2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)

Communication encryption scheme in multi-embedded systems based on distributed architecture

Shou Yingjie
School of Artificial Intelligence and Computer Science
Jiangnan University
Wuxi, China
6181914026@stu.jiangnan.edu.cn

Zhang Xihuang
School of Artificial Intelligence and Computer Science
Jiangnan University
Wuxi, China
18921160516@163.com

***Abstract*—With the increasing use of Internet-based embedded devices, multi-embedded systems appear in the form of distributed architectures, forming a large-scale intelligent system. However, this trend inevitably connects the information and infrastructure of a large number of embedded systems to the Internet, so that the data security threats faced by many. In this article, by discussing the requirements for node user access control on embedded devices, the inherent properties of distributed multi-embedded system environment requires support for multi-authority attribute-based encryption (ABE) to achieve access control for each node. Therefore, a secure node access control solution is raised for data transmission in the IoT environment. This solution is a hidden user access control solution. It sustains multi-authority ABE and is highly scalable. In addition, we certificated that the proposed solution provides greater functional characteristics while its performance is comparable to or better than existing cloud computing solutions.**

***Keywords*-distributed architecture; attribute encryption; multiple embedded systems; privacy protection**

I. Introduction

The Internet of Things has many devices, which can exchange information directly or indirectly through the public Internet[1]. By 2025, the number of IoT devices is estimated to reach 7 billion. In the future, IoT devices will become more intelligent, and eventually they can work normally without any manual intervention here[3].

In most cases, these IoT smart devices exist as embedded systems, and these embedded systems are independent of each other and cannot share resources, making it difficult to complete computing tasks through collaboration. However, in a distributed computing environment, embedded devices can meet the needs of users through collaborative work. Therefore, with the development of distributed computing,the collaboration between multiple embedded systems in a distributed architecture will become an important research direction of embedded technology, and the concept of multi-embedded systems has been proposed.

The promise of connectivity in multi-embedded systems drives the growth of IoT device applications, which in turn exposes related security and privacy challenges. In a distributed architecture, in order to ensure the integrity of private data transmitted through certain unsecured networks, a secure and effective solution needs to be offered in the embedded system environment.[6]

Ciphertext policy attribute-based encryption (CP-ABE) is a fine-grained data encryption method that is used in distributed computing. It solves fine-grained access control and large-scale users in complex information systems The problem of dynamic expansion provides an ideal access control scheme for an open network environment.

Attribute-Based Encryption (ABE) is a new public key encryption mechanism put forward by Sahai et al.[2] in 2005, which implements one-to-many encryption of public-key cryptosystems. To express more flexible access control strategy, Bethencourt et al.[10] proposed encryption based on ciphertext policy strategy (CP-ABE), in which the access strategy can be defined during the encryption process. In terms of specifying who can decrypt the encrypted text in the encryption step itself, CP-ABE has more uses. In the key strategy attribute-based encryption mechanism, the pravite key is interrelated to the access structure, and the ciphertext is interrelated to the attribute set. In the ciphertext policy attribute-based encryption mechanism, the key is interrelated to the attribute set, and the ciphertext is interrelated to the access structure[4]. In the ciphertext policy attribute-based encryption mechanism, the encryptor uses the access structure and public key to encrypt the message. The decryptor obtains the decryption key from a trusted authorized party in advance according to its own attribute set. If the properties' attributes of the decryptor do not satisfy the access structure embedded in the ciphertext, the decrypter cannot decrypt the ciphertext.

For a multi-embedded system environment, the number of attributes in the attribute set of each device may be very large, and the size of the key is restricted by the flash space in the node chip. Therefore, if the size of the key and ciphertext is too large, the access control scheme cannot be used in an embedded system environment. Therefore, these values must be minimized.

Most of the ABE scheme mainly stores the ciphertext in the big data platform or cloud environment, but the multi-embedded system has the characteristics of miniaturization and distribution. This paper proposes a communication encryption solution between multiple embedded systems based on attribute encryption. There are three main contributions:

1) The CP-ABE solution is applied to multiple embedded systems with a distributed architecture for the first

2473-3636/20/$31.00 ©2020 IEEE
DOI 10.1109/DCABES50732.2020.00017

Table 1 Symbol description

Parameter	Meaning
GP	Global system parameters
GID	Unique identification of each node
λ	Safety factor
U	System property collection
PK	System public key
SK_U	System master key
S	User's attribute set
SK_S	User's attribute private key
A	Access structure
M	Access matrix
k	Secret shared private key
f	Secret share
m	Plaintext
CT	Ciphertext

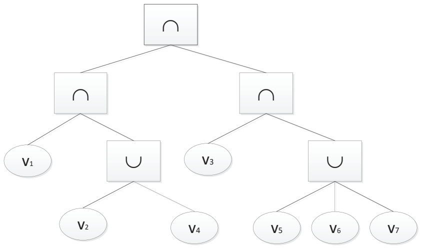

Figure 1. Access tree

time to improve the security of communication in multiple embedded systems;

2) Realize the anti-collusion of the solution by directly embedding the recognition mark into the user's private key structure;

3) Use the access tree and access matrix to embed the access structure in the ciphertext, increase the flexibility of the system, and enhance the ability of encryption and decryption.

II. Preliminary knowledge

A. Parameters

The symbols involved in this article are shown in Table 1.

B. DBDH assumption

Randomly choose $a, b, c, \mu, P \in Z_p^*$,tuple $X = (P, aP, bP, cP, abcP)$ and tuple $Y = (P, aP, bP, cP, \mu P)$, does not exist A probabilistic algorithm makes X and Y indistinguishable in polynomial time with non-negligible advantage.

C. Access structure

Suppose the two-dimensional matrix $U = \{U_1, U_2, ..., U_n\}$ represent a given attribute set, $\{1, 2, ..., n\}$ are the labels in the attribute set U, and the user's attribute set table is $S = \{S_1, S_2, ..., S_n\}$, the access structure is $A = \{A_1, A_2, ..., A_n\}$, where $A_i \subseteq U_i$.For $\forall i \in [1, n]$, there is $S_i \subseteq A_i$, which says that the user's attribute set satisfies the access structure.

In this paper, multi-value AND gates are used to represent the access structure, and the access structure is transformed into an access tree. Non-leaf nodes use "∩" and "∪" to represent thresholds, leaf nodes represent attributes, and all leaf nodes under each non-leaf node Form an attribute, where each leaf node under "∩" constitutes an attribute, and all leaf nodes under "∪" constitute an attribute, and the identity of the user is represented by a specific set of attributes.

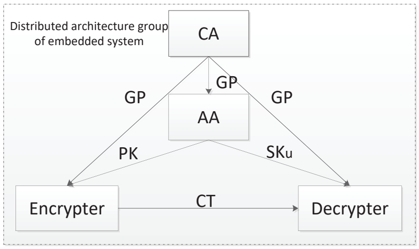

Figure 2. System model

An access tree[5] shown in Figure 1 represents the access structure $A = [\{v1\}, \{v2, v4\}, \{v3\}, \{v5, v6, v7\}]$, attribute set $S = \{v1, v2, v3, v5\}$ or attribute set $S = \{v1, v4, v3, v6\}$ all meet the access structure A.

The improved CP-ABE algorithm in this paper adopts the monotone span program[**?**] to complete the conversion of the access structure to the access matrix. During the conversion process, for the system attributes and their access structure A = $[\{v1\}, \{v2, v4\}, \{v3\}, \{v5, v6, v7\}]$, first the plan formats "∩" as "2", format "∪" as "1", and then expand the attribute elements in order from left to right.

Suppose (a"∩"b) is formatted as (a, b, 2), which means that two of the attributes a and b must be satisfied; (c"∪"d) is formatted as (c, d, 1), which means that it must be satisfied in d or c. Then A is formatted as
$A = ((v1, (v2, v4, 1), 2), (v3, (v5, v6, v7, 1), 2), 2)$

The detailed process of converting the access structure A into the access matrix M is shown in Table 2.

In the light of the linear secret sharing solution[7], for a attribute set $S = \{v1, v2, v3, v5\}$ satisfying the access structure A, a set of vectors w can be found, so $f = \sum wM$=(1,0,0,0).

III. Model definition

A. System model

There are four main participants in the ciphertext attribute encryption scheme in this paper: a trusted central authorization center CA, an attribute authorization center AA, Encrypter, and Decryptor. The model is shown in Figure 2 below.

CA is responsible for establishing and initializing the system, and at the same time defining global system parameters to ensure the credibility of CA; AA is responsible for initialization of attribute authorization, generating system public key PK, system master key SK_U and user private key SK_S; The access structure needs to be satisfied, and the plaintext is encrypted at the same time.

Table 2 Matrix transformation

access structure A	$((v1,(v2,v4,1),2),(v3,(v5,v6,v7,1),2),2) \rightarrow \begin{pmatrix} (v1,(v2,v4,1),2) \\ (v3,(v5,v6,v7,1),2) \end{pmatrix} \rightarrow \begin{pmatrix} v1 \\ (v2,v4,1) \\ v3 \\ (v5,v6,v7,1) \end{pmatrix} \rightarrow \begin{pmatrix} v1 \\ v2 \\ v4 \\ v3 \\ v5 \\ v6 \\ v7 \end{pmatrix}$
access matrix M	$\begin{pmatrix} 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 2 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 2 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

B. *Security model*

In this aticle, the solution can achieve the Indistinguishability of Ciphertext under Chosen-Message, the adversary challenge model constructed by it is:

In the first step, adversary A submits to challenger B the access structures W_0 and W_1 to be challenged. B selects the security factor "λ" and runs the initialization algorithm to obtain the system public key PK and the system master key SK_U. B keeps the SK_U and sends PK to A.

In the second step, A accesses attribute set S to B, but S must not satisfy both W_0 and W_1 provided by the adversary before B can run the private key generation algorithm and send the private key SK_S to A. Adversary A can make polynomial degree queries.

In the third step, A formulates two plain text messages M_0 and M_1, B randomly selects b'(b'∈0,1) and encrypts M_b with W_b. B runs the encryption algorithm and returns the ciphertext to A.

In the fourth step, repeat the second and third steps, but the inquiry initiated by adversary A must be limited to attribute set S does not meet W_0 and W_1.

In the fifth step, adversary A outputs the guess b'(∈0,1) for b. If b'=b, the adversary wins, otherwise A fails.

In the challenge game, opponent A's victory advantage is $\varepsilon = \left| Pr\left[b' = b\right] - \frac{1}{2} \right|$.

Definition If the opponent's victory advantage is negligible in polynomial time, this paper's scheme is safe.

IV. Scheme construction

A. *Distributed architecture of multi-embedded systems*

A multi-embedded system is composed of N embedded systems. In a multi-embedded system environment, having complex multi-task goals can be accomplished by scheduling between tasks in a distributed system. For example, as shown in Figure 3 below, a distributed architecture is constructed for 8 single-chip microcomputers(SCM) through the Internet, and data analysis and calculation are realized through cooperation.

From a physical level, a multi-embedded system can be considered as a collection of multiple embedded systems. Each embedded system performs a specific function. The collection of all functions is to complete a complex task, so the security of communication between individuals appears especially important.

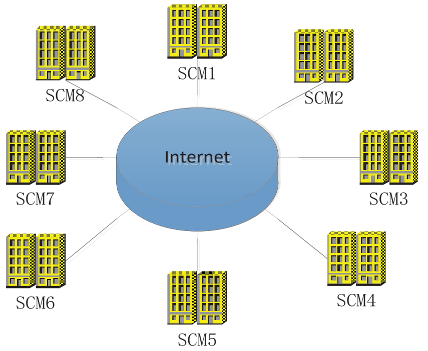

Figure 3. Multi-embedded system with distributed architecture

B. *Encryption algorithm description*

The CP-ABE algorithm is mainly composed of six parts: system initialization, attribute authorization initialization, attribute private key generation, encryption, decryption, and ciphertext policy generation, as follows:

1)$CA\_Setup(\lambda, U) \rightarrow GP$. The node system initialization algorithm,it outputs global parameter GP by inputting the safety parameter λ and the system attribute set U as the input parameter of each algorithm, and each user has own globally unparalleled identifier GID and a set of attribute sets.

2)$AA\_Setup(GP) \rightarrow (PK, SK_U)$. The attribute authorization is initialized, and the algorithm outputs the system public and private key pair (PK, SK_U) by inputting the global parameter GP of the system.

Suppose G be the cyclic group of order q, g be the generator of G, and bilinear map e: $G \times G \rightarrow G_T$. Randomly choose $\alpha, \beta \in Z_p$, the set of elements in G is $T = \{x_1, x_2, ..., x_n\}$, then the output system key pair (PK, SK_U) is

$$PK = \left\{g, e(g,g)^\alpha, g^\beta, T\right\}$$

$$SK_U = g^\alpha$$

3)$KeyGen\left(GP, SK_U, S\right) \rightarrow SK_S$. The attribute private key generation algorithm outputs the user's attribute private key SK_U by inputting the system global parameter GP, the system private key SK_U, and the user attribute set S.

Enter the system private key $SK_U = g^\alpha$ and the user attribute set $S = \{S_1, S_2, ..., S_n\}$,where $\forall i \in S$, select the random parameter $r \in Z_p$ and output the user's attribute private key SK_S as

$$SK_S = \left\{g^{\alpha+\beta r}, g^r, x_i^r\right\}$$

4)$Encrypt\,(GP, m, M) \to CT$. The encryption algorithm outputs the ciphertext CT by inputting the system global parameters GP, plaintext m and access matrix M.

In the encryption process, M is the access matrix. k is the secret shared key, $t_1, t_2, ..., t_n$ are random values, and the random vector $v = (k, t_2, t_3, ..., t_n)$ generates ciphertext information (C_0, C_1). let $f = vM$ represent the secret shared key share, and randomly select $s_1, s_2, ..., s_n \in Z_p$ to add additional information $(C_i, D_i)_{i\in[1,n]}$ in the ciphertext as an access control strategy. Finally, the ciphertext CT form is $\left\{C_0, C_1, (C_i, D_i)_{i\in[1,n]}\right\}$.

Where $C_0 = me\,(g, g)^{\alpha k}$ and $C_1 = g^k$, then CT is

$$CT = \left\{me(g, g)^{\alpha k}, g^k, (C_i, D_i)_{i\in[1,n]}\right\}$$

In order to realize the generation of the access control strategy, after the encryption is completed, the attribute encryption algorithm encrypts k according to the security encryption algorithm DES, which is used as the secret shared encryption information $En(k)$.

5)$AccGen(GP, En(k), M)$. The access control strategy generation algorithm outputs the access control strategy ciphertext $(C_i, D_i)_{i\in[1,n]}$ by inputting the system global parameters GP, the secret shared encryption information $En(k)$ and access matrix M.

According to the above, $C_i = g^{\beta f} x_i^{-s_i}, D_i = g^{s_i}, i \in [1, n]$.

6)$Decrypt(GP, GID, CT, SK_S) \to m$. The decryption algorithm inputs the system global parameters GP, ciphertext CT, and the private key SK_S of the user attribute set S. If the decryptor's attribute set S meets the access policy, the plaintext m is output, otherwise the decryption fails.

The target vector is $(1, 0, ..., 0)$. According to the monotone span program, if the user attributes satisfy the access matrix M, a set of vectors w can be found such that $\sum wM = (1, 0, ..., 0)$. $\sum wf = \sum wvM = v\sum wM = k$. Then the decryption calculation formula is

$$\frac{e(g^k, g^{\alpha+\beta r})}{\prod(e(g^{\beta f} x_i^{-s_i})e(g^{s_i}, x_i^r))))^w} = \frac{e(g, g)^{k\alpha} e(g, g)^{k\beta r}}{\prod e(g, g)^{\beta rwf}}$$
$$= e(g, g)^{\alpha k}$$

Finally, the plaintext is $m = \frac{C_0}{e(g,g)^{\alpha k}}$.

V. Safety and performance analysis

A. Safety analysis

Based on the difficulty of discrete logarithm, this paper uses GID to solve the collusion attacks against multiple attribute authorization centers and direct attacks from different users.

According to the security model of 3.2 above, the following proves that the proposed solution satisfies the indistinguishability of ciphertext under the DBDH assumption.

First step, opponent A submits to challenger B the access structures W_0 and W_1 to be challenged. B selects the safety factor λ and moves the initialization algorithm CA_Ssetup to obtain the global parameter GP and hand over towards the adversary. The challenger generates the corresponding system public key PK and system master key SK_U by executing the AA_Ssetup algorithm. Challenger B keeps the SK_U and sends PK to A. B random selects a random value $\mu \in \{0, 1\}$, which conceals opponent A.

Second step, opponent A selects a group of user GID and user attribute set S, and submits (S, GID) multiple times to the challenger for key access, where each attribute in S does not satisfy access to W_0 and W_1, and comes from reliable attribute authorization center. The KeyGen algorithm is executed, and the user's private key SK_S is generated and sent to opponent A.

Third step, opponent A formulates two plain text messages M_0 and M_1 to B. B randomly selects a value b($b \in \{0, 1\}$), carries out the encryption algorithm, and encrypts M_b with W_b to generate a challenge ciphertext CT, and finally sent CT to opponent A.

Fourth step, Repeat the second step and third step to continue the private key inquiry.

Conjecture: Opponent A makes a guess b'($b' \in \{0, 1\}$). If $b' \neq b$, output $\mu' = 1$, adversary A cannot obtain any information about b, so $Pr[b' \neq b|\mu = 1] = \frac{1}{2}$,naturally $Pr[b' = b|\mu = 1] = \frac{1}{2}$ If $b' = b$, output $\mu' = 0$, opponent A gets the ciphertext of M_b. The advantage of the previously defined adversary is ε, so $Pr[b' \neq b|\mu = 0] = \frac{1}{2} + \varepsilon$, and naturally $Pr[b' = b|\mu = 0] = \frac{1}{2} + \varepsilon$. Finally, its overall advantage is

$$\frac{1}{2}Pr[b' = b|\mu = 0] + \frac{1}{2}Pr[b' = b|\mu = 1] - \frac{1}{2}$$
$$= \frac{1}{2} \times (\frac{1}{2} + \varepsilon) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2} = \frac{\varepsilon}{2}$$

The above proves that when the opponent solves the advantage of the DBDH problem in polynomial time $\varepsilon/2$, the result is negligible, so this scheme is safe.

B. Performance analysis

In this chapter, we conducted a comparative study on the functional aspects of the ABE scheme, and calculate and communicate the access control scheme. The functional characteristics of the proposed scheme and other related access control will be compared.

This experiment runs in the RT-Thread operating system and is implemented in C language. It is configured as multiple STM32F103 microcontrollers with a distributed architecture to form a system. Table 3 summarizes some important ABE solutions related to functional characteristics, most of which are based on cloud computing. We observed that the solution proposed in this article is quite general in embedded systems. In terms of the limitations of this solution, it is not planned to sustain outsourcing of computing burden, such as PHOABE[12] and FLAC[11].

Table 3 Comparison of multiple schemes

	KP or CP	Type of access structure	Private key size	Decryption cost	I	II	III
[3]	KP	LSSS	O(tn)	O(t)			
[6]	KP	Tree	O(n)	O(t)		✓	
[11]	CP	Tree	O(n)	O(n)			✓
[12]	CP	LSSS	O(t)	O(n)	✓	✓	✓
[13]	CP	Tree	O(n)	O(t)			
[14]	CP	AND	O(n)	O(t)	✓	✓	
Ours	CP	LSSS	O(n)	O(t)	✓	✓	

Note: I: With hidden access scheme; II: Whether to support multi-attribute authority; III: Whether to sustain computing outsourcing; n: the number of attributes in U, t: the number of attributes defined for user; LSSS: Linear secret sharing scheme.

It is interesting that, as drew in the first chapter, we constructed the solution to have sufficiently low computational overhead, so it does not require any supported cloud infrastructure equipment. In this article, we focus on the ciphertext scalability and low-cost communication cost above the expressiveness of the solution, but ignore the portability, but the goal of this solution is to solve the non-portability in the following research.

VI. Conclusion

In the article, we discuss the importance of the access control mechanism to the distributed architecture of multiple embedded systems, describe the distributed nature of multiple embedded devices and provide a model, and finally propose a highly scalable and suitable for distributed A multi-attribute CP-ABE-based control solution for access between embedded devices with an integrated architecture.We conducted a security analysis for the proposed solution, and also conducted a related comparative study on the access control solution in the distributed architecture and other existing solutions. It is very important to note that, compared with other solutions, the proposed solution requires less resource-constrained smart devices with lower computing costs and significantly less communication overhead.

Overall, compared with other solutions, this solution makes a better balance between safety and functional characteristics, as well as communication and computing overhead. Therefore, this solution is suitable for practical applications in multiple embedded system environments.

Regarding the next research scope in this aspect of this article, the basic ABE scheme can be further studied in a variety of distributed embedded environments.

Acknowledgment

We thank all the volunteers who participated in the experiment.This work was supported by Jiangsu Province Production and Research Cooperation Project(No. BY2015019-30).

References

[1] Yu Changchang, Yu Li, Hong Zhen. Research on the security capacity of narrow-band Internet of things physical layer based on amplified forwarding and collaborative congestion. *Journal of Transduction Technology*, 2017, 30(4), 575-581.

[2] Sahai, A.and Waters, B. 2005. Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques-Advances in Cryptology Advances in Cryptology* (Aarhus, Denmark, May, 2005). EUROCRYPT'05, Springer, Berlin, Heidelberg, 457-473.

[3] Yu Bo, Tai Xianqing, Ma Zhijie. 2020. Research on RBAC model based on attributes and trust in cloud computing environment. *Computer Engineering and Applications*, 2020, 56(9), 84-92.

[4] Su Jinshu, Cao Dan, Wang Xiaofeng, Sun Yiping and Hu Qiaolin. 2012. Property-based encryption *Journal of Communication*, 2012,33(7), 1129-1145.

[5] Wang Haiping, Zhao Jingjing. 2018. Property-based encryption solution of ciphertext strategy for hiding access. *Compter System*, 34(3),180-184.

[6] Dlixiadi Wupuer, Cheng Cheng, Nulmamati Heilili. 2019. OO-CP-ABE access control solution for verifiable outsourcing decryption based on hidden strategy. *Computer Engineering*, 44(10), 160-174.

[7] Sun Zhixin, Hong Hanshu. Some reflections on security issues in NB-IoT. *ZTE Technologies*. 2017, 23(1), 47-50.

[8] Ma Dandan, Zhou Qin, Dang Zhenqin. 2012. Ciphertext policy encryption mechanism based on multi-attributes organization. *Computer Engineering*, 38(10), 114-116.

[9] Ma Haiying, Zeng Guojun, Wang Zhanjun. 2004. Efficient and provably secure attribute-based online/offline encryption mechanism. *Journal on Communication*, 35(7), 104-112.

[10] Lei Lei, Cai Quanwei, Jing Jiwu, Lin Jinqiang, Wang Zhan and Zhou Bo. 2017. Encrypted cloud storage access control mechanism supporting policy hiding. *Software Engineering*, 18(9), 1324-1336.

[11] Chen Lu, Wang Ze. 2019. ATP-ABE-based access control solution. *Computer Engineering and Applications*, 2019, 44(3), 78-84.

[12] Qi Fang, Li Yanmei, Tang Zhe. 2018. Revocable policy attributes and traceable group key encryption scheme. *Journal on Communications*, 2018,38(22), 62-68.

[13] Yang Hao, Li Tao. 2018. New cloud storage-based CP-ABE access control solution. *Computer Knowledge and Technology*, 2018, 32, 52-56.

[14] Yang Yuhan. 2018. Outsourcing verifiable encryption and decryption CP-ABE program. *Information and Communications*, 2018, 191(11), 23-25.