Research on data transmission encryption algorithm of wireless sensor network in cloud storage

ZHOU Xian-chun[1],WU Qi-xiang[2]

{wangyang19111@163.com[1], ainiyiwantian255@tom.com[2]}

（1.School of Information and Intelligence Engineering,Sanya University, Hainan Analysis and Application Engineering Research Center of Software Gene Virus ,Sanya 572022, China;

2.College of Information Engineering,Fuyang normal university, fuyang 236041,China）

Abstract: In cloud storage, the traditional wireless sensor network data transmission encryption algorithm has the problem of low pseudo-randomicity of key flow, resulting in weak encryption security.Therefore, a data transmission encryption algorithm for wireless sensor network in cloud storage is proposed.Formulate the encryption strategy and the initial key strategy, use the basic mode of developing the debugging board to execute the encryption algorithm, and control the input of the encryption algorithm.Control the iteration times of the algorithm, encrypt the data transmission through the encryption wheel transformation and key expansion, and use the pseudo-code to execute the encryption algorithm to complete the data transmission encryption.The test results show that compared with the traditional encryption algorithm, the key flow of wireless sensor network data transmission encryption algorithm designed for cloud storage has higher pseudo-randomicity and stronger security.

Keywords: cloud storage; data transmission; encryption algorithm;

1 Introduction

Cloud storage technology uses the Internet to get the services needed by users with the advantages of on-demand, dynamic and easy expansion. As an online network service, it uses server cluster application technology, grid technology and distributed file system technology to gather data centers for providing storage services through the Internet[1].So that these data centers can jointly provide users with data storage and business access services[2].Cloud storage technology is a new technology developed from parallel storage, distributed storage and grid storage. It has great development potential and wide application prospect.

On this basis, the wireless sensor network can realize the base wood functions such as data acquisition, data processing and sending and gathering[3]. Due to the large data processing density and forwarding volume of wireless sensor networks, the limited energy of a single sensor, and the outsourcing storage mode of cloud storage, it is likely to expose some or all of the data to cloud storage service providers or privileged users. Privileged users have the ability of unauthorized access to users' private data, which is likely to be used by cloud storage service providers, or data leakage due to poor internal management of service providers, the

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2294626

security of user sensitive data has been completely out of the control of the data owner, which is likely to lead to internal attacks such as the disclosure of user data and privacy information.

For the above problems, literature [4] studies the node encryption of wireless sensor network, first introduces the current situation of wireless sensor network encryption. Then, based on the study of S-box and chaos theory, a multi chaos S-box encryption algorithm is proposed, the mapping relationship between them is established, and the constant chaos iteration is realized. This paper has a good encryption effect. However, this encryption algorithm is easily affected by the amount of wireless sensor network data in cloud storage, which makes the generated key stream less pseudo-random and less secure. Therefore, this paper proposes the research of data erasure hybrid encryption algorithm for wireless sensor network in cloud storage to solve the problems existing in the traditional algorithm.

2 Design of data transmission encryption algorithm for wireless sensor network in cloud storage

2.1Develop encryption strategy

In the data transmission of wireless sensor network in cloud storage, the gateway server encrypts the transmission data packet and uses the basic mode of ssx31-b development and debugging board to implement the encryption algorithm[5].The settings of each bit segment of PE control word of ssx31-b security chip are shown in Table 1.

Table 1 PE control word

BIT	Function	Set
0~6	Keep	
7~8	Packet processing mode	00
9~24	Keep	
25	Send data packet encryption processing, position is 1; Receive packet decryption processing, position is 2	0or1
26	Operating mode	0
27	Output message	0
28	Keep	

29	Enter InPacket to process IPv4 packets	0
30	Enter InPacket to follow SA-Number	0
31	Enter InPacket without UserField	0

In the kernel encryption module of the driver, using the kernel interface of ssx31b, the basic encryption and decryption based on the encryption algorithm is carried out for the data segments of IP packets. The SA function of ssx31b security chip is to specify specific encryption algorithm and corresponding key[6]. The encryption card completes the corresponding encryption processing according to the specified SA. Table 2 shows the settings of each bit segment of SA command word of ssx31b security chip.

Table 2 SA command word

BIT	Function	Set
0~9	Keep	
10~11	00：ECB 01：CBC 10:AES_CTR 11:Keep	01
12~15	0000:DES 0001:3DES 0010:AES128 0011:AES192 0100:AES256 1111:NULL	0001
16~19	000:HMAC-MD5 001:HMAC-SHA-1 010:MD5 011:SHA-1 100:NULL 111:NULL	111
19~31	Keep	

The SA structure contains eight doubleword key fields. For DES key, only key is used; for 3DES key, key ~ Key3 is used; for AES key, all 8 doublewords of key domain may be

used.

In the encrypted IP packets, an encryption mark should be added to identify the encrypted IP packets, but the mark should not change the data segments in the IP packets, so that the gateway server receiving the IP packets can identify and decrypt them.

The implementation of data transmission encryption in wireless sensor network is inseparable from the key. Under the above encryption strategy, the initial key strategy is formulated[7].A random initial key obtained by both sides of data transmission is the security foundation of the whole encryption process. Random selection of a large prime number Q , Smaller number q , random number i , Public key obtained $k = q^i \bmod Q$, Large prime number Q and Smaller number q through negotiation between both parties of data transmission.The server randomly generates a smaller number q calculation $k = q^i \bmod Q$,Client randomly generated $i^{'}$,and calculate $k^{'} = q^{i^{'}} \bmod Q$,exchange between two parties k and $k^{'}$,Successfully obtained the same random key.Because there are only large prime numbers Q ,Smaller number q , k and $k^{'}$ may be intercepted by eavesdroppers,So unless privileged users can compute discrete logarithm to recover random number i and $i^{'}$,Otherwise, the computer will not be able to exit k and $k^{'}$ .therefore k and $k^{'}$ can be used in encryption algorithm as the same secret key which is distributed to both sides of communication.

2.2 Control the input of encryption algorithm

Set an iterative block cipher. The length of plaintext block and key is one of the following three values: 128bit, 192bit, 256bit.The encryption algorithm is run on a 4x4 matrix called "state". Every step of the algorithm acts on this matrix.The plaintext packet and the key are expressed as 4x H_a respectively matrix of 4x H_b , H_a and H_b one thirty second of plaintext packet and key length respectively[8].For plaintext packets or key matrices, each element corresponds to a value on GF (28).The number of iteration rounds of encryption

algorithm H_c is related to H_a and H_b.

In the encryption process, the input of the control encryption algorithm is carried out on the 4X4 matrix, and the plaintext grouping and key length are controlled at the same time, so as to control the number of iterations of the algorithm and avoid too many times making the algorithm too heavy.

2.3Encryption round transformation and key extension

The data transmission encryption process of cloud storage wireless sensor network is determined by the round transformation function, which consists of four modules: byte transformation, row displacement, column obfuscation and round key addition[9]. Each module performs different operations on the state matrix.The radiative transformation formula of state matrix is as follows:

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \\ u_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (1)$$

The above affine transformation is composed of two transformations. The two transformations are implemented with the S-box of 1-byte input / 1-byte output, and the principle is shown in the figure below.

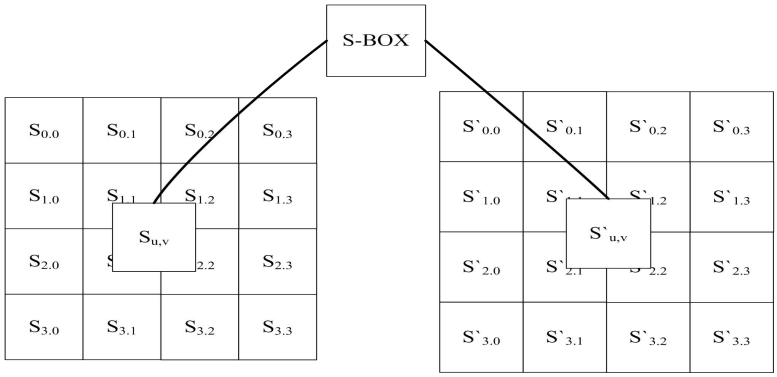

Figure 1 Schematic diagram of byte realization nonlinear transformation

When decrypting, the module corresponding to SubBytes is called InvSubBytes, and

they are the inverse process of each other. The specific process is as follows:For each byte in the state matrix, a new byte is obtained by using the inverse affine change, and then it is multiplied by the inverse, so that the inverse S-box can be obtained. Finally, each byte of the state matrix is transformed by using the inverse S-box[10].

Row shift is mainly a cyclic shift for each row of the state matrix, and each row shift is different. So what I'm going to do is, line 0 doesn't change, line 1 goes around by a_1 to the left. Row 2 loops a_2 to the left.Line 3 loops a_3 to the left.Among them, the selection of displacement a_1, a_2 and a_3 is related to H_a.

When decrypting, the module corresponding to ShiftRow is called InvShiftRows, and they are the inverse process of each other, so the process is exactly the same.

The third step is the mixed transformation of the columns. Each column on the state matrix is treated as a polynomial, where each coefficient of the polynomial is on GF(28) and the degree of the polynomial is less than 4. Then, the polynomial and the expression are:

$$a(v) = '03'v^3 + '01'v^2 + '01'v + '02' \quad (2)$$

In the formula, the coefficient is represented by base 8,(x)='03'x3+'01'x2+'01'x +'02'reversible polynomials multiply over $v^4 + 1$ .We get the final result. The specific transformation process is shown below

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{bmatrix} \quad (3)$$

The sum in formula (3) represents the terms on the state matrix of u and v in the column mixture. Its decryption and row displacement decryption transformation mode is the same.

The round key encryption transformation is just to add the round key and the state matrix. The addition refers to the operation of different fields on GF (28). The round key is obtained through key extension, and the specific extension process is shown in the figure below.

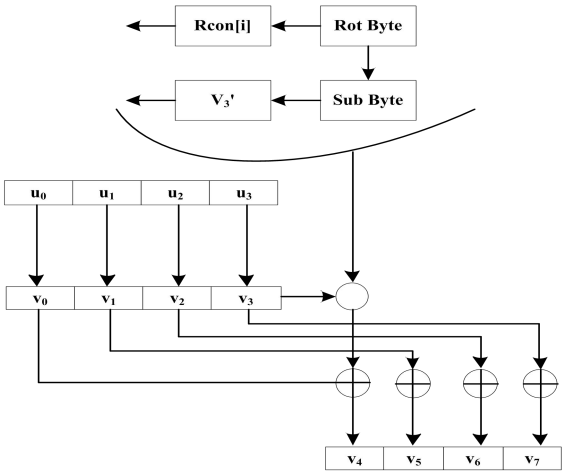

Figure 2 Schematic diagram of key extension

Iteration through the seed key produces a key with a total length of 4 H_a (H_a +1)bytes required for the entire encryption.So you can think of the key as the number of groups from *(N,+1).Each of these elements is 4 bytes in size.Through the above process encryption wheel transformation and key expansion, for the subsequent implementation of encryption preparation.

2.4 Encryption of data transmission

The key distribution strategy is adopted to randomly initialize the key, and the public key of the key exchange is generated through the initialization function of the server in the wireless sensor network, and the public key data stored in the pointer variable is assigned to the public key array to facilitate communication and transmission.The public key data is transmitted to the client, and at the same time the server receives the array of the client public key from the client. The public key of the client is used to generate the Shared key, and the wireless sensor network data transmission is encrypted through the encryption wheel transformation process mentioned above.

3 Simulation test and analysis

3.1 test preparation

The pseudo-randomicity of the key flow is tested by test simulation. In the test, MATLAB tool and in the Windows 7 environment were used to obtain data groups of different data sizes to test and analyze the encryption algorithm.

In the above environment, multiple sets of test data prepared are used to more accurately analyze the pseudo-random test results of key flows of different encryption algorithms.

3.2The test data

Using the open source text data set SemEval, the relevant parameters of the ten sets of data required for the test are shown in the table below.

Table 3 test data parameters

name	The amount of data（MB）	Number of text
Data-1	26	5
Data-2	54	9
Data-3	147	17
Data-4	89	8
Data-5	441	23
Data-6	562	16
Data-7	631	29
Data-8	847	41
Data-9	906	53
Data-10	547	21

Using the above ten sets of data to test the pseudo-random strength of the generated key flow under different encryption algorithms.

3.3 test results and analysis of pseudo-randomness of key flow

MATLAB software is used to simulate the run test. The purpose is to test the pseudo-randomness of the key flow by calculating the number of uninterrupted sub-sequences composed of the same bits in the key flow sequence.

The test group using the designed encryption algorithm was set as the experimental group, and the test group using the traditional encryption algorithm was set as the control group. The test results are as follows:

Table 4 test results of the experimental group

Data set	The amount of data （MB）	Statistics δ	P-value
1	26	0.5006	0.3056
2	54	0.4997	0.4125
3	147	0.4996	0.1741
4	89	0.4991	0.2635
5	441	0.5001	0.2584
6	562	0.5003	0.2633
7	631	0.5007	0.3147

8	847	0.5005	0.1926
9	906	0.4996	0.3341
10	547	0.4992	0.2547

Table 5test results of control group

Data set	The amount of data （MB）	Statistics δ	P-value
1	26	0.5011	0.1746
2	54	0.4983	0.1596
3	147	0.4991	0.1006
4	89	0.4995	0.1079
5	441	0.5021	0.0214
6	562	0.3019	0.0365
7	631	0.2027	0.0694
8	847	0.2015	0.0613
9	906	0.1087	0.0749
10	547	0.3092	0.0893

The statistical value δ in the table represents the proportion of statistical 0 and 1 in the whole sequence, and the standard is $\left|\delta\text{-}0.5\right|<0.1$ .In this interval, the smaller the value is, the stronger the pseudo-randomicity of the key flow generated by the encryption algorithm is and the higher the security is.P - value

Represents the distribution of 0 and 1 in the sequence, and the standard value is $\mathrm{P-value}>0.1$.

According to the results in the above standard observation table, table 4 shows that for different data volumes,the statistic δ is always in the standard $\left|\delta\text{-}0.5\right|<0.1$ range.P-values are all greater than 0.1; As shown in table 5,if the data volume is less than 500MB, the statistical values δ and p-value obtained in the test are within the normal range.However, as the data volume increases and exceeds 500MB, the statistical values δ and p-value are abnormal, which are not within the standard range.Combined with the above results, the proposed encryption algorithm for wireless sensor network data transmission in cloud storage has higher pseudo-randomicity of key flow and stronger security, which is better than the traditional data transmission encryption algorithm.

4 Conclusion

With the development of computer and Internet technology, cloud storage is applied in more and more fields. All kinds of important data are saved and transmitted in the form of cloud data.Due to the divergence and randomness of the Internet, data are copied, tampered and forged in the process of transmission, and data security is seriously threatened.Therefore, an encryption algorithm for data transmission in wireless sensor network in cloud storage is proposed. Through comparison and simulation test, it is verified that the designed encryption algorithm can effectively solve the problems existing in the traditional encryption algorithm and ensure the security of data information in data transmission.As an important research hotspot, data transmission security has great economic benefits and social significance.

5 Fund projects

Sanya City Science and Technology Cooperation Project 2019YD26

Reference

[1]Wang,Q.Wei,Y.D:Simulation of Character Type Data Encryption and Query in Centralized Database . Computer Simulation.Vol.35,pp.359-362(2018)

[2]Lu,Z.Q: Encryption of Wireless Sensor Networks Based on Chaos and WEP.Computer Science.Vol.46,pp.362-364+391.(2019)

[3]Liu,Q.F.Peng,L.Y:Design of cloud storage system for mass optical fiber communication data .Laser Journal.Vol.39,pp.183-187(2018)

[4]Luo,W.X.G,Y:An Encryption Technology in Wireless Sensor Network.Bulletin of Science and Technology.Vol.34,pp.6215-218(2018)

[5]Fu,A.M.Song,J.Y.Su,M:A Security Client-side Deduplication with Encrypted Data in Cloud Storage.Acta Electronica Sinica.Vol.45,pp.2863-2872(2017)

[6]Shi,L.Yu,S:Research on Data Security of Cloud Storage Service in Digital Design Database of Tractor.Journal of Agricultural Mechanization Research.Vol.40,pp.205-209(2018)

[7]Xu,J.Y.Xiong,J.Cao,Z.T:Design of smart meter communication security based on standard encryption algorithm.Electrical Measurement & Instrumentation.Vol.55,pp.125-128+133(2018)

[8]Liu,T.Meng,X.Y.Zhang,L.B:Research on secure channel coding based on polarization code in degraded Gauss eavesdropping channel.Journal of Harbin Engineering University.Vol.39,pp.169-172.(2018)

[9]Wang,X.L.Jiang,X.Z.Li,Y:Model for Data Access Control and Sharing Based on Blockchain . Journal of Software.Vol.30,pp.1661-1669(2018)

[10]Xie,G.B.Jang,X.Z: Double chaotic image encryption algorithm based on two dimensional discrete fractional Fourier transform.Computer Engineering and Applications.Vol.54,pp.40-45(2018)