International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.283-292
http://dx.doi.org/10.14257/ijsia.2015.9.8.25

Extraction Security Indexing Value to use Story-Telling and Attribute-Based Encryption Scheme considering on Big Data Environment

You-jin Song[1] and Jang-mook Kang[2],

[1]*Department of Information Management, Dongguk University, 707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea*
[2]*Department of computer Science and Engineering, Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, 136-701, South Korea*
[1]*song@dongguk.ac.kr,* [2Corresponding author]*Jang-mook Kang, mooknc@gmail.com*

Abstract

In the real world, especially for wearable context with the education information communicating, the diversified contexts need to be considered to apply the Attribute-Based Encryption. However, it is hard to design the optimized dynamic access structures because it is static access structures and properties of Attribute-Based Encryption. In this paper, we propose the attribute-based encryption using the algorithm of context-based service inference model to collect the attributes by data and to provide appropriate services by recognizing the situation. Especially it is analyzed that the students' answering process is sectionalized to several scenarios according to teachers' educational objective and plan in educational environment. And through the process it is described that the application of security policy and technology must be distinguished by tables.

Keywords: *Wearable Context, Big Data, Attribute-Based Encryption, Bayesian Network, Access Structure, Education Information*

1. Introduction

1.1 Background and Purpose

According to commercialization of wearable technology, the sensing information of human walking, heart rate, pupil changes and sweating has been collected. The sensing value is the typical unstructured data. Even if this sensing value is stored in the cloud or analyzed as big data, the risk of development of information technology is still fraught. In these days, due to the development of information technology, the research of cloud computing environment building has been progressed, and the research has provided sharing, utilization and environmental analysis of personal information with adoption of a cloud computing architecture [1].

As a personal information in cloud computing environment contains a lot of information which may compromise the privacy of individuals, only its minimum information have to be shared and applied safely [2-3]. Especially in education or class environment, the adoption of encryption scheme is essential to provide seamless education services (including learning content with personal information) and to ensure the safety at the same time [3].

As a technical measure in above requirement, Attribute-Based Encryption is suggested that only users with legitimate attribute are able to access the class records. However it is difficult to design the access structures considering the dynamically changing context in accordance with the time because it is static access structures of Attribute-Based

ISSN: 1738-9976 IJSIA

Encryption. In other words it is needed that Attribute-Based Encryption considering the medical context.

For example, between Q & A in the class room, the personal information can be created like class participation frequency, learning attitude and the record. In this case this information must be protected. Also it has to be the environment which the applicable service is able to understand the student' context with communication between teacher using the wearable device.

1.2 Scope and Method

In the existing Attribute-Based Encryption the property of access structure is static. That is, non mutable personal information like affiliation, position, and name is used as an attribute. As Context is able to be changed into time-dependent, dynamic information like position, weather, temperature humidity and biometric data is to be used as an attribute. Because of characteristic of this attribute, it is hard to design the access structure considering context using the existing Attribute-Based Encryption. In this paper, Bayesian Network would be used as a statistical method, and the policy- dependable encryption scheme will be designed with inference of users' context that is made by contextual information. In other words, it is suggested the context considering Attribute-Based Encryption throughout the algorithm [4] of context-based service inference model to recognize the context by collecting the attribute data and to provide the appropriate services (for example, acquisition of decryption privilege).

2. Related Works

In this chapter Attribute-Based Encryption and Bayesian Network would be described.

2.1 Attribute-Based Encryption

Attribute-Based Encryption is composed of ID based encryption [5] and secret sharing [6] and it is a method that can be performed for encrypting and decrypting based on the attribute of each object. While ID based encryption has a relation of one to one mapping between object and ID, Attribute-Based Encryption has a relation of one to many, so it is able to have fine-grained access control at Attribute-Based Encryption.

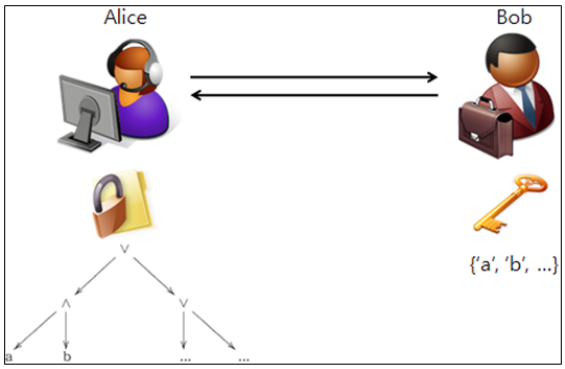

Figure 1. Concept of CP-ABE (Cipher-text-Policy Attribute-Based Encryption)

Attribute-Based Encryption could be classified into KP-ABE (Key-Policy Attribute-Based Encryption) [7] and CP-ABE (Cipher-text-Policy Attribute-Based Encryption) [8] according to what is related to the access structure between a secret key and cipher-text.

In this paper CP-ABE using access structure for composing cipher-text would be introduced [Figure 1]. Secret key is related to attribute set and cipher-text is related to

access structure in CP-ABE. The cipher-text is decrypted when attributes set of users' secret key is satisfied with a specific decrypting policy which is consisted of access structure within a coded message.

For example, the class for influenza has been conducted in medical school. If one of the researcher in the school want to access the data that has been studied, the secret key must be related to professor and should be made with the attribute of the research team, head of the research team or dean of the school. Also the access structure has to be (Professor ^ the research Team) v (Head of the research team v the Dean of the school). When Secret key is satisfied with this access structure, the researcher can decrypt the data.

Below Figure 2 is the patent example to use Attribute-Based Encryption. Attribute-Based Encryption can be used in actual various fields. In this study Attribute-Based Encryption is used as the method and algorithm to protect the personal information in the class room.

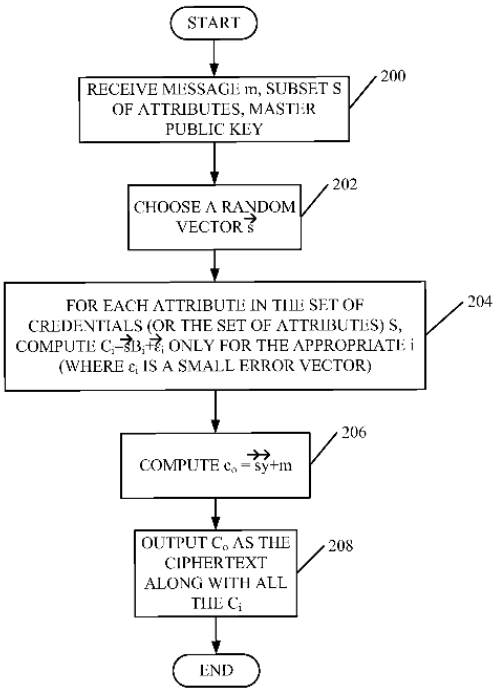

Figure 2. Using Case for Patent (Attribute based Encryption Using Lattices) [12]

The source:
https://www.google.com.ar/patents/US20120155635?dq=US20120155635A1&hl=ko&sa=X&ved=0CBwQ6AEwAGoVChMI1YvDxOOIxwIV2DaICh0pigGO

A key generator component that generates the user secret key based on a set of attributes defining the user and provided in an access structure that identifies a type of information the user can decrypt, the master public key and a master secret key that comprises a set of trap door lattices generated for each of the attributes in the set of attributes provided in the access structure [12].

2.2 Bayesian Network

Bayesian Network is very effective to provide the proper services for the student's conditions using time-dependent changing information with the basis on wearable devices. It is very suitable as a method to judge the student's condition by simplifying the

complicated process which is a context inferring to the quantified relations between nodes (modules) [4, 9] in education environment.

Bayesian Networks is an efficient and effective representation of the joint probability distribution of a set of random variables [13].

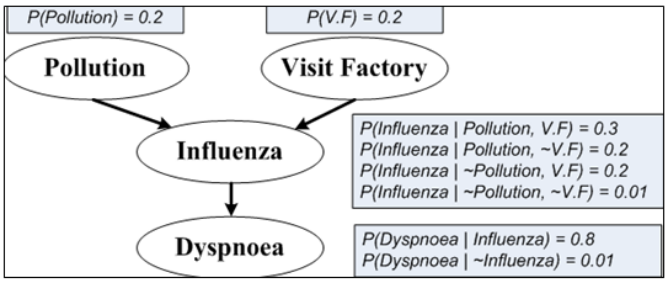

Fig. 3. Example of Bayesian Network [4]

As a model of DAG (Directed Acyclic Graph), Bayesian Network can express the number of probability relations effectively with less effort by CPT (Conditional Probability Table) which is defined in each node [4, 10]. At Bayesian Network, each node means actual environment variables and the relation connecting nodes called arc that is the dependence among the variables [Figure 3]. When the evidence for a certain context is observed after learning the designed network, based on the evidence, the probability for condition of each node is calculated with Bayesian Inference Algorithm using CPT independent condition of each node [4].

3. Attribute-Based Encryption Optimizing Big Data (focus on wearable context)

In this chapter there is a description about the proposed scheme overview, process of analysis and cognition of context, design of access structure, detailed algorithm, and wearable device-on medical environment.

3.1 Overview

It is very limited to analyze the context with the access structure of existing Attribute-Based Encryption when teacher and student have communicated the information with wearable devices (Samsung Gears, Fitbit One, Jawbone, Garmin, Myo and so on). Therefore it is suggested the probability calculating access structure using algorithm of context-based service inference model that is able to consider the context. In the proposed scheme it is added to access structure of CP-ABE the context inference node that is using Bayesian Network.

Each node of CP-ABE is consisted of polynomial-base and calculated as an exponential form of attributes. Where, the attribute is the information of object like affiliation, title and name.

3.2 Recognizing Process of Class Context to Use Story-Telling

Context is the information that makes the situation of an object and context-awareness special, in recognizing the user requiring service using context [11]. The probability is calculated using algorithm of context-based service inference model to realize patients' context awareness in the proposed scheme.

If the probability is satisfied with the attribute of context inference node, the cipher-text can be decrypted. The variables are stipulated 4W1H (Where, Who, When, What, How) in the algorithm of context-based service inference model. If

$P(D2)= P(S|H, W1, W2, W3, W4)$ goes for the probability of context inference node, the access structure is satisfied.

In the classroom it is expected when, where, who, why, what happened because every event has a consequence.

For example, suppose a teacher makes a question like that so far how many unmanned space-crafts have landed on Jupiter, and what are their names. What could be the next story? Firstly students would search on the internet and find the answer. And secondly if students know the answer, they would raise hands and answer it directly.

It is very rare that suddenly all of the students go out or drink alcohol during the class or lay down on the floor. With earlier even we can expect the next event.

If we describe this in the event-centric way, it becomes Storytelling and wearable devices can sense these stories. The sensing examples are as shown below.

Table 1. Storytelling Using Big-Data of Learning System

Event-centric way	Story	Sensing	BigData
A teacher makes a question	Teaching Story	Smart-phone, i-watch, band. Google-glasses	Teach programming
A students would search on the internet	Student respond	Internet device	SNS
They would raise hands and answer	Student respond	Smart-phone, i-watch, band	SNS
the students go out or drink alcohol	Unexpected	n/a	Pattern error

If we structuralize above discussion with Bayesian network as follows. In the proposed scheme the probability is calculated by algorithm of Bayesian Network, and at that time the variables are created to collect the student's context. If the calculated probability value is the attribute of context inference node, the access structure is satisfied and the cipher-text is able to be decrypted.

For example, teacher can design the inference node with Bayesian network. Suppose that teacher has the lesson plan to ask the name of the space craft that landed on Jupiter. In this case, the learning topic would be the comprehension of Jupiter and the scientific investigation for spacecraft. In other words, the appropriate explanation and questions for a lesson plan can be the inference node. Also this question can be developed to student's inference node in other aspects. How do students feel when the teacher asks a question? First of all this question would be made when they have some scientific information or after watching the video of Mar Exploration not suddenly during the class. Tough students are not supposed to prepare the answers by expecting these questions. Therefore these questions need to be encrypted and not let students know until teachers give a question during the class. But after the class, it must be decrypted and help students check the questions and get the answers easily. Above technology is included in the huge story called Class, therefore the security level and the target of education information need to be decided from the lesson plan step. It is demonstrated using Bayesian network.

3.3 Extraction Security Indexing Value to use Story-Telling under Learning Application

In the education environment that is applied by Attribute-Based Encryption, wearable device can provide bios-learning information to understand the class context. The education information from a wearable device helps the teacher to confirm the student-class history when they have learning consultation.

If teacher has no authority to read the class record of students, decryption authority can be given by redesign of access structure and delegation of the attribute. However when student is unconscious, decryption authority cannot be given.

In this paper the proposal scheme is applied to the learning environment considering the student, teacher and teaching authorities who have the wearable devices.

In terms of learning information access, the assumed scenario is that the teacher has no decryption authority to read important information like student's whole education history when it is an emergency or an unexpected event (the students go out or drink alcohol and so on) for students not to be conscious. The realizable scenarios in limited situations are shown below the proposed scheme applied scenarios considering patient's context.

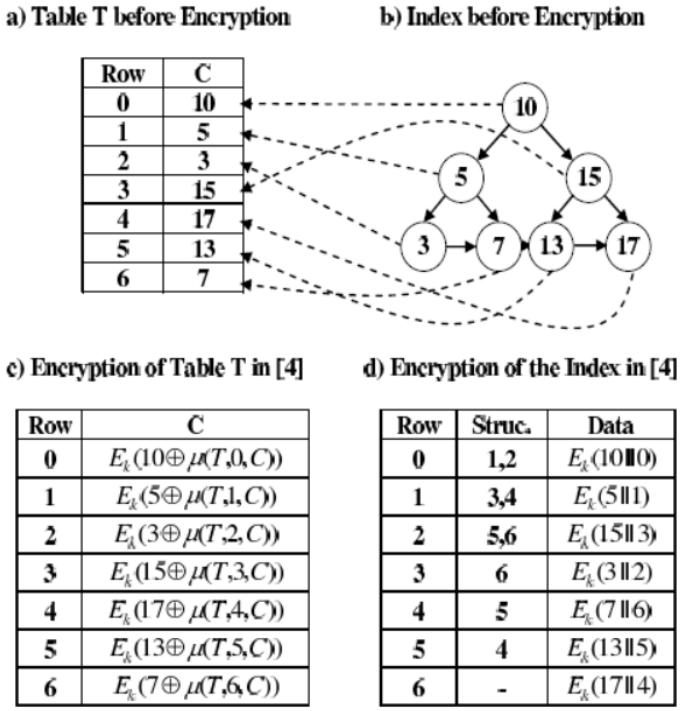

Figure 4. Database and Index Encryption as Described in [16]

The indexing scheme provided in is based on constructing the index on the plaintext values and encrypting each page of the index separately [14]. Whenever a specie page of the index is needed for processing a query, it is loaded into memory and decrypted [15].

Since the uniform encryption of all pages is likely to provide many cipher breaking clues, the indexing scheme provided in proposes encrypting each index page using a different key depending on the page number [17]. However, these schemes, which are implemented at the level of the operating system, are not satisfactory, since in most cases it is not possible to modify the operating system implementation [15]. Moreover, in these schemes, it is not possible to encrypt different portions of the database using different keys [15].

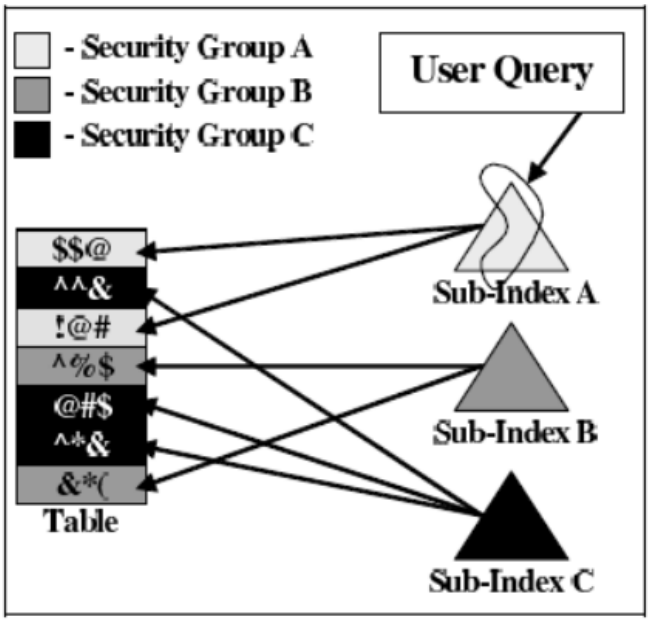

Figure 5. An Encrypted Database Column and its Corresponding Sub-Indexes [15]

Figure 5 shows the changeable security key value depending on the teachers' planned educational contents in so far mentioned classroom environment.

Suppose that Sub-index A group can answer the question which is about unmanned spacecrafts that have landed on Mars immediately. In that case, the level of security is needed but to make student approach the related video or make the student answer the next question and to not hide their answers. Likewise suppose that Sub-index B group can answer the question after searching for internet. In that case, different level of security is required. Lastly suppose that Sub-index C group shows unexpected behavior like dozing, slacking or trying to go outside. In that case, the access control for his/her wearable device and the disciplinary action is required. Like, it can be realized that this security and controlling factors is made up of each situation through the wearable device.

Table 2. Security Level of Index Using Attribute-Based Access

Event-centric way	Attribute Based Access	Group	Index values
The Design of learning topic	AND	All Group	N/A
A teacher makes a question	OR	All Group	N/A
Students would search on the internet	OR	Group A	Sub-index A
They would raise hands and answer	AND	Group B	Sub-index B
The students go out or drink alcohol	OR	Group C	Sub-index C

Finally throughout all process, the security keyword corresponding the educational information is extracted and based on that the security reinforces structures is organized as shown in the table above.

4. Conclusion

In this paper we proposed Attribute-Based Encryption considering context. As an application of the proposed scheme, the scenario is presented that the education record browsing authority can be given according to the situation or considering the context in the learning environment. However, it hasn't been explained enough in detail how context inference nods works.

This study is started from the process to get the information from the wearable device of students and teachers. Teacher and students are in the classroom wearing the wearable devices like Google Glass, Apple watch and Galaxy Gear (Samsung). This assumption is a considerable situation in the near future.

At that time the situation is flexible because it can be changed according to the teachers' educational objective, plan and method. The process is expressed by Bayesian network which is one of the ways of Network analysis. And from each step the predictable scenario (like answering immediately or not answering but internet searching) and unpredictable scenario (like dozing or chinwag) is sectionalized.

For each situation we can consider Attribute-Based Encryption. Moreover the standard of judgement is analyzed by scenario technique to extract indexing keyword from educational information.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry ofEducation (2013R1A1A2011581). This work was also supported by the Dongguk University Research Fund of 2014.

References

[1] Y.-S. Min, H.-Y. Kim and Y.-K. Kim, “Distributed file system technology for cloud computing”, Journal of Information Science Society, (**2009**), pp. 86-94.
[2] K.-Y. Park and Y.-J. Song, “Attribute Based Encryption”, Journal of Information Security Society, vol. 20, no. 2, (**2010**), pp. 85-92.
[3] J.-E. Song, S.-H. Kim, M.-A. Jeong and K.-I. Jeong, “Security Issues and Trend of U-healthcare”, ETRI, vol. 22, no. 1, (**2007**), pp. 119-129.
[4] K.-E. Ko, I.-H. Jang and G.-B. Shim, “User environment information based Context-based Service Inference Model”, Korea intelligence system Society, vol. 17, no. 7, (**2007**), pp. 907-912.
[5] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing”, CRYPTO 2001, LNCS, vol. 2139, (**2001**), pp. 213-229.
[6] A. Shamir, “How to share a secret”, Commun. ACM, vol. 22, no. 11, (**1979**), pp. 612C613.
[7] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-Policy Attribute-Based Encryption”, IEEE Computer Society, Proceedings of the 2007 IEEE Symposium on Security and Privacy, (**2007**), pp. 321-334.
[8] V. Goyal, O. Pandey, A. Sahai and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data”, Association for Computing Machinery, in Proc. of CCS’06, (**2006**).
[9] J.-H. Park, “context awareness system in ubiquitous environment”, Journal of Korea engineering Society, vol. 21, no 11, (**2004**), pp. 31-37.
[10] K.-S. Hwang and S.-B. Cho, “Learning of Bayesian Network”, Journal of Robot Engineering Society, vol. 3, no. 4, (**2006**), pp. 15-27.
[11] A. K. Dey and G. D. Abowd, “Towards a better understanding of context and context-awareness”, Georgia Institute of Technology, GVU Technical Report;GIT-GVU-99-22, (**1999**).
[12] https://www.google.com.ar/patents/US20120155635?dq=US20120155635A1&hl=ko&sa=X&ved=0CBwQ6AEwAGoVChMI1YvDxOOIxwIV2DaICh0pigGO.
[13] http://www.slideshare.net/gladysCJ/lesson-71-bayesian-network-classifiers.

[14] B. Iyer, S. Mehrotra, E. Mykletun, G. Tsudik and Y. Wu, "A Framework for Efficient Storage Security in RDBMS", E. Bertino et al. (Eds.): EDBT 2004, LNCS 2992 (**2004**), pp. 147-164.
[15] E. Shmueli, R. Waisenberg, Yuval Elovici, and Ehud Gudes, "Designing Secure Indexes for Encrypted Databases", http://www.ics.uci.edu/~ronen/Site/Research_files/Secure%20Indexes.pdf
[16] Y. Elovici, R. Waisenberg, E. Shmueli and E. Gudes, "A Structure Preserving Database Encryption Scheme", SDM 2004, Workshop on Secure Data Management, Toronto, Canada, August, (**2004**).
[17] R. Bayer and J. K. Metzger, "On the Encipherment of Search Trees and Random Access Files", ACM Trans Database Systems, vol. 1, (**1976**), pp. 37-52.
[18] J.-m. Do, J.-m. Kang and Y.-j. Song, "Attribute-Based Encryption Scheme considering Wearable Context", Advanced Science and Technology Letters Vol.109 (Security, Reliability and Safety 2015), (**2015),** pp. 18-23.

