Using AES Encryption Algorithm to Optimize High-tech Intelligent Platform

CHUNG-CHIH LEE
Graduate School of Business and Operation Management
Chang Jung Christian University
TAIWAN

HSING-CHAU TSENG
Department of Business Administration
Chang Jung Christian University
TAIWAN

CHUN-CHU LIU
College of Continuing Education
Chang Jung Christian University
TAIWAN

HUEI-JENG CHOU
Department of Accounting and Information Systems
Chang Jung Christian University
TAIWAN

Abstract: AES encryption algorithm is a universal algorithm, which can be used in many fields, including intelligent marketing. In the field of modern intelligent marketing, every enterprise adopts the platform model to carry out marketing activities, which gives birth to the high-tech intelligent marketing platform. The use of this platform does bring great convenience to marketing activities and effectively improve the success rate and efficiency of marketing. However, with the in-depth use of the intelligent marketing platform, people find that there are many security risks in this platform, including Marketing information may be damaged by people, indicating that the platform needs further optimization. At this time, AES encryption algorithm has become the main method of platform optimization. In order to understand the optimization performance of AES encryption algorithm in the high-tech intelligent marketing platform, this paper will analyze the concept of the algorithm, the existing defects of the platform, the optimization scheme of the platform under the algorithm, and finally simulate the results of the optimization scheme to verify the feasibility of the application of the algorithm.

Key-words: AES encryption algorithm; high tech intelligent marketing platform; marketing information risk.

Received: April 18, 2021. Revised: November 25, 2021. Accepted: December 7, 2021. Published: December 26, 2021.

1 Introduction

As a new form of technology born in the Internet environment, intelligent marketing platform has outstanding performance in function and performance, and begins to move closer to the function of "human" in the development direction, which shows that platform application can replace human and give human help to some extent [1]. The necessary conditions for people to use the intelligent marketing platform to carry out marketing activities include the Internet, network equipment (such as computer, smartphone or other network electronic communication equipment). Therefore, the information in marketing activities must be stored in the Internet environment through the hands of network equipment. At this time, because some marketing information belongs to the confidentiality of marketers, it needs to be protected, but the early intelligent marketing The information protection function of the marketing platform is relatively weak, especially in the Internet environment, the original information protection function of the platform is further reduced, the reason is that the Internet environment has the open characteristics, and the intelligent marketing platform, as an Internet-based platform, has the same characteristics. In addition, the marketing business needs to open the upload / download interface, so it has several advantages It can't be lower than the invasion of external information. It can be seen that if the intelligent marketing platform is not protected by other means, the rights and interests of the marketers will be affected. Once this phenomenon spreads, it will become a social problem, causing a negative impact on the use of the Internet [2-3].

Under this condition, modern people's awareness of Internet information protection began to improve rapidly, especially in marketing enterprises. Before using intelligent marketing platform to carry out marketing activities, they will inevitably inspect the security of the platform. If the inspection results show that the security is not up to standard, they will not carry out marketing activities, but this way is to solve the problem, and the Internet security threat has always been There is [4]. Then the relevant research began to study the problem of "how to eradicate the security threat of intelligent marketing platform". Through the research, it came to the conclusion that "if the intelligent marketing platform is encrypted, the current problem can be solved". Therefore, how to eradicate the problem has become the key research object in the field of network cryptography.Network cryptography is a professional field specialized in the research of network cryptography technology. It aims to block the data and information with practical significance by using encryption technology, so as to provide information protection. At the same time, it provides information operation channel for the correct user through the random sequence data information without practical significance (generally referring to account number and password), so as to prevent the incorrect user from accessing the platform Illegal operation of data and information. However, with the development of encryption technology, the decryption technology is also developing. The relativity of the two kinds of technology makes them form the relationship of competing against each other, so encryption technology has to maintain its own strong development momentum. After a long-term development, modern encryption technology is divided into two types, namely asymmetric key encryption and symmetric key encryption, in which asymmetric key encryption. In essence, encryption is a key protection technology, which is usually applied to the encryption requirements with complex algorithm and low efficiency of data realization. Symmetric key encryption technology is a technology for both sides of data receiving / sending, that is, both sides must use the same key to encrypt and decrypt data or information, which is higher in applicability and security level than before The only defect is that the operation is relatively complex, but this does not prevent users from loving the encryption technology. Therefore, symmetric key encryption has gradually developed into the mainstream technology in the field of modern encryption, and has been widely used in the intelligent marketing platform [5-7].According to the development of symmetric key encryption, the early symmetric key encryption was mainly implemented by data encryption standards (DES), but des has been broken by decryption technology in modern times, while the modern symmetric key encryption was implemented by Advanced Encryption Standard. With the help of AES, it has successfully improved the security of symmetric key encryption, and can provide users with comprehensive information security. Therefore, it is favored by the intelligent marketing platform. As the implementation algorithm of symmetric key encryption, AES algorithm has good sensitivity and diffusion. At the same time, it can be divided into two types, sequence cipher and block cipher. In encryption, sequence cipher is a symmetric cipher algorithm which processes data information according to the time change. It takes a bit as the basic unit. Its conversion speed is very fast and it is commonly used in the military field, the block cipher is a technology that does not change the encrypted data according to time. It can divide the encrypted data into different processing units of different sizes. The size specifications are generally 64 bit and 128 bit [8-11]. In the modern intelligent marketing platform, the main use is block cipher, so this research will also analyze the AES encryption algorithm.

2 AES Algorithm Concept

2.1 Algorithm Description

The AES algorithm is described from algorithm encryption, decryption and key extension.

(1) Algorithm encryption

AES algorithm encryption is a kind of encryption characterized by chaotic code sequence, that is, the original information encrypted by AES algorithm will become unavailable, which is characterized as chaotic code sequence. The original information in this state cannot be used directly. The whole process of AES encryption is divided into three stages: byte substitution, row displacement and column obfuscation.

① Byte substitution (sub Bytes): byte substitution is mainly performed according to the non-linear replacement of S-box. In the process, each byte in the input state and intermediate state will be searched in the S-box table to get the corresponding new bytes (note that the "state" of input state and intermediate state refers to the result of transformation of input data or intermediate data), and then the new bytes will be used to replace the original bytes for output, so as to construct a new byte Garbled. The search method for new bytes in the S-box table is: first, the high four bits or the first four bits of the input 8-bit binary number are used as the row value of the query table, and the last four bits or the low four bits of the 8-bit binary number are used as the column value of the query table; secondly, the coordinates corresponding to the new bytes in the S-box table can be confirmed according to the row value and the column value; finally, the new bytes can be found according to the coordinates for replacement. At the same time, byte substitution needs three steps in AES algorithm, that is, first initializing the S-box, recording the first four bits of the input eight bit byte as row value and listing them in line x, and then listing them in line y as column value, then mapping each byte in the S-box to the inverse of the finite field GF (28) through the method of calculating the inverse of multiplication of finite field GF (28), and finally mapping each byte in the result of multiplication of inverse element Each element is written as (a7a6a5a4a3a2a1a0) bit by bit, and each bit of each byte is transformed by affine transformation method, which is written as (b7b6b5b4b3b2b1b0) [12-13]. Formula (1) is the AES algorithm byte substitution meta expression. Where CI is a byte element given in AES algorithm whose value is {63} of hexadecimal number.

② Shift Rows: row displacement is the displacement action to byte replacement, which represents that the byte is gradually shifting. In practice, the size of byte offset depends on the length of the key, that is, the larger the key length, the larger the offset, otherwise the smaller. In principle, the shift process is to rotate the i-th line of the state matrix to the left by CI bytes, where I is 1, 2, 3. Table 1 shows the relationship between key packet length and byte offset [14]. In addition, in the 128 bit encryption operation, the row bit transformation encrypted by AES algorithm circulates each row of the state matrix.

Table 1. Relationship between Key Packet Length and Byte Offset

Key packet	C0 (Bytes)	C1 (Bytes)	C2 (Bytes)	C3 (Bytes)
Length (Bits)				
128	0	1	2	3
192	0	1	2	3
256	0	1	3	4

PS: the content of Table 1 is only an example. In actual operation, the same fixed changes will not occur.

③Mix Columns: in column confusion, first of all, each column of the state matrix is regarded as a polynomial of the finite field GF (28), and each polynomial is recorded as a (x), then a (x) is multiplied by formula (2), and a (x) and formula (3) are modular [15-16]. Formula (4) is a polynomial implementation method.

Formula (2)：c x 03x3 01x2 01x 02
Formula (3)：h x x4 1
Formula (4)：b x c x a x mod h x

After column obfuscation, the substitute byte can be disorderly programmed on the basis of finite field, which can replace the original byte arrangement, ensure the encryption effect, and also play a good diffusion role in data processing.

(2) Algorithm decryption: the decryption process of AES algorithm is basically the same as that of encryption process in terms of calculation method, which will not be covered in this article. However, in terms of calculation direction, each process of decryption algorithm is the opposite of encryption algorithm, so each link of AES algorithm decryption process can be called "reverse link", which includes reverse byte substitution Reverse row displacement, reverse column obfuscation [17].

(3) Key expansion: key expansion is the final step to realize AES algorithm encryption or decryption, and it is the basis to support encryption and decryption operation. In the process, the initial key should be filled with data first. The filling object is n rows and N columns of the state matrix. For example, on the basis of 128 bit key length, n rows and N columns are respectively 4 and 4 [18]. Secondly, each word in the state matrix is recorded as w [0], w [1], w [2], w [3] (each word must be composed of four bytes), so that an array of word units composed of four words appears in the state matrix, which represents the key judgment logic of AES algorithm. If the input or output key does not conform to the array, the judgment fails, otherwise it passes.

2.2 Algorithm Mode

See Table 2 [19] for the operation mode of AES algorithm.

Table 2. Operation Mode of AES Algorithm

Mode serial number	Pattern	Features
1	Codebook mode	Encrypting one group of plaintext at a time and using the same key can be applied to the secure transmission of single data.
2	Password group link mode	Using the former group of ciphertext and the latter group of plaintext XOR operation and then encryption operation with the key can be applied to general packet oriented transmission and data authentication.
3	Password feedback mode	Each time the fixed data bits are processed, the ciphertext obtained from the previous encryption is used as the input to generate the pseudo-random number, and then the pseudo-random number and the plaintext are XOR operated to get the next ciphertext. It can be used in data stream oriented general transmission and data authentication.
4	Output feedback mode	In the encryption algorithm, the input is obtained from the output of the previous encryption and the whole packet is used. It can be applied to data stream transmission over noisy channels.
5	Counter mode	In the encryption algorithm, the input is obtained from the output of the previous encryption and the whole packet is used. It can be applied to data stream transmission.

(1) Electronic codebook mode (ECB)
In the block cipher work of AES algorithm, if the electronic codebook mode is adopted, the algorithm and the same key should be used to group the plaintext. This is to make the block data independent from each other, and to encrypt and decrypt separately, so as to realize the distributed arrangement of encryption and decryption of each block data. The operation of this mode is almost "impeccable" in theory, because when the whole plaintext data becomes scattered, the external invasion must be broken one by one, but this will inevitably bring huge difficulty to the invasion, so in theory, AES algorithm encryption or decryption in the electronic codebook mode can hardly be broken. In fact, if the plaintext packets in the electronic codebook mode are divided into a, B, C and so on, as long as any of the packets have the same information, the AES key sequence in the electronic codebook mode will be homogenized, which makes the external intrusion only need to break through one of the component data, obtain the same information with other packet data, and then "follow the rules of the gourd" To break through other packet data greatly reduces the difficulty of intrusion, indicating that the encryption security of the electronic codebook mode needs to be improved. Therefore, the electronic codebook mode is generally only used in the case of relatively less data, or there is no same information in all data, and the actual application scope is relatively small [20].

(2) Cipher group link mode (CBC)
In the block cipher mode, first of all, an initial vector is introduced to eliminate the same information in a certain information data and avoid the problem of producing the same key. Secondly, AES algorithm is used for encryption. It can be seen that the block cipher mode can avoid the problem of the same key. With the help of the theoretical security of the block cipher, it can effectively prevent external invasion, which shows that it has high security. The defect of the block cipher mode is that the encryption operation of AES algorithm needs to operate on each key, which is very slow, so there is operation in this mode These two defects are acceptable from a general perspective, indicating that the method has a wide range of applications.

(3) Password feedback mode (CFB)
In the password feedback mode, the block cipher multiple is defined as "stream cipher", which makes the encryption not need to fill in the data, but also provides the initial vector and increases the number of encryption. In terms of encryption principle, firstly, register data and key data are used as encryption function to input into AES algorithm, secondly, encryption information and output of encryption function are obtained through calculation, and then the ciphertext can be obtained by exclusive or operation according to the output result. Finally, the process of ciphertext input register is cycled, and all packets of the device are encrypted. The characteristic of the password feedback mode is that it can effectively hide the plaintext information and play a role in ensuring the information security, but the disadvantage is that the calculation ability of AES algorithm in this mode is poor in education of other modes, and the initial vector provided by the mode is single, which is easy to bring error transmission, which indicates that the

encryption stability of the mode is insufficient, so it needs to be carefully considered when using.

(4) Output feedback mode (OFB)
The output feedback mode is the same as the password feedback mode in structure, but the difference between them is that the output feedback mode mainly uses the output result of encryption function to fill in the register, while calculating the whole group. It can be seen that the AES algorithm operates faster in this mode, which can avoid the overall error caused by a single error. Therefore, this mode is suitable for in the data transmission with high encryption redundancy. The defect of the output feedback mode is that the ability to resist message tampering is weak, which needs other measures to make up.

(5) Counter mode (CTR)
In the application of counter mode, first of all, a count scale with the same length as the encrypted packet data must be set, and the count scale value of each packet data in the overall encryption cannot be the same, then the counter is initialized, and then a series of operations such as encryption operation using AES algorithm can be done. The advantage of counter mode is simple operation, but the disadvantage is that the encryption security is relatively low, and there are limitations at the same time, so the application of this mode is relatively rare.

3 Existing Defects of Hightech Intelligent Market Platform

3.1 Low Encryption Security

Generally speaking, the encryption status of modern high-tech intelligent marketing platform is not good, especially in the security, there are many problems, so the overall encryption security is low, need to be improved. There are two manifestations of low security of platform encryption, which are incomplete encryption and backward encryption methods. The following three performances will be analyzed.

(1) Incomplete encryption
Most modern high-tech intelligent marketing platforms use AES algorithm for encryption, because of the lack of recognition of the algorithm, they will use the wrong mode for encryption, so the whole encryption is incomplete due to the mode defects. For example, in the encryption of a marketing platform, the enterprise adopts AES counter mode for the sake of cost and convenience. In this mode, because of the lack of recognition, they can be set at will According to the characteristics of counter mode, it can be seen that the counter with the same value is not effective, indicating that the overall encryption of the platform is incomplete.

(2) Backward encryption method
A considerable number of high-tech intelligent marketing platform enterprises are still backward in their understanding of encryption technology. Therefore, when they choose encryption technology, they usually choose des technology, which has been broken down. For the "intentional person", it is like nothing, indicating that the whole encryption security is low.

3.2 Difficult Encryption

Many high-tech intelligent marketing platforms will encounter great difficulties when using AES algorithm for encryption. For example, the algorithm cannot automatically encrypt the new data groups, resulting in recalculation of each group of new data groups. As a marketing tool, the platform has a huge amount of daily information, so the frequency of new data groups is high, making algorithm recalculation The operation of the platform can not keep up with the data group update, which brings a huge security risk.

4 Design of AES Algorithm Encryption Scheme for High-tech Intelligent Market in Platform

4.1 System Design Scheme

Considering the existing problems of AES algorithm encryption in high-tech intelligent marketing platform, firstly, this paper will choose the group link mode of AES password which has strong applicability to design the optimization scheme design. Secondly, the design form of the scheme is divided into modularization and layering. The system of the algorithm in the design is composed of data port, control unit, key extension unit and wheel function transformation unit. The functions of each component are shown in Table 3.

Table 3. Functions of Algorithm System Components

Component	Function
Data port	Finish loading data input and output
Control unit	Coordinated encryption and

	decryption control
Key extension unit	Support key expansion operation and key storage, and provide round key for encryption or decryption
Transformation unit of wheel function	Each round of key addition, byte substitution transformation, row bit transformation and column obfuscation transformation is realized

4.2 Module Control Design

In the module control design, because the encryption operation in AES algorithm will not be executed synchronously with the decryption operation, and the method is basically the same, this paper only analyzes the encryption design of AES algorithm. First of all, considering the use conditions and platform security of cipher block link mode, the length of encrypted block data in the design is 128 bits, so in the initial stage of AES encryption design, 10 rounds of encryption are needed. Secondly, in the 10th round of 10 rounds of encryption process, it is necessary to distinguish the 10th round of transformation from the first nine rounds, and the encryption key operation of each round should be consistent with the specific key. Therefore, in the module design, this paper designs a control module composed of transformation signal, signal receiving interface and transformation value. This module can encrypt all existing data automatically, which solves the problems of incomplete encryption, backward encryption methods and difficult encryption. The module control logic is shown below.

(1) Step 1

The transform signal is located in the key expansion. When the key is expanded every time, the transform signal will automatically add 1, and the transform value will be added 1. In principle, if the transform signals after 10 rounds of key expansion in 128 bit encryption is 10, the signal will be obtained by the signal receiving interface, and the signal value is 1. Then the interface will perform the encryption round transform operation according to the external selection signal, so that the transform value will change the same.

(2) Step 2

On the basis of step 1, the transformation value will have dynamic performance. When the transformation value changes in value, the same number of packet data will be encrypted. Therefore, when the transformation signal extension is completed, the transformation value is equivalent to the number of packet data included in the extension, and all packet data can be encrypted. In addition, each time the key extension stops, the transformation value will also stop after the encryption is completed. At this time, because there is no new packet data in the key, the transformation value will be cleared. Only when the new packet data enters step 1 and the key extension movement is triggered, the transformation value will continue to move, which can not only avoid transmission errors, but also ensure that the new data is encrypted at the first time. In theory, it can improve the security of high-tech intelligent marketing platform and achieve the purpose of optimization.

5 Simulation Test

In order to verify the effectiveness of the standard design system, this paper will carry out simulation test, the test steps are shown below.

(1) Fundamentals of testing

Three groups of data are selected for testing, as shown in Table 4.

Table 4. Simulation Input Data

Serial number	128 Bit initial key	128 Bit plaintext data	128 Bitciphertext data
1	0123456789ABCDEF	0F1571C947D9E8590	FF0B844A0853BF7C
	FEDCBA9876543210	CB7ADD6AF7F6798	6934AB4364148FB9
2	73512D4F09ABE764C	F183749EAFCD5547	458E09B6E40AA102
	DFF4A181329EC66	9A1F882734AE2276	2FC8BA1488AE770E
3	4D766CD37F091464E	F18D6B11DC9817AA	1EB722CA4D77A92F
	5F68C99ACB7012A	640CFE3BEACC398F	C0CD29FF2098ABA3

(2) Test method

Firstly, the VHDL hardware description language is used to program and build a simulation model, which includes clock signal loading port (CLK), function control port (AES FUCS), 128 bit initial key input port (AES key), 128 bit initial data input port (AES DIN), 128 bit data output port (AES dout) components. Secondly, load 128 bit data encryption function on the basis of the model to test.

(3) Test results

In the above test methods, firstly, the 128 bit data encryption is completed by inputting control signals from the outside, and then the conventional forced cracking method is imported to verify the encryption performance. The results show that in the three groups of data, the conventional forced cracking method takes about 70 days to crack a single group of data key, and if it takes about 1260 days to crack all the data keys, and the encryption in this design will be replaced according to the timer, that is, every 24 hours, which shows that the design scheme cannot be cracked, with high security.

6 Conclusion

To sum up, through the overview of AES algorithm, we know that this algorithm has a high application value in encryption. Compared with the traditional DES algorithm, it has outstanding advantages and is worth learning. At the same time, the overview also describes the encryption process of AES algorithm. According to the analysis of the encryption status of the modern high-tech intelligent marketing platform, we can see that the application of AES algorithm of the platform is not good. In this paper, AES encryption design is carried out for the purpose of optimization. According to the logic judgment, the design can play an optimization effect in theory, improve the encryption level of the platform, and ensure the internal information security. Finally, the test is carried out by means of simulation, and the result is obvious The theoretical effect of the display design can also appear in practical application, which shows that the system design is successful and can be used for reference.

References:

[1] Z. J. Xiao C. Hu and Z. T. Jiang “Optimization of AES and RSA algorithm and its mixed encryption system”, Application Research of Computers., (2014), pp. 393-403.

[2] X. Liu Y. B. Hao and T. L. Fan, “Application of intelligent algorithm in the optimizati on of novel protein regulatory pathway:Mechanism of action of gastric carcinoma protein p4 2.3”, Journal of Cancer Research&Therapeutics., vol. 12, no. 2, (2016), pp. 650-656.

[3] O. K. J. Mohammad S. Abbas and E. S. M. Elhorbaty, “Innovative Method for Enhancing Key Generation and Management in the AES-Algorithm”, vol. 4, no. 4, (2015), pp. 14-20.

[4] W. Snehal and M. Rashmi, “Dynamic Partial Reconfiguration Implementation of AE S Algorithm”, International Journal of Computer Applications, vol. 97, no. 3, (2014), pp. 15-18.

[5]N. Lalithamani and M. Sabrigiriraj. “Dual Encryption Algorithm to Improve Security in Hand Vein and Palm Vein-Based Biometric Recognition”, Journal of Medical Imaging&Health Informa tics, vol. 5, no. 3, (2015),pp. 545-551.

[6] N. P.Smart “Physical Side-Channel Attacks on Cryptographic Systems”, vol. 1, no. 2, (2015), pp. 6-13.

[7] C. Ünal K. Sezgin and Z. Ahmet “A novel hybrid encryption algorithm base d on chaos and S-AES algorithm”, Nonlinear Dynamics, vol. 92, no. 3, (2018), pp.1-15.

[8] Z. Lu H. Liu, J. Ma, “DPA platform design for AES encryption equipment”, Journal of H uazhong University of Science&Technology, vol. 45, no. 8, (2017), pp. 1-5.

[9] X. Zhang X. Zhao and HZhang, “Encryption algorithm based on improved layered and revers ible cellular automata”, Journal of Nanjing University of Science&Technology, vol. 38, no. 3, (2014), pp. 313-317.

[10] N. Hwang O. Yi and D. Kwon, “Software Implementation of Lightweight Encryption Algorit hm Using Single Instruction”, Multiple Data Instructions, vol. 21, no. 3, (2015), pp. 571-576.

[11] C. H. Baek J. H. Cheon and H. Hong, “White-box AES implementation revisited”, vol. 18, no. 3, (2016), pp. 273 -287.

[12] K. Shahbazi and M. Eshghi, “Design of a Specific Instructions Set Processor for AES Algorith m”, International Journal of Computer Applications. vol. 93, no. 93, (2014), pp. 36-40.

[13] D. S. Dayana, “An Efficient Approach for Network Mobility Based on AES Algorithm”, Ad vanced Materials Research, (2014), pp. 1269-1275.

[14] K. Puneet and B. R. Shashi, “Development of modified AES algorithm for data security”, Optik-International Journal for Light and Electron Optics, vol. 127, no. 4, (2016), pp. 2341-2345.

[15] H. B. Ma,Y. L. Wang, “Gaoling Li.Implementation of Audio Data Packet Encryption S ynchronization Circuit”, Advances in Intelligent Systems&Computing, vol. 298, (2014), pp. 321-329.

[16] X. Zhang and K. K. Parhi. “On the Optimum Constructions of Composite Field for the AES Algorith m”, IEEE Transactions on circuits and systems II: express briefs, vol. 53 ,no. 10, (2015), pp. 1153-1157.

[17] Xiao X. Z. Dai, H. B. Qi, H. K. Liu, Q. S., Zhang and Y. X. Wang, “High-Speed Parallel Implementation of AES Key Expansion

Algorithm Based on FPGA", Applied Mechanics&Materials, (2015), pp. 712-716.

[18]Z. Lu H. Liu and J. Ma, "DPA platform design for AES encryption equipment", Journal of Huazhong University of Science&Technology, vol. 45, no. 8, (2017), pp.1-5.

[19]S. Wankhade, R. Mahajan, "Dynamic Partial Reconfiguration Implementation of AES Algorithm", International Journal of Computer Applications, vol. 97, no. 3, (2014), pp. 15-18.

[20]Y. W. Huang, P. Mishra. "Trace Buffer Attack on the AES Cipher", Journal of H ardware&Systems Security, vol. 1, no. 1, (2017), pp. 68-84.