Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5936390, 12 pages
https://doi.org/10.1155/2021/5936390

Research Article

Based on the Role of Internet of Things Security in the Management of Enterprise Human Resource Information Leakage

Zhen Zeng[1] **and Jiajia Zhang**[2]

[1]*Business School, Central South University, Changsha, 410083 Hunan, China*
[2]*College of Business Administration, Shanghai Business School, Shanghai 201400, China*

Correspondence should be addressed to Jiajia Zhang; 21210036@sbs.edu.cn

Received 6 August 2021; Revised 31 August 2021; Accepted 11 September 2021; Published 5 October 2021

Academic Editor: Zhihan Lv

In recent years, the Internet of Things technology, which is an important part of the new generation of information technology, has developed rapidly. The Internet provides more comprehensive conditions for resource sharing at all levels of society. However, while the Internet provides convenience to the society and users, corporate human resource information security has been increasingly impacted, and the channels for personal information leakage on the Internet are also emerging endlessly and in various ways. This article studies the role of Internet of Things security in the management of enterprise human resource information leakage, in order to use Internet of Things security technology to reduce the possibility of information leakage and play the role of efficient and safe management of enterprise human resource information. Therefore, in the experiment, aiming at the problem of personnel information privacy, a privacy protection method based on secure network coding is proposed. This method uses the hybrid coding mechanism of network coding to effectively resist traffic analysis attacks, thereby protecting the information privacy of nodes. Aiming at the threat of data pollution and malicious attacks in the network coding process, GPU host is introduced, and a network coding method based on the CUDA parallel algorithm is proposed to improve the throughput of the network. Theoretical analysis and simulation experiments show that the method has good performance in privacy protection, computational overhead, and communication delay. In the final experimental results, it is concluded that with the support of IoT security technology, the average accuracy and recall rate of information privacy leakage detection results are not less than 85%.

1. Introduction

At present, the Internet has become an inseparable part of our work and life. People are used to browsing news on the Internet and communicating with friends through WeChat. The data of the Internet has exploded, and we have entered the era of "big data." While the Internet is maintaining rapid development, there are also various security issues. For example, online game users pay more attention to account security than other Internet users, while online shopping users pay more attention to issues such as online banking accounts and payment security. Every step of people's activities on the Internet will leave traces on the server, so it is very important to maintain information. The collection of some information will consume a lot of energy and financial resources, and once some privacy is exposed, it will have a very negative impact on the person. This is especially applicable to some social networking sites and mobile phone software on the Internet. They meet the needs of people who need to be recognized and "posted" by others. They are very popular in society. Some personal logs, pictures, schedules, etc., have been "posted" on friends. In the circle, on the one hand, the value of personal information has been expanded, and on the other hand, businesses have obtained huge profits

through commercialized information. However, if you do not pay attention to standardizing this process and do not improve the degree of security in a timely manner, it is prone to excessive information collection, data trading, and illegal acts such as hacker intrusions and virus attacks greatly threaten personal information security. In the era of big data, the value of users' personal information is greater, the impact of personal information security on the Internet is also increasing day by day, and incidents of personal information leakage are also endless. The security problem of the Internet is reflected not only in the leakage of social security information but also in the leakage of user network information from large databases. Data leaks have spread to various types of websites. These well-known websites collectively leak users' personal information. This is the most far-reaching and worst incident that has occurred in my country from the birth of the Internet to the present. Whether it is a government or a company, it pays more attention to personal information security. The leakage of database information not only happened at home but also similar things happened abroad. For example, several large-scale Internet companies such as Apple and Google have reported cases of personal information leakage. Therefore, while mining the value of big data, we should pay attention to ensuring information security and strive to improve users' ability to control personal information and solve the major problem of personal information leakage on the Internet.

At present, it is necessary to highlight a "new" word in terms of information security, mainly to clarify the new situation of personal information security in today's network environment and new channels for information leakage. The research idea is to first summarize the new characteristics of personal information in the new era and introduce the protection of personal information on the Internet. Secondly, it selects the specific case analysis of personal information leaked by large databases in the new era, focusing on the analysis of the online personal information leakage problem caused by "Duokumen." Then, summarizing the network personal information leakage channels in the new era, there are large database security vulnerabilities that lead to personal information leakage, mobile Internet, website and software collection information, operating platforms, and malicious programs. Finally, strategies for protecting online personal information under the new situation are proposed, including strengthening legislation at the government and social levels, accelerating the promotion of real-name systems, strengthening publicity, strengthening moral education, and establishing an independent safety supervision system; strengthening industry self-discipline at the industry and enterprise levels, strengthen technical input; ideologically at the level of individual users, attention is paid to protecting information security, carefully registering identity information, avoiding leakage of personal information, and improving self-protection skills. From a theoretical perspective, put forward a new concept of online personal information and deeply analyze a series of new problems faced by information protection problems. This multiangle analysis helps to deepen the understanding of this problem and handle information exchange and information protection well. The relationship between the two has formed a relatively complete protection mechanism. In a practical sense, conducting relevant investigations on users' personal information protection will help to objectively understand users' behaviors, analyze online personal information leakage channels, and provide countermeasures and suggestions for relevant management departments and Internet companies to take corresponding measures. According to his own work resources and experience accumulation, he conducts in-depth research and thinking on this issue from different angles and different depths.

In the relevant research on the security information leakage of the Internet of Things, Wang et al. used the generalized Bell state and entanglement swap to propose a new quantum dialogue protocol. In this protocol, a series of ordered two-quantum entangled states are used as quantum information channels for direct and simultaneous exchange of secret information. In addition, a secret key string is shared between communicators to overcome information leakage, but the efficiency of other schemes is very low and cannot meet the requirements of information protection [1]. Lin and Lin investigated the possibility of unintentional and involuntary disclosure of personal information on Facebook. The leaked information may be useful for social engineering and spear phishing by malicious users. We designed an inference method based on the interaction between Facebook pages and friends on the group to find the birthday and educational background of Facebook users and used J-measure to find inference rules. Reasoning increases the discovery rate of birthdays from 71.2% to 87.0%, and the accuracy rate is 92.0%. Although the accuracy rate has improved, the stability of his method is not good enough [2]. Gong and Kiyavash proposed that when the user's job arrival rate is very low (close to zero), both first-come, first-served (FCFS) and round-robin schedulers fully reveal the user's arrival pattern. In the work-saving version of the TDMA (WC-TDMA) scheduler, the nearly complete information leakage in the low-rate traffic area was proved to be reduced by half, and the result proved to be the best privacy in the deterministic work category-conserving (det-WC) The scheduler based on the general lower bound of information leakage that he derives for all det-WC schedulers. However, it is easy to extend many other security risks [3]. Kim et al. said that if employee information is leaked, the company will be negatively affected. To prevent this, they have implemented various security solutions provided by information security vendors. Through the analysis of the stock price fluctuations of information security companies, the hypothesis about the impact of the value of information security companies is verified. They found that with the occurrence of personal information leaks, the stock price of information security companies has risen. And the difference according to the amount of leakage and the type of business is not statistically significant. But according to the business classification of information security companies, there are significant differences. Although this discovery has a certain effect, this method does not reduce the probability of information leakage [4]. Wang et al. said that Spectre-style attacks expose data leakage scenarios through cache side channels. Specifically, the speculative execution path caused by branch misprediction may bring secret data into the cache,

and even after the speculative execution is compressed, the data will be exposed through the cache-side channel. The tool KLEE SPECTER is built on the KLEE symbolic execution engine, so it can provide a test engine to check the data leakage through the cache side channel, but this method is not efficient enough [5]. Roy et al. believe that glitch attacks are a powerful implementation-based attack that can destroy encrypted devices within a few milliseconds. Among the large number of failures that may occur in the device, only a very small number can leak the key, but this failure can easily cause a large amount of information to be leaked [6]. Gao et al. proposed a quantum dialogue protocol using asymmetric quantum channels. They studied the security of the protocol and found that it has the flaws of information leakage. So, this protocol is not secure enough [7].

With the continuous development of science and technology, people rely more on the Internet in modern life. Particularly in the "big data" era, the Internet provides more comprehensive resource sharing conditions, faster communication methods, and more convenient communication channels for all levels of society. However, while the Internet provides convenience to the society and users, the security of online personal information has been increasingly impacted, and the channels for online personal information leakage are also endless, and the security of online personal information is undergoing more and more severe tests. Personal information protection based on the network environment in the past few years has fallen behind in concepts and ideas, and the protection of personal information on the Internet in the new era needs to be further studied and improved. This article analyzes the personal information leakage cases caused by the Internet in the new era, clarifies the new situation of personal information security in today's technological environment and new channels for information leakage, and proposes corresponding countermeasures. First of all, it defines the concept of online personal information in the new era, summarizes the types and characteristics of online personal information, especially the characteristics of the new era, and puts forward the necessity of protecting online personal information. Summarize and analyze the new channels and new methods of online personal information privacy leakage, such as large-scale database security vulnerabilities, mobile Internet vulnerabilities, information collected by Internet websites and software, mobile phone operating platforms, and malicious programs. Finally, around the current problems of personal information exposure on the Internet, researched targeted protection countermeasures and ideas from the government management level, the corporate industry protection level, and the personal protection level to provide references for the current and future protection of online personal information.

2. Introduction of IoT Security Technology and Establishment of Information Leakage Prevention Model

2.1. IoT Security Technologies. If you compare the Internet of Things system with the human body, the perception layer is like the limbs of the human body, and the transmission layer is like the human body and internal organs. Then, the application layer is like the human brain. Software and middleware are the soul and central nervous system of the Internet of Things system [8]. The perception layer includes information collection and networking and collaborative information processing. It automatically recognizes and collects information through sensors, one-dimensional/two-dimensional bar codes, RFID, and other multimedia information, and how the collected information is counted into the network layer [9]. The collected information needs to be transmitted to the upper end. At this time, it is necessary to use networking technology and collaborative information processing technology, including long-distance and short-distance data transmission technology, self-organizing networking technology, collaborative information processing technology, and information collection intermediate Piece technology. The network layer mainly refers to the network system composed of mobile communication network, radio and television network, Internet, and other private networks to realize data transmission. The application layer includes the supporting technology of the Internet of Things application and the practical application of the Internet of Things [10]. In the system architecture of the Internet of Things, we can also see that the Internet of Things involves public technologies, such as coding, identification, analysis, information services, and security, as shown in Figure 1.

The physical entity layer mainly contains various entities in the physical world, and these physical entities are embedded with various sensors and actuators [10]. The physical entity is associated with the Internet of Things system through sensors and actuators. Some information in the physical entity will be transmitted to the Internet of Things system through sensors, and at the same time, some control commands in the system will also be transmitted to the physical entity through the actuator to achieve an impact on the physical world [11]. The main function of the Internet of Things service layer is to call various resources in physical entities and virtual entities to implement specific services or functions. The system layer of the Internet of Things mainly realizes its related applications by calling related services or functions of the service layer. Virtual entities mainly include two parts, one is the mapping of physical entities, and the other is various virtual resources (such as weapons in online games and virtual pets). The system layer of the Internet of Things mainly provides users with various applications or services by calling virtual entities and various services [12]. At the same time, the system layer can also control physical entities through virtual entities. The system layer of the Internet of Things is responsible for the operation of the entire system and for interacting with users. The system layer decomposes the various requirements of users into various tasks and further subdivides them into the services that the service layer can provide [13]. The user's needs are finally fulfilled by calling various services in the service layer. The Internet of Things realizes the integration of the physical world and the digital world through various communication and sensing technologies, so as to realize the automatic identification of various physical entities and the sharing of related information. At the same time, through the use of data mining or semantic analysis and other technologies for further processing of the

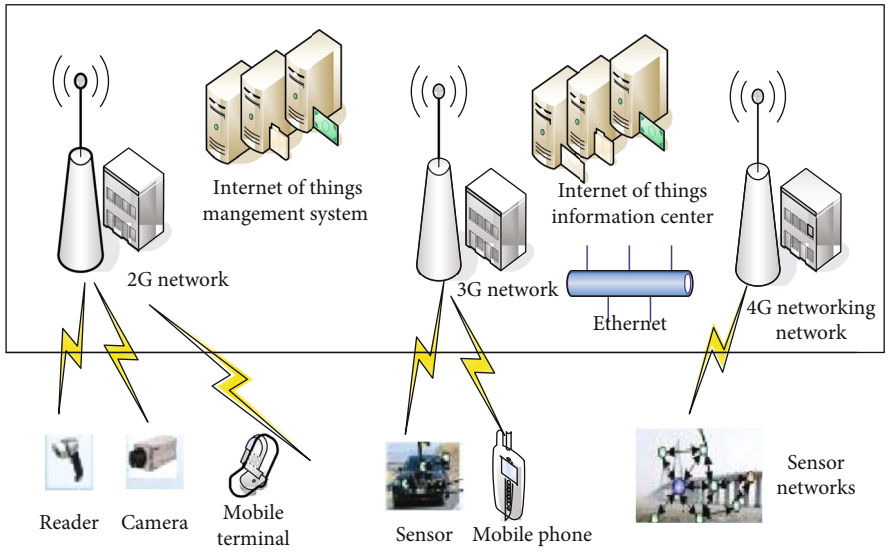


Figure 1: Framework diagram of a typical system of the Internet of Things.

collected information, more valuable applications or functions are generated [14], as shown in Figure 2.

The characteristics of the Internet of Things security in the protection of human resource information are that it includes a client, a security gateway, and a terminal node; the client and terminal node include a data encryption/decryption module; the security gateway includes a secure communication module, user access control and node identity authentication module [15], trusted platform module, and log audit and alarm module; the data encryption/decryption module in the user terminal and terminal node is used to use a preset encryption program pair on the remote client or terminal node. The sent control commands and the received data are encrypted/decrypted; the secure communication module is used to cooperate with other modules to ensure the security of the two-way data transmission process [16]; the user access control and node identity authentication module is used in order to realize the control of user access and the authentication of node identity; the log audit and alarm module is used to record user access and node authentication behavior and perform security audits on the operation of viewing logs and at the same time monitor the security of the gateway system. The abnormal phenomena found in the process will be reported to the police in time [17–18], as shown in Figure 3.

2.2. Enterprise Human Resource Information Management. The Internet continues to develop rapidly, and while prospering the economy, it also brings many new experiences to people's lives, work, and learning. Enterprises can make full use of the Internet to enrich their lives, improve work efficiency, and help learning [19]. The nature of enterprise human resource information mainly includes the following aspects: (1) Cognizability. Enterprise human resource information is personalized and identifiable, especially in the process of online membership registration and various account applications; it must have an identifiable mark that distinguishes it from others in order to enjoy exclusive network services [20]. (2) Spreadability. It is also the commonality of information. Different from the traditional way of information transmission, corporate human resource information is stored and transmitted in the form of digital information through the network, which also fully reflects the personality of online registered members. (3) Value and availability. There is a close relationship between corporate human resource information and economic benefits, so corporate human resource information in this area also has greater practical value, and the corresponding information security issues are also very important. (4) It is not easy to detect. In the new era, it is not only traditional virus creators and hackers who illegally infringe personal information, but some well-known Internet companies also use the services they provide to collect personal information, such as domestic netease and 360, foreign Google, and Amazon; Google's CEO Larry Page even bluntly stated in an internal email: Collecting user location information is of unprecedented importance to the company's mobile strategy. From the perspective of users, because they trust these companies and hope to provide personal information to obtain more value and services and enjoy the satisfaction of others' recognition by sharing information, they ignore and find it difficult to detect when, where, and how these companies violate users, rights, and disclosure of personal information, as shown in Figure 4.

2.3. Information Protection. Information services play a very important role in the application of the Internet of Things, and the protection of information privacy is an important aspect of the privacy protection of the Internet of Things [21]. For wireless sensor networks, node location information often plays a role of identification in wireless sensor networks. Positioning technology is a key basic technology in wireless sensor networks. The personal information it provides is of great significance in wireless sensor networks. It is used in providing monitoring events or target personal information,

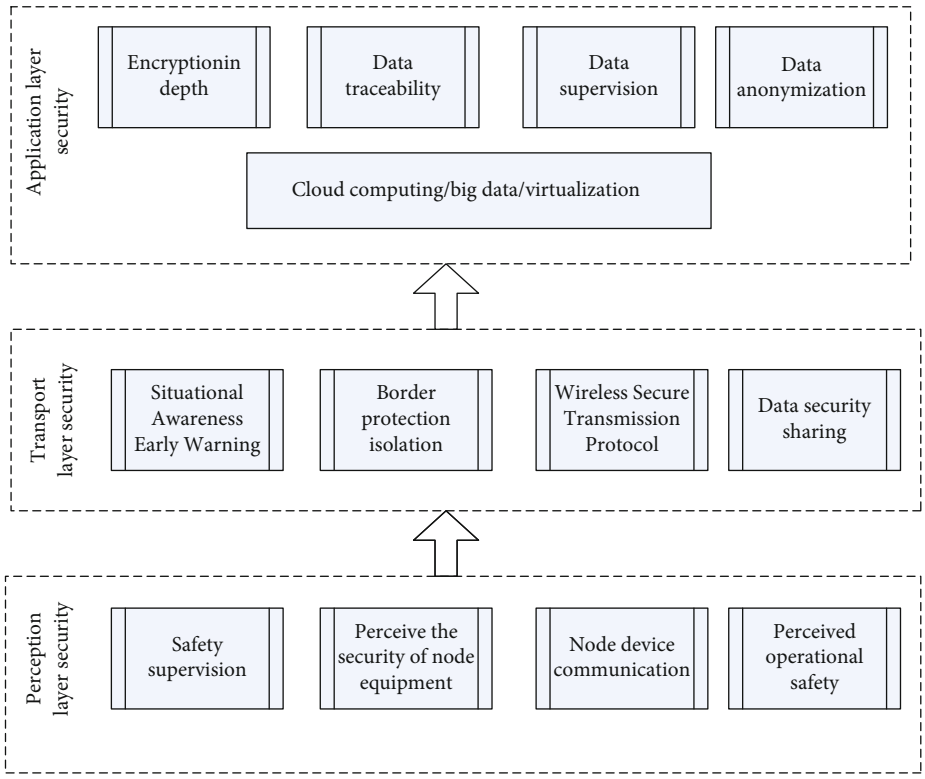


Figure 2: LOT security protection architecture.

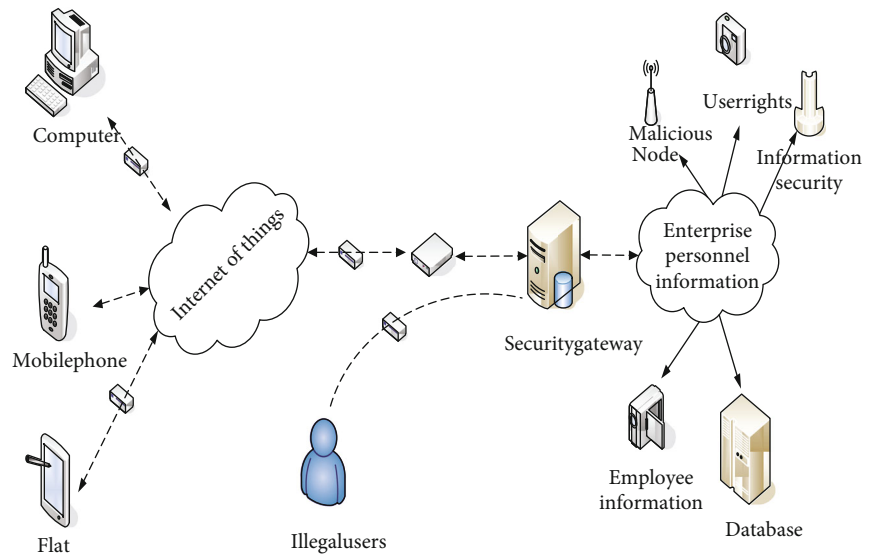


Figure 3: Internet of Things technology and enterprise personnel information protection.

routing protocols, coverage quality [22], and other related research. The key role once the node's location information is illegally abused, it will cause serious security and privacy problems [23–24]. Therefore, information privacy has a special and critical position in wireless sensor networks. Information privacy is an important part of wireless sensor network privacy [25]. Information privacy protection can be divided into source node information privacy and sink node information privacy, and sink node privacy issues include local privacy attacks and global privacy attacks. Source node information privacy includes fixed information privacy issues and mobile information privacy issues.

Lack of strong legal protection. According to the principle of statutory crimes and punishments, there is no effective

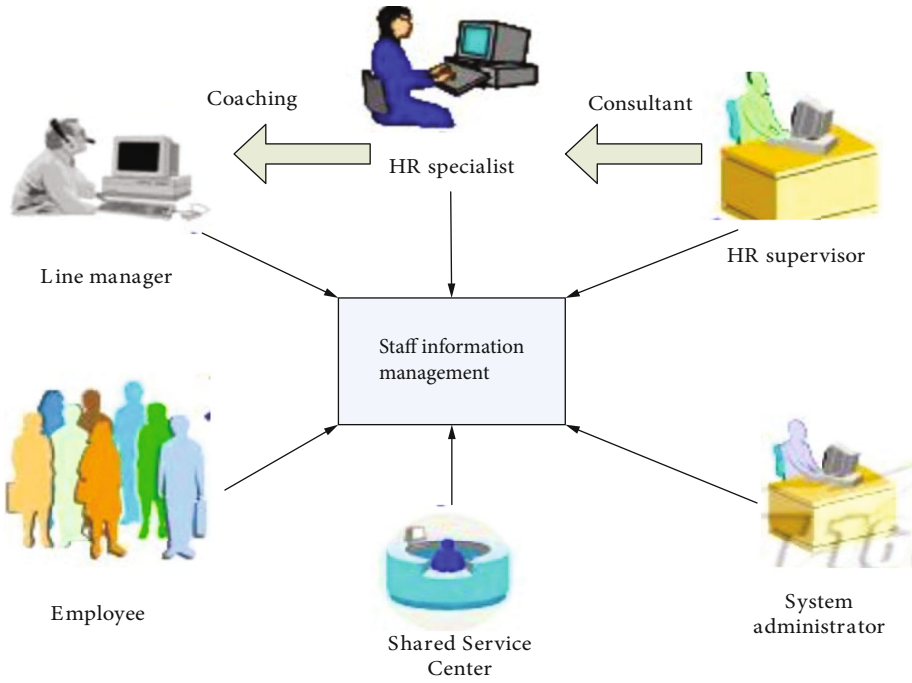


Figure 4: Enterprise human resource information management.

legal restriction on the negligence of management that leads to the leakage of information by employees. This has become one of the reasons why this phenomenon of information leakage has been repeatedly banned and intensified.

In a society with unsatisfactory integrity, it is far from enough to rely solely on people's moral self-discipline. Coupled with the lack of strong legal means to protect people, even if they discover that their information has been leaked, they will be worried. The results of the rights protection were not satisfactory, and they eventually gave up protecting their legal rights and interests.

2.4. Information Leakage Prevention Algorithm Model Construction. Taking into account the advantages of the elliptic curve cryptosystem, the base point and its multiple points on the elliptic curve are selected to design the encryption private key for private communication protection in WSNs. The main selection methods are randomly selecting and constructing an elliptic curve of a given order [26]. The former randomly selects an elliptic curve E/L and calculates its order parameters until a satisfactory curve is obtained. Due to the randomness of this method, it is a good method from a security point of view [27–28]. The latter idea is to use complex multiplication to construct an elliptic curve with a specific order on the prime domain Z.

Judging from the research results in recent years, the large prime domain is more effective. This scheme chooses the prime domain Z elliptic curve, because its implementation is simple; on the contrary, the finite domain elliptic curve with feature 2 is not suitable for tiny processors. The elliptic curve on Z is defined as

$$C(x, y) = y^2 - x^2 - Ax - B, 4A^3 + 27B^2 \neq 0. \quad (1)$$

Among them, A and B are coefficients, and the variables x and y only take values in a finite field, which can be expressed as $E(A, B)$. The base point on an elliptic curve can be expressed as $O = (x, y)$ where x, y, Z. The elliptic curve in the Z domain has various important calculations, and the double point and point addition calculations will be used in the scheme of this article. The double point is also a point on the elliptic curve, that is, O is a base point on the elliptic curve, and then $2O$ is also on the curve. The mathematical description of this double point is if $O = (x, y)$ and $O \neq 0$, then $2O = O + O = (x, y)$, which is determined by the following equation:

$$\begin{aligned} x_{2o} &= \left(X^3 - 2x_{2o}\right), \\ y_{2o} &= X(x_o - x_{2o}) - y_o. \end{aligned} \quad (2)$$

其中:

$$X = \left\lfloor \frac{A + 3x_o^{\,2}}{2y_o} \right\rfloor. \quad (3)$$

The points added are the same points. However, for $3O = 2O + 1O$, the points included are different. In this case, the following formula is used to calculate:

$$\begin{aligned} X &= \frac{y_{2o} - y_o}{x_{2o} - x_o}, \\ x_{3o} &= X^2 - x_o - x_{2o}, \\ y_{3o} &= X^2(x_o - x_{3o}) - y_o. \end{aligned} \quad (4)$$

When the aggregation result is forwarded between

cluster head nodes, intercluster network coding can be further performed. Cluster head node A can aggregate the aggregation results sent by cluster head node C: similar to the intracluster network coding, the intercluster network coding can also verify data integrity. The signature data of each node is

$$\begin{aligned} p(H_i) &= q^{i-1}(1-q), \\ p(H_{1+}) &= (1-q)\sum_{I=1}^{L-1} q^{i-1} = 1 - q^{L-1}. \end{aligned} \tag{5}$$

$p(l)$ represents the probability of an event set between the malicious node discovered for the first time and the previous node.

$$p(I) = p(H_i) \times p\left(\frac{I}{H_i}\right) + P(H_2) \times p\left(\frac{I}{H_2}\right). \tag{6}$$

At the same time,

$$p(I) = p(H_{1+}) \times p\left(\frac{I}{H_{1+}}\right). \tag{7}$$

So,

$$\begin{aligned} 1 - q &= \left(1 - q^{L-1}\right) \times p\left(\frac{I}{H_{1+}}\right), \\ p\left(\frac{I}{H_{1+}}\right) &= \frac{1-q}{1-q^{L-1}}. \end{aligned} \tag{8}$$

Because from the perspective of the attacker, the malicious node on the anonymous path cannot be the sender, and the probability of the nonmalicious node being guessed is P:

$$p_i = \frac{q - q^{L-1}}{(1-q^{L-1}) \times (N-c-1)}. \tag{9}$$

The entropy provided by the system to the sender is

$$H(x) = p\left(\frac{I}{H_{1+}}\right) \log_2 N + (N-c-1)p \log_2\left(\frac{1}{p_i}\right). \tag{10}$$

Suppose the anonymity of this system is d, because the maximum entropy is equal to $H = \log(N-c)$. So the anonymity is

$$d = \frac{H(x)}{H_{\max}}. \tag{11}$$

Data extraction stage: after successfully performing two-way authentication with the cluster head node and establishing a session key, the mobile node can extract the stored sensing data from the cluster head node.

$$E_r = E_0\left(1 - \frac{r}{R}\right). \tag{12}$$

The ECC holomorphic encryption method encrypts each piece of data. The source node selects a random number r for each piece of data and uses public keys G and r to perform holomorphic encryption calculations on each piece of data and obtain

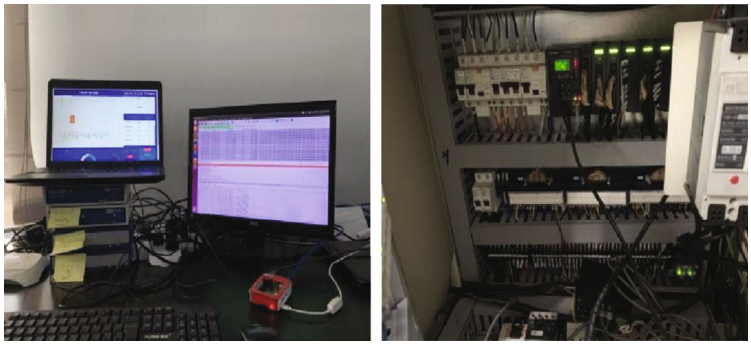
$$\begin{aligned} M_i &= \mathrm{map}(m_i), \\ C_{1i} &= r_i G, \\ C_{2i} &= r_i K + M_i. \end{aligned} \tag{13}$$

3. Construction of Test Platform and Analysis of Experimental Results

3.1. Test Platform Deployment and Environment Construction. The information security protection technology at the transmission layer of the Internet of Things designed in this paper will be tested on the Internet of Things simulation platform. The actual application scenarios of the Internet of Things are diverse, but the secure transmission technology of this design has universal applicability due to the encapsulation of the message protocol. The simulation platform consists of three industrial PCs, a laptop, data collectors, midea transformer production line labeling units, remote monitoring terminals, and various network peripherals. In order to test the function and performance of the transmission security technology designed this time, an industrial IoT production data monitoring system was deployed using the above equipment and related tools of the Hyperledger Fabric block chain project, using a laptop as a client for receiving. The sensor data collected from the labeling unit of the production line, notebook computers, data collectors, and industrial PCs are all deployed as IoT network nodes to deploy multiple modules designed under secure transmission technology, as shown in Figure 5.

The certificate and key services in the network are provided by the Fabric CA blockchain project, which is a subproject of the Hyperledger Fabric. In order to test the subsequent secure storage technology, the production line data collected by the data collector will also be stored. After the deployment of the platform equipment is completed, the configuration files of each node need to be prepared before the network runs. In order to facilitate the monitoring of the operating status and the comparative analysis with traditional information security technology, three industrial PCs and laptops are configured as the consensus node group and storage node group, and the laptop is also used as a client to operate the network. The experiment will compare the security of the information security technology designed in this paper and the traditional information security technology and then perform performance testing and analysis on the design of this paper. The network topology of the Internet of Things simulation experiment platform is shown in Figure 6.

First of all, use the relevant components of the Fabric blockchain project to generate the required files and improve the configuration file information of each node. The identity and name of each node in the network are shown in Table 1.



IOT simulation platform Human resources information database

Figure 5: IoT simulation experiment platform.

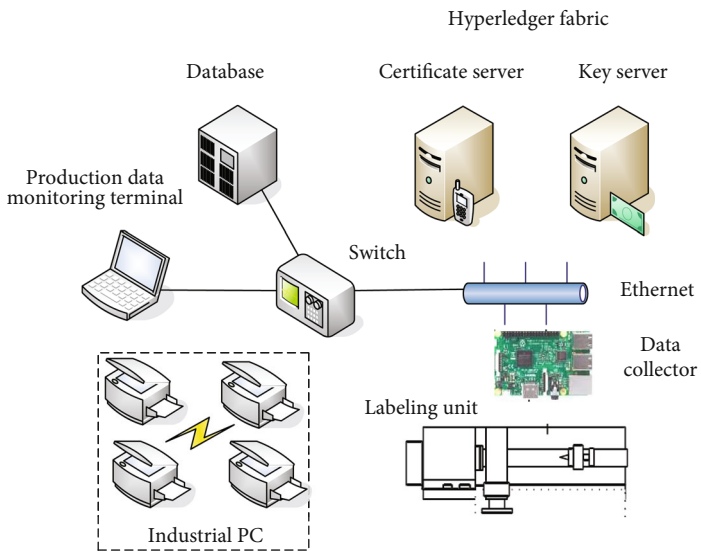


Figure 6: Internet of Things simulation experiment platform network topology.

Table 1: Node identity and startup configuration file.

Equipment	Node identity	Website address	Configuration file
Laptop	Client,Node1(Org1)	192.16.10.119	Channel profile
Industrial PC1	OrdererOrg,master	192.16.10.239	Channel profile
Industrial PC2	Node0(Org2)	192.16.10.64	Channel profile
Industrial PC3	Node0(Org1)	192.16.10.72	Channel profile
Data collector	Node1(Org2)	192.16.10.46	Channel profile

3.2. Experimental Analysis Results. Although the protocol in this article lags behind the most cutting-edge protocols in terms of information calculation time, from the perspective of protocol security performance, the protocol in this article is superior to other protocols. The protocol in this article not only provides two-way authentication but also has higher security. In order to protect the privacy and security of the RFID system, at least the privacy protection requirements such as reader authentication, confidentiality, untraceability, and forward security must be met. However, there is a contradiction between the RFID privacy and security requirements and the cost. Compared with other protocols, the protocol in this paper greatly improves the privacy and security protection of the system under the condition that the cost is not increased much and basically meets the privacy protection needs of the RFID system, as shown in Table 2.

The security performance of the protocol in this article is compared with other related protocols (0 means no; 1 means yes), as shown in Table 3.

The method in this paper has achieved recognition accuracy that is basically the same as other methods and at the same time has higher energy efficiency, as shown in Table 4.

Table 2: Comparison of storage, computing, and communication performance between this protocol and other related protocols.

—	Agreement one	Agreement two	Agreement three	This article agreement
Memory (byte)	41	82	82	82
Computation time	0.064	0.128	0.192	0.31
Communication (byte)	61	82	82	82

Table 3: Comparison of the security performance of this protocol and other related protocols.

—	Agreement one	Agreement two	Agreement three	This article agreement
Two-way authentication	0	0	0	1
Confidentiality	0	0	1	1
Untraceability	0	0	0	1
Forward safety	0	0	1	1

Table 4: Comparison of the method in this paper and other methods in recognition accuracy and energy efficiency.

Method	Recognition accuracy	Energy consumption
Razzak [164]	69%	7822
Muraleedharan [165]	70%	7439
Yan [166]	75%	7375
Proposed	71%	6834

In order to verify the computational performance of the scheme, we carried out conceptual simulation experiments to verify the proposed scheme. The running time of the encryption operation in different environments is shown in Table 5.

The GPU-based parallel algorithm and its acceleration strategy are used to accelerate the speed of human resource information protection. The larger the CPU throughput, the higher the protection rate against information leakage. The GPU and CPU throughput are used to reflect the security based on the Internet of Things. The effect of technology is on the management of human resource information leakage. The following discusses the impact of parallelization on the throughput of data information encoding. Among them, 64 threads are used for parallel computing, the data block size ranges from 1 KB to 128 KB, and the original data block size is 64. It can be seen from the figure that after the use of GPU for parallel computing, the encoding throughput has been significantly improved. When the data block size is 128 K bytes, the throughput of a 64-thread GPU after parallelization is about 23 times that of a single CPU, as shown in Figure 7.

When encoding multiple data blocks, the parallel computing power of GPU can be more fully utilized. The throughput (MB/s) of encoding a data block and encoding 16 data blocks at the same time is compared when using 64 threads for parallel computing. The data block size ranges from 1 KB to 128 KB, and there are 64 original data blocks. When the data block size is 128 K bytes, the throughput of encoding 16 data blocks is about 1.2 times that of encoding a single data block, and about 27.6 times of the throughput of a single CPU. Change the data block size, the network transmission time also changes. When the number of data blocks is 1, it can be regarded as the transmission time without coding, and the transmission time is longer at this time. As the number of data blocks increases, the transmission time is gradually reduced, reflecting the superiority of network coding. However, when the number of data blocks is too large, the transmission time will increase due to the large amount of calculation and complexity brought about by the encoding and decoding, as shown in Figure 8.

We selected a total of 160 sample APKs from the 769 sample APKs, among which 5 benign APKs and 5 malignant APKs were selected for each service type. We conducted a total of 16 sets of experiments according to the number of service types. Each set of experiments verifies the accuracy, recall, and F-measure of current service testing results. Each group has a total of 10 APKs, which are tested successively using the prototype system implemented by PDDMSB. Record the experimental test results of each APK in |TP(M)|, |TN(M)|, |FP(M)|, and |FN(M)| by group. Finally, the accuracy rate, recall rate, and F-measure of each group's detection are calculated. In addition, we only use FlowDroid for static analysis of 16 sets of sample APKs, record the data, and compare the accuracy, recall, and F-measure of the two detection mechanisms. The results of the comparative experiment are shown in Figure 9.

We can conclude that the privacy leakage detection mechanism based on service binding proposed in this scheme has significantly improved the accuracy of experimental detection results. Analysis of the reasons shows that FlowDroid will mark applications with privacy leakage paths as malicious applications, so the probability of misjudged benign applications as malicious applications increases, resulting in a decrease in the overall accuracy of detection results and a decrease in the recall rate of benign applications. Therefore, the accuracy of the experimental detection results of this program is higher than the accuracy of FlowDroid detection results, as shown in Figure 10.

Table 5: The running time of encryption operation in different environments.

—	T pair	T mac	T h	T Gh	T add
Mobile terminal	0.015 s	0.01 s	<0.001 s	<0.01 s	0.012 s
Server	3.58 ms	1.71 ms	<0.001 ms	<0.01 ms	0.001 ms
Management side	0.024 s	0.013 s	<0.001 s	<0.01 s	0.014 s

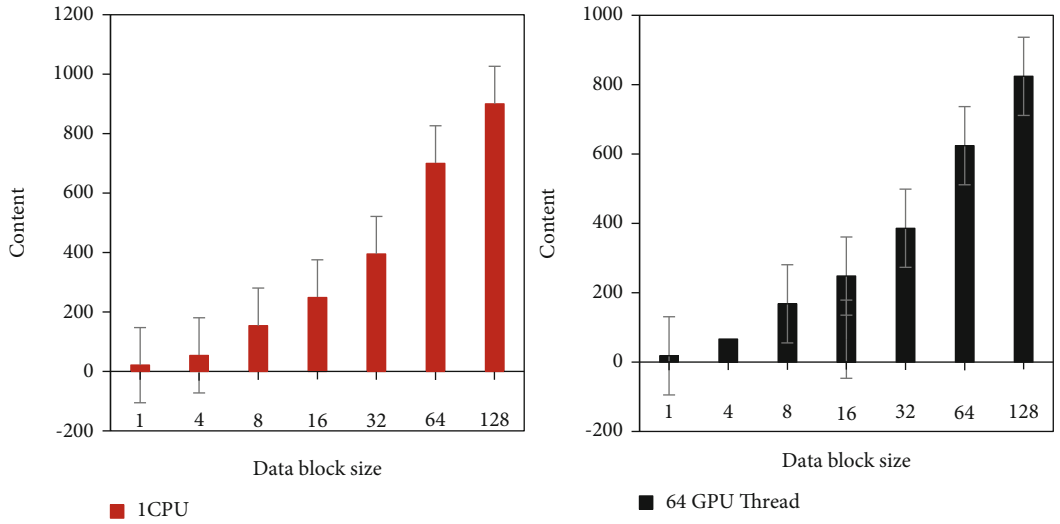


Figure 7: Comparison of encoding throughput (MB/s) before and after parallelization.

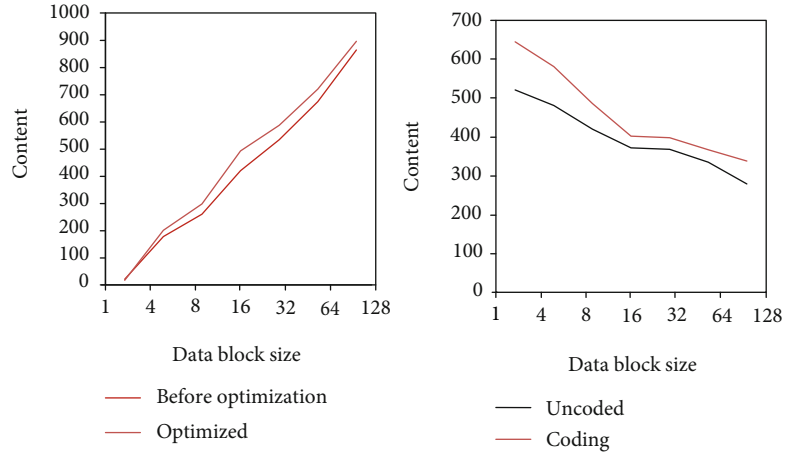


Figure 8: Encoding multiple data blocks encoding throughput (MB/s) comparison.

4. Discussion

After the previous relevant experimental research, the results are that in terms of enterprise human resource information leakage, we need to adopt methods based on IoT security technology if we want to reduce the possibility of information leakage and improve the accuracy of information leakage alarms. Compare the accuracy, recall, and F-measure of PDDMSB and FlowDroid privacy leak detection results. Because FlowDroid takes a long time to analyze the static flow of the application, we have not performed service detection on all application APKs. The accuracy of system detection results achieved by the privacy detection mechanism based on service binding is close to 90%, while the accuracy of system detection results achieved by using FlowDroid for static analysis is close to 87%. Since the privacy permissions bound to different application services are not the same, we have chosen to verify the effectiveness of the detection results of this scheme from the dimensions of different service types. Information leakage prevention is based on encryption technology, combined with security audit mechanisms, strict control mechanisms to master and control internal document operations, and effectively prevent the leakage of internal data and information assets in any state (use, transmission, and storage), and leakage prevention based on this technology. The system includes UniBDP and DLP. A large amount of sensitive information

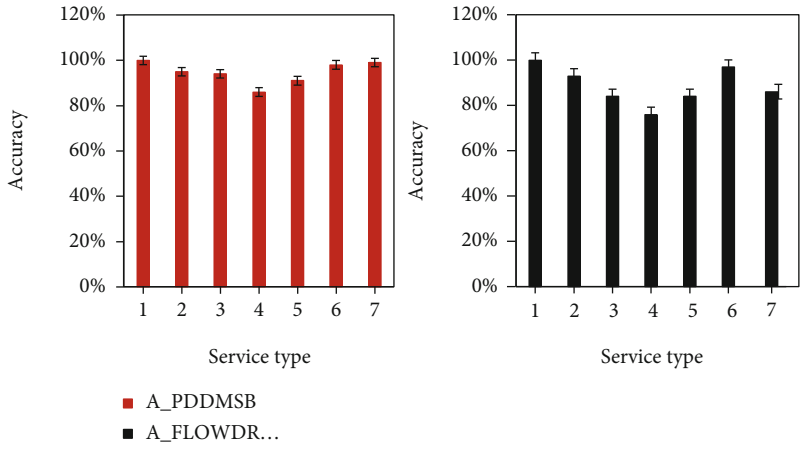


Figure 9: Solution detection accuracy rate.

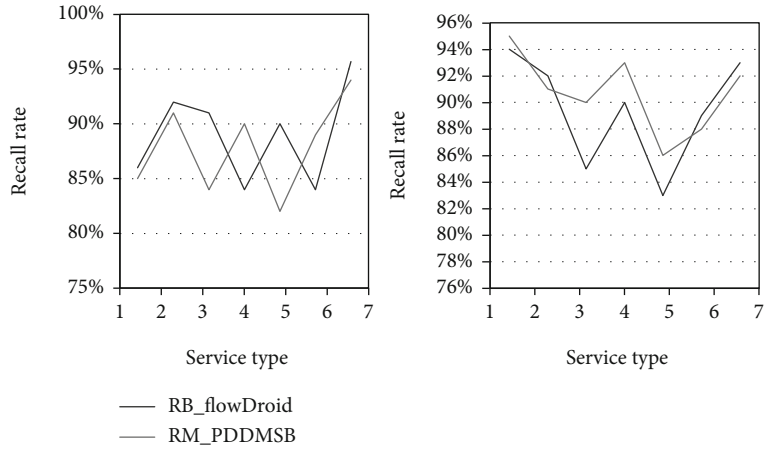


Figure 10: The scheme detects the recall rate of benign APKs and malicious APKs.

is stored in the database. Information leakage prevention can be protected by database security technology. Database security technology mainly includes database leak scan, database encryption, database firewall, data desensitization, and database security audit system.

5. Conclusions

In the new era, the dissemination of personal information on the Internet is becoming faster and faster, and the risks of various leaks are becoming more and more serious. Faced with many rampant behaviors of chasing interests and taking risks, we must give a heavy blow, strive to clarify laws and regulations as soon as possible, and strictly punish them. However, only relying on the law cannot solve the protection of all corporate human resource information, so we should strengthen industry self-discipline, government, social supervision, and other aspects of cooperation to ensure that corporate human resource information protection has achieved good results. Since network technology is a new thing, its process from generation, development, and prevalence to maturity requires support and supervision from all aspects. We can draw the following conclusion: lack of ethics, laws, and systems to intervene in corporate human resource information security; new technologies must be applied to protect the safety of enterprise human resource information; enterprises need to enhance their own safety protection awareness to prevent the leakage of enterprise human resource information at the source. In the future, the rapid development of network technology will inevitably bring new security risks, and corporate human resource information will also be leaked and violated in ways that we cannot predict and imagine now. This requires both management and technical investment. All should be in the forefront of technological development. Therefore, how to keep up with the speed of technological development, advance with the times to improve the protection of corporate human resources, and effectively guarantee the safety of corporate human resource information still requires the efforts of the government, enterprises, and the general public.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there is no conflict of interest with any financial organizations regarding the material reported in this manuscript.

References

[1] H. Wang, Y. Q. Zhang, X. F. Liu, and Y. P. Hu, "Efficient quantum dialogue using entangled states and entanglement swapping without information leakage," *Quantum Information Processing*, vol. 15, no. 6, pp. 2593–2603, 2016.

[2] P. C. Lin and P. Y. Lin, "Unintentional and involuntary personal information leakage on Facebook from user interactions," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 7, pp. 3301–3318, 2016.

[3] X. Gong and N. Kiyavash, "Quantifying the information leakage in timing side channels in deterministic work-conserving schedulers," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1841–1852, 2016.

[4] M. J. Kim, N. Heo, and J. Yoo, "A study on the stock price fluctuation of information security companies in personal information leakage," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 26, no. 1, pp. 275–283, 2016.

[5] G. Wang, S. Chattopadhyay, A. K. Biswas, T. Mitra, and A. Roychoudhury, "KLEESpectre," *ACM Transactions on Software Engineering and Methodology*, vol. 29, no. 3, pp. 1–31, 2020.

[6] I. Roy, C. Rebeiro, A. Hazra, and S. Bhunia, "FaultDroid," *ACM Transactions on Design Automation of Electronic Systems*, vol. 26, no. 1, pp. 1–27, 2021.

[7] G. Gao, W. Y. Li, and Y. Wang, "Information leakage in quantum dialogue by using non-symmetric quantum channel," *Communications in Theoretical Physics*, vol. 67, no. 5, pp. 507–510, 2017.

[8] Y. Lin, S. Sun, and B. School, "Effectiveness of the management system for hospital's deceased person information leakage," *Shanghai Ligong Daxue Xuebao/Journal of University of Shanghai for Science and Technology*, vol. 40, no. 5, pp. 455–460, 2018.

[9] R. T. Aune, A. Krellenstein, M. O'Hara, and O. Slama, "Footprints on a blockchain: trading and information leakage in distributed ledgers," *Journal of Trading*, vol. 12, no. 3, pp. 5–13, 2017.

[10] A. M. Nia, S. Sur-Kolay, A. Raghunathan et al., "Physiological information leakage: a new frontier in health information security," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 321–334, 2017.

[11] D. Fujimoto, N. Miura, M. Nagata et al., "Power noise measurements of cryptographic VLSI circuits regarding side-channel information leakage," *IEICE Transactions on Electronics*, vol. E97.C, no. 4, pp. 272–279, 2014.

[12] S. Dhavale and B. Lokhande, "Comnoid: information leakage detection using data flow analysis on android devices," *International Journal of Computer Applications*, vol. 134, no. 7, pp. 15–20, 2016.

[13] N. Shen, F. G. Liu, L. Chang, K. Li, and Y. Li, "Modeling and experimental study on computer electromagnetic information leakage base on power line," *IPPTA: Quarterly Journal of Indian Pulp and Paper Technical Association*, vol. 30, no. 4, pp. 308–315, 2018.

[14] В. Р. Воронов, В. Заболотний, and В. Лиско, "Accounting for the interference component in the technical channel of information leakage of spurious electromagnetic radiation in the video path with diversity reception," *Radiotekhnika*, vol. 3, no. 202, pp. 99–105, 2020.

[15] C. H. Wu and S. B. Tsai, "Using DEMATEL-based ANP model to measure the successful factors of E-commerce," *Journal of Global Information Management*, vol. 26, no. 1, pp. 120–135, 2018.

[16] S. Salnyk, P. Sydorkin, S. Nesterenko et al., "Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems," *Journal of Scientific Papers Social Development & Security*, vol. 10, no. 6, pp. 29–39, 2020.

[17] J. Y. Lee, G. Y. Lee, and H. Y. Kwon, "Insider information leakage detection method using scenario technique," *Journal of Digital Contents Society*, vol. 21, no. 3, pp. 617–626, 2020.

[18] J. Mao, J. Liu, J. Zhang, Z. Han, and S. Shi, "A method for detecting image information leakage risk from electromagnetic emission of computer monitors," *Journal of Intelligent and Fuzzy Systems*, vol. 40, no. 2, pp. 2981–2991, 2021.

[19] C. H. Wu, Z. Yan, S. B. Tsai, W. Wang, B. Cao, and X. Li, "An empirical study on sales performance effect and pricing strategy for E-commerce: from the perspective of mobile information," *Mobile Information Systems*, vol. 2020, Article ID 7561807, 8 pages, 2020.

[20] M. J. M. Bohmann and V. Patel, "Information leakage in energy derivatives around news announcements," *The Journal of Derivatives*, vol. 27, no. 4, pp. 13–29, 2020.

[21] S. N. Molotkov, "On the side quantum—classical binary channel of information leakage with Gaussian noise," *JETP Letters*, vol. 111, no. 9, pp. 506–511, 2020.

[22] S. N. Molotkov, "On eavesdropping in quantum cryptography through side channels of information leakage," *JETP Letters*, vol. 111, no. 11, pp. 653–661, 2020.

[23] S. N. Molotkov, "Trojan horse attacks, decoy state method, and side channels of information leakage in quantum cryptography," *Journal of Experimental and Theoretical Physics*, vol. 130, no. 6, pp. 809–832, 2020.

[24] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[25] W. P. Wong, H. C. Tan, K. H. Tan, and M. L. Tseng, "Human factors in information leakage: mitigation strategies for information sharing integrity," *Industrial Management & Data Systems*, vol. 119, no. 6, pp. 1242–1267, 2019.

[26] P. Liu, S. P. Yi, and Y. Long, "Research on the co-opetition relationship of a closed-loop supply chain based on private information leakage," *Journal of Computers*, vol. 30, no. 3, pp. 176–191, 2019.

[27] J. Liao, O. Kosut, L. Sankar, and F. du Pin Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 8043–8066, 2019.

[28] T. Y. Kim, "Effect of pre-disclosure information leakage by block traders," *Journal of Risk Finance*, vol. 20, no. 5, pp. 470–483, 2019.