Journal of Engineering and Applied Sciences 13 (Special Issue 2): 2986-2991, 2018
ISSN: 1816-949X

2-Factor Based Fine-Grained Access Control Scheme for 5G Environment

Yoon-Su Jeong and Jin-Hee Ku
Division of Information and Communication Convergence Engineering,
Mokwon University, 88 Doanbuk-ro, Seo-gu, 35349 Daejeon, Korea

Abstract: Recently, with the 4th industrial revolution, the necessity of 5G technology is socially emerged and the requirements for access control and quality improvement of services are increasing. In performance evaluation, the proposed method obtained 8.1% lower server overhead than the existing method and the attribute processing rate per data was higher than 7.7%. Also, the delay time according to the access control method is 5.7% lower than the conventional method. we propose a 2-factor based attribute approach that minimizes service latency by stochastically assigning attribute information according to 2-factor function (forward and backward). The proposed scheme performs the process of controlling the intermediate medium in the first place and the encryption/decryption key in the sec place according to the access control. In particular, the proposed scheme can efficiently handle high capacity multimedia according to the 5G environment, minimizing the burden on the server and maximizing the efficiency of the equipment in the cluster to which the intermediate medium belongs.

Key word: Fine-grained, access control, 5G environment, encryption/decryption, key generation, minimizing

INTRODUCTION

Recently, 5G technology, which is one step advanced to support streaming service and minimization of delay time, is emerging as a new mobile communication technology (Haller *et al*., 2008; Raza *et al*., 2013). The 5G technology will be used in all devices such as smart phones, automobiles and IT products as early as 2020 instead of 3G/LTE technology. The reason why 5G technology is more interested in 3G/LTE technology is that it can support more users such as delay time, high speed and streaming service (Roman *et al*., 2013).

The 5G technology can define various ways of differentiated requirements such as transmission speed, traffic capacity, power consumption and coverage. In particular, 5G technology requires end-to-end communication or MTC (Machine Type Communications) problem solving. In a wireless communication system an MTC device receives a notification message informing reception of an MTC message from a base station and transmits an acknowledgment message regarding whether to receive the MTC message. In general, the MTC is divided into a massive MTC and a critical MTC depending on the function. Massive MTC provides a foundation for connecting a huge number of ultra-small devices such as sensors and typical requirements are that low-power communications should prevent unauthorized users from unauthorized access to sensitive items in the 5G service environment. Recently, the property-based encryption (i.e., ABE) method has been studied to be applied to 5G technology. In the ABE system, each user is associated with a access policy and a private key and the decryption statement must check whether the ciphertext attribute or secret key is appropriate for the access policy.

We propose 2-factor based a fine-grained access control method that minimizes the service delay time of 2-factor by stochastically assigning the attribute information according to the forward and backward functions of the access control of the intermediate medium which acts as a gateway among the devices constituting the 5G environment technique. To grant access control to data, the proposed scheme performs access control primarily on the intermediate medium and secondly processes the encryption/decryption key used on the server side. The proposed method minimizes the burden on the server because it efficiently processes high-capacity multimedia. In addition, proposed scheme can maximize the efficiency of the equipment in the cluster to which the intermediate medium belongs by sharing the role of the server according to the attribute information of the data.

Literature review: Hur and Noh (2011) technique based DAC has designed an efficient property abolition planning system through a vulnerable forward security

Corresponding Author: Yoon-Su Jeong, Division of Information and Communication Convergence Engineering, Mokwon University, 88 Doanbuk-ro, Seo-gu, 35349 Daejeon, Korea

plan. However, systems with a single trusted authority also have the problem that the data owner must re-encrypt the outsourcing.

Liu *et al*. (2013) proposed technique for a secure sharing data using a unique method called Mona. This technique is characterized by providing granular access control and security. However, this technique has the disadvantage that canceled users and cloud can easily compromise and attack (Zhu *et al*., 2013).

Bethencourt *et al*. (2007) scheme proposed the CP-ABE system by explicitly formulating the concept of CP-ABE (ciphertext-policy ABE). However, this technique is based on a commonly used group model rather than a specific domain in the CP-ABE certification process.

Cheung and Newport (2007) scheme proposed another CP-ABE scheme. This scheme supports the AND, access policy. The technique used in the scheme is characterized in that the security of the CP-ABE technique is proved under a dual linear Diff-Hellman decision.

Chase scheme proposed a MA-ABE scheme (Chase, 2007; Lin *et al*., 2010; Rouselakis and Waters, 2015). In this scheme, each AA consists of several AA and one Central Authority (CA). When a CA distributes a global unique ID with a private key to a user, the user issues a set of attribute private keys.

Emura *et al*. (2009) scheme proposed a CP-ABE scheme. However, since it supports only (n, n) threshold access policies for multi-value attributes, the multi-attribute values must be fixed to a certain size. To solve these problems, Herranz *et al*. (2010) scheme proposed another CP-ABE scheme with a certain size of ciphertext. This technique emphasizes the differentiation of policy decisions, so that, the threshold access value for multi-valued attributes can be applied to (t, n) (Emura *et al*., 2009).

Chen *et al*. (2011) scheme which proposed the CP-ABE scheme, reduced the computational cost of uniformly sized ciphertext and access policies. Sreenivasa scheme adopts the scheme by Emura *et al*. (2009) for the composite order bilinear group (Rao and Dutta, 2013). To solve the revocation problem in attribute-based systems, various CP-ABE schemes have been proposed to support attribute-level discard (Hur and Noh, 2011; Yang *et al*., 2013; Yu *et al*., 2010; Zhang *et al*., 2014). When a user's property level is canceled, the user whose property level has been revoked loses only partial access because only some attributes are removed. A user whose access is revoked can still access the data while the remaining characteristics meet the access policy. In addition to binding expiration times to each attribute, the processing method of the CP-ABE technique can be classified into two categories, direct discard (Zhang *et al*., 2014) and indirect discard (Hur and Noh, 2011; Yang *et al*., 2013; Yu *et al*., 2010).

Zhang *et al*. (2014) scheme draws the complementary function to check which ciphertext is associated with the revocation event to update the associated ciphertext. Yu *et al*. (2010) scheme proposed the CP-ABE scheme with indirect attribute-level abolition by a semi-trust proxy placed on the data server. Yang *et al*. (2013) scheme of re-randomizes the key was adopted in. Hur and Noh (2011). mechanism proposed an immediate attribute-level revocation method in the CP-ABE utilizing a key tree encrypted with a binary key for group key distribution (Hur and Noh, 2011). Unlike termination at the attribute level, the termination at the user level loses all access to the system by the revoked user. The CP-ABE scheme of N. Attrapadung *et al*. scheme proposed a direct user-level abolition method by combining broadcast encryption and ABE techniques (Attrapadung and Imai, 2009).

MATERIALS AND METHODS

Fbased probabilistic access control: In this study, we propose 2-factor based probability access control technique that optimizes the role of the intermediate medium constituting the 5G environment according to the data attribute information to minimize the data processing delay time. The proposed scheme is to enhance the role of the intermediate medium that acts as a gateway in the 5G environment, thereby reducing the server load and minimizing the data processing delay time.

System model: The proposed method performs access control of data by dividing the function of the intermediate medium constituting the 5G environment into forward and backward so as to stably assign 2-factor based access control. In particular, the proposed scheme performs the following two processes to satisfy the requirements to be considered in the 5G mobile communication system (increase in traffic, increase in the number of devices, dependence on cloud computing, appearance of various 5G-based convergence services, etc.). In the first stage, the intermediate medium performs access control and in the second stage, the access right is performed, so that, the server can process the encryption/decryption key. Through this process, the proposed method can efficiently process high capacity multimedia as well as data transmitted and received in 5G environment.

The proposed scheme adopts the same system model as the 5G environment because it has to reflect 4 characteristics to be considered in the 5G mobile communication system (increase in traffic, increase in

number of devices, dependence on cloud computing, appearance of various 5G-based convergence services, etc.). The system model of the proposed method consists of various kinds of entities.

In order to share data with the cloud storage server in the 5G environment, each user must specify a set of attribute labels in addition to the globally unique identifier. At this time, the function of recovering outsourced data can be performed only by the user who has been given specific authority.

Definition: The access control scheme in the proposed scheme consists of three steps: setup, key generation, encryption and decryption. Step 1: Setup (S (ω)→(HL, PK, LK)).

The setup algorithm receives the security parameter ω according to the hierarchical level HL as shown in Eq. 1 to set the access control and generates the attribute set S(ω). The proposed scheme outputs the public key PK and each level key LK according to the hierarchical level HL:

$$S(\omega) = \sum_{i=1, j=1}^{n} \omega_i^j \quad (1)$$

Step 2: Key generation (KeyGen (PK, LK, A)→SK). This Step outputs the attribute secret key SK in which the public key PK and the level key LK match the attribute set A according to the hierarchical level HL.

Step 3-1: Encryption : ((PK, d, (D, ρ)) → (DE, ABF)). The data encryption algorithm includes data encryption ABF and block function ABF of data attribute information.

$$\text{-Enc (PK, d, (D, } \rho)) \rightarrow CT$$

The data encryption subroutine generates the ciphertext CT through the PK, the data information d and the data group access structure (D, ρ).

$$\text{-ABF (D, } \rho) \rightarrow ABF$$

The block function ABF of the data attribute information inputs and outputs the access policy (D, ρ).

Step 3-2: Decryption ((D, ABF, PK, SK, CT)→d). The decryption algorithm includes a process of extracting the attribute information ρ and the data d.

$$\text{-ABFQuery (A, ABF, PK)} \rightarrow \rho$$

The ABF query algorithm outputs attribute information ρ through a hierarchical group attribute set A, a block function ABF of data attribute information and a public key PK.

$$\text{-Decryption:Dec (SK, CT, (D, } \rho)) \rightarrow d$$

The data decryption algorithm extracts attribute information ρ as an input if it can satisfy access policy through the data access pair (D, ρ) as well as the attribute secret key SK and ciphertext CT.

Data processing: The process of the proposed method for data processing consists of four steps (system initialization, secret key generation and authorization generation, data encryption/decryption, attribute level adjustment, etc.) as follows.

Step 1; System initialization: The CA creates common parameters for the system. Both AA registration and user registration are allowed in the CA. The AA and the data owner each generate a common parameter and secret information that is used to run the system.

Step 2; Generate secret key and permission: If there is an attribute registration request to the AA, the certificate is checked and the attribute secret key is distributed to the user. The data owner generates the authentication key and delivers it to the user.

Step 3; data encryption/decryption: After the data owner encrypts the data according to the access policy, the data owner outsources the cipher text to the CSP. At this time, the encryption operation uses the public key set and the data owner's authentication private key from the AAs to encrypt/decrypt the outsourced data.

Step 4; Hierarchical property level adjustment: The attribute level is created hierarchically using an attribute update key for the user and a set of ciphertext update components for the CSP. The user updates the attribute secret key according to the hierarchical level condition according to the attribute information. The updated attribute information is performed so that the cipher text associated with the attribute is updated by the CSP. The proposed technique updates the CSP with a set of permission update keys for the user and a set of components for the cipher text update.

Data attribute key generation and association process by hierarchical level: The proposed scheme constructs a

hash chain to efficiently link high capacity multimedia as well as data transmitted and received in the 5G environment. In order to guarantee the integrity of data that can not be processed smoothly according to the communication state of the 5G environment, the proposed scheme generates attribute key so as to minimize the processing delay time of the intermediate medium by stochastically generating the attribute information key as follows. This is done in four steps.

Step 1: When the number of data to be processed is n and the seed of the data is s to generate the attribute key for access control of the intermediate medium, the first data is expressed as $_R\{0, 1\}^n$.

Step 2: To perform the 2-factor of the intermediate medium, we choose two random numbers x_1^0, x_1^1 that act as private keys from $_R\{0, 1\}^n$. The i-th selected $\delta[i]$ of δ selects a binary value from 0 and 1 to display the private key (x_1^0, x_1^1).

Step 3: The intermediate medium generates a public key corresponding to two new private keys x_{i+1}^0 and x_{i+1}^1 using Eq. 2.

$$PK_{i+1}^{\delta} = h(x_{i+1}^{\delta}) = \begin{cases} PK_{i+1}^{\delta} = h(x_{i+1}^{\delta}) & ,if\delta = 0 \\ PK_{i+1}^{\delta} = h(x_{i+1}^{\delta}) & ,if\delta = 0 \end{cases} \quad (2)$$

Step 4 : To minimize overhead of intermediate medium, proposed method assigns the access right to the first factor of the 2-factor to perform the access control of the intermediate medium and the second factor to process the encryption/decryption key in the server, It is used to check authentication and integrity. In particular, to process the merging of data ensuring integrity, a hash value is generated according to the number of data n as Eq. 3:

$$HK_n = \begin{cases} h(k_{n-1} \| y_n) & \text{mod n} \\ h(k_{n-1} \| y_n) & \text{mod n} \end{cases} \quad (3)$$

At this time, the generator repeats the process sequentially until the value of n becomes zero.

Performance evaluation: The performance evaluation of proposed method compares the overhead of the server, the efficiency of the intermediate medium, and the delay time according to the access control method.

Environment setting: We use OMNet++ as a simulation tool to validate the proposed method and the existing method. Table 1 set up the experimental environment to perform the simulation to show the objective evaluation.

Table 1: Parameter setting

Parameters	Setting
Channel capacity	11 Mbps
Backoff slot time	20 μs
Minimum contention window size (voice/data)	8/32
Maximum contention window size (data)	1024
Backoff stage limit (data)	5
Retransmission limit(data)	7
PLCP&preamble	192 μs
MAC header	24.7 μs
RTP/UDP/IP headers(voice)	4.8/11 μs
Packet payload length (data)	1884/11 μs
AIFS/DIFs (data)	50 μs
Minislot duration	0. 3 msec
Time slot duration	1.5 msec
Transmission time(data)	1.18 msec
Gurad time (T_{gt})	20 μs
Average on/off time(1/α/1/β)	352/650 msec
Minislot contention provbability(data)	0.2
Transmission queue length	10,000 packets
Superframe time(delay bound)	100 m

RESULTS AND DISCUSSION

Figure 1 compares the processing delay time of the data processed in the intermediate medium that acts as a gateway among the devices constituting the 5G environment compared with the existing method. Experimental results show that the latency is reduced by 5.7% on average as the number of processed data in intermediate media is increased by stochastically assigning attribute information according to forward and backward functions. The results show that the data attribute information is linked with the data based on the probability value of the data used in the proposed method. Also, the result is that the key used to process the data in real time between 5G components was generated using a hierarchical multiple hash chain.

Figure 2 compares the overhead of the 5G device with the existing technique by using the attribute key used for data processing between the devices constituting the 5G environment. In the experimental result of Fig. 2, the overhead of the intermediate device acting as a gateway among the 5G devices is 8.1% lower than the conventional technique. In Fig. 2, the proposed scheme shows that the overhead change is more constant than the existing scheme as the number of 5G devices increases. In particular, the proposed method does not use the additional algorithm for data processing and the change of the overhead is not higher than that of the existing method because the attribute key of the data is generated so that the data processing configuration can be hierarchically represented according to the data attribute.

Figure 3 shows the attribute throughput per data processed by the intermediate device acting as a gateway in the 5G environment. As shown in Fig. 3, since, the

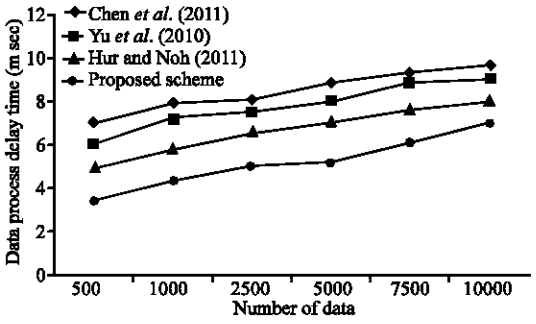

Fig. 1: Delay time of data processing

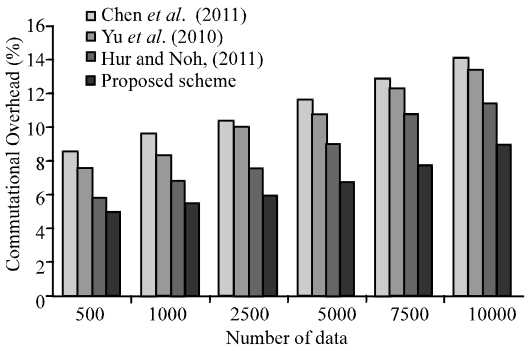

Fig. 2: Communication overhead of device

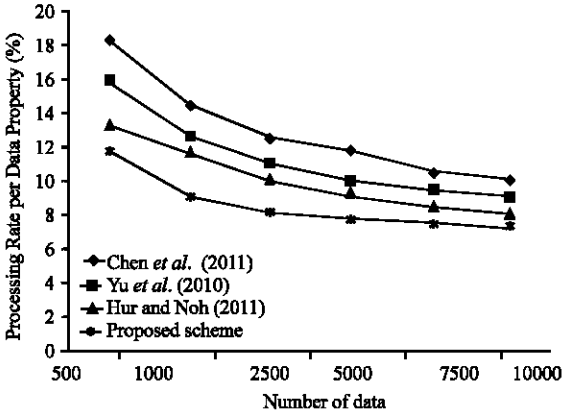

Fig. 3: Processing rate per data property

intermediary medium shares the role of the server according to the data attribute information, the attribute processing rate per data is higher than that of the existing method by 7.7% or more because the efficiency of the apparatus in the cluster in which the intermediate medium belongs can be maximized. This is because the proposed method generates two attribute keys to perform a 2-factor function and processes the data without additional algorithms. In particular, even if the number of intermediate devices that serve as gateways increases, the proposed method has high attribute throughput per data because it distributes data using two attribute keys.

CONCLUSION

Recently, 5G technology is expected to be used in all devices such as smart phones, automobiles and IT products, so interest in 5G technology is rapidly increasing in place of 3G and LTE technologies. In this study, we propose a 2-factor based probabilistic access control scheme suitable for 5G technology. The proposed scheme minimizes the service latency by stochastically assigning the attribute information according to the 2-factor function (forward and backward) of the access control of the intermediate medium acting as a gateway. In particular, the proposed scheme can efficiently process high-capacity multimedia in accordance with 5G environment requirements, thereby maximizing the efficiency of the intermediate apparatus. In the performance evaluation, the proposed method has lowered the server overhead by 8.1 % on average and the attribute throughput per data is higher than 7.7%. Also, the delay time according to the access control method is 5.7% lower than the conventional method. Future studies will be based on the results of this study and applied to 5G devices to compare and evaluate performance evaluation.

ACKNOWLEDGEMENT

This reserach was supported by the security engineering research center granted by the ministry of trade, industry and energy.

REFERENCES

Attrapadung, N. and H. Imai, 2009. Conjunctive Broadcast and Attribute-Based Encryption. In: Pairing-Based Cryptography-Pairing, Shacham, H. and W. Brent (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-03297-4, pp: 248-265.

Bethencourt, J., A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption. Proceedings of the IEEE International Symposium on Security and Privacy, May 20-23, 2007, IEEE, Berkeley, California, USA., pp: 321-334.

Chase, M., 2007. Multi-Authority Attribute Based Encryption. In: Theory of Cryptography, Vadhan, S.P. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-70935-0, pp: 515-534.

Chen, C., Z. Zhang and D. Feng, 2011. Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost. In: Provable Security, Boyen, X. and C. Xiaofeng (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-24315-8, pp: 84-101.

Cheung, L. and C. Newport, 2007. Provably secure ciphertext policy ABE. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 28, 2007, ACM, New York, USA., ISBN:978-1-59593-703-2, pp: 456-465.

Emura, K., A. Miyaji, A. Nomura, K. Omote and M. Soshi, 2009. A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. In: Information Security Practice and Experience, Bao, F., L. Hui and W. Guilin (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-00842-9, pp: 13-23.

Haller, S., S. Karnouskos and C. Schroth, 2008. The Internet of Things in an Enterprise Context. In: Future Internet, Domingue, J., D. Fensel and P. Traverso (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-00984-6, pp: 14-28.

Herranz, J., F. Laguillaumie and C. Rafols, 2010. Constant Size Ciphertexts in Threshold Attribute-Based Encryption. In: Public Key Cryptography-PKC 2010, Nguyen, P.Q. and D. Pointcheval (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-13012-0, pp: 19-34.

Hur, J. and D.K. Noh, 2011. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Trans. Parallel Distrib. Syst., 22: 1214-1221.

Lin, H., Z. Cao, X. Liang and J. Shao, 2010. Secure threshold multi authority attribute based encryption without a central authority. Inform. Sci., 180: 2618-2632.

Liu, X., Y. Zhang, B. Wang and J. Yan, 2013. Mona: Secure multi-owner data sharing for dynamic groups in the cloud. IEEE Trans. Parallel Distrib. Syst., 24: 1182-1191.

Rao, Y.S. and R. Dutta, 2013. Recipient Anonymous Ciphertext-Policy Attribute Based Encryption. In: Information Systems Security, Bagchi, A. and I. Ray (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-45203-1, pp: 329-344.

Raza, S., H. Shafagh, K. Hewage, R. Hummen and T. Voigt, 2013. Lithe: Lightweight secure CoAP for the internet of things. IEEE. Sens. J., 13: 3711-3720.

Roman, R., J. Zhou and J. Lopez, 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Netw., 57: 2266-2279.

Rouselakis, Y. and B. Waters, 2015. Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption. In: Financial Cryptography and Data Security, Bohme, R. and T. Okamoto (Eds.). Springer, Berlin, Germany, ISBN:978-3-662-47853-0, pp: 315-332.

Yang, K., X. Jia and K. Ren, 2013. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, May 08-10, 2013, ACM, New York, USA., ISBN:978-1-4503-1767-2, pp: 523-528.

Yu, S., C. Wang, K. Ren and W. Lou, 2010. Attribute based data sharing with attribute revocation. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, April 13-16, 2010, Beijing, China, pp: 261-270.

Zhang, Y., X. Chen, J. Li, H. Li and F. Li, 2014. Attribute-based data sharing with flexible and direct revocation in cloud computing. KSII. Trans. Internet Inf. Syst., 8: 4028-4049.

Zhu, Z., Z. Jiang and R. Jiang, 2013. The attack on Mona: Secure multi-owner data sharing for dynamic groups in the cloud. Proceedings of the 2013 International Conference on Information Science and Cloud Computing Companion (ISCC-C), December 7-8, 2013, IEEE, Guangzhou, China, ISBN:978-1-4799-5245-8, pp: 213-218.