Hindawi
Scientific Programming
Volume 2022, Article ID 4588493, 13 pages
https://doi.org/10.1155/2022/4588493

Research Article

Computer Information Processing System Based on RFID Internet-of-Things Encryption Technology

Chunyan Yuan

School of Management, Xingzhi College of Xi'an University of Finance and Economics, Xi'an 710038, Shaanxi, China

Correspondence should be addressed to Chunyan Yuan; ycy@zcmu.edu.cn

Received 22 June 2022; Revised 29 July 2022; Accepted 9 August 2022; Published 14 September 2022

Academic Editor: Juan Vicente Capella Hernandez

With the increasing development of information science and technology and the vigorous use and promotion of new technologies, profound changes have taken place in all aspects of our daily life. With this huge change, the IoT industry was born. And it analyzes and processes the large amount of data generated between them, and finally, it helps the development of the economy. The RFID system studied in this paper is the radio frequency identification system, which is an automatic signal identification system. The relationship between the RFID system and the Internet of Things is that the former will obtain a large amount of Internet of Things information data by identifying the Internet of Things. However, it is difficult to guarantee the analysis and processing of data and the security of data in the RFID system. This paper aims to study the effective processing and security guarantee of a large amount of data obtained by the RFID system after processing the identification of the Internet of Things. It is expected to overcome the problems of conventional related art. This paper proposes the encryption technology for the Internet of Things RFID system, as well as the corresponding algorithm, and establishes a processing system for information data. The experimental results of this paper show that the cryptographic mechanism run by the algorithm PECC has better security performance compared with other cryptographic mechanisms, and its computational complexity can be reduced by 28.35%.

1. Introduction

The concept of the Internet of Things was proposed and described by the International Telecommunication Union at the World Summit on the Information Society in 2005. The RFID system studied in this paper is an important step in the construction of the Internet of Things. Because with the establishment of the Internet of Things, it is necessary to collect and organize the data of the equipment, and the RFID system can realize the automatic identification of the data, which can make the operation efficiency of the Internet of Things system higher. However, the resulting large amount of data involves individuals, so there is a great demand for data security technology. However, the RFID system's ability to process data is relatively very limited, so this paper studies the Internet of Things encryption technology of the RFID system to ensure the security of the data.

The large amount of data generated by the Internet of Things can be realized through the application of computer information processing technology. With the emergence of supercomputers in various countries in the world, the information processing capabilities of computers have been qualitatively improved. Because the Internet of Things is in the process of establishing, there will be a large amount of branch data generated. Therefore, for the processing of the above-mentioned large amounts of data, this paper adopts a computer-related information processing system. This paper firstly organizes a large number of IoT device data with this system and uses corresponding software and technology to encrypt the data. It realizes the guarantee of data security, in order to help the construction of the Internet of Things system, in order to hope that the Internet of Things can be improved and perfected.

For the application of RFID systems in the Internet of Things, there have been many related experimental studies, and corresponding technologies are being applied in many fields. Below are some of the researchers and their findings. Feng used the physical signal in the collision slot to separate unknown tags and known tags, which is a new technology to accelerate ID collection [1]. The scientist's point of view is closely related to the research in this paper because the collection of data by the Internet of Things is a challenging task in China, a country with a large population. Narges focused on the application of RFID in the retail industry, especially in store operations [2]. For the retail industry, the use of RFID can accelerate the rapid integration of this field into the Internet of Things system. Ramadan proposed an innovative real-time manufacturing cost tracking system (RT-MCT), which integrates the concepts of lean manufacturing and RFID [3]. This combined concept has received feedback from practical applications. Youm developed an automatic sampling system based on radio frequency identification (RFID) and applied it to the aerobic fitness test [4]. This is the application of RFID in the field of hygiene. Shen proposed a new multitag RFID packet authentication protocol for lightweight mobile environments [5]. This protocol is proposed for its security and privacy. Popoola developed an intelligent, economical, and environmentally friendly vehicle identification system using RFID and solar photovoltaic (SPV) technology [6]. This is the application of the system in the automotive field. The following are related studies on the Internet of Things. Lu and his team proposed a new low-overhead HEVC encryption scheme for energy-constrained multimedia IoT [7]. Bansod proposed an ultralightweight, compact, low-power block cipher [8], which can achieve better performance. The researchers have made different related research articles on RFID systems and their applications. It is mainly used for data collection. The feature of the system is automatic identification, which simplifies the process of data collection. At the same time, the related research on the Internet of Things reflects the requirements for the security of the Internet of Things data. In this paper, compared with the above research, the RFID system and the Internet of Things are combined and applied. The following are some of the innovations of this article.

The innovations of this paper are as follows. (1) This paper expounds the application of the RFID system in the Internet of Things in detail and compares its advantages and disadvantages. (2) This paper uses special encryption technology for the data collected by the RFID system in the Internet of Things system to ensure the security of the data. This is already the most concerned part of the social crowd because this part involves more personal privacy. (3) For the data obtained by the RFID system in the Internet of Things system, this paper adopts an advanced computer information processing system to analyze and process the collected data. In this paper, a corresponding database is established to better guarantee the security of the data.

2. Establishment of Internet of Things RFID Information Encryption Technology and Related Computer Processing System

2.1. RFID System Composition and Algorithm Overview

2.1.1. Composition and Working Principle of RFID System. The RFID system is an automatic identification system, which is derived from satellite technology and can realize two-way communication. As more researchers are joining the research on this technology, the results obtained today are quite large and have been widely used. Because the advantage of this technology is to improve the efficiency of our daily life and work, its application scenarios are very large in reality. The first is to introduce the basic components of the technology, and its specific structure is shown in Figure 1.

Figure 1 is the basic structure of the RFID system. In the actual operation process, it needs to read the electronic tag. When sending and receiving the obtained information, the function of the reader is to transmit the obtained information to the software system. It processes and analyzes the obtained data through a software system [9].

The structure of the important part of the RFID system and its working principle are described below. The first is the introduction of the reader, which plays a central role in the RFID system. The premise of the operation of the RFID system is the normal operation of the reader. Figure 2 is the structure diagram of the reader.

In the RFID system of the reader, the identification distance of the RFID system is determined by its power, and the relevant frequency of the RFID system is also determined by the reader [10]. The workflow of the reader basically determines the operation of the RFID system. The specific workflow is shown in Figure 2.

This article introduces the important components of the reader, as well as the electronic tag. The component exists as a carrier in the RFID system. Only when the electronic tag is activated, valid data can be read. Its structure is shown in Figure 3.

After the electronic tag is activated by the reader, it will receive the signal, and then through the function of the internal device of the electronic tag, it will release a new signal and attach it to the corresponding object. This is the working principle of electronic tags and readers in RFID systems. Electronic tags can be divided into active, passive, and semiautomatic types according to whether they have their own power supply. The first feature is that it can store a large amount of data, which can be applied in some cases where a large amount of data needs to be processed. The second feature is the price advantage and can be widely used. The third advantage is that the reaction speed can be faster than the second, and its price is lower than the first, which can improve the overall work efficiency [11]. The selection of the three types should be determined according to the actual application scenario. For the types and frequencies of various electronic tags, Table 1 has been listed.

Because the working principle of the RFID system is the same as that of the radar, both are two-way communication systems, and both rely on the form of scattered signals to obtain target information. The calculation formula is as follows:

$$Q_{Back} = S\partial = \frac{Q_{Lx}G_{Lx}}{4\pi r^2}\partial = \frac{Q_P}{4\pi r^2}\partial. \quad (1)$$

Q_{Back} in the above formula represents the collected return signal, and Q_P represents the actual working power of the antenna. It can be seen from the formula that Q_P plays a major role in the entire operation of the RFID system [12].

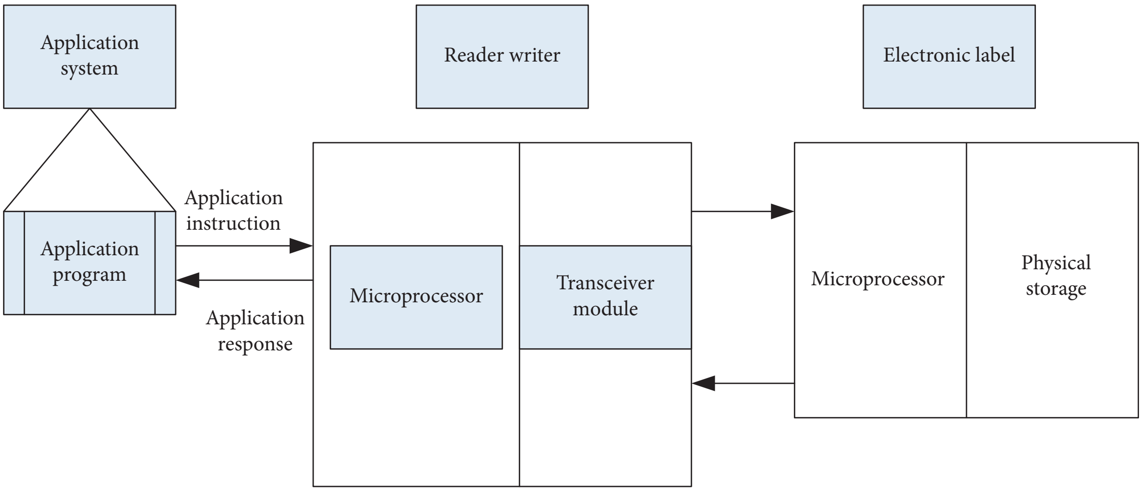

Figure 1: Composition of an RFID system.

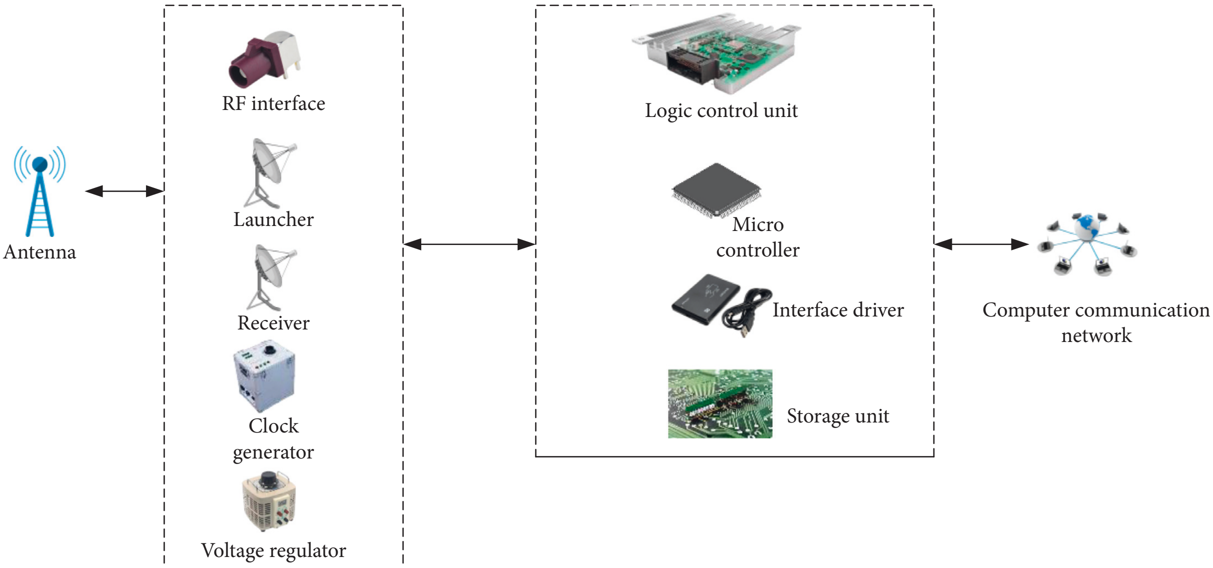

Figure 2: Structure diagram of the reader.

2.1.2. Information Processing Method of RFID System. Since the RFID system involves a large amount of data in the process of use, it adopts a special data control method to reduce the manufacturing cost for other components in the RFID system. The following three different methods are introduced and compared accordingly. The first is amplitude keying, which is expressed as

$$T_2(t) = T(t) \cdot a\cos\theta t. \tag{2}$$

$T(t)$ in the above formula is the digital baseband signal, $a\cos\theta t$ represents the size of the carrier, and the result is a binary signal wave [13].

The second method is called frequency shift keying, which controls the frequency through the digital information of the signal, and its expression formula is as follows:

$$Y_0(x) \equiv Y(x) \cdot \cos\left(\theta_1 x + \alpha\right) + \cdot \cos\left(\theta_2 + \beta\right). \tag{3}$$

$Y_0(x)$ in the formula is also a digital baseband signal, and $\cos(\theta_1 x + \alpha)$ and $\cos(\theta_2 + \beta)$ are both frequency waveforms and are also binary signals.

The third method is the keying method of phase shift, which can be divided into absolute and relative, and its signal expression is as follows:

$$H_0(t) = H(t) \cdot \cos\theta. \tag{4}$$

The above formula $H_0(t)$ here also represents the baseband signal, $\cos\theta$ represents the wave frequency, and the above formula is also a binary expression. The above three data control methods have their own characteristics and should be selected according to different needs in practical applications. These three methods are also commonly used in RFID systems. In order to ensure the integrity of the information data during the transmission process, it is necessary to correct the data. This paper firstly introduces

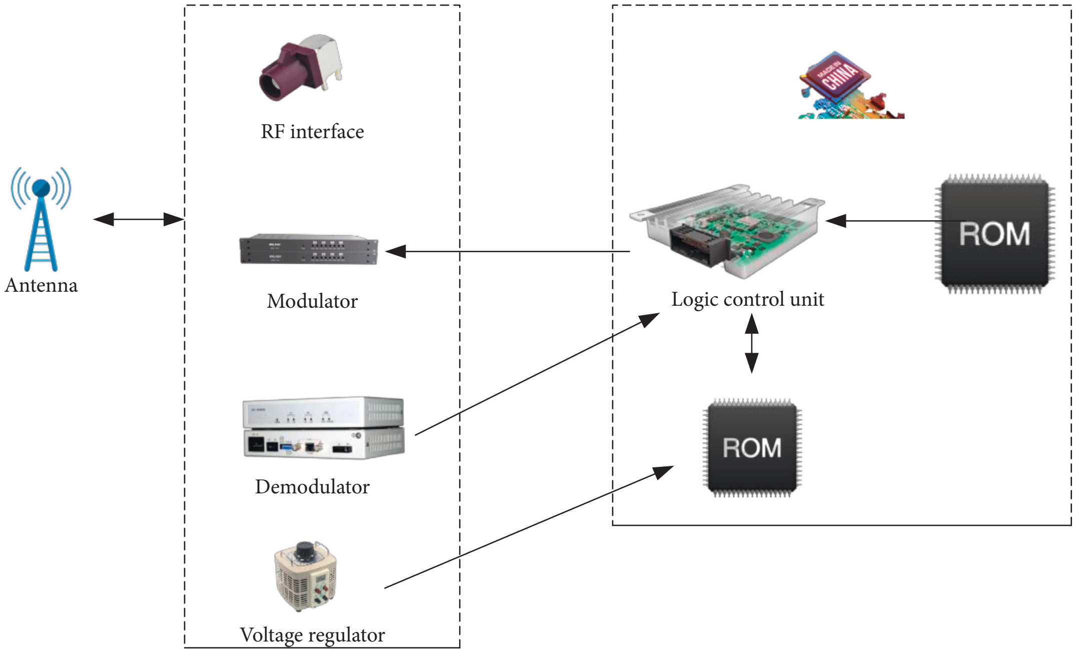

Figure 3: Electronic label structure diagram.

Table 1: Frequency of each type of tag work.

Label type	Working frequency	Typical value	Communication distance
Low-frequency label	30~300 kHz	125 kHz、134 kHz	Within 10 cm
Medium high-frequency label	3~30 MHz	13.56 MHz, 433.92 MHz	Within 1 m
UHF tags and microwave tags	300 MHz~5.8 GHz	2.45 GHz、5.8 GHz	4~6 m

the verification method of cyclic redundant data. Because the data is transmitted in binary, it can be expressed by the following polynomial:

$$Q(t) = e_7t^7 + e_6t^6 + e_5t^5 + e_4t^4 + e_3t^3 + e_2t^2 + e_1t^1 + e_0t^0, \tag{5}$$

e_i in the above formula represents 0 or 1, and $Q(t)$ is the code formula of information. The final check formula can be processed by using a check code polynomial [14], which can be written as follows:

$$t^{m-u}Q(t) = P(t)K(t) + R(t). \tag{6}$$

$K(t)$ in the formula is the polynomial of the check code, which can be used to correct some errors in the code of the information data, so as to avoid errors in the collected data. The error correction of this method can also achieve high-reliability verification for a large amount of data, and its application scenarios are very wide. In addition, there is a method of parity checking, which is simpler and easier to operate than the previous method, but its shortcomings are also very obvious. The disadvantage is that it is impossible to detect an even number of errors in the data bits. That is, when the transmitted data has an even number of errors, the parity check is invalid. For data processing, in addition to the above data regulation, it is also necessary to model the data processing flow. The model structure diagram is shown in Figure 4.

The data model in Figure 4 is extracted from the database, and its design idea is very similar to the database in the traditional sense, data view is a virtual data Table customized according to the user's needs from one or several basic database tables, and its design is similar to that of a traditional relational database, but it is not based on those single data, so there are some differences [15].

2.1.3. Adjustment Method of RFID System Reader Antenna. In addition to the above-mentioned information processing method, the working utility of the RFID system is closely related to the antenna and the channel of information transmission. Because the work of the RFID system needs to identify the distance in the scene, the transceiver capability of the antenna needs to withstand a certain distance test. In this paper, regarding the distance factor of the RFID system, a special antenna with circular polarization that can achieve high gain and can read long-distance information is selected, so that the working distance of the RFID system can be as far as possible p [16]. The relationship between the transmit antenna and the receive antenna is as follows:

$$Q = \frac{1 + 2A_1A_2\cos(\alpha_1 - \alpha_2) + A_1^2A_2^2}{\left(1 + A_1^2\right)\left(1 + A_2^2\right)}. \tag{7}$$

The above formula expresses the utility of the operation between the transmitting antenna and the receiving antenna. But for the gain of the antenna, the calculation method is different from the above. Its gain expression is as follows:

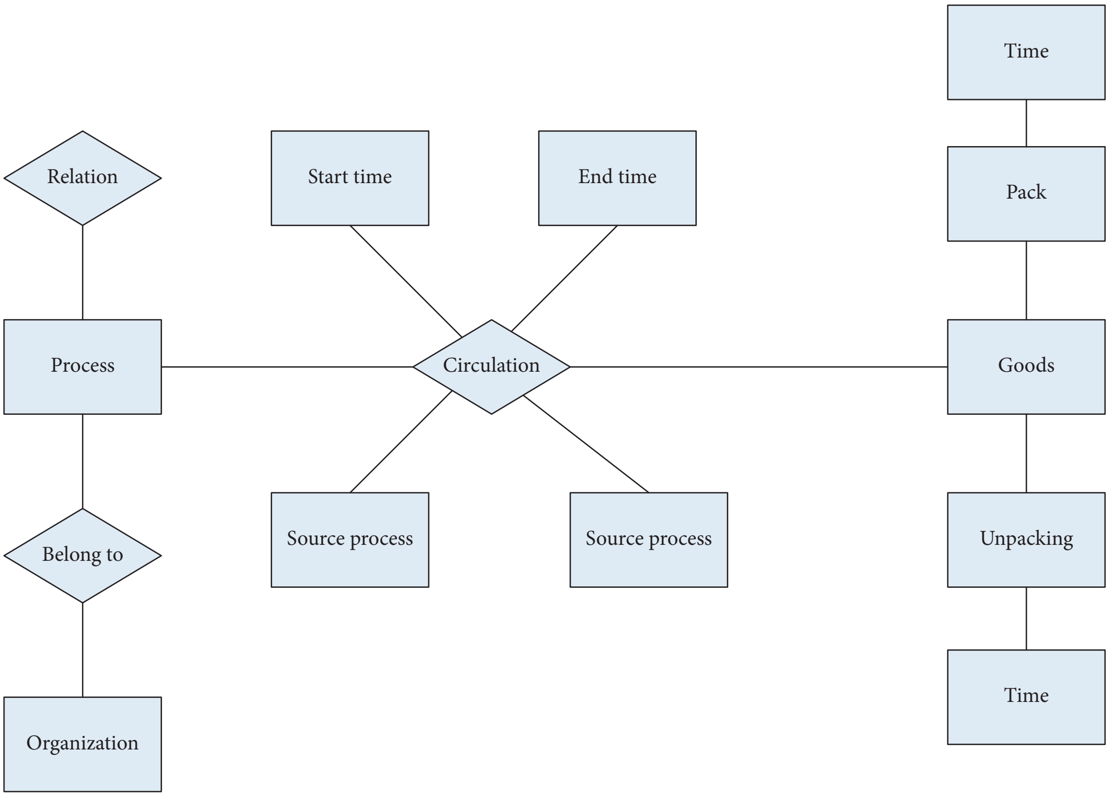

Figure 4: Data processing flow model structure diagram.

$$T(C) = H(C) + 3 + 20\log\left[0.6\left(1 + 10^{-\frac{ER}{20}}\right)\right], (C = dBic). \tag{8}$$

It can be known from the above expression that the particularity of the reader can change the overall role of the RFID system. At the same time, the gain of the antenna will also affect the read and write characteristics of the RFID system. There are actually many kinds of methods to increase the antenna gain, but for this study, the array structure of the antenna is used to improve its efficiency. The array structure of the antenna not only improves the working efficiency of the RFID system but also can achieve excellent characteristics such as anti-interference, thereby improving the performance of the entire RFID system. The following is a comparison of different antenna types. In this paper, the array method of the dipole antenna is first introduced, and its model structure is a circularly polarized model [17]. In fact, it is equivalent to a simple circularly polarized antenna array, and the array characteristics of multiple antennas are also obtained from a simple binary array. For the characteristics of the dipole antenna, the rate of current passing on it needs to be considered, so the resistance of the antenna is calculated as follows:

$$D = \frac{l30}{\sin tk_1 \sin tk_2}\int_{-k_2}^{k_2}\left[\frac{1}{R_1}\exp\left(-itR_1\right) - 2\cos tk_1\frac{1}{R}\exp\left(-itR\right)\right]\cdot \sin t\left(k_2 - |\alpha|\right)d\delta. \tag{9}$$

This formula is a method for calculating the resistance between parallel antennas because the resistance between them is small. The above formula applies to the case between two antennas. On the basis of the above expression, it first calculates the resistance on the antenna, as follows:

$$H_1 = H_2 = H_3 = H_4 = BE^{i\lambda_1}, \left(H_{12} = bE^{i\lambda_2}, H_{34} = dE^{i\lambda_3}\right). \tag{10}$$

The above is the calculation of the resistance, and the following is the calculation of the current. The specific formula is as follows:

$$I = Z\frac{C}{B}E^{I\left(\theta + \frac{\pi}{4} + \mu_3 - \mu_1\right)}\overrightarrow{B_X}. \tag{11}$$

Through the above resistance and current, the value of the axial ratio can be finally obtained, and the final superposition value can be calculated by the following expression:

$$L = \frac{\max}{\min}\left\{\sqrt{\left[d\cos\left(\alpha t + \theta_1\right)\right]^2 + \left[c\cos\left(\alpha t + \theta_2\right)\right]^2}\right\}. \tag{12}$$

The above is the calculation formula of the superposition value of the current on the four antennas. Such calculation processing can obtain the final axis value ratio of the

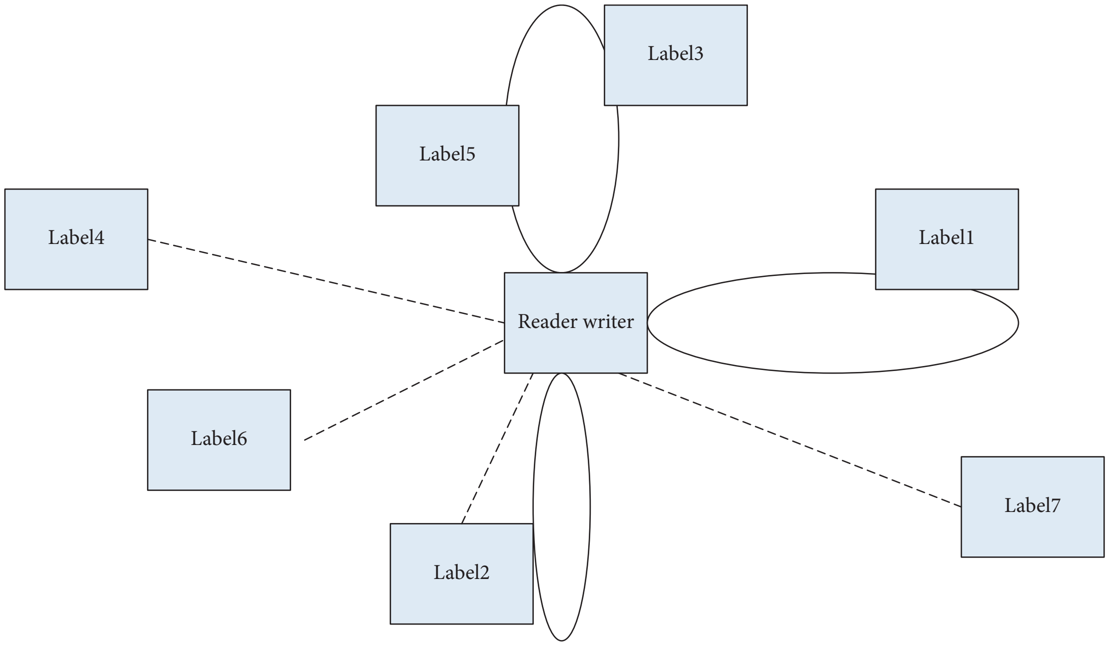

Figure 5: Diagram of spatial discrete recognition method.

antenna. In the axial ratio calculation directly above, the components of each polarization are equivalent to the same frequency radiated by different antenna elements. Signals of different amplitudes and phases are superimposed.

2.2. *Construction Method and Algorithm of RFID System Electronic Label*

2.2.1. Examples of Construction Methods of Electronic Tags. The RFID system is characterized by automatic identification. The identification of electronic tags on items can work normally when the number of items is small. However, when the number of items increases to a certain extent, the RFID system will be disturbed when identifying the electronic tag. The construction of electronic tags here is based on avoiding the situation where two or more electronic tags are repeated, which leads to a decrease in the working efficiency of the RFID system [18]. There are several methods for this problem: there are four major categories: space division multiplexing (SDMA), frequency division multiplexing (FDMA), code division multiplexing (CDMA), and time division multiplexing (TDMA). The first is the spatial discrete identification method. Its characteristics can be represented in Figure 5:

The above method has a relatively large complexity, which is not suitable for the wide application scenarios of the RFID system, so the scope of its use is relatively narrow. Then, there is the wave frequency discrete distribution method, whose specific operation is to use the band information transmission channels of different frequencies to process and transmit the data information on the electronic tag [19]. Its workflow chart is shown in Figure 6.

It can be seen from the method flow chart in Figure 6 that the characteristic of this method is to avoid the repetition of the electronic label of the RFID system through the difference in the wave frequency. However, this method can only be a channel for processing signals, and the frequency receiving device needs to be modified, which increases the overall economic cost and is also not suitable for popularization. In addition to the above two methods, there are transmission channel distribution methods and time discrete distribution methods. The former will bring more signal processing problems due to its immature technology, and the latter will be directly discussed here [20], such as low-frequency band utilization, low channel capacity, difficulty to select address codes, and long acquisition time, so it is difficult to apply in the actual radio frequency identification system. The basis of its operation is to allocate the information reserves of the RFID system according to the required amount of time. The workflow is shown in Figure 7.

The method in Figure 7 is characterized by corresponding distribution according to the time when the item signal is collected. It is divided according to the time of transmitting the signal so that different signals are transmitted at different times. It also divides the entire transmission time into many time intervals, and each time slice is occupied and used by a signal. The transmission of multiple signals by one circuit can thus be accomplished by interleaving a portion of each signal in time. In this way, at each brief moment of the circuit, there is only one signal. The repeatability of the RFID system electronic tag is effectively reduced, and this advantage also makes it applicable to a variety of scenarios.

2.2.2. Related Algorithms for the Construction of Electronic tags in RFID Systems. The methods used in the construction of the above-mentioned electronic tags have been discussed differently [21], and the time discrete distribution method is finally selected in this paper. In this paper, the corresponding algorithm needs to be introduced for this method, so as to

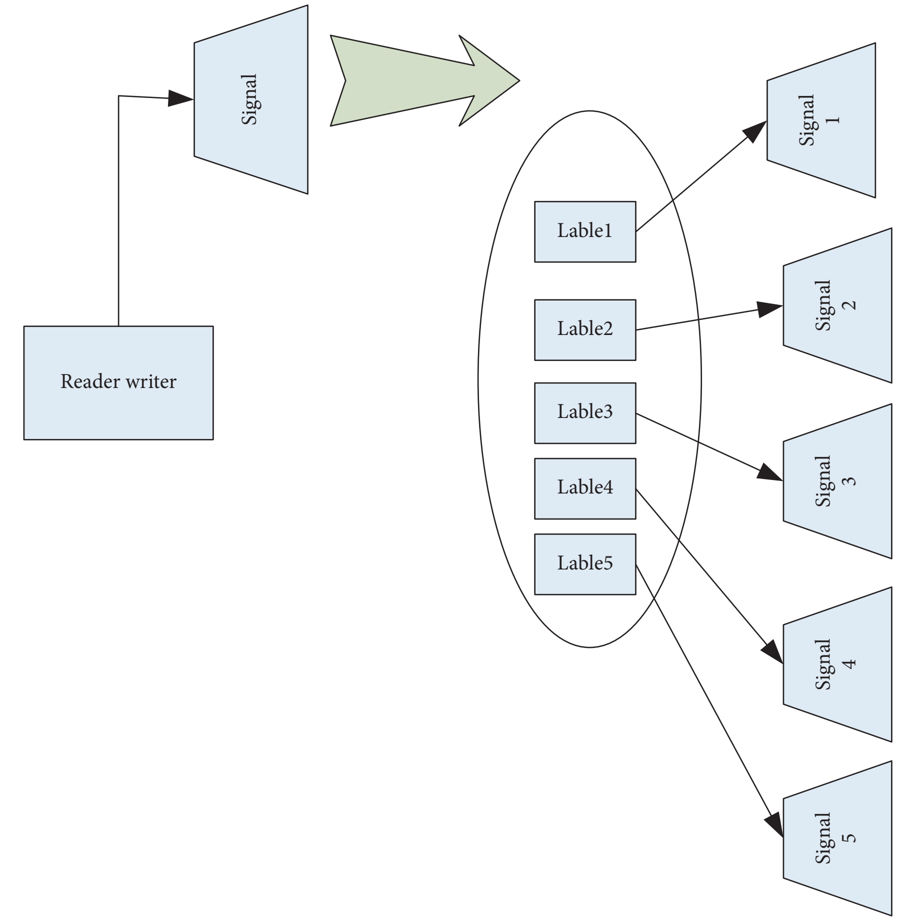

Figure 6: Wave frequency discrete identification method diagram.

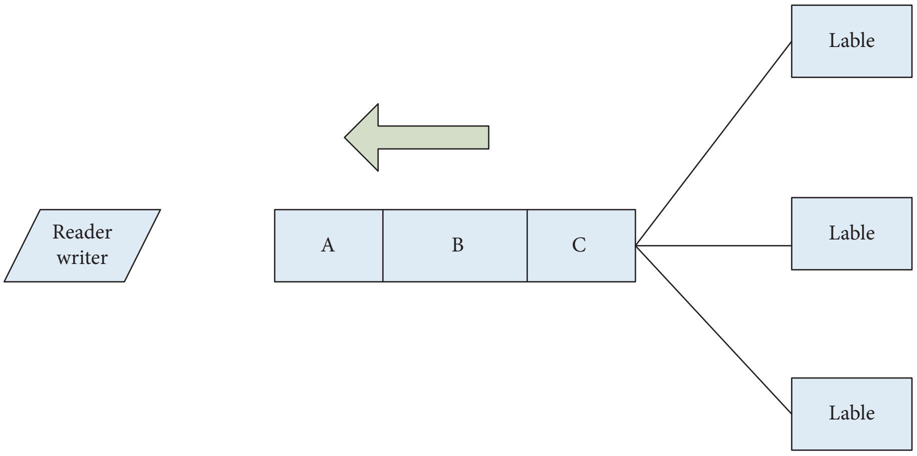

Figure 7: Diagram of time discrete distribution method.

reduce the repetition of the information collection process. The first is the ALOHA algorithm, which is characterized by its application scenario when the number of labels is small. Its working efficiency can be expressed by the following formula:

$$P - Q(m) = \frac{(\mu T)^m a^{-\mu T}}{m^{!}}. \tag{13}$$

The above formula shows that in the time of T, the amount of information m is transmitted, and u is the amount of information sent in the unit of time. The efficiency of the ALOHA algorithm can finally be expressed as follows:

$$P = Ha^{-2H}, (H = \mu T). \tag{14}$$

$H = \mu T$ of the above formula represents the amount of information transferred in time T. Equation (14) is the final expression of the ALOHA algorithm. Next is the FSA algorithm, the frame slotted ALOHA algorithm (FSA) is based on the SA algorithm, and the slotted ALOHA (Slotted ALOHA) algorithm is based on the pure ALOHA algorithm, which is improved based on the ALOHA algorithm above. The calculation principle of this method is described below. Its principle formula is as follows:

$$P = C_M^N \left(\frac{1}{R}\right)^N \left(1 - \frac{1}{R}\right)^{M-N}. \tag{15}$$

$1/R$ here represents the probability that an electronic tag is selected, and the final selection probability of the tag is as in the above formula. The expected value of the identified N electronic tags in unit time is calculated as follows:

$$G = R \times P. \tag{16}$$

When no electronic label is identified in the identification gap, the repeatability calculation of the electronic label occurs as follows:

$$P = 1 - \left(1 - \frac{1}{R}\right)^M - \frac{M}{R}\left(1 - \frac{1}{R}\right)^{M-1}. \tag{17}$$

(3) Prediction method of the number of electronic tags in the RFID system

The use of this method is to predict the number of upcoming electronic tags so that the identification process of the RFID system can be carried out in an efficient and orderly manner until all tags are identified [22]. It is assumed here that there are j times of queries, and there is a proportional relationship between the related parameters, as shown in the formula:

$$m(j+1) = \mu \times D_\mu(j). \tag{18}$$

u in the above formula can be modified according to different usage situations. The algorithm of the formula can predict the number of electronic tags that will appear next.

It is also assumed that after j+1 identifications, the number of electronic tags is as follows:

$$m_0(j+1) = D_1(j+1) + 2.4 \times D_\mu(j+1). \tag{19}$$

This formula is a verification formula, which is calculated by formula 18, so as to obtain the actual number of electronic tags. For the relative error-free between the two, it can be expressed by the following formula:

$$\Delta = \frac{m_0(j+1) - m(j+1)}{m_0(j+1)}. \tag{20}$$

The error formula between the above formulas can realize the error correction between the predicted value and the actual check value so that the prediction ability of the formula can be more perfect. The establishment of the entire prediction process above is obtained after adjustment based on the prediction algorithm of the electronic label of the traditional RFID system.

2.3. Data Storage and Encryption Method of IoT RFID System

2.3.1. Key Technologies of the Internet of Things and Solutions to Security Problems. The Internet of Things was originally proposed to realize the intelligent application of human beings to the objects in life. The birth of this concept is based on the rapid development of information technology in today's society. The understanding of the concept of the Internet of Things should be a data system based on big data, in which a large number of emerging technologies are used. The most important is computer science and technology [23]. In order to realize the interconnection between objects, the Internet of Things has many technical applications; it includes information perception technology, information processing technology, information transmission technology, and perception technology which mainly includes sensing technology, identification technology, and positioning technology, and the specific relationship is shown in Figure 8.

As can be seen from Figure 8, the establishment of the Internet of Things is closely related to the joint action of multiple technologies. At the same time, more advanced network transmission technology is needed to realize the efficient processing of the transmitted data by Internet technology. Because the Internet of Things needs to use related technologies of information conversion in the process of data collection, it is also necessary to implement the establishment of a computer information processing system.

The establishment of the Internet of Things and its role in people's lives have become increasingly prominent, so related security issues have also received extensive attention. For the large data system of the Internet of Things, the biggest security risk is data-related issues, which involve data storage and protection, and it faces serious threats such as leakage. For the IoT system, its defects can be shown in Figure 9.

As can be seen from Figure 9, the system of the Internet of Things is a three-dimensional network system, and the data involved is very large. The electronic tag is the key information, but due to the traditional means, the protection for this place is very limited. In view of the above-mentioned risks, this paper does relevant research and introduces relatively effective protection protocols for different technical levels of the Internet of Things. Its overall content is shown in Table 2.

The birth of the Internet of Things is a collection of modern network technologies and the integration of various network systems. Its complexity can be imagined, and its security is similar to the security of these networks. Therefore, the solution to the security problem of the Internet of Things will refer to the traditional network security method.

2.3.2. Internet of Things RFID System Security and Encryption Methods. Since the RFID system needs to contact a large amount of data, it may leak during its working process. Due to the characteristics of the RFID system and the structure of the electronic label device, the traditional encryption

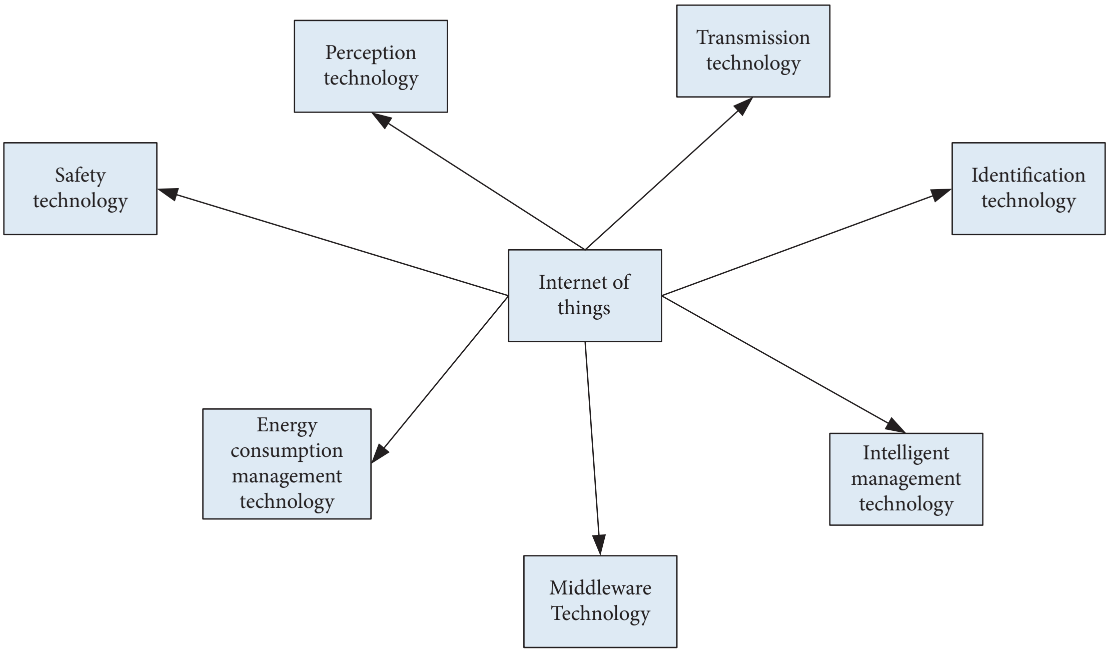

Figure 8: Related technologies for IoT.

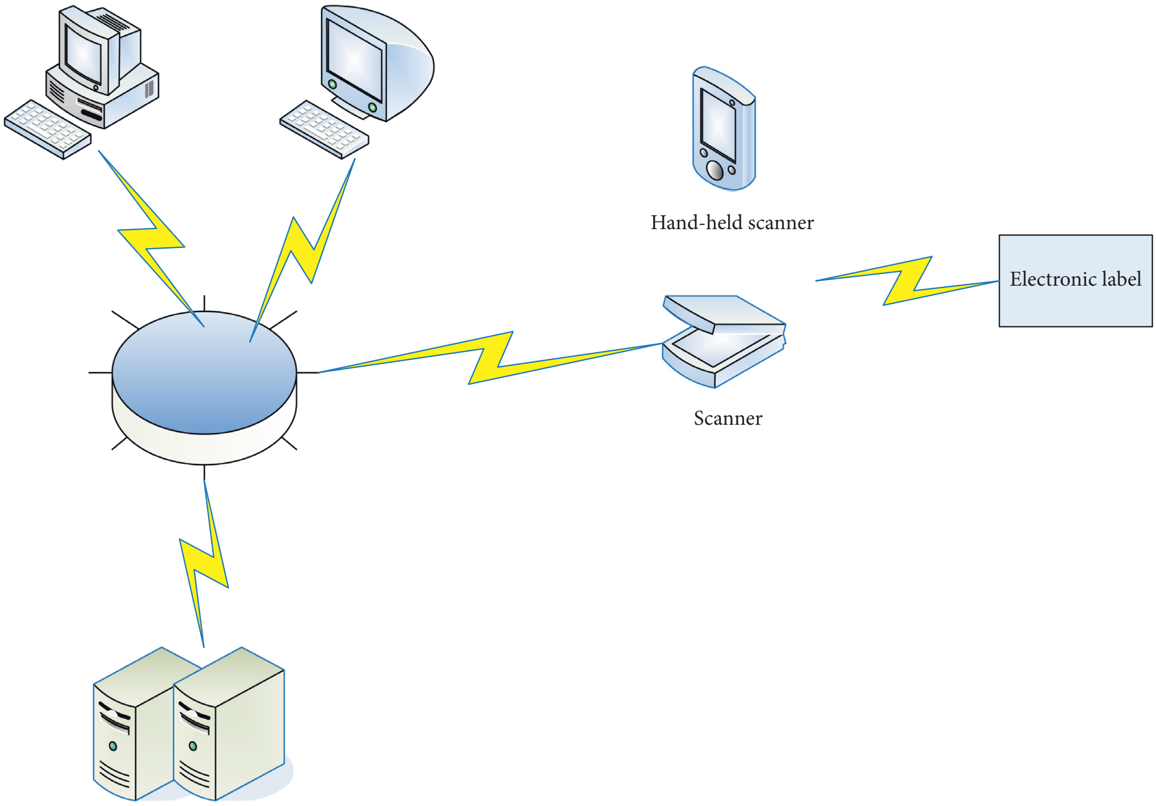

Figure 9: Diagram of key links in the Internet of Things.

technology may not be suitable for this situation. This paper establishes a new encryption mechanism. It is expected to achieve higher security and privacy of the Internet of Things. The encryption algorithm introduced here is the ECC algorithm, and the following is a comparison between it and other encryption algorithms.

It can be known from Table 3 that the reliability of ECC is relatively high. A shorter key length can be used to achieve the same or even higher security strength, and at the same time, it has the technical advantages of low memory resource usage and low bandwidth requirements, which is one of the reasons for choosing this method in this paper, but the ECC

Table 2: Security methods at different levels of IoT.

Technical level	Safe mode
IOT perception layer	Hash-Lock, Hash, Random hash-lock
IOT transport layer	HTTP, SSH, SFTP
IOT application layer	Institutional constraints, privacy authority setting, identity concealment, data confusion

Table 3: Comparison of ECC and various cryptographic mechanisms.

Algorithm	Key length	Security	Execution efficiency
AES	132	Strong	Poor efficiency
DES	56	Weak	Poor efficiency
PRESENT	90	Middle	Efficient
ECC	180	Strong	Poor efficiency

Table 4: Performance comparison before and after ECC improvement.

Decoding time	Improved length	Original length	Key ratio
105	523	118	5.5 : 1
109	760	142	6 : 1
1010	1050	165	7.5 : 1.5
1020	2058	220	10 : 1.5

encryption method also has the disadvantage of low execution efficiency. Therefore, this paper needs to improve the method to some extent, so as to achieve the purpose of improving work efficiency.

The first is the related elaboration of ECC cryptography, which is a kind of public key cryptography, and its characteristic is high security performance. At the same time, the electronic storage space required by the password itself is small, so it has the basis for wide application. For the RFID system, although this kind of password has the above-mentioned storage advantages and high security performance, it still requires high execution power when using it in the system of the Internet of Things, which is a relatively lacking part. This paper will improve the ECC algorithm process to improve its execution efficiency. This paper firstly optimizes and adjusts the scalar, which can directly guarantee the security performance of the password. The first introduces the binary algorithm whose expression can be expressed as follows:

$$P = [A]Q = \sum_{i=0}^{m} A_i 2^i \times Q = \sum_{i=0}^{m} A_i \times \left(2^i \times Q\right). \quad (21)$$

The above formula is for the traditional algorithm between points and points, and our research is improved on the basis of the above formula. In this paper, the traditional modulo operation is replaced by the bit operation, the division operation is replaced by the shift operation, and the parity of the scalar d is no longer judged. After the improvement, this paper analyzes the performance of the corresponding algorithm. Table 4 is a comparison of the security performance before and after the improvement.

From Table 4, it can be seen that the ECC within the unit will be better than the improved security performance. But this is only for a relatively small number of cases, and the advantages of improved encryption for large amounts of data will be more obvious. Its work efficiency will be higher.

3. Related Experiments and Encryption and Perfection of Internet of Things RFID System

3.1. RFID System Electronic Label Reliability Test and Result. The electronic tag of the RFID system is the most frequently used part of the RFID system, but with the particularity of its structure, this part has become one of the biggest safety hazards. In the method part, the corresponding working mechanism and related algorithms of electronic tags have been introduced. The following are the comparison results of the security performance under different security protocols.

From the comparison results in Table 5, it can be seen that various security protocols have a good protective effect on antitracking and antieavesdropping. From the comparison results in the table, it can be seen that the security performance of the BAP protocol is the best, but because the electronic tags of the RFID system do not have the ability to run complex algorithms. Therefore, the use of this algorithm needs to be readjusted. The result of the adjustment of this algorithm can solve the cost problem of the electronic label of the RFID system, and at the same time, its security will be improved correspondingly compared with the traditional one. It ensures that the important part of the electronic label of the Internet of Things RFID system is guaranteed.

3.2. Experiment and Result of New Antenna Array of RFID System Reader Antenna. In the above antenna adjustment algorithm, the algorithm structure for a new type of antenna array is introduced, and corresponding experiments are carried out for this new type of antenna array. First of all, it is to consider the effect of distance on the performance of the reader antenna. This experiment is divided into two types: the experimental model and the actual model. Figure 10 shows the experimental results of the experimental model.

Figure 10 is an illustration of the results under the experimental situation of the antenna performance. It can be seen from the figure that the influence of the antenna coupling on the performance of the antenna is small, but the distance can have a certain influence on the coupling. It can be seen from the figure that the optimal axial ratio of the antenna changes with the distance is not obvious. Next is the relationship between antenna angle and antenna performance, and the research results are shown in Figure 11.

From the results in Figure 11, it can be seen that the different angles of the antenna can make the performance of the antenna change greatly. Therefore, the control of the antenna angle is also very important. Then, there is the effect of different antenna arrangements on the antenna performance, and the results are shown in Figure 12.

As can be seen from Figure 12, the stability of a single antenna is more prone to interference than the other three, but when there are more antenna array structures, its overall performance will be more stable. Under the condition of the quaternary array, the pattern of the antenna changes greatly.

Table 5: Comparison Table of safety performance.

Security protocol type	Anticounterfeiting attack	Antiretransmission attack	Antitracking	Antieavesdropping
Hash-lock	Uncertain	Uncertain	Uncertain	Uncertain
Hash	Uncertain	Uncertain	Security	Uncertain
Dynamic ID-Hash	Uncertain	Uncertain	Security	Uncertain
GR	Uncertain	Security	Uncertain	Security
DAP	Security	Security	Security	Security
RandomHash-lock	Security	Uncertain	Security	Uncertain
BAP	Security	Security	Security	Security

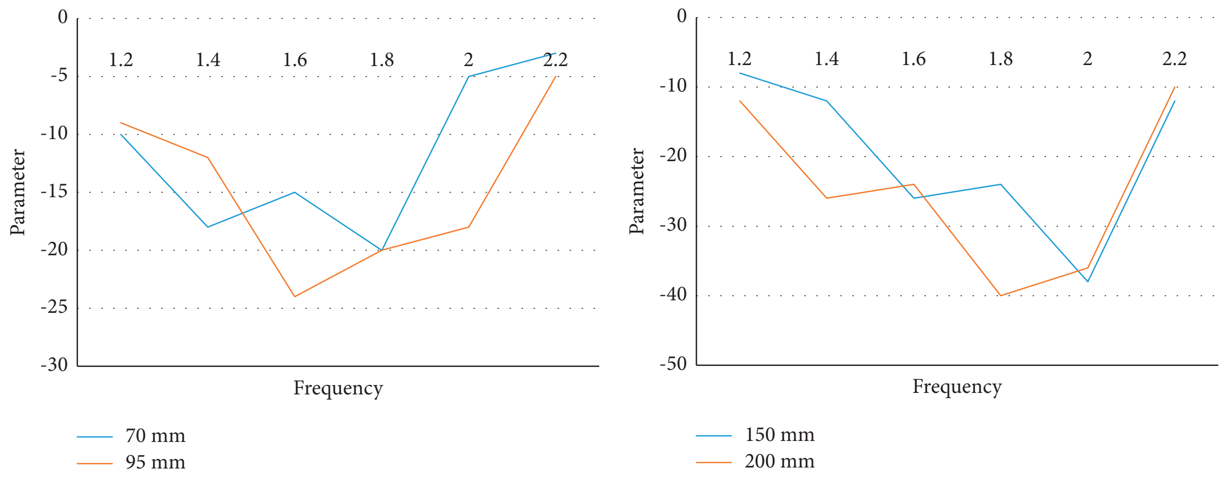

Figure 10: Variation of antenna parameters at different distances.

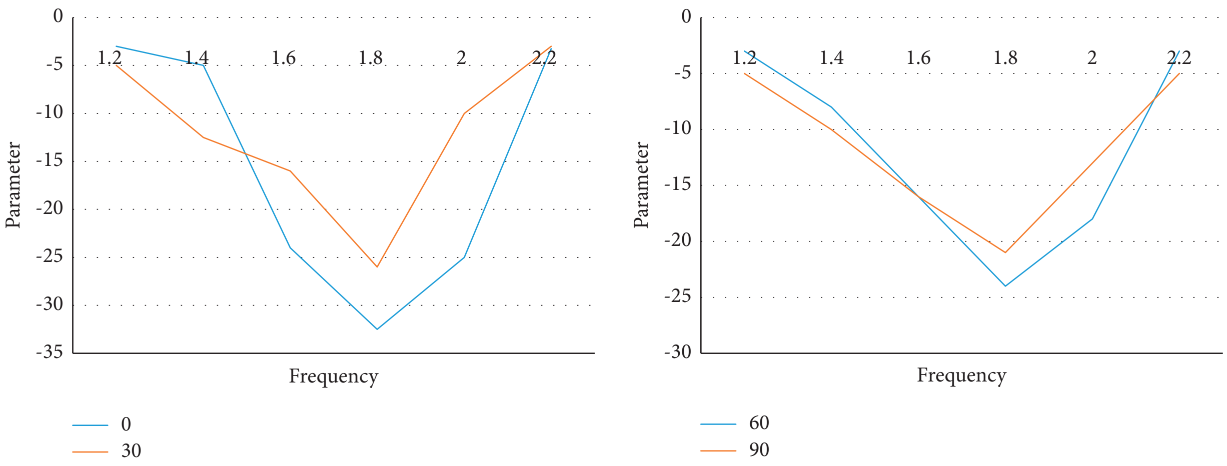

Figure 11: Effects of different angles on antenna performance.

Therefore, it can be judged that if there are a large number of other antennas around, the change in the antenna pattern will be more obvious.

3.3. Experiment and Result of Encryption Algorithm of IoT RFID System. For the information encryption of the Internet of Things, it is ultimately the improvement of the key. The algorithm of this experiment is the calculation of the scalar. Its operation process is to treat the value obtained after processing the collected data as a key. It uses the IDEA programming tool and JAVA programming language to realize PECC-CRT scalar multiplication and PSM-NAF scalar multiplication respectively. The following is the experimental result graph, as shown in Figure 13.

As can be seen from the above figure, the efficiency of the key performance under different algorithms is not the same. But the memory it occupies is not much different. And the operation under the algorithm PECC can reduce the operation amount by 28.35%. It can be seen that the application of this method is helpful to improve the performance of the key.

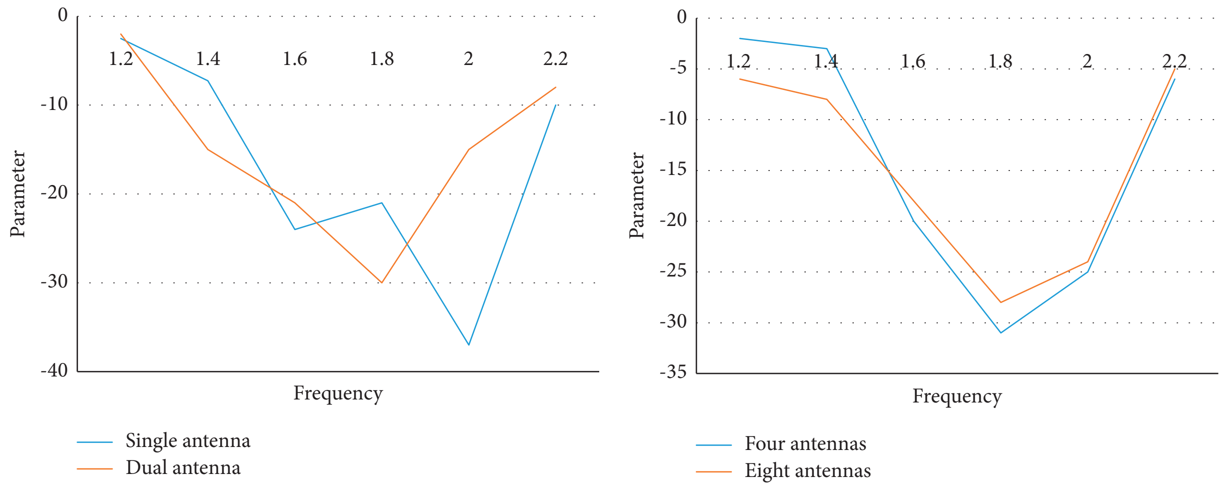

Figure 12: Effects of different antenna arrangements on antenna performance.

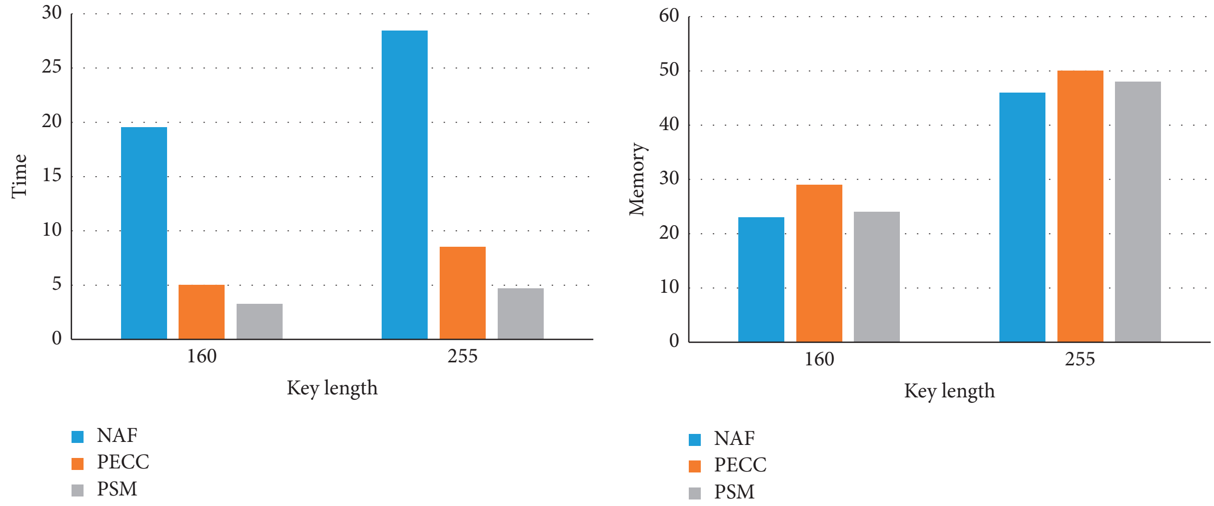

Figure 13: Memory and time versus key length comparison graph.

4. Discussion

This paper is a research on the encryption technology of the Internet of Things RFID system; the purpose is to establish security that can make the Internet of Things system. Although the science and technology involved in the Internet of Things system is closely related to computer technology, it is not only the application of a single technology but the integrated application of multiple technologies. In the method part, the Internet of Things RFID system is expounded accordingly, and its principle and mechanism are explained.

The reader is an important component of the Internet of Things RFID system. The method section proposes corresponding solutions for its structure and influencing factors. First of all, the adjustment of the antenna is made to solve the problem of the reader's own antenna, because this problem will greatly affect the stability of the reader so that the information in the identification process will be leaked. Then, the corresponding research on the algorithm and password of the corresponding electronic tag of the Internet of Things RFID system is made. Because of the special structure of the electronic tag, it has higher requirements on the algorithm. Finally, the more scientific operation of the electronic tag in the algorithm and the identification FID system is realized.

The last is the use of encryption methods for the Internet of Things RFID system. The Internet of Things involves a large amount of user data, and the importance of data security and privacy protection is self-evident. The research on encryption technology in this paper has improved the security performance of the Internet of Things.

5. Conclusion

This paper is a related research article to achieve higher security of the Internet of Things. The purpose of the Internet of Things is to realize the interconnection of all things, which is to make the future human society more efficient. It has an efficient drive in all aspects and fields it touches. The research on the encryption technology of the Internet of Things in this paper is to provide an effective security guarantee for it. At the same time, the research in this paper is also a major expansion of computer science, which makes the integration between disciplines better.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declares that there are no potential conflicts of interest in this study.

Acknowledgments

This work was supported by the Scientific Research Planning Projects of the Shaanxi Provincial Department of Education (no. 21JK0641).

References

[1] Z. Feng, B. Xiao, L. Jia, and U. Chen, "Efficient physical-layer unknown tag identification in large-scale RFID systems," *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 283–295, 2017.

[2] K. Narges, S. Ramesh, and H. Bill, "A balanced scorecard for item-level RFID in the retail sector: a Delphi study," *European Journal of Information Systems*, vol. 21, no. 3, pp. 255–267, 2017.

[3] M. Ramadan, H. Al-Maimani, and B. Noche, "RFID-enabled smart real-time manufacturing cost tracking system," *International Journal of Advanced Manufacturing Technology*, vol. 89, no. 1-4, pp. 969–985, 2017.

[4] S. Youm, Y. Jeon, S. H. Park, and W. Zhu, "RFID-based automatic scoring system for physical fitness testing," *IEEE Systems Journal*, vol. 9, no. 2, pp. 326–334, 2015.

[5] S. H. Tan, Y. Z. x Sun, and Y. Xiang, "A new lightweight RFID grouping authentication protocol for multiple tags in mobile environment," *Multimedia Tools and Applications*, vol. 76, no. 21, pp. 22761–22783, 2017.

[6] Sl Popoola, V. O. Matthews, A. Atayero, and A. Ao, "Solar photovoltaic automobile recognition system for smart-green access control using RFID and LoRa LPWAN technologies," *Journal of Engineering and Applied Sciences*, vol. 12, no. 4, pp. 913–919, 2017.

[7] K. Thiyagarajan, R. Lu, K. El-Sankary, and H. Zhu, "Energy-aware encryption for securing video transmission in internet of multimedia things," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 3, pp. 610–624, 2019.

[8] G. Bansod, N. Pisharoty, and A Patil, "BORON: an ultra-lightweight and low power encryption design for pervasive computing," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 3, pp. 317–331, 2017.

[9] J. Yu, L. Chen, R. Zhang, and K. Wang, "Finding needles in a haystack: missing tag detection in large RFID systems," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2036–2047, 2017.

[10] Sw Lee, S. M. Park, and K. B. Sim, "Smart door lock systems using encryption technology," *Journal of Korean institute of intelligent systems*, vol. 27, no. 1, pp. 65–71, 2017.

[11] N. Sun, T. Li, G. Song, and H. Xia, "Network security technology of intelligent information terminal based on mobile internet of things," *Mobile Information Systems*, vol. 2021, no. 8, pp. 1–9, Article ID 6676946, 2021.

[12] M. Ali, C. Xu, and A Hussain, "Authorized attribute-based encryption multi-keywords search withPolicy updating," *Journal of New Media*, vol. 2, no. 1, pp. 31–43, 2020.

[13] R. S. Boparai, A. Alexandridis, and ZZilic, "Multi-point security by a multiplatform-compatible multifunctional authentication and encryption board," *Journal of Computing and Information Technology*, vol. 26, no. 4, pp. 235–250, 2018.

[14] N. Ha, A. Hussien, LAl-Dabag, and A. Hts, "Paper-encryption system for hiding information based on internet of things encryption system for hiding information based on internet of things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 2, pp. 172–183, 2021.

[15] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857–10872, 2021.

[16] P. Krishnakumar, "Lightweight cryptography and its algorithms in internet of things:an overview," *International Journal of Innovative Research in Science Engineering and Technology*, vol. 10, no. 5, pp. 4900–4904, 2021.

[17] L. S. Abdulla, M. K. Mahmood, A. F. Salih, and S. M. Karim, "Analysis and evaluation of symmetric key ciphers for internet of things smart home," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 1191–1198, 2021.

[18] N. N. Mohamed, Y. Mohd Yussof, M. A. Saleh, and H. Hashim, "Hybrid cryptographic approach for internet of things applications: a review," *Journal of Information and Communication Technology*, vol. 19, no. 3, pp. 279–319, 2020.

[19] K. Han, W. K. Lee, and S. O. Hwang, "cuGimli: optimized implementation of the Gimli authenticated encryption and hash function on GPU for IoT applications," *Cluster Computing*, vol. 25, no. 1, pp. 433–450, 2021.

[20] C. Guo, J. Jia, Y. Jie, C. Z. Liu, and K. K. R. Choo, "Enabling secure cross-modal retrieval over encrypted heterogeneous IoT databases with collective matrix factorization," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3104–3113, 2020.

[21] T. Premalatha and S. Duraisamy, "Secure communication process in IoT using media gate network transmit protocol with reliable data transport protocol," *International Journal of Internet Technology and Secured Transactions*, vol. 9, no. 1/2, p. 136, 2019.

[22] J. Sun, Z. Bie, H. Bie, P. He, and M. Jin, "Secrecy analysis of cognitive radio networks over generalized fading channels," *Security and Communication Networks*, vol. 2020, no. 1, pp. 1–9, Article ID 8842012, 2020.

[23] J. See, K.-M. Mok, W.-K. Lee, and H.-G. Goh, "RISC32-E: field programmable gate array based sensor node with queue system to support fast encryption in Industrial Internet of Things applications," *International Journal of Circuit Theory and Applications*, vol. 48, no. 8, pp. 1209–1226, 2020.