking sites (Armstrong et al. 2016) . Open to the public. If the public is interested in the project, they will choose "reward" and provide corresponding financial support. If the project sponsor successfully uploads the project within the scheduled time, the smooth implementation of the project can be guaranteed. In return to the organizers, the project sponsors will provide them with reading, priority to participate in activities organized by the project sponsors, and will receive small gifts from the project sponsors.

## 2.3 Advantages of News Crowdfunding Compared with Traditional News Production Models

The traditional news production process is very troublesome and requires mutual cooperation between teams [12]. The choice of topics reported by reporters should be reviewed twice by the author, and should be reviewed by the leader, which can be seen as a level of control. Before determining the type of news that can be applied, these contents must be strictly inspected and controlled. Traditional media belong to the national political power system and will be restricted by various factors (Caviglione et al. 2017). The production of traditional media news must go through a series of review processes, as shown in Figure 3:

In news crowdfunding, reporters skip the media and immediately face the public. They use the mouse and the money in their hands to determine the possibility of reporting (Cath et al. 2017). Many crowdfunding news programs were cancelled because they did not raise funds for the plan. Although reporters will not be restricted by the system during the investigation and reporting process, they will continue to be controlled by consumers. Whether the choice of news topics can arouse public attention, and whether project funds can be raised within a specified time, should be controlled by the public (Yang et al. 2017).

**Figure 3. The review process of the production of traditional media news.**




## 2.4 Encryption Algorithm for Artificial Intelligence Data Protection

Function definition:

(1) $P_j = PKeyGen()$ : This function is used to generate a public parameter $P_j$ function. At the initial stage, a bilinear group G with a prime number p and a generator g will be selected, and the bilinear pairing operation $e: G \times G \to G_l$ will be performed. Attribute space $V = \{V_1, V_2, ....V_n\}, V_i \in V(1 \le i \le n)$, $y_i \mathbf{c} d \in Z_p$ is randomly selected. The function $PkeyGen()$ is shown in formula (1):

$$\{G_l, g, g_d, e(g,g)^c, \{T_i = g_{y_i}\}_{i=1}^n\} \tag{1}$$

(2) $M_j = MKeyGen()$ : This function is used to generate the master key $M_j$ . Among them, g, c, d are defined as the above function $MKeyGen()$ as shown in formula (2):

$$\{g^c, d, \{y_i\}_{i=1}^n\} \tag{2}$$

(3) $A = Encrypt(P_j, N, L)$ : This function uses the public parameter $P_j$ and the access control structure $L$ to encrypt the plaintext $N$ , and obtains the ciphertext $A$ . $\Gamma$ is to meet the authorization set collection requirements of the corresponding access control structure. Among them, $att(y)$ returns the attribute information of node y.

$$(\Gamma, A^{\sim} = Ne(g,g)^{cs}, A = g^{ds}, \forall y \in Y : A_x = g^{q_{y(0)}}, A_x^{'} = L_{att(y)}{}^{q_{y(0)}}) \tag{3}$$

(4) $S_j = SKeyGen(N_j, B)$ : This function uses master key $N_j$ and user attribute set B to generate user private key $S_j$. As the attribute set associated with the user's private key, B is a non-empty subset of the data file attribute set V. Choose random number $\gamma \in Z_p$, individual attribute $s \in B$, random number $\gamma_s \in Z_p$. The function $SKeyGen(N_j, B)$ is shown in formula (4):

$$(E = g^{(c+\gamma)/d}, \forall s \in B : E_s = g^{\gamma} T_s^{\gamma_s}, E_s^{'} = g^{\gamma_s}) \tag{4}$$

(5) $N = Decrypt(D, S_j)$ : This function uses the user's private key $S_j$ to decrypt the ciphertext CT to obtain the plaintext N. Before defining this function, first define the recursive operation $Decrypt(D, S_j, z)$, let $i = att(y)$, each leaf node z can calculate the recursive function $Decrypt(D, S_j, z)$ as shown in formula (5) (6):

$$\frac{e(E_i, A_z)}{e(E_i^{'}, A_z^{'})} = e(g,g)^{\gamma q_z(0)}, i \in B \tag{5}$$

$$\frac{1}{e(E_i, A_z)} = e(g,g)^{rq_z(0)}, i \in B \tag{6}$$

For each non-leaf node z, at least $j_z$ $e(g,g)^{\gamma q_z(0)}$ can be used as Lagrangian polynomial interpolation nodes. After calculation, $e(g,g)^{\lambda q_{Z_s}(0)}$ can be obtained, and $e(g,g)^{\gamma q_z(0)}$ can be calculated by the child node $\{Z_s\}$ of node z. Assuming $U = e(g,g)^{\gamma q_R(0)} = e(g,g)^{\lambda s}$, $Decrypt(D, S_j)$ is as shown in formula (7):

$$D^{\sim} \Big/ \left(e(D,E) \Big/ U\right) \tag{7}$$

## 3. EXPERIMENTS ON DATA PRIVACY PROTECTION RESEARCH IN NEWS CROWDFUNDING IN THE ERA OF ARTIFICIAL INTELLIGENCE

### 3.1 Current State of Data Security in the Era of Artificial Intelligence

With the development of artificial intelligence technology, more and more personal data of citizens are recorded online. Big data sellers have a deeper understanding of individuals, and more and more personal information data (Armstrong et al. 2016). All industries attach great importance to data, and all industries use data for relative analysis and mining to make the best decisions, but many problems have arisen:

(1) Individual users are not very familiar with data security and privacy. Please do not hesitate to register for an online platform account, browse informal websites and download unverified software. Users disseminate personal information intentionally or unintentionally, and users steal and sell other people's information for personal benefit (Caviglione et al. 2017).
(2) Enterprises do not pay attention to data security and user privacy protection. Enterprises have not yet developed a comprehensive data security management system, nor can they adapt to the ever-changing application privacy environment of users (Nasr et al. 2017). Not all employees of the company have procedures and systems to monitor each other's data security and privacy. For example, the information collected by the company is randomly obtained from other affiliated companies, or even sold to illegal elements (Modongo et al. 2016).
(3) The laws concerning data security and privacy and citizens are incorrect. The law is the fundamental guarantee for data security and citizens' privacy. However, when the country establishes a legal system, it only focuses on solving citizens' privacy and security issues. The timeliness of the law is insufficient, the changes in the network environment and the complexity of information leakage are not considered, and they cannot be effectively protected for a long time (Agrawal et al. 2017). In the era of artificial intelligence, the use of data is complex and volatile, and the repeated use of personal information has led to insufficient relevance and law enforcement.
(4) Surveillance cannot keep up with the pace of technological progress, which leads to the loss of technological control, which brings hidden dangers to data security and privacy. Artificial intelligence technology pays more attention to data correlation and is not interested in causality. For example, the complexity of the convergent neural network algorithm is very high. If it loses control, people will not be able to understand the internal function of the mechanism. Artificial intelligence relies more on data, so it is difficult to determine whether the data has been infected by citations (Bryson et al. 2017).

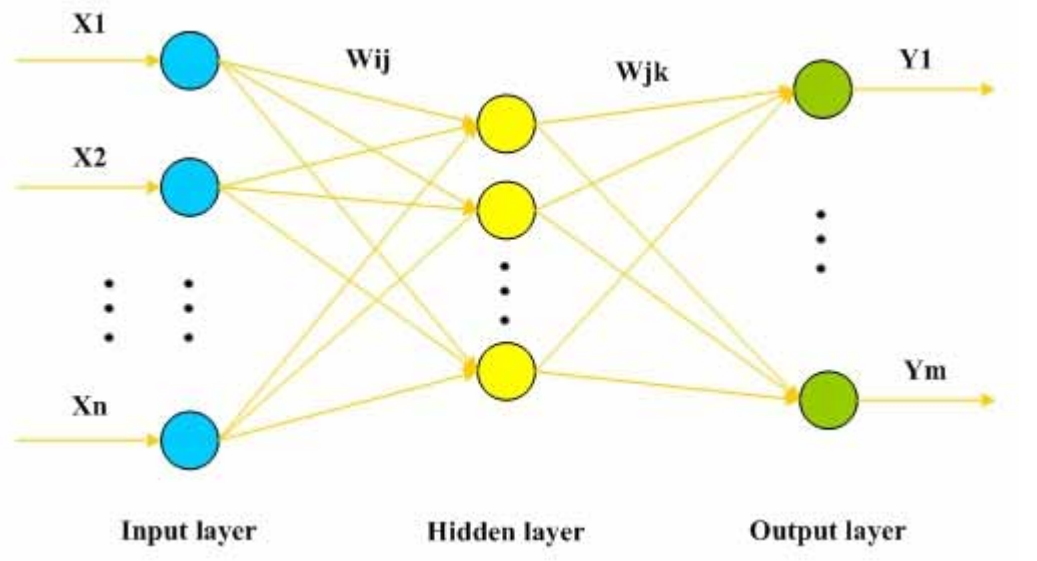
### 3.2 BP Neural Network Prediction Model

With the rapid development of artificial intelligence, neural networks have been applied to many researches due to their excellent performance in dealing with high-dimensional nonlinear problems. Among them, the BP network is the best, most essential and core part of the forward neural network. The data shows that more than 80% of the networks use the BP network or its related deformation and optimization (Price et al. 2017). The related deformation and optimization are different in different research objects and purposes. The research method in this chapter is artificial neural network, and the research object is Shibor's overnight variety and daily data. Therefore, the BP neural network prediction model is first established as a basic model, so that it can be used as a reference standard for model performance in further research (Burton et al. 2017).

The most critical step of the BP network is to adjust the weight of the network through error propagation, the so-called BP (Back Propagation) learning algorithm (Baum et al. 2017). It is a multi-level feedforward neural network. During the network training process, the signal is propagated forward. The BP neural network can learn and memorize a large number of pattern mapping modes between input and output, but there is no need to explicitly express the mathematical equation of this pattern mapping mode in advance. In the forward signal transmission, the signal input from the input plane is processed by the hidden layer and reaches the output plane. The neurons in each layer are not connected to each other, but the state of the neurons in the lower layer is affected by the method of complete interconnection (Polina et al. 2018). If the output level cannot get the expected output, then it enters the backward propagation process according to the decline, updates the network weights and predicts, and continuously improves the network performance so that the output gradually approaches the expected output. The topological structure of BP neural network is shown in Figure 4:

The relevant expression is:

**Figure 4. BP network topology structure diagram.**




(1) Hidden layer activation function f

$$f(x) = \frac{1}{1+e^{-x}} \tag{8}$$

(2) Hidden layer output H:

$$H_j = f(\sum_{i=1}^{n} \omega_{ij} x_i - a_j), \quad j = 1,2,...,l \tag{9}$$

(3) Predicted output O:

$$O_k = l\sum_{j=1} H_j \omega_{jk} - b_k, \quad k = 1,2,...,m \tag{10}$$

(4) Calculate the prediction error e, Y is the expected output:

$$e_k = Y_k - O_k, \quad k = 1,2,...,m \tag{11}$$

(5) Weight $\omega_{..}$, $\omega_{jk}$ update

$$\omega_{ij} = \omega_{ij} + \eta H_j(1-H_j)x(i)\sum_{k=1}^{m} \omega_{jk} e_k \quad \begin{matrix} \mathrm{i} = 1,2,...,n \\ j = 1,2,...,l \end{matrix} \tag{12}$$

$$\omega_{jk} = \omega_{jk} + \eta H_j e_k \mathrm{i} = 1,2,\ldots,\mathrm{l}\mathrm{k} = 1,2,\ldots,m \tag{13}$$

(6) Threshold a, b update:

$$a_j = a_j + \eta H_j (1 - H_j) x(i) \sum_{k=1}^{m} \omega_{jk} e_k j = 1,2,\ldots,l \tag{14}$$

$$b_k = b_k + e_k k = 1,2,\ldots,m \tag{15}$$

## 4. DATA PRIVACY PROTECTION RESEARCH IN NEWS CROWDFUNDING IN THE ERA OF ARTIFICIAL INTELLIGENCE

### 4.1 Design and Implementation of Questionnaire Surveys for Data Privacy Protection

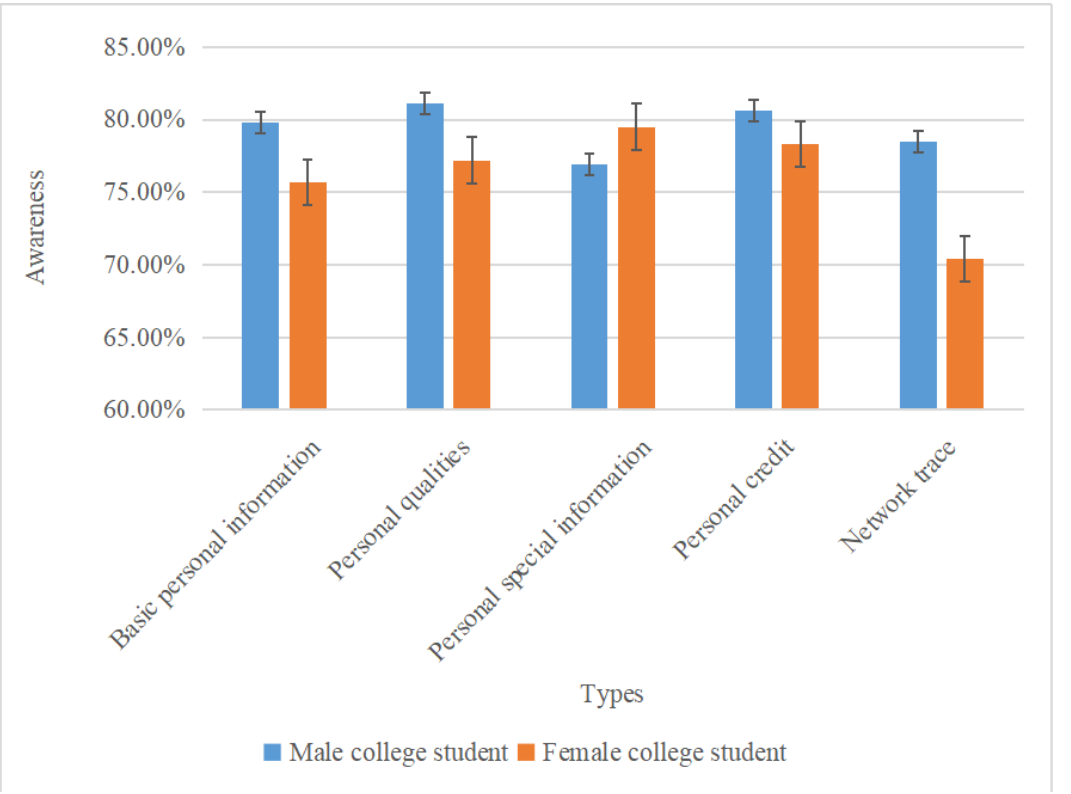
In this survey, 500 questionnaires were distributed, 400 valid questionnaires, and the recovery rate was 80.0%. Among them, male college students accounted for 55.6% and female college students accounted for 44.4% of the questionnaires. The main focus of this questionnaire survey is college students. The reason is that college student groups are an important part of Internet users, and they are very representative in protecting the privacy of personal data. Actual survey questionnaire research is also easier to conduct.

Regarding the cognition of personal data privacy content, all survey respondents believe that personal basic data information, personal special data information, and personal credit information belong to the scope of personal data privacy, while male college students only have 81.1 in terms of cognition of personal trait information. %, the cognition level of network trace information is only 78.5%, and the cognition of personal credit of female college students is only 78.3%, and the cognition of personal basic information is only 75.7%. It shows that most members of the public have a high level of privacy awareness in terms of name, gender, age, ID number, file information, property status, bank card account passwords, credit records and repayment status, and business reputation. Height, weight, IP address, recycle bin files, historical records, etc. are less important to privacy. The personal data privacy content awareness of college students is shown in Figure 5:

In terms of the main reasons for personal data privacy leakage, all survey respondents believe that the main reasons are weak personal protection awareness, interest-driven, and lack of regulations. The proportion of male college students who think it is because of enterprises or organizations is 56.5%, and the proportion of male college students who think it is due to business or organization is 56.5%, 70.2% think it is the reason for the lack of morality. On the other hand, the percentage of female college students who believed personal reasons was 84.6%, the percentage who thought profit-driven reasons was 80.1%, and the percentage who thought the reasons for legal defects were 83.1%. The main reasons for personal data privacy leakage of college students are shown in Figure 6:

In terms of the use of Internet applications, all survey respondents often use online shopping, social interaction, information acquisition, and games. About 84.1% of male college students often use online audiovisual applications, and about 66.5% of male college students often use online audiovisual applications. The mobile office application is used. In terms of personal data privacy, online shopping and social interaction have the highest involvement rate, reaching 100%, and about 100% of female college students often use online shopping applications, and about 9.37% of female

**Figure 5. Personal data privacy content awareness.**

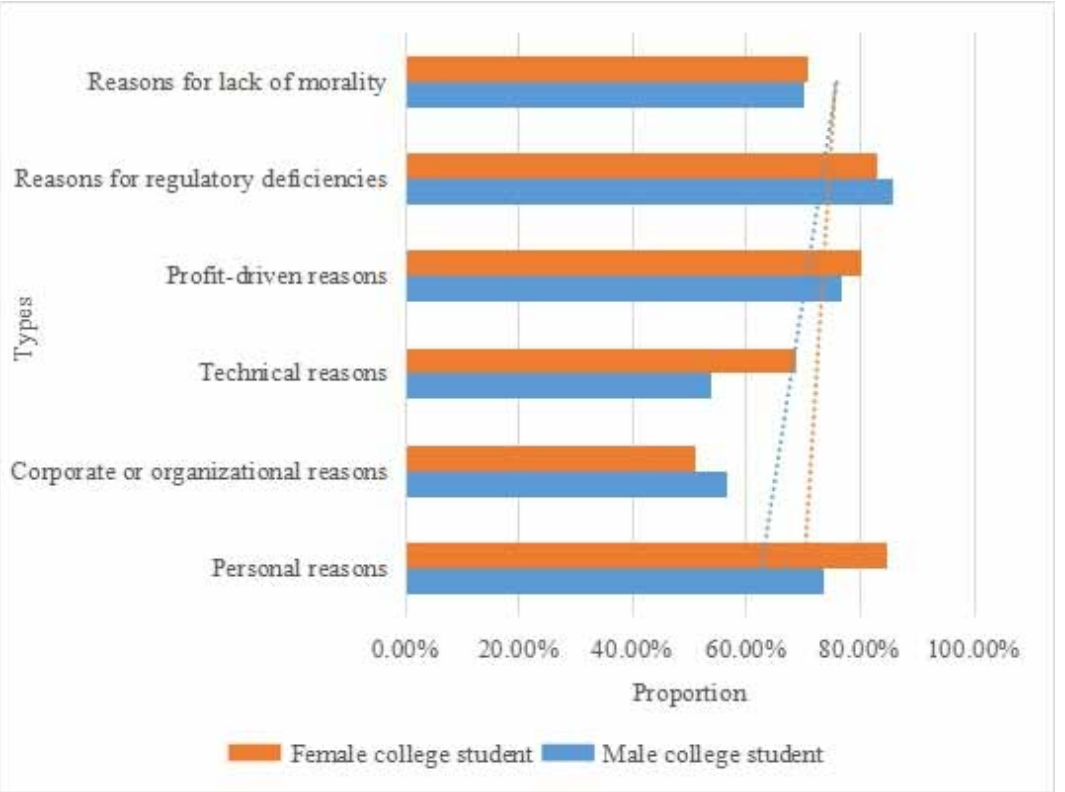



college students often use online shopping applications. There are some applications (Singh, 2018; Shankar, 2019; Wan, 2020.). The main applications of college students involved in personal data privacy are shown in Figure 7:

The statistical results in Table 1 show that most college students believe that their home address (91.2%), bank card number (90.6%), ID number (89.8%), phone number (79.8%), and the privacy of college students in the era of big data, 36.2% College students believe that online social activities are not part of the privacy of college students in the era of big data, and college students also have different attitudes toward funding and rewards and punishments at school. 31.2% and 25.0% of students believe that their name and gender are not in the privacy of college students in the era of big data. In addition, in the subjective part of the questionnaire, college students in the era of big data have a certain degree of privacy awareness, but this perception is not sufficient. Only a few college students have expressed their awareness of the importance of privacy protection in the era of big data, but they all expressed concern for themselves (Lv et al. 2017). There is a certain degree of difficulty in protection, and there is no way to start.

Table 2 investigates whether college students will trade privacy in exchange for convenience. The percentage of e-commerce individuals is the highest, reaching 91.6%, and online social applications and takeaway apps rank second and third. Most college students expressed their willingness to trade privacy for convenience, using e-commerce, takeaway apps, and social networking applications (Kim, 2019). The prerequisite for using them is to provide some real personal information, and privacy leakage is unavoidable. In the questions that followed, only 14.98% of college students expressed their opposition to the practice of businesses, online companies, and service providers for material benefits and convenience in exchange for personal privacy.

**Figure 6. The main reason for personal data privacy leakage.**




When asked "If your privacy is violated on the Internet, would you choose?", 40.4% of college students said that they would defend their rights online, and 37.6% of college students said they would defend their rights through legal means, and to the school teachers The proportion of asking for help is only 5.4%, which shows that students have a strong awareness of rights protection. Safeguarding rights via the Internet shows that college students do not trust the work of protecting privacy in schools, and there is even no department that deals with the infringement of student privacy. It also shows that colleges and universities lack privacy and personality education. See Table 3:

The prerequisite for improving privacy awareness is to understand the nature and value of privacy. Through interactive analysis of "Do you know the previous secrets?" and "What do you think are the most serious consequences of privacy leaks?", to a certain extent, "very conscious" issues are more worthy of attention. "And the individual does not think that "violation of personal dignity" is the most serious consequence of leaking secrets to prove privacy issues. There are certain differences in knowledge. See Table 4:

Through research, we analyzed the impact of different ways in which schools conduct privacy education on the understanding of privacy, and found that different educational channels have different results on the understanding of privacy. Among them, the ideological and political courses of privacy education, other classrooms and initial education have different effects on students' privacy. The degree of understanding has a greater impact, and the activities of the club have an overall impact on the degree of understanding of students' privacy, as shown in Table 5:

**Figure 7. Major applications of college students involving personal data privacy.**

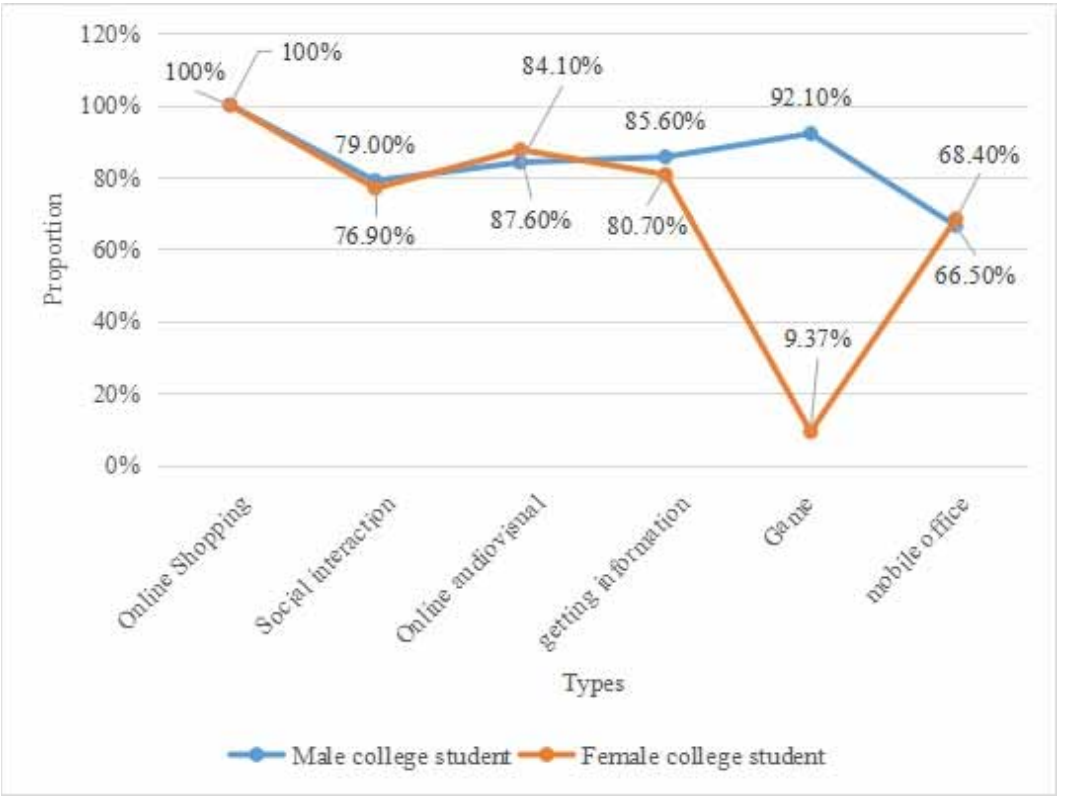



**Table 1. The specific situation of college students' privacy awareness in the era of artificial intelligence.**

| category | Name | gender | date of birth | identity number | Home address | telephone number | photo | other |
|---|---|---|---|---|---|---|---|---|
| N=200 | 63 | 50 | 153 | 101 | 182 | 160 | 146 | 2 |
| % Of cases | 31.2% | 25.0% | 50. 6% | 89. 8% | 91. 2% | 79. 8% | 72.8% | 1.2% |

**Table 2. Privacy for convenience.**

| category | Meituan and other takeaway apps | Taobao, JD and other e-commerce | mailbox | Network social applications | learning software |
|---|---|---|---|---|---|
| N=200 | 120 | 183 | 62 | 137 | 56 |
| % Of cases | 59.8% | 91.6% | 31.0% | 68.6% | 27.8% |

## 4.2 Data Privacy Protection Measures in the Era of Artificial Intelligence

Issues such as reselling user information, extortion, bank card theft, and scanning indicate that privacy is not a single issue, but must be protected at multiple levels, such as national policies, industry and business, and personal awareness. Create a safe and reliable data market model.

**Table 3. If your privacy is violated on the Internet, what would you choose?**

| category | Endure silently | Ask the teacher for help | Network rights | Legal rights protection | other |
|---|---|---|---|---|---|
| Frequency | 27 | 11 | 81 | 75 | 6 |
| percentage | 13.6% | 5.4% | 40.4% | 37.6% | 3.0% |

**Table 4. Interaction analysis table of different levels of privacy understanding and the most serious consequences of the leakage of privacy considered by the subjects?**

| | | Privacy awareness | | | | |
|---|---|---|---|---|---|---|
| | | Know very well | Better understand | General understanding | Understand a little | Don't understand |
| Encountered the consequences of a leak | Money loss | 31.8% | 9.6% | 9.2% | 5.3% | 6.7% |
| | Personal dignity is violated | 27.3% | 38.0% | 40.6% | 18.4% | 35.6% |
| | Harassed | 36.4% | 47.6% | 43.2% | 63.2% | 44.4% |
| | Not clear | 4.5% | 4.5% | 6.6% | 7.9% | 8.9% |
| | It doesn't matter | 0% | 0% | 1.4% | 5.3% | 4.4% |

**Table 5. Analysis table of the interaction of different levels of non-governmental education on the degree of understanding?**

| | | Privacy awareness | | | | |
|---|---|---|---|---|---|---|
| | | Ideological and Political Class | Other classrooms | social activity | Beginning Education | Not clear |
| Encountered the consequences of a leak | Know very well | 10.6% | 4.1% | 12.5% | 0% | 1.2% |
| | Better understand | 37.4% | 44.6% | 12.5% | 41.7% | 31.1% |
| | General understanding | 44.7% | 47.3% | 62.5% | 50.0% | 46.0% |
| | General understanding | 5.7% | 2.7% | 0% | 0% | 9.9% |
| | Don't understand | 1.6% | 1.4% | 12.5% | 8.3% | 11.8% |

(1) Government legislation to protect data privacy

The state's promulgation of laws and regulations is the fundamental guarantee for protecting the market and the legitimate rights and interests of citizens. With the support of laws and regulations, when privacy is violated and violations need to be investigated, some laws may need to be followed. At present, computer data protection laws are relatively weak, and there is an urgent need to accelerate the development and improvement of related laws to protect the privacy of artificial intelligence.

National regulatory agencies need to strengthen supervision, severely crack down on excessive collection of personal information and privacy, severe punish individuals and individuals who leak personal protection, protect citizens' privacy rights, and establish legal authority.

(2) The enterprise strengthens self-discipline, assumes social responsibility and abides by the bottom line of the law

Currently, many large companies regard population mobility and big data collection as their main competitiveness, but companies sometimes leak and abuse user privacy. Data brings benefits to the company and requires the company to abide by the basic principles of the law and assume the social responsibility of protecting user privacy. Try to require all company applications to collect user data to comply with the "minimal collection" principle and collect and use it reasonably. At the same time, companies need to improve internal systems and increase data protection capabilities. In the data life cycle, improve the system in terms of data collection, data recovery and data security measures to improve the company's ability to protect data privacy.

(3) Improve personal awareness to protect user privacy

At present, when a personal smart device installs an APP, a permission request is required, and almost all users agree, which shows that the public does not pay attention to the degree of privacy protection. Therefore, privacy must "start from childhood, from me" and protect the first obstacle to preventing privacy leakage. When using a copy of the daily certificate, please indicate the purpose of use and point out that another use is invalid. Do not disclose personal information to other institutions and individuals, and close the unused rights of the smart device, and be careful. Read the content of the privacy policy. "Start with me" through the above channels to protect personal privacy.

(4) Improve privacy protection technology

In the above three privacy levels, analyze the vulnerabilities in the big data environment, study privacy technology in a targeted manner, and develop effective data suitable for the era of artificial intelligence through data traceability research, data watermarking, identity verification and anonymous data protection technology.

## 5. CONCLUSION

Artificial intelligence will become the focus of scientific and technological development in the next ten years or more, and will change the world in more detail and bring human society into a new era. In the development of artificial intelligence, there are many hidden dangers in data security and privacy. However, with the advancement of technology, the protection of national legislation, honest cooperation between companies and the awakening of citizenship, data security and privacy rights, better services will provide people with more convenience and services. This article combines the research results and theories on the protection of personal data privacy at home and abroad, clarifies the definition of personal data and privacy, and analyzes the reasons, results, behaviors and forms of current personal data leakage, and classifies personal data privacy . The company's related technologies discussed the current status of personal data privacy in my country. This article also combines the questionnaire survey method to understand the current status of the public in terms of privacy awareness, attitude, privacy, etc., and discover the main problems and shortcomings, and then we can carry out targeted improvements and perfect strategies to protect our country the privacy of your personal data.

## ACKNOWLEDGMENT

This work was supported by the major achievements of disciplinary scientific research of China-ASEAN Art College of Chengdu University, ichuan Provincial Department of Education Humanities and Social Sciences Key Research Base-Meteorological Disaster Prediction and Early Warning and Emergency Management Research Center 2021 Key Project "Emergency Research on the Construction of Health Communication System in Public Events" ,Zhejiang Philosophy and Social Science Planning Project "Research on Human-Machine Communication and Governance Mechanism Innovation under the Background of Digital Anti-epidemic-Taking Zhejiang Urban Brain as an Example" (21NDQN275YB).

## ACKNOWLEDGEMENT

This work was supported by the major achievements of disciplinary scientific research of China-ASEAN Art College of Chengdu University, ichuan Provincial Department of Education Humanities and Social Sciences Key Research Base-Meteorological Disaster Prediction and Early Warning and Emergency Management Research Center 2021 Key Project "Emergency Research on the Construction of Health Communication System in Public Events" ,Zhejiang Philosophy and Social Science Planning Project "Research on Human-Machine Communication and Governance Mechanism Innovation under the Background of Digital Anti-epidemic-Taking Zhejiang Urban Brain as an Example" (21NDQN275YB).

## REFERENCES

Agrawal, A., Gans, J. S., & Goldfarb, A. (2017). What to expect from artificial intelligence. *MIT Sloan Management Review*, *58*(3), 23–26.

Armstrong, S., Bostrom, N., & Shulman, C. (2016). Racing to the precipice: A model of artificial intelligence development. *AI & Society*, *31*(2), 201–206. doi:10.1007/s00146-015-0590-y

Armstrong, S., Bostrom, N., & Shulman, C. (2016). Racing to the precipice: A model of artificial intelligence development. *AI & Society*, *31*(2), 201–206. doi:10.1007/s00146-015-0590-y

Barzegar, R., Adamowski, J., & Moghaddam, A. A. (2016). Application of wavelet-artificial intelligence hybrid models for water quality prediction: A case study in aji-chay river, iran. *Stochastic Environmental Research and Risk Assessment*, *30*(7), 1797–1819. doi:10.1007/s00477-016-1213-y

Baum, S. D. (2017). On the promotion of safe and socially beneficial artificial intelligence. *AI & Society*, *32*(4), 1–9. doi:10.1007/s00146-016-0677-0

Boulay, B. D. (2016). Artificial intelligence as an effective classroom assistant. *IEEE Intelligent Systems*, *31*(6), 76–81. doi:10.1109/MIS.2016.93

Bryson, J., & Winfield, A. (2017). Standardizing ethical design for artificial intelligence and autonomous systems. *Computer*, *50*(5), 116–119. doi:10.1109/MC.2017.154

Bundy, A. (2017). Preparing for the future of artificial intelligence. *AI & Society*, *32*(2), 285–287. doi:10.1007/s00146-016-0685-0

Burton, E., Goldsmith, J., Koenig, S., Kuipers, B., Mattei, N., & Walsh, T. (2017). Ethical considerations in artificial intelligence courses. *AI Magazine*, *38*(2), 22–34. doi:10.1609/aimag.v38i2.2731

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2017). Artificial intelligence and the 'good society': The us, eu, and uk approach. *Science and Engineering Ethics*, *24*(7625), 1–24. doi:10.1007/s11948-017-9901-7 PMID:28353045

Caviglione, L., Gaggero, M., Lalande, J. F., Mazurczyk, W., & Urbanski, M. (2017). Seeing the unseen: Revealing mobile malware hidden communications via energy consumption and artificial intelligence. *IEEE Transactions on Information Forensics and Security*, *11*(4), 799–810. doi:10.1109/TIFS.2015.2510825

Caviglione, L., Gaggero, M., Lalande, J. F., Mazurczyk, W., & Urbanski, M. (2017). Seeing the unseen: Revealing mobile malware hidden communications via energy consumption and artificial intelligence. *IEEE Transactions on Information Forensics and Security*, *11*(4), 799–810. doi:10.1109/TIFS.2015.2510825

Dblm, A., & Gwb, B. (2019). Imaging quality control in the era of artificial intelligence. *Journal of the American College of Radiology*, *16*(9), 1259–1266. doi:10.1016/j.jacr.2019.05.048 PMID:31254491

Glauner, P., Meira, J. A., Valtchev, P., State, R., & Bettinger, F. (2017). The challenge of non-technical loss detection using artificial intelligence: A survey. *International Journal of Computational Intelligence Systems*, *10*(1), 760–775. doi:10.2991/ijcis.2017.10.1.51

Jha, S., & Topol, E. J. (2016). Adapting to artificial intelligence: Radiologists and pathologists as information specialists. *Journal of the American Medical Association*, *316*(22), 2353–2354. doi:10.1001/jama.2016.17438 PMID:27898975

Kim, H. (2019). Investigating the mediating role of social networking service usage on the big five personality traits and on the job satisfaction of korean workers. *Journal of Organizational and End User Computing*, *31*(1), 110–123. doi:10.4018/JOEUC.2019010106

Kotsenas, A. L., Balthazar, P., Andrews, D., Geis, J. R., & Cook, T. S. (2021). Rethinking patient consent in the era of artificial intelligence and big data. *Journal of the American College of Radiology*, *18*(1), 180–184. doi:10.1016/j.jacr.2020.09.022 PMID:33413897

Lu, H., Li, Y., Min, C., Kim, H., & Serikawa, S. (2017). Brain intelligence: Go beyond artificial intelligence. *Mobile Networks and Applications*, *23*(7553), 368–375.

Lv, Z., Song, H., Basanta-Val, P., Steed, A., & Jo, M. (2017). Next-generation big data analytics: State of the art, challenges, and future research topics. *IEEE Transactions on Industrial Informatics*, *13*(4), 1891–1899. doi:10.1109/TII.2017.2650204

Modongo, C., Pasipanodya, J. G., Magazi, B. T., Srivastava, S., Zetola, N. M., Williams, S. M., Sirugo, G., & Gumbo, T. (2016). Artificial Intelligence and Amikacin Exposures Predictive of Outcomes in Multidrug-Resistant Tuberculosis Patients. *Antimicrobial Agents and Chemotherapy*, *60*(10), 5928–5932. doi:10.1128/AAC.00962-16 PMID:27458224

Nasr, M., Mahmoud, A., Fawzy, M., & Radwan, A. (2017). Artificial intelligence modeling of cadmium(ii) biosorption using rice straw. *Applied Water Science*, *7*(2), 823–831. doi:10.1007/s13201-015-0295-x

Pigozzi, G., Tsoukias, A., & Viappiani, P. (2016). Preferences in Artificial Intelligence. *Annals of Mathematics and Artificial Intelligence*, *20*(3-4), 1–41.

Polina, M., Lucy, O., & Yury, Y. (2018). Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*, *9*(5), 5665–5690. doi:10.18632/oncotarget.22345 PMID:29464026

Price, S., & Flach, P. A. (2017). Computational support for academic peer review: A perspective from artificial intelligence. *Communications of the ACM*, *60*(3), 70–79. doi:10.1145/2979672

Raedt, L. D., Kersting, K., Natarajan, S., & Poole, D. (2016). Statistical relational artificial intelligence: Logic, probability, and computation. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, *10*(2), 1–189. doi:10.2200/S00692ED1V01Y201601AIM032

Rongpeng, L., & Zhifeng, Z. (2017). Intelligent 5g: When cellular networks meet artificial intelligence. *IEEE Wireless Communications*, *24*(5), 175–183. doi:10.1109/MWC.2017.1600304WC

Shankar, D. K., Elhoseny, M., & Damasevicius, R. (2019). Trust based cluster head election of secure message transmission in manet using multi secure protocol with tdes. *Journal of Universal Computer Science*, *25*(10), 1221–1239.

Singh, P., & Agrawal, R. (2018). A customer centric best connected channel model for heterogeneous and iot networks. *Journal of Organizational and End User Computing*, *30*(4), 32–50. doi:10.4018/JOEUC.2018100103

Wan, S., Qi, L., Xu, X., Tong, C., & Gu, Z. (2020). Deep learning models for real-time human activity recognition with smartphones. *Mobile Networks and Applications*, *25*(2), 743–755. doi:10.1007/s11036-019-01445-x

Yang, T., Asanjan, A., Welles, E., Gao, X., Sorooshian, S., & Liu, X. (2017). Developing reservoir monthly inflow forecasts using artificial intelligence and climate phenomenon information. *Water Resources Research*, *53*(4), 2786–2812. doi:10.1002/2017WR020482

*Xu Zhiqiang was born in Chengdu, Sichuan, China, in 1981. He received the master's degree from Nanyang Technological University, Singapore. He was an winner of China Film and Television Youth Science and Technology Award and IEEE Senior Member. Now, he is an professor and senior engineer who works in School of Film and Animation, China-ASEAN Art College, Chengdu University, China. He has long been engaged in research on the integration of big data and all media, key technologies of interactive media and intelligent media, information consumption and communication technology, etc. He has more than 80 papers published (including many SCI/EI), and as the first author published one monograph, four textbooks for editors-in-chief (deputy editors).*

*Xiang Dong was born in Zhongxian, Chongqing, P.R. China, in 1977. He received the Master degree from Sichuan University, P.R. China. Now, he works in College School of Digital Media and Creative Design, Sichuan University of Media and Communications, He has long been engaged in the integration of digital media, film and television production, information consumption and other fields. He is the corresponding author of this paper.*

*He Jialiang was born in Heilongjiang, P.R. China, in 1977, received the PhD degree in computer software and theory from Jilin University of China in 2012 and the Master degree in computer application from Jilin University of China in 2004. Now, he is an associate professor in College of Information and Communication Engineering, Dalian Nationalities University, China. His papers have been published in some well-known international Journals and IEEE conferences. His main interests include Mobile Internet, Internet of Things, and Intelligent Business Information Processing.*