Dynamic Monitoring System of Big Data Leakage in Mobile Network Based on Internet of Things

Yan-ning Zhang and Ying-jian Kang(✉)

Beijing Polytechnic, Beijing 100016, China
witgirl_ninger@126.com, kangyingjian343@163.com

Abstract. Aiming at the problem of large acquisition time synchronization error caused by data explosion in traditional monitoring systems, a dynamic monitoring system for mobile network big data leakage based on Internet of Things is designed. The wireless sensor network is arranged in the system, the multi-channel base station node is designed, and the sensors are arranged in different channels to achieve the purpose of data diversion. Ep3c16q240 chip is selected as the core control chip of the multi-channel base station node, Based on the above hardware design, cluster monitoring, node performance monitoring and job operation monitoring functions are designed to upload the big data status information of the mobile network for job operation monitoring step by step to meet the needs of dynamic monitoring of data leakage. So far the overall design of the system is completed. The experimental results show that: compared with the traditional monitoring system, the designed monitoring system based on the Internet of things has smaller acquisition time synchronization error, better data acquisition synchronization performance, and improves the dynamic monitoring accuracy of mobile network big data leakage.

Keywords: Internet of Things · Mobile network · Big data leakage · Dynamic monitoring

1 Introduction

As an important milestone in the modern history of human development, the Internet is a symbol of human innovation and wisdom, and an important symbol of the rapid development of science and technology [1]. From its emergence to the present, the Internet has brought great changes to the industry and life of the whole world. It not only realizes many people's entrepreneurial dream, but also makes people's life inseparable and mutual influence. It also makes great changes in the organizational structure of the society [2]. The Internet has a wide and far-reaching impact, people's lives have become more convenient, and the ways of disseminating information have also become diverse. With the rapid development of science and technology, the development of the Internet has always maintained a relatively fast level. With the rapid development of the scale of the network, the services provided by the network are also diversified, which greatly facilitates people's lives [3]. The development of the Internet has become more in-depth, especially the development of mobile clients has

S. Liu and L. Xia (Eds.): ADHIP 2020, LNICST 347, pp. 134–146, 2021.
https://doi.org/10.1007/978-3-030-67871-5_13

profoundly changed the lives of Internet users. With more and more mobile applications such as mobile banking, train ticket ordering and takeaway ordering entering mobile clients, the Internet has begun to fully meet the needs of users, making people's life increasingly "networked" [4].

In the first decades after the emergence of computer network, it was mainly used by University researchers to send e-mails and by company employees to share printers. In these cases, security will not be noticed [5]. Nowadays, millions of ordinary people use the Internet. What we want to do in the real world is to be done on the Internet; make private calls, save personal documents, sign letters and contracts, vote online, electronic publishing, and handle Banking and shopping require security protection [6]. Network security is the basic condition for the existence of the Internet, which makes the computer network from an important business tool of academic concern. Security limitations have also become the limitations of the Internet [7]. Security vulnerabilities have been discovered one after another, and network security has become a hot topic that people pay close attention to. At this time, facing the problem of big data leakage in mobile networks, it is particularly important to introduce a monitoring mechanism into the network security management summary and establish a powerful dynamic monitoring system for big data leakage in mobile networks [8]. Using this monitoring mechanism, the data security of mobile network can be monitored in real time, and the abnormal situation such as data leakage can be warned. In case of failure, the management personnel should be informed in time after the problem occurs, so as to ensure the data security of mobile network.

In previous research, there are many mature monitoring technologies and open source monitoring systems in foreign countries. The monitoring system can provide information data about the network and system operating status, and also provide abnormal notification functions. Both local and remote servers can be monitored. Only need to modify the configuration file [9, 10]. At present, facing the problem of data leakage in mobile network, many domestic enterprises begin to study cloud computing and study different big data monitoring solutions. Obvious results are ZigBee-based monitoring system and web-based monitoring system. However, in the face of the current state of data explosion, the above two systems are difficult to ensure the synchronization of data collection, and there is a problem of large synchronization error in collection time. In view of this phenomenon, this paper proposes and designs a mobile network big data leakage dynamic monitoring system based on the Internet of things. The hardware of the monitoring system is designed. Ep3c16q240 chip is selected as the core control chip of multi-channel base station node. On the basis of hardware design, the system software is designed, including cluster monitoring function, node performance monitoring function and operation monitoring function Through the system hardware design and software design, the mobile network big data leakage dynamic monitoring system design based on the Internet of things is completed, which reduces the acquisition time synchronization error, improves the mobile network big data leakage dynamic monitoring accuracy, and improves the data acquisition synchronization performance.

2 Hardware Design of Dynamic Monitoring System for Mobile Network Big Data Leakage Based on Internet of Things

Internet of things technology is to connect any object with the network through information sensing equipment, according to the agreed protocol, and to exchange and communicate information through information media, so as to realize intelligent supervision and other functions [11, 12]. The wireless sensor network is adopted in the monitoring system, multi-channel base station nodes are designed, and the sensor nodes are arranged in different channels to realize data exchange monitoring. The node arrangement in the monitoring system using the Internet of Things technology is shown below (Fig. 1).

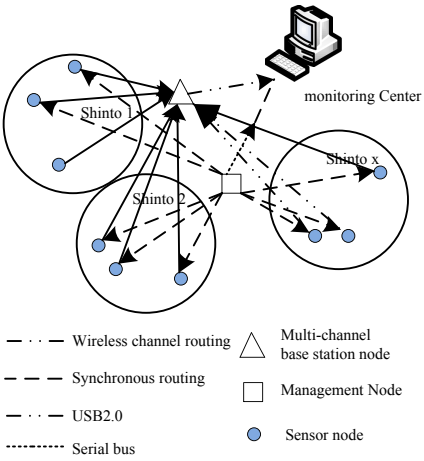

Fig. 1. Node layout of monitoring system

The multi-channel base station node and the monitoring center are connected through the USB2.0 bus, which can meet the requirement of simultaneously uploading 8 wireless channels of data to the monitoring center at a high speed and complete [13, 14]. The network data transmission rate is doubled from the original 250 Kbps of a single channel. Can reach 2 Mbps. The speed of USB2.0 bus can reach more than 12 Mbps, which can solve the problem of throughput limitation caused by using serial port.

The hardware structure of the designed multi-channel base station node is shown in Fig. 2.

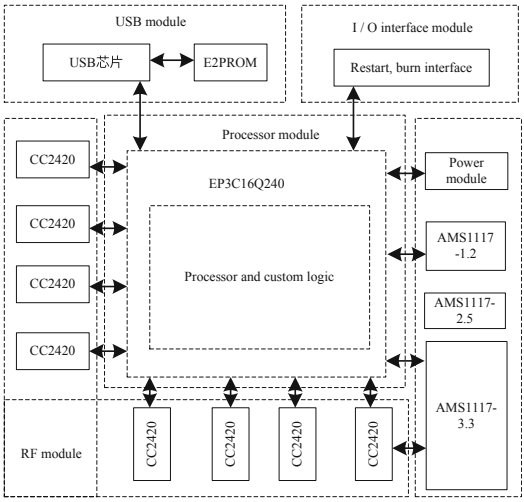

Fig. 2. Hardware structure of multi-channel base station node

The hardware of the multi-channel base station node includes FPGA chip, USB chip, 8 independent CC2420 radio frequency modules, electrically erasable programmable read-only memory chip, power management module, clock module and peripheral circuits of each chip. Among them, 8 RF modules, each pin of USB chip and part of FPGA chip can be connected with I/O pin, and functional configuration of available I/O pin of FPGA chip can be realized through program, so as to realize the operation of PLD module on RF module and communication module. The CC2420 radio frequency module is responsible for receiving and sending wireless data, and its initial configuration and work are controlled by the FPGA chip. Multiple CC2420 RF modules are used to receive data in different channels in parallel, and there is no competitive interference between them. After the USB chip is powered on and initialized, the data stream is uploaded under the control of FPGA chip.

FPGA is the product of further development based on programmable array logic, general array logic GAL, complex programmable logic devices and other programmable devices. It appears as a semi-custom circuit in the field of special integrated circuits, which not only solves the shortcomings of custom circuits, but also overcomes the shortcomings of the limited number of gates of original programmable devices. Considering the universality of multi-channel base station node design, FPGA chip selection mainly investigates Altera's products, which produce general-purpose FPGA chips. The research contents include FPGA chip selection manual, chip manual and online quotation provided by Altera. Research shows that Altera's main products include low-end chip series (cyclone IV Series), middle end chip series (ARIA Series), etc. With the further introduction of the series products, the Cyclone series can provide more available pins and memory cells, and further reduce the static power consumption, which can achieve the function of a multi-channel base station node, and the cost is significantly lower than the Arria series chips. Through the analysis, the multi-channel base station node needs more available I/O pins and logic units, so choose the

appropriate FPGA chip as the processing core chip of cyclone II series and cyclone III series multi-channel base station nodes. The comparison of the specific parameters between the cyclone II series and the cyclone III series is shown in Table 1.

Table 1. Cyclone II and Cyclone III series chip parameters

Model logical unit RAM unit PLL module available I/O pins	Model logical unit RAM unit PLL module available I/O pins	Model logical unit RAM unit PLL module available I/O pins	Model logical unit RAM unit PLL module available I/O pins	Model logical unit RAM unit PLL module available I/O pins
EP2C5	4.608	119.808	2	142
EP2C8	8.256	165.888	2	138
EP2C20	18.752	239.616	4	142
EP3C5	5136	423936	2	106
EP3C10	10320	423936	2	106
EP3C16	15408	516096	4	160
EP3C25	24624	608256	4	148

Considering the actual application of monitoring, we must complete the configuration of the USB chip function, control the USB chip to realize the function of uploading data at high speed; obtain the status of the RF module in real time, and control the 8 RF modules to complete the data receiving operation in parallel at high speed according to the reception status of the data packet; Encapsulate and verify the received data packets, and use the HDLC mechanism to parse the data packets to ensure that the host computer program can be completed at high speed; CRC verification mechanism is adopted to ensure the correctness of data packets uploaded to the monitoring center. In conclusion, the ep3c16q240 chip of the cyclone III series is selected as the core chip of the multi-channel base station node.

3 Software Design of Dynamic Monitoring System for Big Data Leakage in Mobile Network

Based on the above hardware design, the software part of the monitoring system is designed. The dynamic monitoring of big data leakage in mobile network can be divided into three levels: cluster monitoring, node performance monitoring and job operation monitoring.

Managing and scheduling nodes is an important part of big data clusters. Whether the cluster is operating well or not directly determines the efficiency of the entire cluster, so the system needs to monitor and manage the various information resources of each node in real time. The administrator can adjust the cluster in real time according to the cluster performance, improve the cluster bottleneck, and ensure the good operation of the job.

The cluster monitoring agent is mainly responsible for the collection of monitoring index data of the cluster. For cluster monitoring, you can view the cluster status information, the total number of machines in the cluster, cluster users, host groups and other information. The acquisition of cluster performance data is mainly achieved through the command line. Such as uptime: view the load of the machine, output the number of processes waiting for CPU resources and the number of processes blocked in uninterruptible IO; mpstat-pall: display the occupancy of each CPU; pidtat1: CPU output of continuous output process will not cover before the data.

The cluster monitoring plug-in is mainly responsible for receiving the monitoring indicator data sent by the agent process. When monitoring the cluster, the implementation process of the plug-in process is to use the Icings expansion mechanism to encapsulate the command to receive cluster performance data, and follow Icings' custom plug-in expansion mechanism to form a plug-in, change the Icings configuration file, and plug the plug-in Deployed on Icings server. Restart the icings service to view the cluster performance indicators.

Node performance monitoring is mainly to monitor the underlying nodes and collect various performance indicators, so that managers can timely and comprehensively grasp the performance information of cluster nodes. The node performance monitoring module is mainly completed by Icinga. Node performance monitoring agent is mainly responsible for collecting node performance data and data processing, including performance monitoring data collection module and performance monitoring data processing module.

The monitoring data collection module includes monitoring of public services and monitoring of private services. For public service monitoring, you can access by using some standard protocols of the public network, such as HTTP, POP3, IMAP, FTP, and SSH. Some Icinga's own plug-ins can directly collect performance data. As a result, agents do not need to be installed on nodes to monitor these services. Private service is the opposite of public service. Private service cannot be accessed through the public network. Information cannot be accessed directly through the network. Therefore, when monitoring private services, the corresponding agent must be installed on the monitored object.

In the performance monitoring data receiving module, after the Icinga agent returns the performance index data, Icinga supports two methods to process the performance data, that is, use the command line to process or write directly to a specific file, which can be configured through the configuration file. If the first method is used, define the processor of plug-in performance data in the icinga configuration file. After executing the plug-in, execute the performance data processor. At this time, the performance processor obtains the data from the environment variables. Icinga starts the plug-in through the command line to perform the corresponding status check, and then captures the standard output stream of the plug-in to obtain the results after execution. The plug-in The execution result of icinga includes at least one line of readable text to represent the current state, and the performance data related to the plug-in is also included in the result. If the second method is used, icinga can directly put the obtained performance data into the performance data file, use the component to process the file, or configure a command in icinga to periodically process the performance data file.

Job operation monitoring is an important part of the monitoring system, and the monitoring object is the mobile network data of operation status. Job monitoring includes data acquisition module, data processing module and data sending module. The object of data collection is the logs generated during the operation of the mobile network. IDEA packages the executable shell code and the dependent jar packages through submit, generates the corresponding jar files, and submits them to the cluster through the command line. For tasks, save the running logs in the work directory, and create a new folder for each task to save its log files and dependent jar packages. The status information of mobile network big data can be obtained from the log.

After the data collection is completed, the data is filtered and extracted, stored in a certain data structure, and completed by the agent resident on the cluster node. In the data processing module, the user calls the data processing function module after the performance data collection. First, the mobile network operation task generates logs, which are stored in the work folder. Using the log collection method based on text analysis, readfile analyzes and processes the collected logs, and obtains the task Ido of the operation task Readformfile processes the collected logs, extracts the running indicators of each task, including monitoring indicators such as user, start time, duration, running status information, and stores them in a predetermined data structure. In SNMPUtilSend, all monitoring indicators are aggregated to form an SNMP data packet, ready to be sent.

The data sending module uses the event driven mechanism to send monitoring information through SNMP. It does not need the monitoring server to poll, saves bandwidth and server utilization, and provides system performance. So far, the design of a dynamic monitoring system for mobile network big data leakage based on the Internet of Things is completed.

4 Experimental Research on Dynamic Monitoring System of Big Data Leakage in Mobile Network

In order to verify the time synchronization effect of the mobile network big data leakage dynamic monitoring system, a time synchronization effect function verification experiment platform was built. In the experiment, the monitoring system is used to collect the fixed frequency waveform generated by the signal generator in real time. After the experiment, the acquisition time synchronization error of the sensor node is obtained by analyzing the collected data, and then the acquisition synchronization performance of the traditional monitoring system and the designed mobile network big data leakage dynamic monitoring system is compared.

4.1 Experimental Scheme Design

It is found that most of the experiments are based on computer simulation. In addition, based on the experimental platform of wireless sensor network for structural health monitoring, foreign researchers have verified the synchronization effect of network acquisition. The experimental method they used was to use a signal generator to generate a fixed-frequency waveform for the sensor network to collect, and then

analyze the data collected by all nodes. Based on this method, an experimental method based on standard waveform acquisition is designed to verify the synchronization performance of the monitoring system.

The equipment used in the experiment included 16 Telosb sensor nodes, a dual RF relay node, management node, AFG3021 arbitrary waveform generator and laptop. Afg3021 arbitrary waveform generator has 14 bit output accuracy. Among them, 16 nodes are divided into 8 different channels. In the experiment, the AFG3021 arbitrary waveform generator was set to generate a standard signal under test for 16 nodes to collect. The waveform generated by the measured signal is set as a triangular wave signal, and the output end is connected to the ADCO and GND pins of 16 nodes with multiple leads. The voltage range of the output waveform is 0-two point five 5. To meet the allowable range of voltage input of AD sampling channel of telosb node and avoid damaging telosb node. The slope of the rising edge of the output triangle wave is set to 300 V/s. Since the AD sampling accuracy of the Telosb node is 12 bits, the range of the AD sampling value can be calculated from 0 to 4960. The reference voltage selected by the Telosb node is 2.5 V, and the voltage resolution calculation formula is as follows:

$$P = \frac{1}{\mu} \times 2.5\,V \tag{1}$$

In the formula, μ represents the AD sampling value. According to the above formula, when the AD sampling value changes by 1, the measured voltage value correspondingly changes by P. Therefore, when the AD sample value changes by 1, the corresponding time change on the rising edge of the output waveform is calculated as follows:

$$t = \frac{P}{\kappa} \tag{2}$$

Where κ is the slope of the rising edge of the output waveform. When multiple sensor nodes collect data at the same time, if the collection time is fully synchronized, the data collected from the same serial number data should be consistent. When there is a sequential error at the node's collection time, you can use the AD sampling values collected by different nodes in the same collection cycle to calculate the voltage value collected at this time and the average collection voltage value of all sensor nodes. Then, the voltage value collected by each node is subtracted from the average voltage value, and the time synchronization error of the node relative to the average sampling time is calculated using the formula. The formula is as follows:

$$\triangle t = \frac{\triangle V}{\kappa} \tag{3}$$

In the formula, $\triangle V$ represents the difference between the collected voltage value and the average voltage value.

The entire experiment lasted 2 h. Before the experiment, turn on the arbitrary waveform generator, adjust the output waveform accurately according to the set value, connect the positive voltage output terminal to the ADCO pins of all sensor nodes, and connect the negative voltage output terminal to the GND pins of all sensor nodes. After the experiment starts, the host computer control management node sends a start command to all sensor nodes to start monitoring the network. During the working process, the management node synchronizes the collection time of all sensor nodes in the network according to its own program. The base station node in the monitoring system receives the data packet sent by the sensor node in real time and uploads it to the upper computer for storage, waiting for the end of the experiment for analysis.

4.2 Experimental Results and Analysis

After the experiment, according to the package number of the data package stored in the upper computer, select three time points randomly, record the AD sampling values collected by all sensor nodes at the three time points, and convert them into voltage values, as shown in the table below.

Table 2 shows the experimental measurement data of the proposed physical network-based mobile network big data leakage dynamic monitoring system, and the synchronization effect cannot be intuitively seen. For this reason, the measurement data of the other two monitoring systems are not listed one by one, directly Compare the time error jitter and synchronization effect measurement results. The experimental results of the traditional ZigBee Based monitoring system are as follows (Table 3).

Table 2. Synchronous effect experimental measurement data

Node number	Measuring voltage (V)		
	1	2	3
3	1.1684	1.2019	1.3412
6	1.1721	1.2341	1.3681
9	1.1745	1.2471	1.3124
11	1.1617	1.2036	1.3369
13	1.1702	1.2571	1.3154
15	1.1629	1.2347	1.3274
17	1.1794	1.2367	1.3096
19	1.1624	1.2903	1.3264
21	1.1454	1.2036	1.3746
22	1.1564	1.2461	1.3091
23	1.1754	1.2412	1.3325

Table 3. Synchronization effect analysis of monitoring system based on ZigBee

Index	Measuring voltage		
	1	2	3
Maximum	1.2936	1.4216	1.6047
Minimum value	1.1021	1.3011	1.4214
Maximum difference	0.1915	0.1205	0.1833
Average value	1.1974	1.3824	1.5691
Synchronization error	232 μs	304 μs	357 μs

The jitter of time error is as follows (Fig. 3):

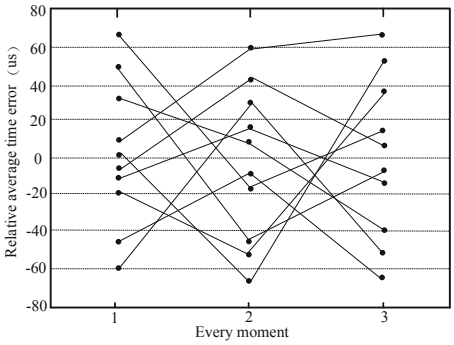

Fig. 3. ZigBee-based system time error jitter

The experimental results of the web-based monitoring system are shown below (Table 4).

Table 4. synchronization effect analysis of web-based monitoring system

Index	Measuring voltage		
	1	2	3
Maximum	1.3147	1.5007	1.6214
Minimum value	1.1724	1.2374	1.4025
Maximum difference	0.1423	0.2633	0.2189
Average value	1.2371	1.3725	1.506
Synchronization error	201 μs	262 μs	304 μs

The time error jitter is as follows (Fig. 4):

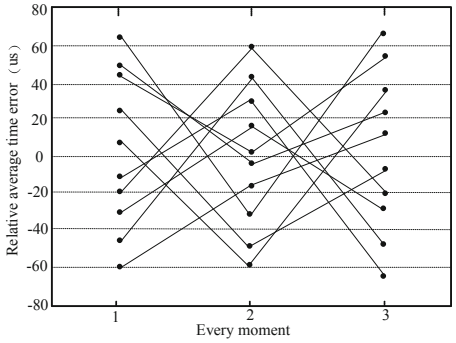

Fig. 4. Web-based system time error jitter

The experimental results of the designed monitoring system based on physical network are as follows (Table 5).

Table 5. Analysis of synchronization effect of monitoring system based on physical network

Index	Measuring voltage		
	1	2	3
Maximum	1.1794	1.2903	1.3746
Minimum value	1.1454	1.2019	1.3091
Maximum difference	0.034	0.0884	0.0655
Average value	1.1663	1.2360	1.332
Synchronization error	29 μs	38 μs	49 μs

The jitter of time error is as follows:

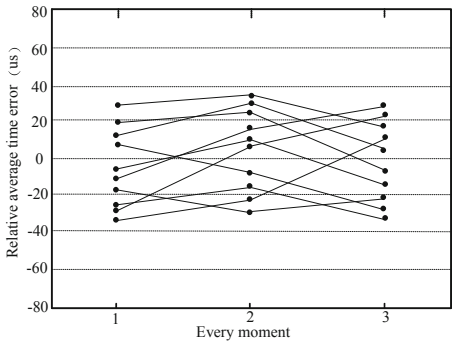

Fig. 5. System time error jitter based on the Internet of Things

The points in the figure represent the nodes. Observing the above results, it can be seen from the time error jitter results of the relative average in Fig. 5 that the time error jitter range of the relative average in Fig. 5 is narrower than that of the other two results, and the synchronization error shown in the synchronization effect analysis table of the measured voltage is always within 90 μs, while the synchronization error of the monitoring system based on ZigBee and web is above 200 μs, which is far away Out of standard time error range. In conclusion, the designed mobile network big data leakage dynamic monitoring system based on the Internet of things has a smaller time synchronization error. Within the allowable range of normal application of the system, the system has a good collection synchronization function.

In order to further verify the effectiveness of the system in this paper, the traditional ZigBee Based System and the Internet of things system proposed in this paper are used to compare and analyze the dynamic monitoring accuracy of mobile network big data leakage. The comparison results are shown in Fig. 6.

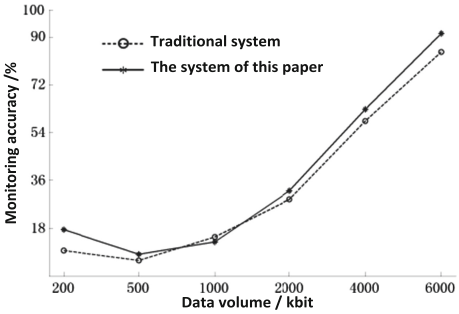

Fig. 6. Monitoring accuracy comparison results

According to Fig. 6, the maximum dynamic monitoring accuracy of mobile network big data leakage in this system can reach 98%, while the highest dynamic monitoring accuracy of mobile network big data leakage based on ZigBee system is only 82%, which shows that the dynamic monitoring accuracy of mobile network big data leakage of this system is higher than that of traditional mobile network big data leakage monitoring based on ZigBee system.

5 Conclusion

Mobile network big data as the trend of social development, its challenges in network security need more attention. Using the characteristics of the Internet of things and the characteristics of big data, this paper designs a mobile network big data leakage dynamic monitoring system based on the Internet of things. Taking ep3c16q240 chip as the core control chip of multi-channel base station node, the system hardware is designed, and the system software is designed through the functions of cluster monitoring, node performance monitoring and job operation monitoring Complete the

design of mobile network big data leakage dynamic monitoring system based on Internet of things, solve the problems existing in the traditional monitoring system, and lay a good foundation for the future development of monitoring system [15].

References

1. Zhang, L., Shao, F.: Design of abnormal risk monitoring system for network big data platform. Mod. Electron. Tech. **41**(22), 143–146 (2018)
2. Du, S.: Application of online monitoring system in urban rail transit based on the big data. Urban Mass Transit **21**(S2), 30–33 (2018)
3. Chen, Z., Sun, J.: Simulation of mobile network information transmission security defense under big data. Comput. Simul. **35**(05), 207–210 (2018)
4. Zhang, Y., Liu, K., Yang, L., et al.: Platform construction and data processing application technology in coal industry monitoring big data. Coal Sci. Technol. **47**(03), 75–80 (2019)
5. Leng, X., Chen, G., Jiang, Y., et al.: Data specification and processing in big-data analysis system for monitoring and operation of smart grid. Autom. Electr. Power Syst. **42**(19), 169–178 (2018)
6. Liu, S., Lu, M., Li, H., et al.: Prediction of gene expression patterns with generalized linear regression model. Front. Genet. **10**, 120 (2019)
7. Liu, W., Zong, L., Xing, C., et al.: Design of the overall information collection of wind farm monitoring system based on EDPF-CP system. Renew. Energy Resour. **36**(08), 1204–1208 (2018)
8. Deng, Z., Cui, J., Liang, Z.: Condition monitoring system of mine hoist based on storage test. Coal Technol. **38**(05), 179–181 (2019)
9. Deng, M.: Regulation and protection of personal data in the context of big data. J. Beijing Univ. Posts Telecommun. (Soc. Sci. Ed.) **21**(01), 19–25 (2019)
10. Zheng, P., Shuai, L., Arun, S., Khan, M.: Visual attention feature (VAF): a novel strategy for visual tracking based on cloud platform in intelligent surveillance systems. J. Parallel Distrib. Comput. **120**, 182–194 (2018)
11. Fu, X., Gao, Y., Luo, B., et al.: Security threats to hadoop: data leakage attacks and investigation. IEEE Netw. **PP**(2), 12–16 (2017)
12. Buesing, H., Vogt, C., Ebigbo, A., et al.: Numerical study on CO_2 leakage detection using electrical streaming potential (SP) data. Water Resour. Res. **53**(1), 455–469 (2017)
13. Liu, S., Liu, D., Srivastava, G., et al.: Overview and methods of correlation filter algorithms in object tracking. Complex Intell. Syst. (2020). https://doi.org/10.1007/s40747-020-00161-4
14. Blackford, J., Artioli, Y., Clark, J., et al.: Monitoring of offshore geological carbon storage integrity: implications of natural variability in the marine system and the assessment of anomaly detection criteria. Int. J. Greenhouse Gas Control **64**, 99–112 (2017)
15. Lu, M., Liu, S.: Nucleosome positioning based on generalized relative entropy. Soft. Comput. **23**(19), 9175–9188 (2018). https://doi.org/10.1007/s00500-018-3602-2