Journal of Multimedia and Information System VOL. 3, NO. 3, September 2016(pp. 103-110): ISSN 2383-7632(Online)
http://dx.doi.org/10.9717/JMIS.2016.3.3.103

Privacy of Capability Token in the IoT Service System

Deresa Jang[1], Jin-bo Kim[1], Mi-Sun Kim[1], Jae-Hyun Seo[1, *]

Abstract

The recent development of the Internet of things (IoT) has led to the introduction of new access control measures. Even during the access control for security, however, there might be privacy infringements due to unwanted information provision and collection. Measures to control this process are therefore required. This paper defines the structure and policies of tokens to protect privacy that can be exposed through the token information when you use the capability token in the IoT service system.

Key Words: Privacy, Capability, IoT, Token

I. INTRODUCTION

The Internet of things (IoT) has brought rapid change in our lives and industries by eliminating the constraints of time and space for physical devices and networks. The convenience presented by various techniques and devices has also increased security threats when they communicate with each other [1].

The devices connected to IoT create a lot of information and communicate through networks. In the process, information related to the user's privacy is collected and sent to unwanted recipients. In addition, the information on a device that provides the service, which is one of the subjects of the information, can also be released indiscriminately [2].

The IoT environment needs new privacy protection measures to protect the information subjects, including the devices that generate information and provide services, in addition to the users.

In the IoT environment, the capability-based access control method is a new access control technology that is gaining popularity. This approach has the advantage of being able to prevent speed degradation due to security problems because it can minimize repeating patterns better than ACL-based access control methods. In ACL (Access Control List), the server has all the information of the information subjects and confirms identities. [3] On the other hand, in the capability mode, the subject has its own information and directly communicates with the devices, thus causing a privacy breach.

In this paper, we examined the privacy protection for token-based access control in the IoT environment. In the process of using the access control, you should be able to avoid unnecessary exposure of information by identifying the flow of your information. You also have to avoid any unwanted exposure of resource information, which is the device information. The target of privacy protection in this paper is the information of the user in capability tokens and resource services. For this purpose, we defined privacy and the structure of the token for the protection of privacy, as well as privacy management policies.

This paper is organized as follows. In Chapter 2, we explain the access control technology in the IoT environment and the access control method based on capability tokens in the IoT service system, which is the basis of this paper. In Chapter 3, we explain our proposal regarding the privacy policies and the structure of capability tokens for privacy protection. Finally, in Chapter

Manuscript received August 30, 2016; Revised September 25, 2016; Accepted October 10, 2016. (ID No. JMIS-2016-0015)

Corresponding Author (*): Jae-Hyun Seo, 1666, Yeongsan-ro, Cheonggye-myeon, Muan-gun, Jeollanam-do, Korea, 061-450-6480, jhseo@mokpo.ac.kr.

[1]Interdisciplinary Program of Information & Protection, Mokpo National University, Mokpo, Republic of Korea, jdrs0405@mokpo.ac.kr, Progress97@mokpo.ac.kr, misun@mokpo.ac.kr.

4, we provide our conclusions and directions for future research.

II. RELATED RESEARCH

2.1 Access Control Technology in the IoT Environment

The issue of access control in the IoT environment should be approached by considering the difference between IoT and the existing Internet environment as follows. First, in the Internet of Things, interactions occur within a short period of time, and the same requests are often performed, unlike the existing Internet environment. Second, the analysis and permission for resources and services in the IoT may not be the same each time, even for the same requests. This is because it may be changed according to the surrounding situations. Therefore, in an open and wide range of computing environments, it is necessary to find an access control technology by considering scalability, device management issues, and flexible authority delegation [4,5,6].

In capability-based access control, the subject owns the list that defines permissions for the object. The subject presents its capability to their objects, and the object provides services accordingly [4,5].

S. Gusmeroli[3,7] proposed a capability-based access control method to control access to the IoT system and named CapBAC. This paper enables the subject to control access to its service and information with the principle of least privilege and authority delegation.

The subject has access rights that can be delegated, and it can access the resources within the limit of its delegated authority. In addition, access rights can be disposed of and dynamic adaptability can be provided through the fragmentation of information. In this paper, the capability-based access control is referred to as SAML/XACML [3,4,7].

Mark S. Miller [9] presents the differences between the new capability-based system and the existing resource system used in traditional access control techniques as follows.

First, the access control list and the capability list have the same format.

Second, the capability list does not provide any limitation, and it cannot revoke its rights. In fact, the list of capability-based access control is similar to the access control list in its format because it is based on Lampson's access matrix. In its expression of rights, however, it takes an approach from another perspective.

Third, capability-based access control provides delegation, but has clearly presented the boundaries of delegation, and the delegated authority cannot be canceled.

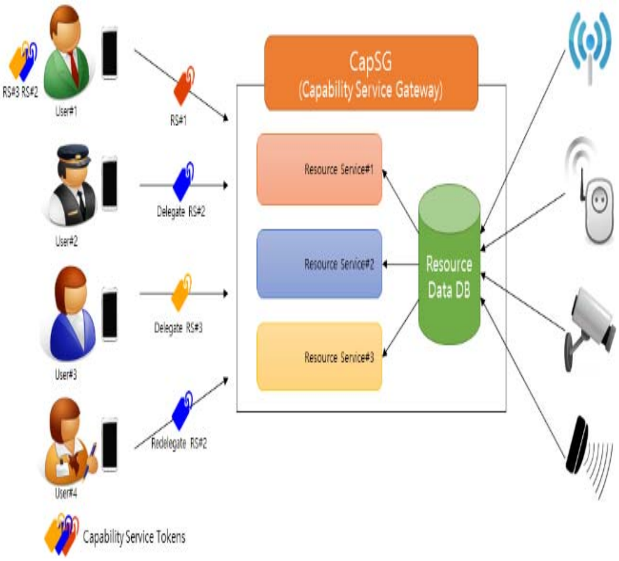


Fig. 1. Access Control in IoT Service System Structure.

2.2 Access Control in IoT Service System

This paper provides the measures to protect the privacy of users and resources contained in the tokens in the capability token-based access control systems. It was conducted in an IoT environment that was implemented in existing studies [4].

The configuration of the existing IoT systems is shown in Figure 1.

The IoT service system consists of two zones: one is the service domain area working as a device to generate practical information, and the other is a gateway that collects and processes data from the domain area and provides services.

The gateway manages resource data and services, and it also issues tokens to the users who request resource services to authenticate them or control access to the resource services. The gateway also manages the delegation of capability tokens.

The resource service provides data received from the relevant resource devices and saved in the gateway. This data is provided to the users after being processed according to the services users' needs.

Users can access the services by using the CaC (Certificate and Capability) token that includes authentication and access rights. Users authenticated by using the certificate token can be provided with the desired resource services by using the capability tokens. The capability tokens are first issued by the resource manager and can be delegated to other users. If a delegated token is valid, then the delegated user can be provided with the relevant resource services. The token can also be re-delegated to other users [4,10].

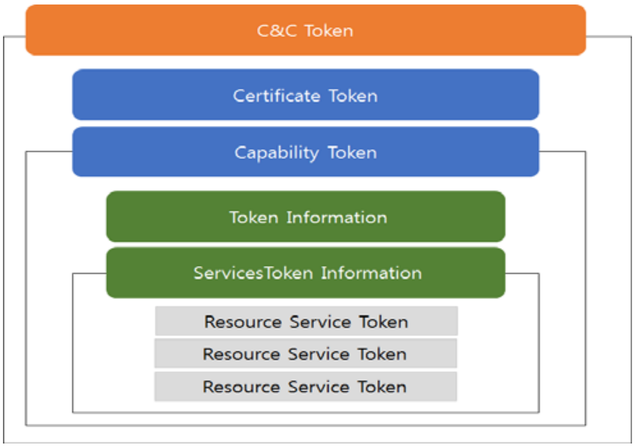


Fig. 2. C&C Token Structure.

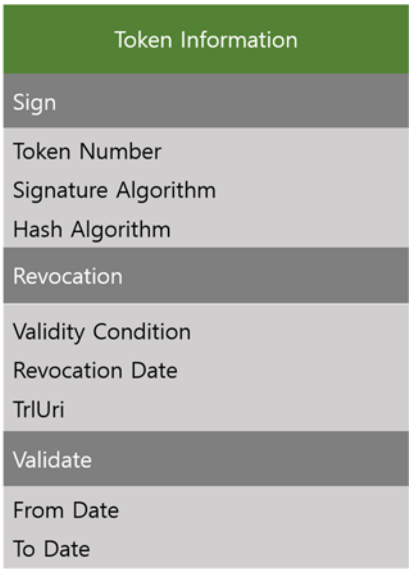
III. PRIVACY OF CAPABILITY TOKEN IN THE IOT SERVICE SYSTEM

In this Chapter, we explain our proposal regarding the privacy policies and the structure of capability tokens for privacy protection. We explain also define the token privacy for this purpose.

3.1 Capability Token

CaC tokens use an XML format containing user authentication information and resource service information. As shown in Figure 2, CaC tokens are classified as either certificate tokens for authentication information or capability tokens for controlling access to services [4].

Capability tokens include token information and service token information. A service token refers to a token that controls access to the resource services.



Token Information

Sign

Token Number
Signature Algorithm
Hash Algorithm

Revocation

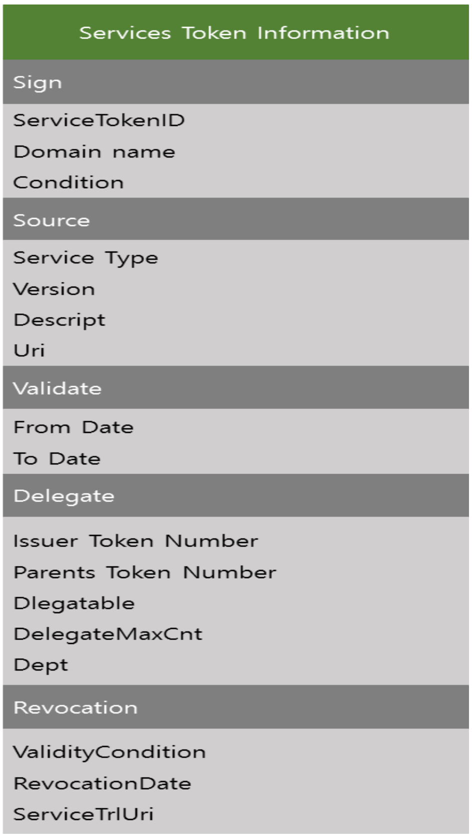
Validity Condition
Revocation Date
TrlUri

Validate

From Date
To Date

Fig. 3. Token Information

Token Information contains a Token Number, Signature Algorithm, and Hash Algorithm for CaC tokens. When you issue or renew certification tokens, you will create your signature by using the Token Number and Algorithm in the Token Information. In the Token Information, Validate shows the validity of the token, and Revocation manages the tokens expired or to be disposed. You can also send the data to TrlUri to manage it on the server.



Services Token Information

Sign

ServiceTokenID
Domain name
Condition

Source

Service Type
Version
Descript
Uri

Validate

From Date
To Date

Delegate

Issuer Token Number
Parents Token Number
Dlegatable
DelegateMaxCnt
Dept

Revocation

ValidityCondition
RevocationDate
ServiceTrlUri

Fig. 4. Service Token Information.

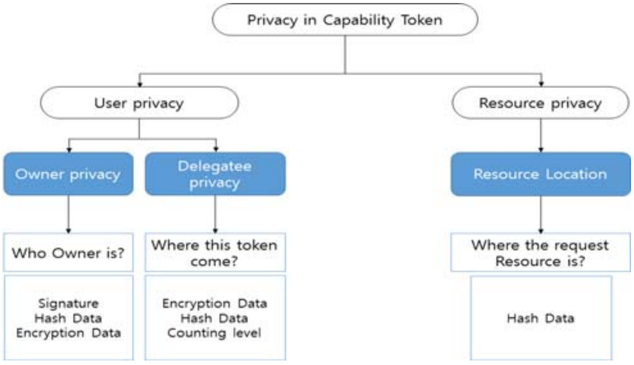


Fig. 5. Privacy in Capability Token

.

The Service Token Information segment serves as an actual capability token that can access each service. This segment enables you to distinguish tokens by ServiceTokenID, Domain name, and Condition. The Source has definitions about the services that can be accessed by tokens: Service Type, Version, Descript, and Uri. To delegate the token to someone else, Delegate manages the related information: Issuer Token Number, Parents Token Number, Delegatable, DelegateMaxCnt, and

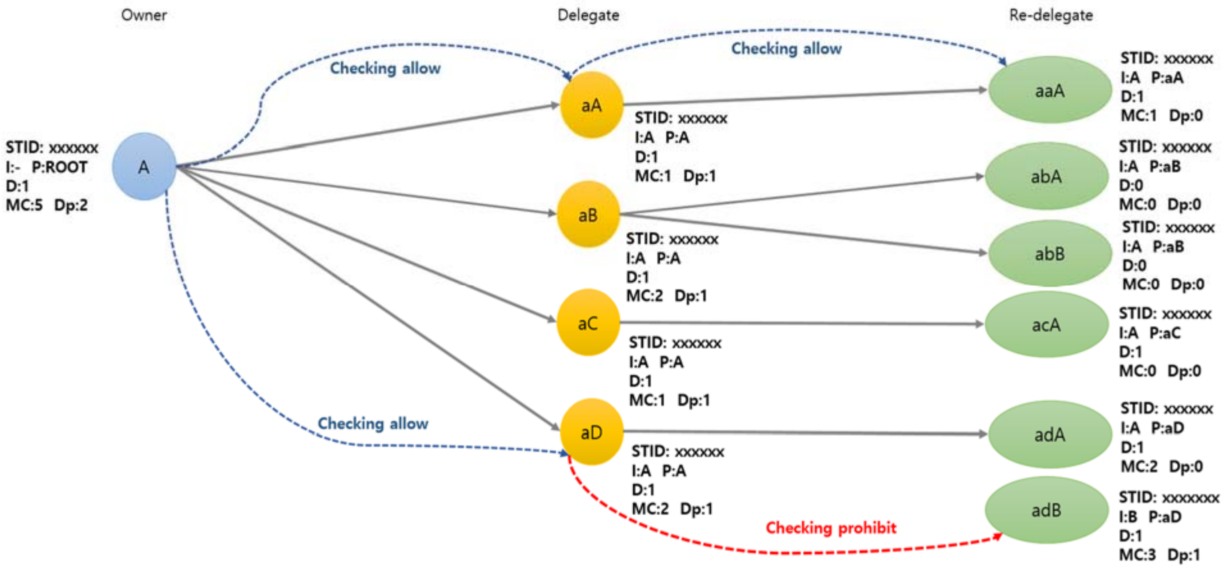


Figure 6 Privacy Protection of Token Owner flow diagram

Dept. Issuer Token Number is the token number of the first issuer of the token. Parents hold the Token Number of the person who is entrusted with the token. You can easily identify whether the token can be delegated to others. When the value of Delegatable is 1, delegation is allowed, but when it is zero,
delegation is not allowed. DelegateMaxCnt represents the maximum number of tokens that the user can delegate. Dept represents the count of re-delegations of the token available for the initial issuer. In the Token Information, Validate shows the validity of the token, and Revocation manages the tokens expired or to be disposed. You can also send the data to ServiceTrlUri to manage it on the server.

3.2 Definition of Token Privacy

In this paper, we studied the privacy of capability token in the IoT service system. For this purpose, we defined capability token-based privacy in an IoT service system environment with what was defined in existing studies.

The privacy that is to be implemented through the capability tokens is divided into two groups: User Privacy and Resource Privacy.

For User Privacy from the users' perspectives, their information should not be exposed to other users through the capability tokens, and they should be able to check the flow of the token they issued. We sub-divided the User Privacy group again into two sub-groups: Owner Privacy for token issuer and Delegate Privacy for those who are entrusted to use the tokens.

For Owner Privacy, you may use encryption and hash techniques to hide your information contained in the token. When the token is to be delegated to other people, you should be able to check the information about the delegate, and identify and control the flow of the token. For delegate privacy, a delegate who was entrusted with the token can only see his delegator and the fact that the token is a delegate. At the time of re-delegation, the delegator should be able to hide his own information contained in the token, similarly to the token creator. Re-delegation information should also be able to be hidden.

Resource Privacy is defined from the resource service perspective. This means that when a user uses the services with a capability token, you can hide the resource service device and the location of the data storage. To do this, you can apply the hash to the resource service data.

3.3 Privacy Protection of Token Owner

To protect the Owner Privacy, the delegating user needs to have the information about who has been delegated with the token. The delegator should also be able to search traces of his tokens and dispose of them if desired.

In addition, the owner should be able to hide his own information contained in the token.

Figure 6 shows an example of an owner who checks the traces of his token in the process of delegation in relation to the token owner privacy policy.

In the example given to illustrate the token owner privacy policy, the token is limited to only containing information about ServiceTokenID, IssuerTokenNumber, ParentsTokenNumber, Delegatable, DelegateMaxCnt, and Dept.

A token with ServiceTokenID xxxxxx was issued to Owner "A" from Root. Delegation is available as the value of Delegatable is 1. DelegateMaxCnt is 5. and Dept value is 2. "A" delegated this token to aA, aB, aC, and aD. In this case, "A" can set the values of Delegatable and DelegateMaxCnt. But, "A" cannot enter a value greater than his for DelegateMaxCnt. Then, aA, aB, aC, and aD re-delegated the token xxxxxx.

In this scenario, when "A" wants to check the flow of the tokens with ServiceTokenID xxxxxx, he collects the tokens that ServiceTokenID is xxxxxx and IssuerTokenNumber is

"A". After collecting the tokens that has "A" for ParentsTokenNumber, "A" collects the tokens that have ParentsTokenNumbers that are the same as the TokenNumbers that he collected. A flow chart in a linked format is created and shown to "A". When aA or aB also create their own flow chart, they should collect the tokens that have ParentsTokenNumber starting with their TokenNumber.

Limit the maximum number of token delegation by maximum delegation count, "DelegateMaxCnt(MC)", and maximum level number, "Dept(Dp)." Here, Dept is set as the initial token Owner and cannot be reset later. Dept is reduced by one each time the token is delegated. If Delegatable or DelegateMaxCnt or Dept is zero, then delegation is not possible.

In this paper, we let the token owners control the flow of their tokens by using Delegatable, DelegateMaxCnt, and Dept information that is pre-defined in the tokens.

3.4 Privacy Protection of the Token Delegate

For delegate privacy, the delegatee should not be able to see whether the delegator has re-delegated the token to him, though he should be able to see his direct delegator.

In this paper, we set up the following privacy policies for delegatee privacy.

1. Delegatee can only see his own ParentTokenNumber.
2. Delegatee cannot see whether his delegator delegated or re-delegated the token to others.
3. Delegatee cannot see whether he is a member of the parallel delegation of tokens from his delegator.

Figure7 shows the flow of the tokens where the policies are applied

The token has been delegated and re-delegated starting from the initial owner "A". aaaA can find through the ParentsTokenNumber that aaA delegated the token xxxxxx to him. IssuerTokenNumber values are encrypted, however, and he cannot see that the initial Owner of the token is "A". Moreover, aaaA cannot see who comes before aaA. That is, he cannot find if this token was given as a result of delegation or re-delegation. Likewise, aC can see that "A" delegated the token to him, but he cannot see any information about aA, aB, and aD who received the tokens together with him. In addition, he cannot see that "A" is the initial owner.

By applying these delegatee privacy policies, delegatees can access the system with a minimum amount of information.

3.5 Resource Privacy Protection

For the Resource Privacy, the device and data storage location should be hidden when the resource services are provided. In this paper, we applied the hash to the resource service data for this purpose.

In an IoT environment, communication with the device is generally provided by applying the REST concept. REST is a communication method for distributed hypermedia systems and provides services in HTTP format. It is configured as a hierarchical structure, like "/groups/groupid/groupid/member/sensor".

Service provision based on REST has a risk in that the service URI information can be directly exposed in text.

Accordingly, the data storage position is revealed when the services are provided, which can cause a privacy infringement to the device owner.

Therefore, in this paper, we applied encryption so that the URI information cannot be inferred, even if non-authorized subjects acquire information about the resource

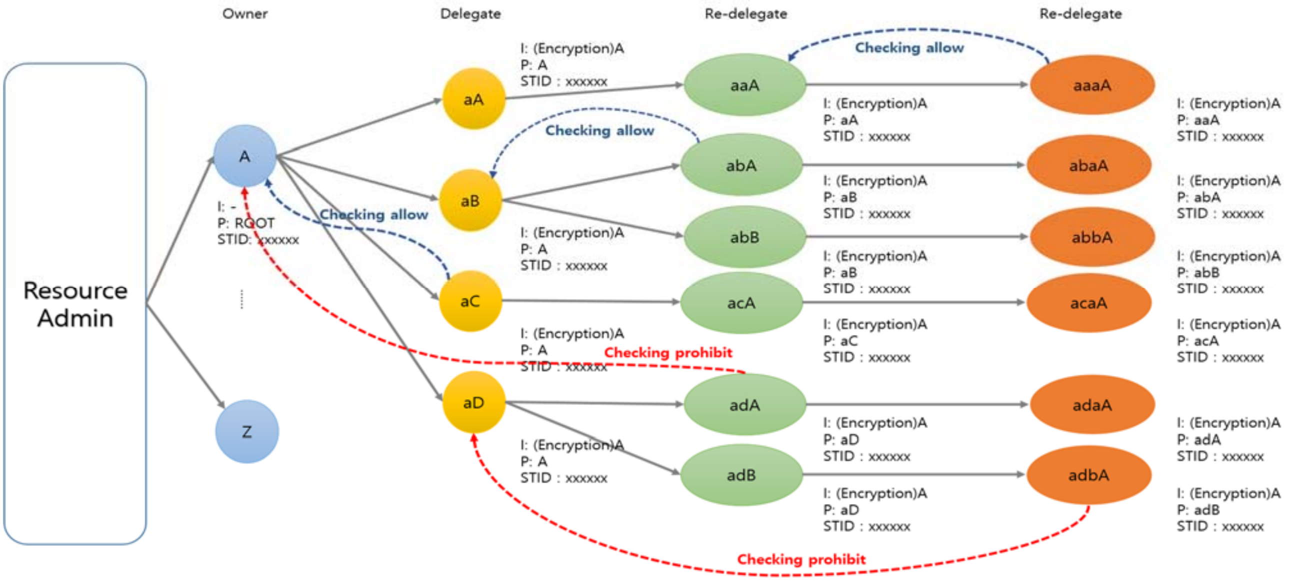
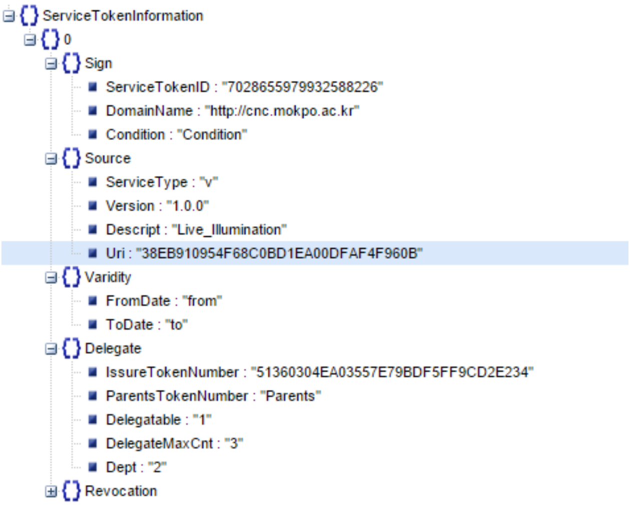


Figure 7 Privacy protection of the Token Delegatee flow diagram

services. By creating a hash-mapping table in the service, you can access the services with the hash value.

Figure8 shows an example of a hash of the resource service URI. By using the hash of the URI of resource services, you can hide the storage location of the data provided by the device to minimize the exposure of privacy resources.



```
ServiceTokenInformation
  0
    Sign
      ServiceTokenID : "7028655979932588226"
      DomainName : "http://cnc.mokpo.ac.kr"
      Condition : "Condition"
    Source
      ServiceType : "v"
      Version : "1.0.0"
      Descript : "Live_Illumination"
      Uri : "38EB910954F68C0BD1EA00DFAF4F960B"
    Varidity
      FromDate : "from"
      ToDate : "to"
    Delegate
      IssureTokenNumber : "51360304EA03557E79BDF5FF9CD2E234"
      ParentsTokenNumber : "Parents"
      Delegatable : "1"
      DelegateMaxCnt : "3"
      Dept : "2"
    Revocation
```

Fig. 8. Service Token Information Structure

IV. CONCLUSION

In this paper, we established the privacy protection policies through the capability tokens that are used to access the resource services in the IoT service system. The target of privacy protection in this system is defined like this: the subjects are the token users who access the object, and the objects are the resources that are to be accessed.

The owners must be able to hide their own information, check the flow of information that they have, and limit the information diffusion. The delegatee can see the information of the delegator, but they cannot see the source of the information. Resources can provide services, but they can hide the device location and data storage location.

By doing so, we can minimize any unwanted information exposure and the privacy infringement that can occur from the tokens in capability token-based access control systems. This also enables user to set their own privacy policies.

However, since the amount of the tokens can increase with the increase in the service users and resource services, there is a need for a study that explores ways to manage this information efficiently.

Acknowledgement

This work was supported by the National Research Foundation(NRF) grant funded by the Korea government(MSIP) (No. NRF-2014RIA2A1A11053774).

REFERENCES

[1] National Information Society Agency, “Dysfunctions and establish a comprehensive information dissemination measures to enable radio frequency identification”, 2004.

[2] National Information Society Agency, “Study on the legal aspects Things communications intelligence,” 2010.

[3] S. Gusmeroli, S. Piccione and D. Rotondi, "IoT access control issues: a capability based approach," *IMIS-2012*, pp.787–792, 2012.

[4] Jin-bo Kim, Deresa Jang, Mi-sun Kim and Jae-Hyun Seo, “The Access Control Platform of the IoT Service Using the CapSG,” *Journal of Information Processing Systems*, vol.4, no.9, pp.337-346, 2015.

[5] Bum-Ki Lee, Mi-Sun Kim and Jae-Hyun Seo, "Design and Implementation of The Capability Token based Access Control System in the Internet of Things," *Journal of The Korea Institute of Information Security & Cryptology*, vol.25, no.2, pp.439-448, 2015.

[6] Romuald Thion, *Access Control Models*, Cyber Warfare and Cyber Terrorism, Hershey, pp.318-326, 2008.

[7] Sergio Gusmeroli, Salvatore Piccione and Domenico Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Mathematical and Computer Modelling*, pp.1189-1205, 2013.

[8] Jos´e L. Hern´andez-Ramos, Antonio J. Jara, Leandro Mar´ın and Antonio F. Skarmeta1 "Distributed Capability-based Access Control for the Internet of Things," *Journal of Internet Services and Information Security*, Volume 3, Number 3/4, pp.1-16, 2013.

[9] Mark S. Miller, Ka-Ping Yee and J. Shapiro, "Capability Myths Demolished," Systems Research Laboratory, Johns Hopkins University, Tech.Report SRL 2003-02, 2003.

[10] Deresa Jang, Jin-bo Kim, Mi-Sun Kim and Jae-Hyun Seo, “Privacy-preserving Access Control in the IoT Service Platform,” *MITA2016*, pp.52~54, 2016.

Authors

Deresa Jang

2015 Bachelor of engineering, Department of information security, Mokpo national university.
2015 ~ Now The master's course in engineering, Interdisciplinary Program of information and Protection, Mokpo national University.

Jin-Bo Kim

2003 Bachelor of engineering, Department of multimedia engineering, Mokpo national university.
2007 Master of engineering, Interdisciplinary Program of information and Protection, Mokpo national University.
2016 Doctor of engineering, Interdisciplinary Program of information and Protection, Mokpo national University.

Mi-Sun Kim

1996 Bachelor of engineering, Department of computer engineering, Mokpo national university.
2000 Master of engineering, Department of computer engineering, Mokpo national University.
2007 Doctor of engineering, Interdisciplinary Program of information and Protection, Mokpo national University.
2012 ~ Now Visiting Professor, Department of information security, Mokpo national university.

Jae-Hyun Seo

1985 Bachelor of engineering, Department of computer engineering, Chonnam national university
1988 Master of engineering, Department of computer engineering, Chonnam national University
1996 Doctor of engineering, Interdisciplinary Program of information and Protection, Chonnam national University.
1996 ~ Now Professor, Department of information security, Mokpo national university.