International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.165-174
http://dx.doi.org/10.14257/ijsia.2016.10.11.15

Approach of HeDSS (Health-care Decision Support System) using Context-aware Technique

You-Jin Song[1], Jin-Mook Kim[2]

[1.] *Department of Management, Dongguk University Gyeongju Campus*
[123], Dongdae-ro, Gyeongju-si, Gyeongsangbuk-do, 38066, KOREA
[2.] *Division of IT Education, Sunmoon University*
221 bun-gil 70, Sunmoon-ro, Tangjeong-myeon, Asan-si, Chungchungnam-do, 31460, KOREA
[1.] *song@dongguk.ac.kr*, [2.] *calf0425@sunmoon.ac.kr*

Abstract

We are living in the Internet era of things. This has the advantage that things delivered collects information decision can be facilitated, and using the result of effective decision-making. Re-encryption scheme based on the existing attributes, situational awareness, we have the restrictions that apply to the Internet environment of things. Therefore, we will try to design a re-encrypted access structure of context-based new dynamic attribute-based. Structure of the proposed new approach, to take advantage of the Bayesian network technology to reflect the dynamic situation of the data. Comparing the differences of HeDSS system newly proposed and re-encryption scheme based on an existing attribute, HeDSS is possible to secure data sharing.

Keywords: *Internet of Things, Attribute-Based Encryption, Context-aware, Bayesian Network*

1. Introduction

Things of the Internet to participate as a subject of the communication (IoT, Internet of Things) is in full swing. IoT utilizes communication between things, collect information during things, processing an infrastructure that enables the process to recognize the situation (context) to which the user belongs, the intelligent service to the user to provide [1] [14].

Status (context) includes a user's personal conditions and environment, example of a situation related to the personal status of the user, may become gender, age, example of a situation related to the environment, temperature and there is to be a humidity [11]. Context awareness, things and humans using various sensors and wired communication technologies can be created significant value that can communicate.

In addition to collecting status information of things based on the context awareness, the user's interests and needs, in combination with the personal data, it has evolved in the direction of providing optimized information. Context awareness IoT art recognizes the user's situation, a technique that can provide services that can improve the ease by using the infrastructure IoT. In this context awareness IoT environment, for transmission accurate information, to infer the information collected in accordance with the user's situation, it is important to generate status information.

On the other hand, big were collected via a sensor to the spread of IoT - data stored in the cloud server, a wired / wireless network to protect data that is shared over a high service reliability and safety provided to security technology There is required. Information distribution in the cloud should be the minimum amount of information securely shared and used as a legitimate objective information, especially because it may

ISSN: 1738-9976 IJSIA

contain sensitive personal information such as an individual's biometric data collected by a sensor that could violate the privacy of individuals [1] [2].

Such securely share information sensitive situations, privacy data can utilize attribute-based capable of limiting the rights encryption technology (ABE: Attribute-Based Encryption) is required [5] [6]. Only users with a valid attribute access structure of the way the existing property-based encryption method that encrypts data to be accessed time because static means that frequently change affiliations, information about the object, such as title, name, used as a property that does according to the access structure it can be configured to reflect the (time-dependent) status changing dynamically. In this way time-varying location where you want to, should the weather, temperature, humidity, the attributes of the sensor data, such as biometric data is utilized to approach the structure to reflect the context. For example, in the case of emergency patient is unconscious, even doctors can be confirmed only low medical records of security evaluation must be able to gain access to some of the critical data, such as all of the medical history of the patient.

In this paper, safely collected, the access structure to reflect the dynamic characteristics of the sensitive sensing data should be stored and design, to take advantage of the Bayesian network (Bayesian Network) technology in order to reflect the dynamic situation of data on, to reconfigure the access policy. Here, access policy (Access Policy) means decryption condition of Tree structure represented by access structure considering the Context. Also, by collecting the properties of the sensor data to awareness the situation, for example, utilizing a decryption algorithm of context-based services reasoning model for providing the appropriate decryption services for rights acquisition [7] for cloud data sharing service dynamic design a property-based encryption method that reflects the access policy.

2. Related Researches

This section described the secret sharing method required for the access structure representation that reflects the access policy. In addition, we describe a Bayesian network and context-based service reasoning model using it.

2.1. Secret Sharing

「(k, n) threshold secret sharing scheme」 is a typical way of secret sharing. (k, n) threshold secret sharing scheme is a structure that is used in many attribute-based encryption. Secret sharing scheme is based on the value of what the secret to a tree structure, a method of dispersing from the root to the leaf.

(K, n) threshold secret sharing scheme sets a threshold condition (the number to distributed: n and the number needed to restore: k) for each node of the tree. If each node has a dispersion value equal to or more than the threshold number, it is possible to calculate the value of parent node. If dispersed value to the leaf has a number that satisfies the threshold set for the each node of the tree, it can be calculated from the leaf to the root. Accordingly, it is possible to restore the secret value of the root.

In the attribute-based password, first, to express the decryption policy in the form of a logic tree. The AND / OR logic tree node of the decoding policy. And, the attributes of the decryption policy made the leaves of the logic tree. Encryption processing (ie, secret dispersion method) are dispersed in a leaf the value of the secret from the root of the tree, distributed value to the leaves (example, attribute value) to include the encryption. When decrypted, it contains the value calculated from an attribute with the decryption of the private key. Thus, using the distributed value to the leaves in the calculated value and pass phrase, go back through the logic tree from the leaf to the root.

Descriptors' attribute in the private key, only if satisfied the conditions of the logical tree (approach structure that represents the decoding policy), it is possible to go back in the tree to the root. And, it is set to the root it is possible to restore the secret value.

Further, it is possible to restore the passphrase on the basis of the secret value to the plaintext.

CP-ABE is an attribute-based encryption was proposed early in the study (k, n) threshold secret sharing scheme property-based password encryption policy using. This is the basis of several other properties based password.

2.2. Bayesian Network

By utilizing time-dependent varying dynamic sensing data, it is effective to apply a Bayesian network to provide services appropriate for situation a person. A complex process in order to infer the situation by simplifying the relationship between the quantified nodes (module) in the IoT environment, are suitable to determine the user's situation.

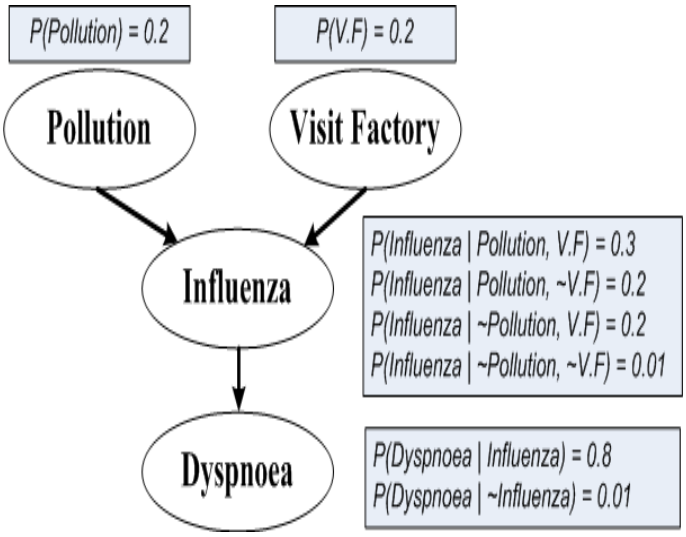

Figure 1. Examples of Bayesian network

Bayesian networks, as directional acyclic graph (DAG: Directed Acyclic Graph)model, it is possible to efficiently express the relationship of a number of probability with less effort by the conditional probability table (CPT, Conditional Probability Table) defined for each node. In this paper, constitute the encryption policy (Ciphertext Policy) make up the Tree to represent the access structure based on Bayesian network in order to configure the access policy (Access Policy).

Each node in the Bayesian network refers to actual sensing environment variables, the relationship connecting between nodes, No. called (arc), which is dependent among each variable [Figure 1]. After learning network designed and evidence of any circumstances (*e.g.* hurt) is observed, and based on the evidence, using the CPT independence condition of each node, using the Bayesian inference algorithm, probability of the state of each node is calculated.

2.3. Context-based Service Reasoning Model

In order to provide a personalized service in IoT environment, context-based service inference model that utilize Bayesian network [10] have been proposed. IoT environment information 4W1H of the sensing environment (Where, Who, When, What, How) and defined by, at the same time as the inference of the user of the situation, and is configured to be able to provide to infer the appropriate service to the situation there [Figure 2]. In other words, to take advantage of the user of the situation that was reasoning in Bayesian network (How), to infer the service depending on the situation. Together to represent

these relationships in the form of probability and the following formulas are possible representation.

$$P(D1) = P(H|W1, W2, W3, W4)$$
$$P(D2) = P(S|H, W1, W2, W3, W4)$$

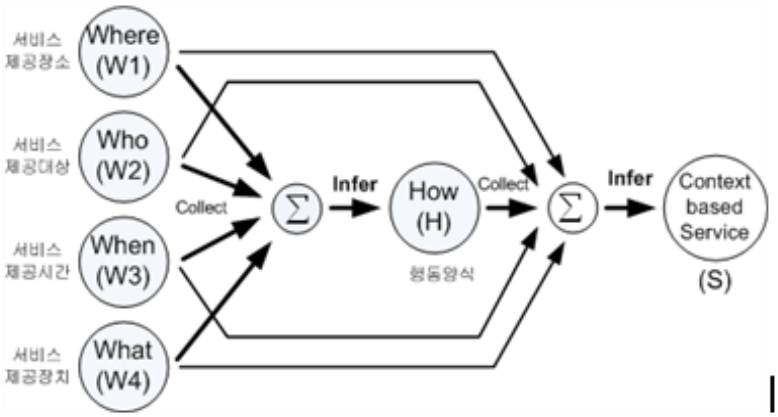

Figure 2. The Formula for the Context-Based Service Inference Process and the Probability Representation

3. Design of Context-aware Recognition and Attribute-based Access Structure

In this chapter, we subscribe a design of our proposed system that have context recognition process step, a structure that is attribute based access control policy. In first section, we explain context recognize process. And we will subscribe HeDSS design and implement scenario in second section.

3.1. Context Recognition Step

Context is meant information that can be characterized the status of the object. Therefore, the context-aware (context-aware), the user is meant to recognize the process by using the context of the necessary services [11]. We are, in order to implement the user's context recognition process, to try to take advantage of the algorithm used in the context-based service reasoning model. And, we will calculate the probability using the algorithm used in the context-based service reasoning model. It can decrypt only when the attribute of each node matches the calculated probability.

Algorithm of context-based service reasoning model, five variables: having (4W1H Where, Who, When, What, How) a. Each node is an access structure probability and attribute values calculated using five variables to see if it matches.

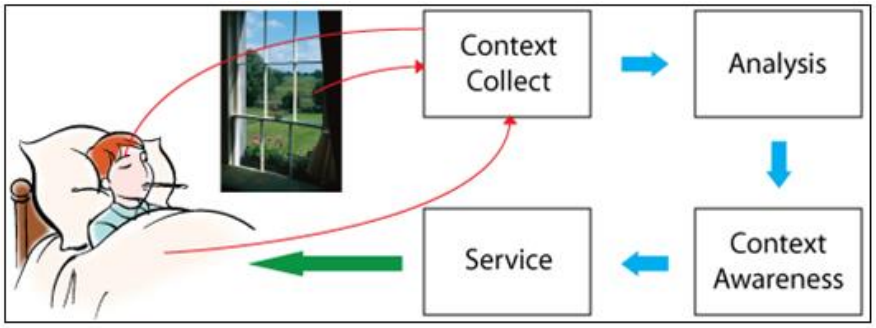

Figure 3. Context Recognition steps in IoT Environment

As in Figure 3, HeDSS collects the patient's context, changing the collected context to the situation variable. Situation variables, using the Bayesian network algorithm, is stochastically calculation. If the calculated probability matches the attribute value of the node that is matched to the access structure, the node is able to decrypt the cipher-text.

3.2. Scenario of HeDSS

We have configured the scenario of the following experiment in order to design and implementation of the proposed system in this paper. Users of the health-care system (the elder) were hurt by stumbling in climbing in IoT environment.

Patient is no change during a certain period of time. Special there is attention hurt the place, fog note that is a section of the high-risk. So, health-care system no change his positioning data that is very dangerous. Because his heart rate of the shock is very fast and his blood pressure is high. In this time, various sensor collect patient context such as his location data, bleeding state data, heart rate, and blood pressure. This is a biometric data of patient (the elder). Then smart device send the biometric data with encryption using his session key.

Next, rescue team receive the encrypted biometric data. And fire-fighter send this message to hospital with re-encryption by his session key. And rescue team request a authority about patient's biometric data. Then hospital or doctor decrypt a received cipher-text of patient and check his situation through tele-condition. Then doctor decide to patient's condition, empowerment to rescue team, transfer to operation data to rescue team. Fire-officer receive that and he operate a medical service by doctor's offer. In this time, fire-officer able to check patient's diabetes that has been encrypted in the cloud server. And he operate to stop bleeding, aid a blood operation that is emergency operation. At the time, fire-fighter find an optimal transport-path (distance, professionality) and send the patient's context to that. So, doctor and rescue person, patient can access the encrypted data such as patient condition data in our proposed system by attribute values.

If it is possible to attribute-based encryption method is to check the medical history of the patient at the time of practice in applied medical environment, it is possible to effectively treat. If the doctor is able to grant the decryption right through the re-design of the delegation and access structure attributes if you do not have permission to view the medical records of patients. However, in patients with unknown consciousness, it cannot be imparted to the decryption authority.

It is possible to effectively treat. If doctor or rescue team check the medical history of the patient at the time of practice in attribute based health-care system. If the doctor don't have a right about patient's medical history or something, TA give a delegation to the doctor for decryption and read a patient individual medical data. And we can give a right to doctor by access structure re-design. But if patient have no consciousness, it cannot be imparted to the decryption authority.

We are to apply the provision method to the medical environment, configure a scenario in which the doctor the patient does not even have the decryption right to the unconscious of emergency it is possible to view the important data, such as all of the medical history of the patient did. That is, the scenario of applying the proposed method capable of considering the situation of the patient, the following.

Hemophilia patients who need high-speed blood transfusion at the time of bleeding was taken to the emergency room of the remains unconscious in excessive bleeding. An emergency room doctor prior to confirm the patient's medical history, cannot know that there are symptoms of hemophilia. Therefore, he attempting to access the patient's medical record in order to confirm the patient's history.

An emergency room doctor don't have a private-key with the attributes that satisfy the access structure to the patient's medical records. So he unable to grant decryption authority because patient also is unconscious.

① The doctor requesting access to the patient's medical records and he calculate the probability P(D2) with the variable of behavior and environmental information of the patient.

② If probability value P(D2) satisfy expression(N / 10 <= attribute), it is possible to know the polynomial status inference node.

③ Through Decrypt(CT, SK) algorithm, we outputs the $e(g, g)^{rs}$ by calculates the DecryptNode(CT, SK, x).

④ Calculate the DecryptNode(CT, SK, R), we derived patient's medical records such as M

⑤ The doctor confirmed that the patient is a hard hemophilia patient and he start the appropriate treatment about optimally.

3.3. Structure and Procedures

In the scenario of the experiments presented above, the patient is assumed that has occurred an accident while climbing, various sensors dynamic status information that is installed in the climbing course (position information, elderly residence time) collect. To provide the collected context to the hospital the patient's conventional of the elderly had been through (TA). Then, the doctor who recognize this is transmitted to the rescue by encrypting the processing method in accordance with the dynamic status information of the elderly. So, after the rescue workers who received the delegation of authority it has been grasped by receiving the information, to implement the treatment suitable for high-speed structure and elderly patients. And, the rescuer transport the patient to the hospital. It is shown in Figure 4 an overall structural view of a system (HeDSS) that operates.

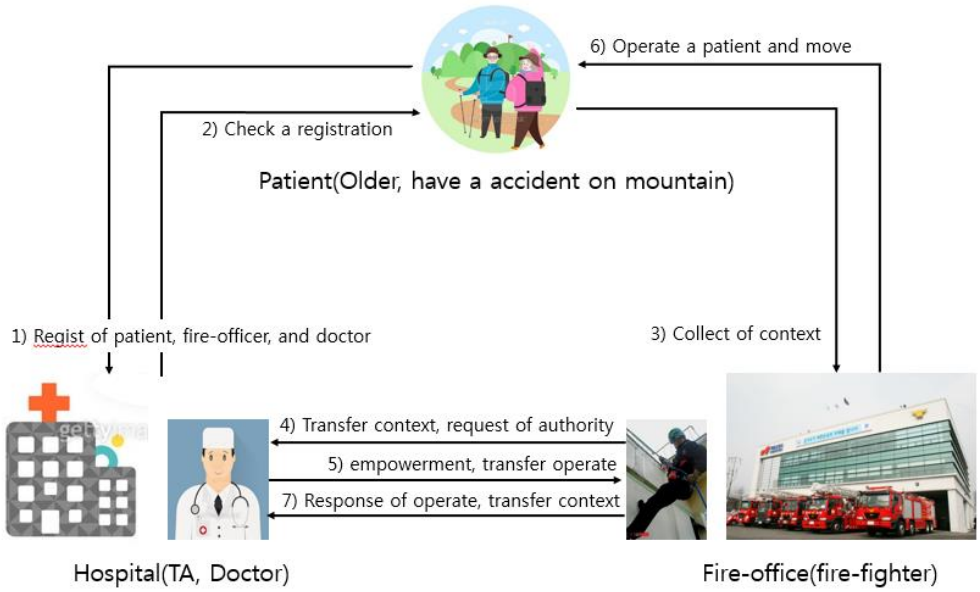

Figure 4. Operation Structure of HeDSS

Looks like a Figure 4, we need three components such as hospital, rescue team, patient for collect a context, the help of the instant and the treatment in accordance with the patient's condition. In this time, hospital construct the doctor and TA. TA process an authentication and store, access, edit of policy. And fire-office have a rescue team and fire-office. They have empowerment and secure communication channels.

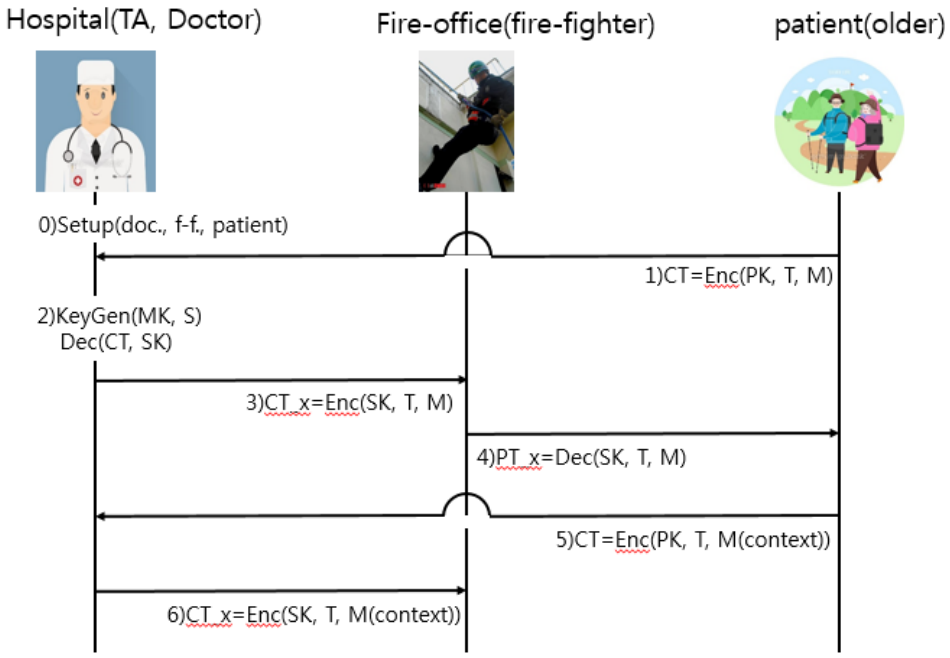

Figure 5. Process Steps of HeDSS

Finally, case of elder patient, we assume that mountain have many various sensor and a sensor collect a context of patient real time. And it send to TA that check a condition of patient on the mountain. If patient have a problem on the mountain, TA request to rescue to fire-officer for medical operations instantly. In this situation, TA encrypt patient medical record and send it to rescue team. Then rescue team decrypt a ciphertext with

theses' session key on the mountain. And they read an instant operation order and operate to patient. And they move the patient to hospital or shortest medical center instantly.

Figure 5 show about this procedures. In this figure, patient, doctor, rescue team must store on the TA. HeDSS have 6 detail steps. TA can delegate to rescue team with doctor because doctor in hospital but patient have accident on mountain. So doctor delegate an authority to rescue team or fire-office for instant medical operation to patient. In this time, TA permit fire-office or rescue team to delegate. Detail steps follow.

① Step 1: Sensor around of patient get context that patient have fallen so he have a sick. Then sensor collect location data, local specific data, accident data, patient blood type, heart rate, and bleeding condition. And sensor send a context to shortest-path hospital or rescue team.

② Step 2: Hospital make encrypted medical operation data and send to rescue team. Then they decrypt by his own session key and they move to patient side. And they want authority delegation to TA.

③ Step 3: Rescue team arrive accident place then they check patient's condition and location information with encrypt by rescue have session key. In this time, some attacker can try to decrypt patient information. But they don't have patient's information because rescue team make encrypted data.

④Step 4: Rescue team have a delegated authority. So they can decrypt the patient's medical operation data. And they operate and move to hospital the patient.

⑤ Step 5: This is an only added step in this research by ours. If patient's dynamic context receive on hospital, TA or doctor can make re-encrypt a new operation data and send. In this time, only delegated rescue team can decrypt this message and operate that.

⑥Step 6: additionally, if doctor receive more sensed data, they make instant medical operation information and encrypt. And they send to rescue team to encrypted message instantly. Then rescue team can access instant message because they only have delegated permit.

Our HeDSS can support to dynamic context process. So it can share secure context and between hospital and fire-officer can make encrypted dynamic context while move to hospital. And they can make an encrypted message and decrypted message in real time. And we design smart-router (proxy) for instant process in the emergency car or fire-office. So they can fast access in the real time about patient medical information, medical operation data, and so on. And it can solve delay time on the hospital against of batch job in the hospital or data center.

4. Analysis of HeDSS vs. Existed Approach

New approach have four advantages compare with existed studies [5] [6] [7] using CP-ABE algorithm. We subscribe about it on the [Table 1].

Table 1. Analysis of Existed Approach vs. HeDSS

	Existed Approach [5] [6] [7]	HeDSS
Authority empowerment	○	○
Man-in-the-middle attack	△	×
Eavesdrop	×	×
Delay-time	△	○
Dynamic context processing	×	○

HeDSS have 4 advantages as follows.

First, it can protect sensitive medical information by authority empowerment skill. Existed CP-ABE based system can empowerment but existed system don't support to protect a sensitive medical information such as privacy and location based data. So, patient can fall into the problem of security and thief. But HeDSS use an authority empowerment method and it can provide to make more secure protocol within patient and hospital. And it can provide to make more secure protocol through patient and fire-exit officer. They can decrypt a patient's sensitive information using sensing key and transfer it to hospital.

Second, we have smart-gateway (proxy) on our proposed system (such as HeDSS) to process patient situation information within real-time (at least 3 second). Therefore patient and fire-exit officer only have low-power device such as smart-phone. But they can access a situation information and calculate a location data, and patient's sensed data such as a heart-ratio data, temperature data, and so on. Sense and Collected data send to smart-gateway by patient's smart-phone. And it can calculate or decide and it change a context-aware information by smart-gateway. Next this context-aware information transfer doctor in hospital using encrypting algorithm. But this situation don't make slowly because HeDSS have smart-gateway.

Third, all information sent encrypted with session key by between the hospital and the patient, between the hospital and fire-officers, between the fire-officers and the patient that have each key in the proposed system. Thus, this message can decrypt only by each person. So this system have a safe to eavesdropping and man-in-the-middle attacks by bad persons. But our system have weakness about eavesdropped message that is don't read. And it can break by powerful attack. However, you will not be able to decrypt the information in the attack to intercept a general eavesdropping or man-in-the-middle attack.

Final, the proposed system does not have the danger due to the centralized information processing with the cloud service system. Not only proposed system also has the advantage that the smart gateways handle dynamic content in real time.

5. Conclusions

In this paper, we want to design the access structure to reflect the status information for the sensitive data were reconstructed to access policies of the context-based. The new proposed approach has the advantage compared to the traditional research methods empowerment is possible. And then our approach have less processing delay-time. And it is possible dynamic context processing. We want to propose further measures to create a system based on Java program, and the processing delay on this to see how much faster compared than in previous studies.

Our proposed model is available for secure data sharing policy that reflects the access to data compared to the CP-ABE manner and stored in a variety of cloud data. In the future, we will study the Context-aware Security Modeling for Context-based encryption, authentication, and access control policies. And to implement the CP-ABE system with secure access policies of the data collected for the health-care.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1D1A1B03931689). This work was also supported by the Dongguk University Research Fund of 2016.

References

[1] CSA, “Security Guidance for Critical Areas of Focus Cloud Computing”, Vol.2.1, (2009)
[2] Yu, S. C., Wang, C., Ren, K. I. and Lou, W. J., “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, INFOCOM, 2010 Proceedings IEEE, (2010)
[3] A. Shamir, "How to share a secret", Commun. ACM, 22(11):612C613, (1979)
[4] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing”, CRYPTO 2001. LNCS, vol. 2139, (2001), pp.213-229.
[5] J. Bethencourt, A. Sahai and Waters, B., “Ciphertext-Policy Attribute-Based Encryption”, IEEE Computer Society, Proceedings of the 2007 IEEE Symposium on Security and Privacy, (2007), pp.321-334.
[6] 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)
[7] Sanjam Garg Craig Gentry Shai Halevi Amit Sahai Brent Waters, “Attribute-Based Encryption for Circuits from Multilinear Maps”, http://eprint.iacr.org/2013/128.pdf
[8] Allison Lewko, Brent Waters, “Decentralizing Attribute-Based Encryption”, Advances in Cryptology – EUROCRYPT 2011 Lecture Notes in Computer Science Volume 6632, (2011), pp 568-588.
[9] Kwangyong Park, Youjin Song, "Attribute-based Encryption Technique", Korea Information Security Association, The Journal of Korea Information Security Association, Vol.20, No.2, (2010), pp.85-92.
[10] Kwang-Eun Ko, In-Hoon Jang, Kwee-Bo Sim, "Context-based Service Reasoning model for user by User Environment Information ", Korea Intelligence System Association, Proceedings of KFIS Autumn Conference2007, Vol.17, No.7, (2007), pp.907-912.
[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] AlRwais, S., AlMuhtadi, J., “A Context-Aware Access Control Model for Pervasive Environments”, IEEE 3rd International Conference on Network & System Security (NSS), (2009).
[13] Tentori, M., Favela, J., and Rodriguez, M. D., “Privacy-Aware Autonomous Agents for Pervasive Healthcare”, IEEE Intelligent Systems, Vol. 21, No. 6, (2006), .
[14] You-Jin Song, Jin-Mook Kim, "A Secure Health Decision Support System Based on Context”, Information2016 10th International Workshop on Psychology and Counseling Welfare Security, Reliability and Safety, Vol. 6 (2016), pp.32-35

Authors

You-Jin Song, he received the Ph.D. in Department of Information Security, Tokyo Institute of Technology University at Japan. He was work and research about various security service and protocol at ETRI (Electronics and Telecommunications Research Institute) from 1988 and 1996 in Korea. He is a Professor in department of business and administration, Dongguk University Gyeongju Campus, Korea from 1996 and now. His research interest are Ubiquitous and IoT securityservices and Privacy, Digital content secure services, SCM/CRM security, services.

Jin-Mook Kim, he received the Ph. D in Department of Computer Science, Kwangwoon University in 2006. He is an assistant professor in the Division of IT Education at Sunmoon University in Korea from 2006 and now. His research interests include network control architecture, security engineering, authentication on the network, and Smart-phone security.

