Hindawi
Mobile Information Systems
Volume 2021, Article ID 3118733, 12 pages
https://doi.org/10.1155/2021/3118733

Research Article

Intelligent Application of Artificial Intelligence Internet of Things Technology in the Economic and Legal Fields

Tingting Tan

School of Finance and Public Administration, Harbin University of Commerce, Harbin 150028, Heilongjiang, China

Correspondence should be addressed to Tingting Tan; tingting8559@163.com

Received 18 August 2021; Revised 16 October 2021; Accepted 26 October 2021; Published 12 November 2021

Academic Editor: Sang-Bing Tsai

In today's globalized situation, people on the one hand enjoy the great convenience brought by the Internet and artificial intelligence Internet of Things (IoT) technology, and, on the other hand, they are also inevitably subject to a series of harms brought by network technology. Internet economic crime is a new type of crime based on Internet technology. Criminals use Internet technology to conduct illegal visits and Trojan horse program attacks, steal user information, and defraud victims of money. This has resulted in the people's personal and property safety and social harmony and stability. Strictly cracking down on cyber economic crimes in accordance with the law is of great significance to safeguarding the interests of the people and maintaining social stability. However, as the methods and forms of cyber economic crimes emerge endlessly, it is very important to collect intelligence information on such crimes. This paper proposes using the sensor technology, embedded system technology, radio frequency automatic identification technology, and cloud computing technology in artificial intelligence Internet of Things technology to design and build a data-mining-based network economic crime intelligent information aggregation collection system to realize network economic crime intelligence of aggregation and analyze and help combat cyber economic crimes. This article takes cyber economic crime cases in various cities in our province as an example, selects 9 cyber economic criminals' intelligence information as sample data, and tests and applies the designed cyber economic crime intelligence information system. The final results show that the numbers of cyber economic crime cases in four cities A, B, C, and D in four provinces are roughly the same, but city A has the largest number; the minimum confidence of the 9 criminals is above 0.60, indicating that the economic crimes of cyber economic criminals are related to their academic background and family status and criminal history are related to a certain extent; illegal fund-raising fraud and online credit card fraud account for the largest proportion of the four cities and are currently the main forms of online economic crime.

1. Introduction

1.1. Background and Significance. In today's world, a multiownership economic structure with a market economy as the mainstay is booming. With the rapid advancement of network technology, the mode of social and economic development is gradually becoming digital and intelligent. On the one hand, this economic development method has brought huge convenience and profits to people, but, on the other hand, due to the complexity and virtuality of the online world, it has become a breeding ground for cyber economic crimes. Many criminals rely on Internet technology. Means to steal user information and defraud people's property, hovering on the edge of economy and law, pose a huge threat to the personal and property safety of the general public. At the same time, because of the continuous increase in the number of people, the continuous development of the economy and society, and the continuous emergence of social polarization, the probability of social problems is also increasing, the rate of economic crime is gradually increasing, and the phenomenon of social unhealthy problems is also increasing frequently. Cracking down on such cyber economic crimes in accordance with the law and regulating the order of the market economy are of great significance to maintaining social harmony and stability and ensuring the safety of the people.

Fighting against cyber economic crimes mainly lies in the collection of intelligence information, investigation and

evidence collection, and the mining and analysis of information and data. Due to the diverse forms of cyber economic crimes, the collection of intelligence information is complex and changeable, and the amount of information is difficult to investigate. Based on this, this article proposes using artificial intelligence IoT sensor technology, combined with information intelligent aggregation means and data mining technology, collecting cyber economic crime information through IoT sensors, and then using data calculation and mining methods to summarize and analyze the acquired intelligence information to find out the nature and characteristics of cyber economic crimes, so as to improve the ability to detect cyber economic crimes.

1.2. Related Work. The IoT technology is a great invention of mankind. It realizes the interconnection and intercommunication between real-world things and creates great convenience to people's lives. With the further development of the IoT technology, its applications in all aspects of society are becoming more and more common. Wu conducted research on the application of the IoT in the logistics industry. He pointed out that the IoT technology is the product of the third technological revolution after computers and the Internet, and the integration of IoT technology into the development of the logistics industry will play a key role in promoting [1]. Jun Zhang and Khaled B. Letaief applied the IoT to the automotive field and proposed a concept of Internet of Vehicles. They said that, as an emerging paradigm, the Internet of Vehicles (IoV) will bring about an intelligent IoV era, which will largely depend on communication, computing, and data analysis technologies. Deploying storage and computing resources at the edge of the wireless network (e.g., wireless access points), edge information systems (EIS) including edge caching, edge computing, and edge AI will play a key role in future smart IoV. EIS will not only provide low-latency content delivery and computing services but also localized data collection, aggregation, and processing [2]. In addition, the IoT technology also has applications in network information collection and security maintenance. Park et al. said that recent network security incidents and internal information leakage incidents have become a major obstacle to access to sustainable intelligence information. In order to ensure sustainable smart media technology and establish an information and information system environment, it is necessary to firmly cultivate the information security industry, and it is necessary to research and form a multidimensional foundation to promote the use of information security products and services by intelligence agencies. To this end, they explored and analyzed the future direction by dividing law and policy, information security business management, and security accident criminal psychology and information into four areas and designed a safe and economically feasible plan [3]. It can be seen from the previously mentioned research that the powerful functionality and practicability of the IoT technology have confirmed its good effects in various fields. Aiming at the current increasing proliferation of cyber economic crimes, this article proposes the use of IoT technology and intelligent information aggregation to collect, aggregate, and analyze cyber economic crime intelligence information to find the characteristics and laws of such economic crimes, so as to provide guidance for improving the investigative ability and case detection level of the public security department on cyber economic crimes. Although the powerful functions of the Internet of Things technology provide important help for effectively combating illegal and criminal activities, among researchers, there is a lack of relevant research on the defects of the Internet of Things technology that is highly dependent on the network and electricity.

1.3. Innovations in This Article. The innovations of this article are mainly reflected in the following aspects: (1) In recent years, cyber economic crimes have emerged one after another, and there are signs of becoming more and more rampant. The application of combating cyber economic crimes has important practical significance. (2) This paper proposes the use of cloud computing, sensor technology, embedded system technology, and radio frequency automatic identification technology using artificial intelligence Internet of Things technology, combined with information intelligent aggregation methods and data mining methods, to design and build a cyber economy crime intelligent information aggregation system to prevent cyber economy during the crime, collect, summarize, and analyze intelligence information, and dig out the laws of economic crimes behind the information, so as to improve the ability to detect cyber economic crimes.

2. AI IoT-Related Technologies and Their Intelligent Information Aggregation in the Economic and Legal Fields

2.1. Artificial Intelligence IoT Technology. The Internet of Things technology originated in the media field and is the third revolution in the information technology industry. The Internet of Things refers to the connection of any object to the network through information sensing equipment according to an agreed agreement, and the object exchanges and communicates information through the information dissemination medium to realize intelligent identification, positioning, tracking, supervision, and other functions. Among them, the Internet of Things refers to the integration of ubiquitous terminal equipment and facilities, including sensors with "intrinsic intelligence," mobile terminals, industrial systems, numerical control systems, home intelligent facilities, and video surveillance systems, and "external enablement," "intelligent objects or animals," or "smart dust" such as various assets affixed with RFID and individuals and vehicles carrying wireless terminals through various wireless and/or wired long distance and/or short distance. The communication network realizes interconnection and interoperability, application integration, and cloud computing-based SaaS operation modes. In the intranet, private network, and/or Internet environment, appropriate information security protection mechanisms are adopted to provide safe, controllable, and even personalized

real-time online monitoring, positioning, and tracing, alarm linkage, dispatching and commanding, plan management, remote control, security protection, remote maintenance, online upgrades, statistical reports, decision support, leadership desktop, and other management and service functions to achieve an efficient and energy-saving management and control operation model and a safe and environmentally friendly marketing integration form. Through the IoT technology, not only between people but also between people and machines being able to interact, things can also get in touch and communicate with each other. The IoT technology closely connects the virtual world with the real world, meets the development needs of the people and society, and brings great convenience to social production and people's daily life [4–7].

2.1.1. Principles of Artificial Intelligence IoT Technology. As the core technology of the IoT, cloud computing has powerful data computing capabilities. Its computing model is to decompose huge data computing tasks into small computing programs and distribute them in a resource pool in the cloud. By decomposing huge resources into small computing programs and distributing them in the cloud resource pool, the resources can be provisioned or released quickly with minimal management overhead and minimal interaction with suppliers. These small programs are processed and analyzed by connecting multiple servers, and then dynamic and virtualized resources are obtained. These resources are sent to users [8–10]. The cloud computing architecture is roughly divided into three horizontal layers and one vertical layer. As shown in Figure 1, the three horizontal layers are the infrastructure layer, the platform layer, and the software service layer. The vertical layer is the cloud management layer, which is for better maintenance and management. The other three layers exist [11, 12].

2.1.2. Key Technologies of the IoT. Sensor technology, embedded system technology, and radio frequency automatic identification technology (RFID tags) are the three key technologies of the IoT system. The key technologies of the Internet of Things and some other related technologies participate in our economic and legal fields to better help us to combat criminal acts in the economic and legal fields, but the three key technologies that are more inclined to use the Internet of Things are because these three key technologies are more mature; people's mastery of them can already meet the needs in daily life. Among them, sensors are the most common and most important. The first step in the IoT to realize the interconnection of objects is to obtain information about objects. And this process needs to rely on sensor technology that has to be realized. It converts the analog signal in the transmission line into a processable digital signal, which is then handed over to the computer for processing. Embedded system technology integrates computer software and hardware, sensor technology, integrated circuit technology, and so forth for data processing and

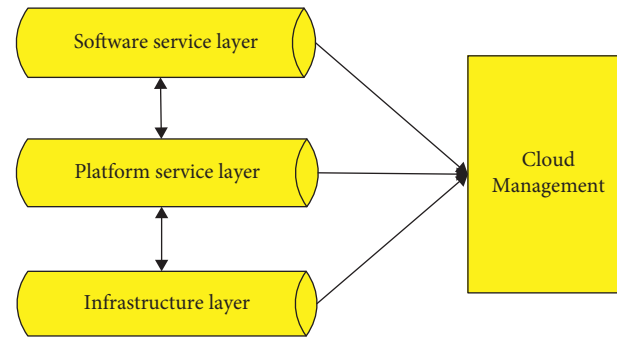

Figure 1: Cloud computing architecture diagram.

analysis [13–15]. Here we mainly introduce the sensor technology and the data mining by the sensor in detail.

As the source of information acquisition, sensors are receiving more and more attention from people. With the further development of modern sensor technology, smart sensors appear. The sensor network composed of these tiny sensor nodes has wireless communication and computing capabilities and can autonomously complete designated tasks according to environmental changes in a self-organizing manner [16, 17]. The data mining calculation method [18] we used in this process is mainly based on the Apriori algorithm of rule association, and its calculation principle is as follows:

First, set frequent item set 1 as L_1, count the number of occurrences of each item in the item set, and record as candidate item set 1 A_1, given the lowest support C_1 of candidate item set 1.

Second, calculate the candidate item set 2 A_2 according to $C_1 * C_1$, and calculate the number of occurrences of each element in C_2 according to the minimum support A_2 of the given candidate item set 2.

Third, keep repeating the above steps until C_K is generated.

Fourth, after completing the above operations, the final calculation result yields all frequent item sets:

$$L_1 = \{\text{large } 1 - \text{itemsets}\}; \quad \text{for}\,(k = 2; L_{k-1} \neq \varnothing; k + 1);$$
$$C_k = \text{Apriori} - \text{gen}\,(L_{k-1}). \tag{1}$$

2.1.3. Network Structure System of Artificial Intelligence IOT. The architecture of the IoT is summed up as "things + servers + people." The data is collected through smart sensors on the terminal and transmitted to the server, and the server stores and processes the data and finally displays the data to the user. It is specifically divided into three layers: perception layer, processing layer, and application layer, as shown in Figure 2. The perception layer mainly collects and transmits signals over short distances, relying on sensor equipment; the application layer connects the computer network and the user, and, through the mobile terminal equipment, the computer network finally sends the data information to the user [19–21].

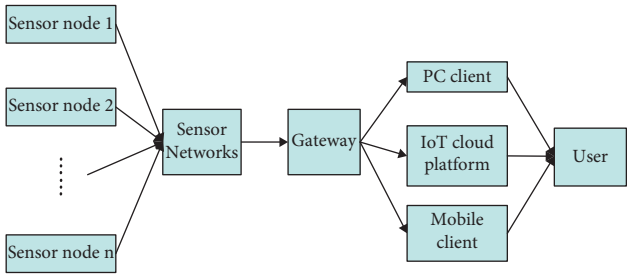

Figure 2: The structural system of the Internet of Things.

2.2. Economy and Law. With the development of cultural diversification, modern forms of economic development have also shown a flourishing situation, and a form of network economy based on the computer Internet has emerged. However, due to the complexity and fictitious nature of the online world, the phenomenon of online economic crimes has also continued to emerge [22, 23]. All these actions and phenomena violate the principles of economy and law. Under the general environment of our country's socialist system, although the economy determines the superstructure and affects the development and changes of law, at the same time, law has a huge countereffect to the economy. Law can confirm, protect, and develop the economic foundation on which it depends. It can also restrict and prohibit the occurrence and development of harmonious and stable social production relations [13, 24]. In short, in the advanced IoT era, we must be good at using the power of network technology to correctly develop the economy and increase social productivity and, at the same time, for those criminals who despise the law and do not abide by the principles of economy and law, we must also be good at using network technology. Severe crackdowns and investigations shall be carried out to prevent the emergence of cyber economic crimes as much as possible.

2.3. Intelligent Aggregation of Information. Aggregation is a computer term that belongs to information science. It refers to the selection, analysis, and classification of relevant data content, and, through certain calculation methods, many complex information data are aggregated into a form that is convenient for people to analyze. The final analysis is that the expected result mainly refers to the data conversion process that can generate scalar values from the array [25]. The expansion of gathering means gathering and fusion and represents the connection between the collection object and the component object. It is called an association relationship. Using association rules, you can find a certain connection between them. By classifying and aggregating a large number of data resources and effectively processing them, the desired results are finally obtained.

With such advanced information technology today, various network information data fill people's brains and lives. How to effectively process this network information and dig out useful parts has become a very important thing at the moment. As an important technology in the Internet system, aggregation can summarize and classify various information on the Internet. Intelligent aggregation can realize a series of operations such as data mining, classification, and analysis through computer machines, without human intervention, and is truly intelligent. The intelligent aggregation structure model of information based on multiple sensors is shown in Figure 3. In this model diagram, there are a total of 4 layers of structure: data layer, data processing layer, data association layer, and application layer. The data layer includes the collection of original data, data abstraction, data integration and fusion, and data feature abstraction; the data processing layer includes data mining and fusion; the data association layer is to store the associated data in the cloud space to form a data cloud; the application layer is to conduct a security assessment of the fused data and events and finally send the correct data information to the user.

3. Design of Intelligent Information Aggregation System for Cyber Economic Crime Based on IoT Technology

Cyber economic crimes are very difficult to collect criminal intelligence due to many restrictive factors such as diverse methods, large number of victims, easy destruction of evidence, and complex technology for obtaining evidence. Based on this, this paper proposes using artificial intelligence IoT technology to establish a complete network economic crime information mining system, using related algorithms to match the acquired crime information with the feature vector of the user's needs, extracting the information that meets the requirements, and sending it to the intelligence personnel of the public security department, and then the intelligence personnel will conduct a comprehensive analysis of the information and finally determine its authenticity and reliability.

3.1. Collection of Cyber Economic Crime Intelligence. The Internet has become an important carrier and tool for economic criminal activities. Some criminals use network technology to use information exchange platforms such as QQ, WeChat, and MSN to conduct false online sales and services by registering domain names and establishing web pages to steal user information and conduct MLM and fundraising fraud. Based on this, intelligence collection on cyber economic crimes is mainly concentrated on e-commerce platforms, securities investment forums, and professional information exchange groups.

3.1.1. Economic Crime Intelligence Collection on E-Commerce Platform. Today, with the rapid development of Internet technology, new types of online business activities such as online shopping are becoming more frequent. However, due to the virtual nature of the network economy, it is difficult to avoid a mixed situation. With the occurrence of a large number of online shopping behaviors, online fraudulent activities are becoming more and more rampant. Many websites, dressed in the cloak of e-commerce platforms, secretly steal private information such as bank account

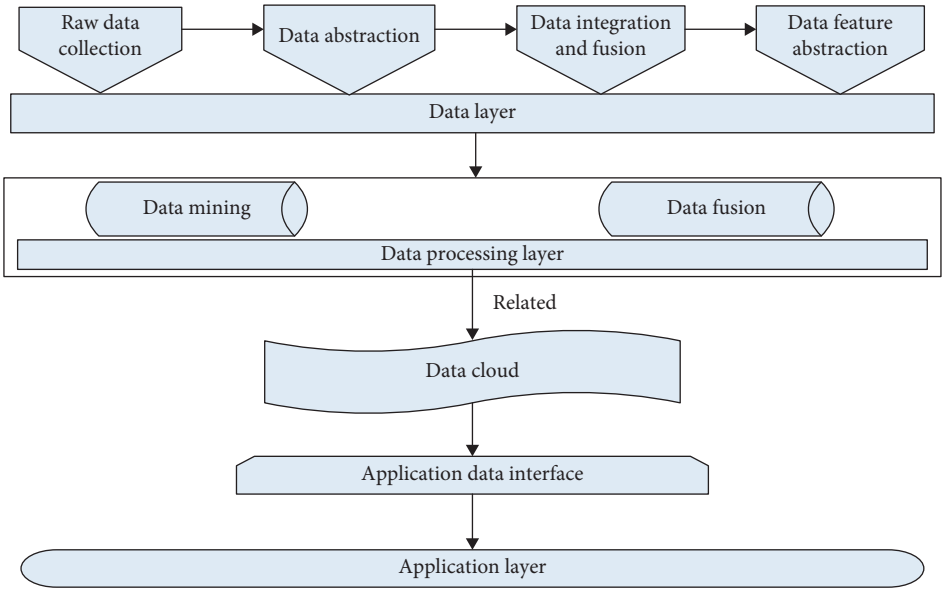

Figure 3: Model diagram of information intelligent aggregation structure.

numbers and passwords submitted by users; some websites conduct fake online merchandise sales. They lure buyers to buy at low prices, and, after the buyers make electronic payments, they actually have no goods at all and will not send any goods to the buyers. Generally, operators of such websites often purchase ID cards, bank cards, and mobile phone cards or QQ numbers online, so their contact methods are in the identity of others. When collecting information on such economic crimes, you should first observe whether the website is legal and whether there is a suspected phishing website; secondly, investigate whether the goods on the website are authentic and reliable; thirdly, observe whether the information on the website is false economic information; finally, observe whether the historical transactions of the website store are normal.

3.1.2. Economic Crime Intelligence Collection on Forums on Securities and Finance Websites. With the popularity and rapid development of the Internet, a great amount of financial information related to securities and finance often appears on the Internet. Although this facilitates people's understanding and learning of financial knowledge and is conducive to people's investment and financial activities, it is also an economic crime. The criminals are provided an opportunity to commit crimes. Criminals publish false advertisements through the Internet's mainstream financial portals to conduct online fund-raising, online pyramid schemes, and online fraud. In the work of intelligence collection, the public security department can monitor the advertising information of mainstream portals, especially the advertising links on the homepage, focusing on the fixed-point and regular monitoring of the advertising information on the homepage of economy, finance, securities, and wealth management to ensure obtaining suspicious information at a time and carry out screening and verification work on suspicious information in a timely manner to quickly and severely crack down on criminals.

3.1.3. Economic Crime Intelligence Collection of Professional Information Exchange Groups. Some criminals use communication groups such as QQ and WeChat to spread false information and toxic links to trick the masses into borrowing or buying equity or commodities. The current cyber economic crime has shifted from a capital-dominant type to an information-dominant type. Many lawbreakers use the Internet to spread false information and turn the money involved in the case to illegally make huge profits. Economic crime intelligence collectors must be good at mining QQ exchange groups or WeChat exchange groups established for the purpose of illegal economic transactions on the Internet. At the same time, because intelligence personnel usually need to be authenticated when accessing exchange groups and social networks, they should be preliminary before collecting criminal intelligence. The work of infiltration is very important. Intelligence personnel must penetrate deeply into the exchange group to collect and study the illegal activities in the group to obtain sufficient criminal evidence.

3.2. Data Mining of Economic Crime Intelligence Information. In combating cyber economic crimes, early intelligence collection is of course important, but the mining and analysis of intelligence information should not be underestimated. The use of data mining technology to mine and process the large amount of economic crime intelligence collected can not only find out the characteristics and laws of economic crime behind the intelligence but also reduce the difficulty of the work of intelligence personnel and public security criminal investigation departments, as well as gaining sufficient time for combating and investigating cyber economic crimes. Today, when cyber economic crimes are becoming more and more rampant, we still use cyber technology to crack down on cyber economic crimes in accordance with the law. Here, this article proposes the use

of data mining and information intelligent aggregation as two technical means: using data mining to fully realize data analysis and using information intelligent aggregation to effectively cluster and sort data and find the law of data hiding, so as to build a comprehensive and efficient intelligence research system to provide help for the criminal investigation work of the public security department.

3.2.1. Data Preprocessing. The information collected from cyber economic crimes is stored in the database. Because the original data cannot be directly applied to data mining, it is necessary to preprocess the data, select clean data, and perform enhanced processing. When data are preprocessed, all the original data are set to a unified format, which contains the criminal's name, gender, age, address, contact information, and other aspects of information. These data are transformed, sorted, decomposed, and summarized, and finally valid data that can be used for mining are obtained.

3.2.2. Improved Apriori Algorithm. Apriori algorithm is a classic data mining algorithm for mining frequent item sets and association rules. Apriori means "from the past" in Latin. When defining a problem, a priori knowledge or hypothesis is usually used, which is called "a priori" (apriori). The name of the Apriori algorithm is based on the fact that the algorithm uses the prior nature of the frequent item sets; that is, all nonempty subsets of frequent item sets must also be frequent. The Apriori algorithm uses an iterative method called layer-by-layer search, where k item sets are used to explore $(k+1)$ item sets. First, by scanning the database, accumulating the count of each item, and collecting items that meet the minimum support degree, find the set of frequent 1 item set. This set is denoted as L1. Then, use L1 to find set L2 of frequent 2 item sets, and use L2 to find L3, and so on, until no more frequent k item sets can be found. Every time an Lk is found, a complete scan of the database is required. The Apriori algorithm uses the a priori properties of frequent item sets to compress the search space.

Based on the previous Apriori algorithm, we once again propose an improved Apriori algorithm. The improved Apriori algorithm reduces the number of scans of the database. The calculation time is reduced, the calculation efficiency is improved, and the mining efficiency of economic crime intelligence information is also improved. The improved Apriori algorithm process is as follows:

Step 1. Set up the relationship matrix. Set vector $H_j = \begin{pmatrix} T_{1j} \\ \cdots \\ T_{nj} \end{pmatrix}$, where T_i is the i transaction; we get

$$T_{ij} = \begin{cases} 0, & I_j \in T_i \\ 1, & I_j \notin T_i \end{cases}, \sup - \operatorname{count}\left(I_j\right) = \sum_{i=1}^{n} T_{ij}. \quad (2)$$

Step 2. Let the matrix of item set 1 be

$$H = \left(H_1, H_2, \ldots, H_n\right) = \begin{bmatrix} d_{11} & \cdots & d_{1n} \\ \cdots & \cdots & \cdots \\ d_{m1} & \cdots & d_{mn} \end{bmatrix}. \quad (3)$$

Step 3. Set the vector of item set 2 to H_{ij}, and let

$$H_{ij} = H_i \wedge H_j = \begin{bmatrix} d_{1i} \wedge d_{1j} \\ \cdots \\ d_{ni} \wedge d_{nj} \end{bmatrix}. \quad (4)$$

Step 4. Set up the binary relationship matrix:

$$H = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ d_{m1} & d_{m2} & \cdots & d_{mn} \end{bmatrix}. \quad (5)$$

Therefore, the support of the j attribute of the item set is $\sum_{k-1}^{m} (r_{kj}/m)$.

3.2.3. K-Means Algorithm. The K-means algorithm is a clustering algorithm. The so-called clustering is to divide data objects with higher similarity into the same cluster according to the principle of similarity and divide data objects with higher dissimilarity into different classes or clusters. The biggest difference between clustering and classification is that the clustering process is an unsupervised process; that is, the data object to be processed does not have any prior knowledge; meanwhile the classification process is a supervised process; that is, there is a training data set with prior knowledge. In the K-means algorithm, k represents the number of clusters, and means represents the average value of the data objects in the cluster (this average is a description of the center of the cluster). Therefore, the K-means algorithm is also called the K-means clustering algorithm. The algorithm flow is as follows:

Step 5. There is a data set D with n data items. Assuming that the data set is clustered into k clusters, the smallest distance between clusters $a(j,q)$ is defined as

$$a(j,q) = \min \frac{\sum_{i=1}^{n_p} \left\| x_i^p - x_j^q \right\|^2}{n_k}, \quad 1 \le p \le k,\ p \ne q. \quad (6)$$

In the above equation, p and q represent cluster items, and i and j represent data items.

Step 6. Set the distance $u(j,q)$ within the cluster to be the average distance from the i data item in the 14th category to all other data samples in the cluster.

$$u(j,q) = \frac{\sum_{i=1, i \ne j}^{n_j} \left\| x_i^q - x_j^q \right\|^2}{n_q - 1}. \quad (7)$$

In the above equation, x_i^q represents the i data item of the q type, where $i \neq j$, and n_j represents the number of items in the j cluster.

Step 7. Let the clustering distance $\mathrm{baw}(j,i)$ of the i data sample of the j type be the sum of the minimum intercluster distance and the intracluster distance of the sample; then

$$baw(j,i) = b(j,i) + u(j,i) = \min \frac{\sum_{i=1}^{n_p} \left\| x_i^p - x_j^q \right\|^2}{n_k} + \frac{\sum_{i=1,i\neq j}^{n_j} \left\| x_i^q - x_j^q \right\|^2}{n_q - 1}, \quad 1 \le p \le k,\ p \neq q. \tag{8}$$

Step 8. Let the clustering distance difference $\mathrm{bsw}(j,i)$ of the i data sample of the j type be the difference between the minimum interclass distance and the intraclass distance of the sample; then

$$bsw(j,i) = b(j,i) - u(j,i) = \min \frac{\sum_{i=1}^{n_p} \left\| x_i^p - x_j^q \right\|^2}{n_k} + \frac{\sum_{i=1,i\neq j}^{n_j} \left\| x_i^q - x_j^q \right\|^2}{n_q - 1}, \quad 1 \le p \le k,\ p \neq q. \tag{9}$$

Step 9. Set BWP as the ratio of the cluster distance difference and the cluster distance sum of the data sample; then

$$\mathrm{BWP}(j,i) = \frac{\mathrm{bsw}(j,i)}{\mathrm{baw}(j,i)} = \frac{\min\left(\sum_{i=1}^{n_p} \left\| x_i^p - x_j^q \right\|^2 / n_k\right) - \left(\sum_{i=1,i\neq j}^{n_j} \left\| x_i^q - x_j^q \right\|^2 / n_q - 1\right)}{\min\left(\sum_{i=1}^{n_p} \left\| x_i^p - x_j^q \right\|^2 / n_k\right) + \left(\sum_{i=1,i\neq j}^{n_j} \left\| x_i^q - x_j^q \right\|^2 / n_q - 1\right)}, 1 p \le k,\ p \neq q. \tag{10}$$

BWP index is based on a certain item in the data as the research object, and the data are effectively evaluated by constructing a geometric matrix to reflect the distance of the cluster structure, and then the number of clusters is determined. When BWP is closer to 1, it means that the clustering result is more correct, and when BWP is closer to −1, it means that the error of the clustering result is larger.

3.3. Construction of an Intelligent Information Aggregation Model for Cyber Economic Crime Intelligence Based on Data Mining. Intelligence is to provide decision-makers and organizations with knowledge about the target object and its surrounding environment. It is a kind of value-added to ordinary information, and information is the basis of intelligence. In traditional intelligence collection and research work, intelligence personnel mainly collect and analyze intelligence through libraries and documentation agencies. This work method is inefficient, is unable to obtain extensive information in time, and cannot effectively study large amounts of intelligence information. With the help of the IoT technology, through the collection of intelligence information by smart sensors, the mining and processing of intelligence information by data mining technology, and the cluster analysis of intelligence information by information intelligent aggregation technology, intelligence personnel can quickly obtain cyber economic crimes. With the help of the Internet of Things technology, intelligence information is collected through smart sensors, intelligence information is mined and processed through data mining technology, and intelligence information is clustered and analyzed through information intelligence aggregation technology, and intelligence personnel can quickly obtain cyber economic crime information, timely and effectively analyze the first-hand criminal investigation information and related information data, quickly locate criminal information, greatly shorten the criminal investigation time, and improve the efficiency of solving cases. The intelligent aggregation system is based on a computer framework and uses cloud computing and big data technology. When the criminal's criminal behavior is determined, it uses video surveillance, sensor technology, and GPS positioning technology to find out the criminal's precise location and then accurately captures it. According to the IoT technology used, this paper designs and constructs a data-mining-based intelligent information aggregation model of cyber economic crime intelligence, as shown in Figure 4.

4. Application and Realization of Intelligent Information Aggregation System for Cyber Economic Crime Intelligence

According to the previous article, we used the Apriori algorithm and the improved Apriori algorithm to conduct data mining on cyber economic crime intelligence information and used the K-means algorithm to aggregate and analyze the intelligence information and therefore established an intelligent information aggregation system for

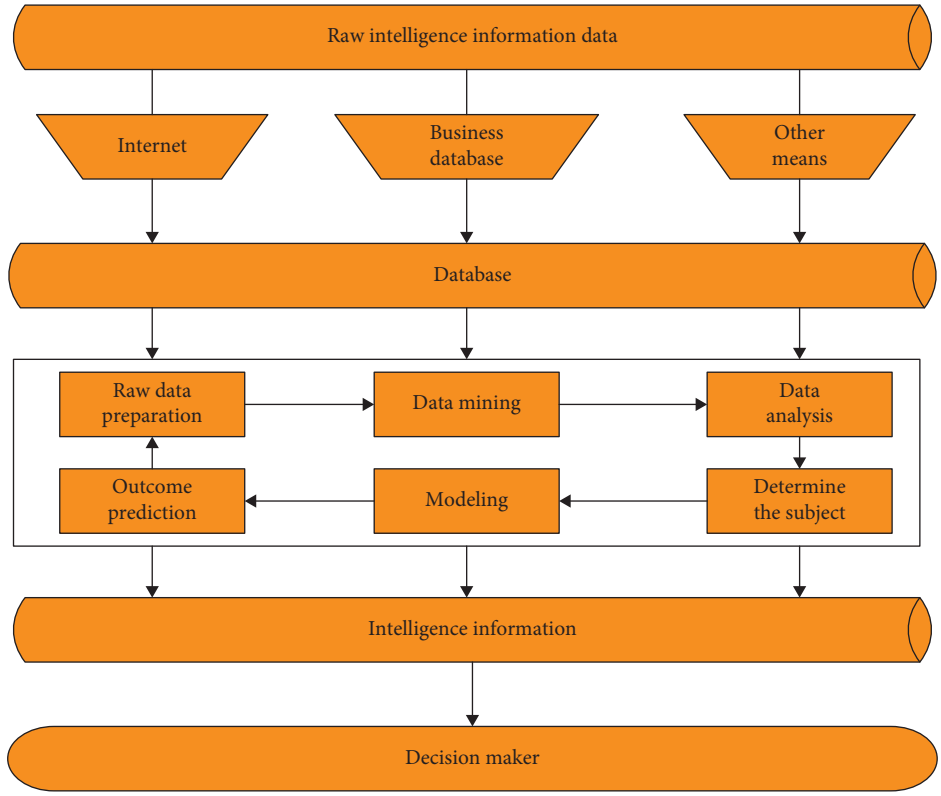

Figure 4: Intelligent aggregation model of cyber economic crime intelligence information based on data mining.

cyber economic crime intelligence. In order to test the performance and effect of the intelligent information aggregation system of cyber economic crime intelligence designed and constructed in this article, it will better assist the public security department in investigating and combating cyber economic crime activities. In this chapter, we will use examples to analyze the system.

4.1. Overview of Cyber Economic Crime Cases in Cities in Our Province in 2019. According to relevant data, in 2019, our province broke 9576 online economic crime cases, including 2792 in city A, 851 illegal fund-raising frauds, accounting for 30.47% of the city's total, and 679 credit card frauds using the Internet, accounting for 24.31%. There were 636 cases of illegal online operations using the Internet, accounting for 22.77%, and 626 cases of using the Internet to commit intellectual property infringement crimes, accounting for 22.45%; there were 2193 cases in city B, with 572 cases of illegal fund-raising fraud, accounting for 26.08% of the city's total. There were 515 credit card fraud cases, accounting for 23.48%, 678 cases of illegal online business operations using the Internet, accounting for 30.91%, and 428 cases of intellectual property infringement crimes using the Internet, accounting for 19.53%; there were 1910 cases in city C, with 474 cases of illegal fund-raising fraud, accounting for 24.81% of the city's total, 571 credit card frauds using the Internet, accounting for 29.89%, 424 illegal online operations using the Internet, accounting for 22.19%, and 441 crimes of infringing intellectual property rights using the Internet, accounting for 23.11%; in city D, there were 2,681 cases of illegal fund-raising fraud, accounting for 27% of the city's total, with 572 cases of credit card fraud using the Internet, accounting for 21.33%, and 709 cases of illegal online business using the Internet, accounting for 26.44%. There were 676 crimes in the use of the Internet to infringe intellectual property rights, accounting for 25.23%. The specific situation is shown in Table 1 and Figure 5.

4.2. Data Mining and Analysis of Cyber Economic Crime Intelligence. The intelligent information aggregation model of cyber economic crime intelligence designed and constructed in this article is used to conduct data mining and analysis on the cyber economic crime case intelligence database in 2019, the characteristics of criminals are extracted, and the law and methods of such economic crimes are summarized. First of all, we selected part of the data in the Internet economic crime case database of the public security economic investigation department as the sample data for this test. The sample data include the criminal's name, gender, age, education, hometown, family situation, and criminal history. Then, using the model, the Apriori algorithm and the K-means algorithm are used to mine and aggregate the sample data.

4.2.1. Basic Situation of Cyber Economic Criminals. The relevant data information of 9 criminals from the database are selected for analysis, and the minimum confidence is calculated. The results are shown in Table 2.

Table 1: Overview of cyber economic crime cases in each city in our province in 2019.

	Illegal fund-raising fraud	Credit card fraud	Illegal business online	Infringement of intellectual property rights
City A	851	679	636	626
City B	572	515	678	428
City C	474	571	424	441
City D	724	572	709	676

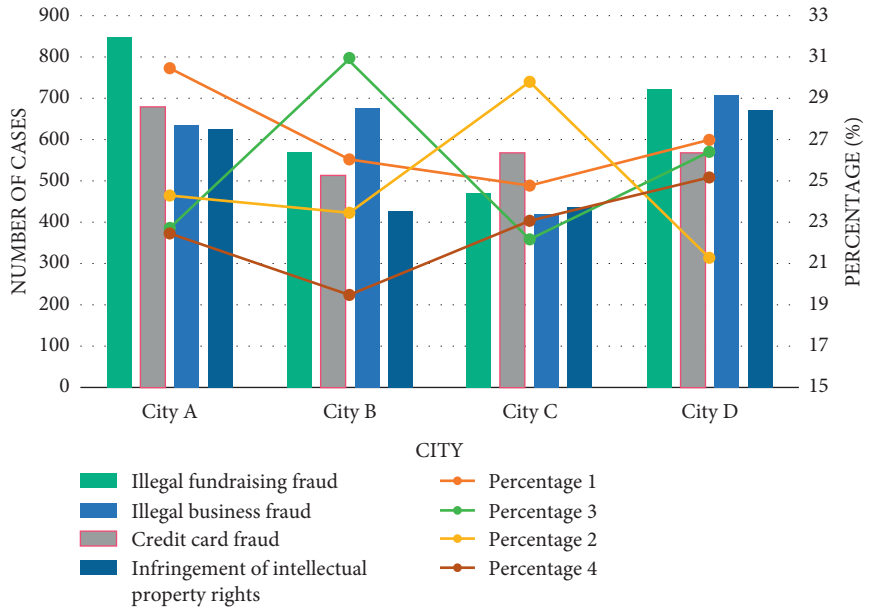

Figure 5: The number and proportion of online economic crime cases in each city in our province in 2019.

Table 2: Basic situation of cyber economic criminals.

	Gender	Education	Hometown	Family situation	Criminal history	Minimum confidence
A	Man	High school	This province	Have a history	Theft	0.78
B	Man	High school	This province	Have a history	Robbery	0.66
C	Man	Undergraduate	Other places	Good	Gambling	0.78
D	Man	Other places	Other places	Good	Robbery	0.64
E	Woman	Junior high school	This province	Parents divorced	Theft	0.72
F	Man	High school	Other places	Good	Economic crime	0.69
G	Woman	Junior high school	Other places	Parents divorced	Theft	0.88
H	Man	Junior high school	This province	Good	Economic crime	0.79
I	Man	Junior college	This province	Family member seriously ill	Robbery	0.68

According to Table 2, among the 9 cyber economic criminals, the majority are young people, most of whom have high school education, and most of them are from other places. Among these people, there are divorced parents, people with criminal records, and family members who are seriously ill. The offenders also have criminal records, mainly theft and robbery, and two have economic criminal records. According to the calculated minimum confidence level, the confidence level of criminal G is the highest at 0.88, and the confidence level of D is the lowest at 0.66. According to the minimum confidence standard, the confidence levels of these 9 cyber economic criminals meet the requirements, which shows that the education, family situation, and criminal history are related to the cyber economic crimes.

4.2.2. Detailed Information about the Criminals' Cyber Economic Crime. The proportion of cyber economy crimes in each city in our province and the type of crime of cyber economy criminals, crime time, number of crimes, and amount involved are recorded. The results are shown in Figures 6–8.

It can be seen from Figure 6 that, in 2019, cyber economic crimes in our province accounted for 4.79% of the country's cyber economic crimes. Among them, cyber economic crimes in city A accounted for 29.15% in the province, those in city B accounted for 22.90%, and those in city C accounted for 19.94%. City D accounted for 28.01%, and city A had the highest cyber economy crime rate.

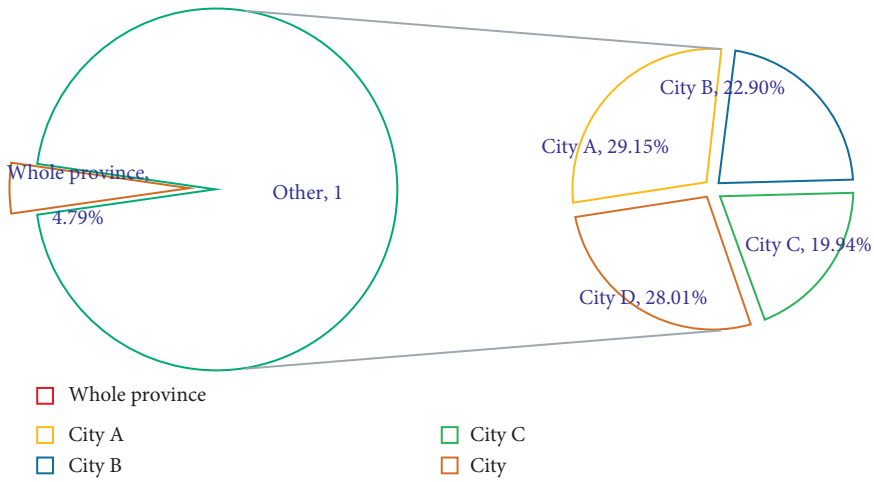

Figure 6: Proportion of cyber economic crimes in our province and cities.

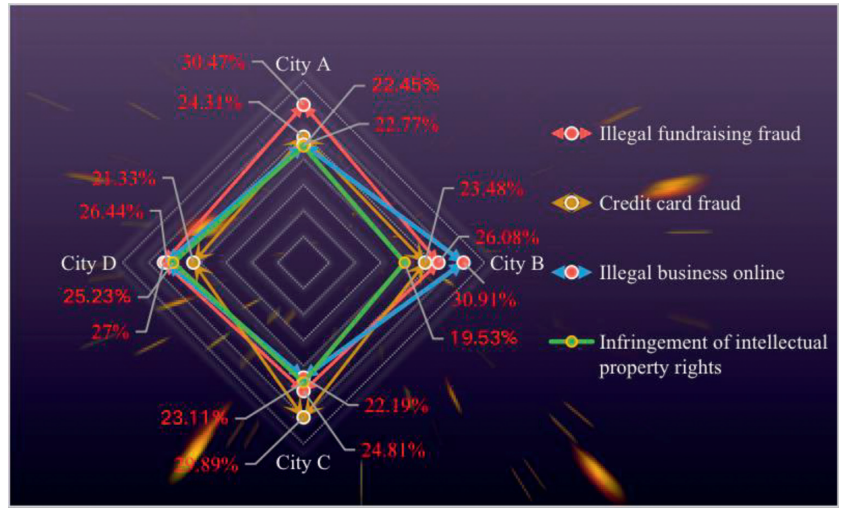

Figure 7: Proportion of forms of online economic crimes in various cities in our province.

As can be seen from Figure 7, the four cities A, B, C, and D all use the Internet to raise funds and use the Internet for credit card fraud. The second is to use the Internet for online illegal operations. Among them, the economic crimes of illegal fund-raising in city A accounted for 30.47% of the city's cyber economic crimes, ranking the highest among the four cities, followed by city D with 27%; credit card fraud in city C accounted for 29.89% of the city's cyber economic crimes, and city A and city B followed closely behind, accounting for 24.31% and 23.48%, respectively; online illegal operations in city B accounted for 30.91% of the city's cyber economic crimes, and city D accounted for 26.44%; in contrast, the use of the Internet to commit crimes of infringement of intellectual property rights represented fewer types of economic crimes, with city D being the highest, accounting for 25.23%, while city B occupied 19.53%.

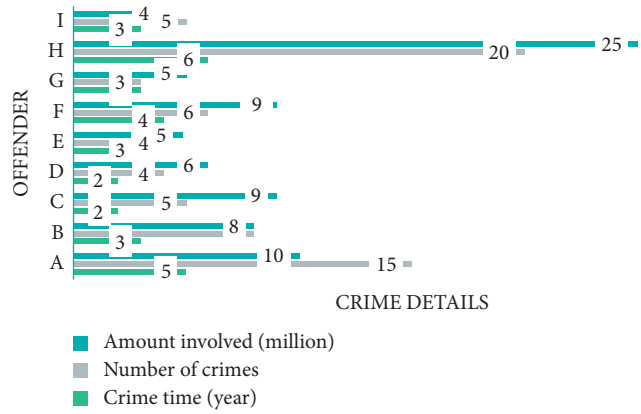

Figure 8: Crime details of cyber economy criminals.

It can be seen from Figure 8 that, in the selected sample data, most of the 9 cyber economic criminals have committed crimes between 2 and 6 years, and the number of crimes ranged from 3 to 20. Among them, criminal H has the biggest number of crimes. In 6 years, the number of crimes reached 20 times, followed by criminal A who committed 15 crimes in 5 years. The amount involved in the case is also the

largest with criminals H and A, reaching 25 million and 10 million, respectively, while criminal I, with the smallest amount involved, has 4 million.

In summary, by taking the cyber economic crime cases uncovered by the provincial public security economic investigation department in 2019 as an example, the criminal intelligence information of 9 criminals, A, B, C, D, E, F, G, H, and I, is selected as sample data, using the network economic crime intelligence intelligent information aggregation system designed and constructed in this article to mine and aggregate the sample data, and it was found that the network economic crime behavior has a certain relationship with the criminal's academic background, family situation, and criminal history. In addition, the test results show that illegal fund-raising fraud and credit card fraud using the Internet are currently the most important forms of online economic crimes. Therefore, the public security economic investigation department can strictly prevent and crack down on these economic crimes. This article uses the IoT technology to design and build an intelligent information aggregation system for network economic crime intelligence. After testing, it has proved its superiority and effectiveness. It can effectively assist the work of the public security economic investigation department and is worthy of application and promotion.

5. Conclusions

While China's Internet technology is booming, Internet crimes have also been accompanied, especially in recent years, by Internet economic crimes. Internet economic crimes mainly include illegal fund-raising, the use of the Internet for credit card fraud, the use of the Internet for illegal operations, and the use of the Internet for infringement of intellectual property rights. Due to the virtuality and complexity of the online world, it is very difficult for the public security departments to investigate such cases. Therefore, the early intelligence collection of cyber economic crimes is very important.

Traditional methods of intelligence gathering mainly rely on intelligence personnel to access documents and past archives. Not only does this method require a lot of work but also it is very inefficient. Based on this, this article proposes using artificial intelligence IoT technology to replace manual collection of intelligent information with intelligent sensors and using data mining technology and intelligent information aggregation methods to conduct data mining and aggregation analysis of intelligent information to find out the laws and characteristics of cyber economic crimes. With the popularization and application of Internet of Things technology, it will inevitably promote the development of social management in the direction of intelligence. Intelligent information aggregation system is an inevitable choice for the development of social management and a revolution in social management. Through the effective integration and application of advanced information technology, cloud computing technology, control technology, sensing technology, computer network technology, and system integration technology, the interaction between people, society, and public security managers can be presented in a new way, so as to achieve the goal of a real-time, efficient, and safe harmonious society.

This study has applied and tested the designed and constructed intelligent information aggregation system of cyber economic crime intelligence by enumerating examples, and the results have confirmed the excellent performance of the system, which is of great help to assist the work of the public security economic investigation department. However, in order to apply the intelligence system to criminal investigation work in other criminal fields, it is necessary to continue improving system functions.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author declares that there are no conflicts of interest with any financial organizations regarding the material reported in this manuscript.

References

[1] L. Wu, "Research on the application of IOT technology in intelligent logistics management," *Journal of Heihe University*, vol. 9, no. 7, pp. 219-220, 2018.

[2] J. Zhang and K. B. Letaief, "Mobile edge intelligence and computing for the Internet of vehicles," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 246–261, 2020.

[3] W. Park, O. Na, and H. Chang, "An exploratory research on advanced smart media security design for sustainable intelligence information system," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 1–12, 2016.

[4] I. Kitouni, D. Benmerzoug, and F. Lezzar, "Smart agricultural enterprise system based on integration of Internet of things and agent technology," *Journal of Organizational and End User Computing*, vol. 30, no. 4, pp. 64–82, 2018.

[5] M. N. Aladwan, F. M. Awaysheh, S. Alawadi, M. Alazab, T. F. Pena, and J. C. Cabaleiro, "TrustE-VC: trustworthy evaluation framework for industrial connected vehicles in the cloud," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6203–6213, 2020.

[6] A. Yeboah-Ofori, "Cyber intelligence and OSINT: developing mitigation techniques against cybercrime threats on social media," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 1, pp. 87–98, 2018.

[7] A. M. Al-Momani, M. A. Mahmoud, and M. S. Ahmad, "Factors that influence the acceptance of Internet of things services by customers of telecommunication companies in Jordan," *Journal of Organizational and End User Computing*, vol. 30, no. 4, pp. 51–63, 2018.

[8] G. Aceto, V. Persico, and A. Pescape, "A survey on Information and Communication Technologies for Industry 4.0: state of the art, taxonomies, perspectives, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 99, pp. 3467–3501, 2019.

[9] H. Chai and J. Jin, "Research and application of urban regional health information platform based on 3S," *Medical Information*, vol. 30, no. 15, pp. 20-21, 2017.

[10] S. Namasudra and P. Roy, "PpBAC," *Journal of Organizational and End User Computing*, vol. 30, no. 4, pp. 14–31, 2018.

[11] R. Zhang, "Research and application of intelligent anti-stealing electricity based on electricity information data mining," *Value Engineering*, vol. 35, no. 35, pp. 51–54, 2016.
[12] K. Kim, G. J. D. Hewings, and K. Kratena, "Household disaggregation and forecasting in a regional econometric input-output model," *Letters in Spatial and Resource Sciences*, vol. 9, no. 1, pp. 73–91, 2016.
[13] Z. Zhang, Y. Weng, and J. Jiang, "The application of intelligent transportation technolo-gy guided by modern information technology in beijing metro," *China Basic Science*, vol. 020, no. 6, pp. 6–10, 2018.
[14] D. S. P. Rao and G. Hajargasht, "Stochastic approach to computation of purchasing power parities in the International Comparison Program (ICP)," *Journal of Econometrics*, vol. 191, no. 2, pp. 414–425, 2016.
[15] R. Parada, J. Melià-Seguí, and R. Pous, "Anomaly detection using rfid-based information management in an iot context," *Journal of Organizational and End User Computing*, vol. 30, no. 3, pp. 1–23, 2018.
[16] M. Faggini and A. Parziale, "More than 20 years of chaos in economics," *Mind & Society*, vol. 15, no. 1, pp. 53–69, 2016.
[17] A. Jeavons, "What is artificial intelligence?" *Research World*, vol. 2017, no. 65, p. 75, 2017.
[18] L. Zhang, X. Gao, and X. Xu, "Fault diagnosis for rolling bearings with stacked denoising auto-encoder of information aggregation," *Journal of Harbin Institute of Technology: English Edition*, vol. 026, no. 004, pp. 69–77, 2019.
[19] Z. Wu, "Public information and information aggregation in committees," *Economic Papers Series*, vol. 47, no. 3, pp. 321–361, 2019.
[20] D. Preuveneers and E. Ilie-Zudor, "Introduction to the thematic issue on Intelligent systems, applications and environments for the industry of the future," *Journal of Ambient Intelligence and Smart Environments*, vol. 9, no. 3, pp. 285-286, 2017.
[21] P. Singh and R. Agrawal, "A customer centric best connected channel model for heterogeneous and iot networks," *Journal of Organizational and End User Computing*, vol. 30, no. 4, pp. 32–50, 2018.
[22] D. W. Mckee, S. J. Clement, J. Almutairi, and J. Xu, "Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 75–82, 2018.
[23] S. Gupta and B. B. Gupta, "Evaluation and monitoring of XSS defensive solutions: a survey, open research issues and future directions," *Journal of ambient intelligence and humanized computing*, vol. 10, no. 11, pp. 4377–4405, 2019.
[24] W. U. Hong-wei, "Application of intelligent technology in automation system," *Digital Technology and Application*, vol. 36, no. 12, pp. 11-12, 2018.
[25] Y. Wang, J. Liu, S. Mandal, and C. Shah, "Search successes and failures in query segments and search tasks: a field study," *Proceedings of the Association for Information Science and Technology*, vol. 54, no. 1, pp. 436–445, 2017.