사물인터넷 엔터티를 위한 역할기반 접근제어에 관한 연구

이용주[1] · 우성희[2]

[1]충북대학교 · [2]한국교통대학교

Research for RBAC of IoT Entities

Yon-Joo Lee[1] · Sung-Hee Woo[2]

[1]ChungBuk National University · [2]Korea National University of Transportation

E-mail : silvianna@naver.com / shwoo@ut.ac.kr

요 약

사물인터넷 기술은 4차 산업 혁명의 원동력이 될 차세대 주축기술로 평가되고 있다. 사물인터넷 응용을 위한 엔터티 들의 특징은 기존 보다 활동적이고 능동적으로 변해가고 있어서, 보다 세분화된 접근제어가 필요하지만 기존의 접근제어 기술은 사용자를 중심으로 설계되어 절차가 복잡하고 가변적인 내용을 적용하기에 시스템 부하가 심해, 시스템의 부하가 적으면서 효율성과 보안성을 유지할 수 있는 접근제어 기법이 필요하다. 따라서 사물인터넷 엔터티에 적합한 역할기반 접근제어에 대한 연구가 반드시 필요하다. 본 연구에서는 사물인터넷 엔터티 들의 접근제어 연구를 위한 관련 연구와 사물인터넷 내의 다양한 엔터티들의 속성을 정의할 수 있는 RBAC와 AC 방식에 대하여 분석하였다.

ABSTRACT

The Internet of Things technology is regarded as the next major technology that will be the driving force behind the fourth industrial revolution. The characteristics of entities for Internet of Things application are changing more actively and actively, requiring a more detailed approach, but existing access control technologies are designed around users, requiring access control techniques that maintain efficiency and security with less system load to apply complex and variable content. Therefore, research on role-based access controls that are appropriate for Internet of Things entities is essential. In this study, the relevant research for the study of access control of the Internet of Things entities and the RBAC and AC methods that can define the properties of the various entities within the Internet of Things.

키워드

RBAC, AC, Attribute, IoT, Entity

Ⅰ. 서 론

사물간의 통신을 주고받는 개념인 IoT의 발전은 우리의 삶에 새로운 패러다임을 가져왔다. IoT를 통해서 기존의 사람과 사람사이에서만 필요하던 통신이라는 개념이, 음성에서 사람뿐만 아니라, 사물이라는 개념으로 확장된다. 4차 산업혁명의 목적은 적응성과 자원의 효율성이 높고, 가치사슬에서 고객과 공급자의 통합 특징을 가지는 지능적(intelligent)이고 스마트(smart)한 환경으로 정의하고 있다. 그리고 4차 산업혁명의 개념을 사물인터넷 엔터티 환경에 도입한다면 모든 자동화 장치, IT 시스템 및 전체 네트워크가 고도로 네트워크화 된 시스템의 특징을 가질 것이다. 이러한 첨단 네트워크화 된 시스템 내에서는 활동적이고 능동적인 다양한 엔터티 들이 존재하게 되며 환경에 따라 수시로 변경될 수 있다[1][2].

Ⅱ. RBAC for IoT

1) RBAC(Role-based Access Control)

RBAC는 Role(역할)에 따라 사용자의 교체나 일의 재 할당을 할 수 있어 전통적인 접근제어보다 관리가 쉽고 보다 효율적인 특징이 있다. RBAC에

서 사용자는 OB(Object)에 접근이 허용된 권한을 가진 Role에 할당되었을 경우, 해당 OB에 접근할 수 있다. RBAC에서 Role의 개념은 조직의 기능적 역할과 유사하며 동시에, 어느 특정한 보안정책을 포함하는 대신 그 정책을 표현하는 방법이기도 하다. Fig 1.에서와 같이 Role은 사용자와 OB의 중간자 위치에 있으며, 사용자가 아닌 Role에 따른 접근권한을 부여받게 된다. 예를 들어 OB가 파일이라면 Role에 따라 tran_a(읽기) 등이 부여된다[3][4].

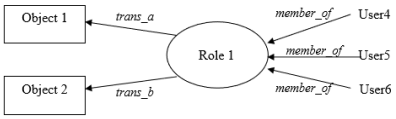

Fig 1. Role Relationships

2) Push and Pull for AC Distribution

ABAC(Attribute-based Access Control)는 사용자의 PKC(Public Key Certificate)에 포함하기 어려운 상세한 속성들을 하나 이상의 AC(Attribute Certificate)로 정의하여 접근제어에 사용한다. 이러한 AC를 분배하고 공유하기 위해 다양한 메커니즘이 제안되었는데 그 중 가장 일반적으로 사용되는 Push/Pull 방법에 대해 살펴보고 문제점을 분석하고자 한다. Push 메커니즘은 클라이언트가 AC를 보관하고 있다가 서버에게 Push(제출) 하는 방법으로, 클라이언트와 서버 간에 새로운 채널이 필요치 않다면 유용한 모델로 서버는 검색에 대한 번거로움을 없애 효율성이 뛰어나다[5]. Pull은 ACR(AC Repository)에 AC를 보관하고 클라이언트 요청이 있을 시 클라이언트의 AC를 확인하고 권한여부를 Pull(통보)하는 방법이다. AC를 분배하고 교환하는 방법은 다양하게 사용될 수 있는데 중요한 것은 AC의 주인인 클라이언트, 인증주체인 서버, AC의 발급자인 ACI와의 프로시저를 효율적이고 안정적으로 정의하는 것이다. Push/Pull 방법은 서버에 의존적인 중앙 집중형의 구조에서 주로 사용되었으나, 클라이언트마다 수개의 AC를 다뤄야 하는 서버 측의 부하가 심하고 매번 같은 동작을 반복해야하며, ACR에 대한 추가적인 보안조치 또한 중요하여 조직의 특성과 역할의 중요성에 따라 가변적으로 적용해야할 필요성이 있다[6].

3) RBAC-SC(Smart Contract)

J.CRUZ[7]는 전자결제 시스템에서 적용 가능한 역할기반인증 방법에 대해 제안하였다. 유저, 역할, 서비스의 관계를 정의하고 모든 유저에게 맞는 역할을 할당하고 특정 서비스를 사용하기 위해 역할을 검증하여 인증과 허가를 받으며 모든 액션은 블록체인을 통해 등록하도록 하였다. 이 연구에서 중요한 의미인 역할은 각 기관에서 부여하게 정의하였으며, 학생의 역할이라면 역할부여 기관은 학교이고 학생 할인을 받아 책을 사고자 한다면 서점의 직원은 학교에서 제공된 역할인지를 검증하게 된다. 이 연구에서 제시한 역할기반 접근제어는 역할의 속성이 자주 바뀌는 환경에서 매번 각 사용자 각각 자신의 역할을 재신청하여 등록하여야 하므로 응용에 한계가 있고 또한 역할로 인증을 받을 시 마다 매번 인증기관에게 질의하여야 하는 번거로움과 비효율성을 가지고 있다. 이러한 효율성을 극복하면서 엔터티 들에 적합한 접근제어 방식이 제안되어야 한다.

III. 결 론

이 논문에서는 사물인터넷 엔터티 들의 접근제어 연구를 위한 관련 연구 등을 진행하였다. 사물인터넷 내의 다양한 엔터티들의 속성을 정의할 수 있는 RBAC와 AC 방식에 대하여 살펴보았다. 향후, 보다 다양하고 효율적이면서 보안성이 강조된 접근제어 기법 등이 연구되어야 할 것이다.

References

[1] YongJoo cho, (2017). National Smart Factory Strategy for The 4th Industrial Revolution. Joutnal of Korea Information Science society. No41. Jun.

[2] Sunghyuck Hong, (2017) "Analysis of the Vulnerability of the IoT by the Scenario, Vol.8. No.9, pp.1-7.

[3] D. F. Ferraiolo, (2001). Proposed NIST Standard for Role-Based Access Control, A C M T r a non InfoSystemSecurity, Vol.4, No.3, pp. 224-274.

[4] Yoon-Su Jeong, (2018), "User Privacy Security Scheme using Double Replication Key in the Cloud Environment", Journal of the Korea Convergence Society Vol. 9. No. 4, pp. 9-14.

[5] R. Sandhu, (1996) C. Youman, "Role-Based Access Control Models", IEEE Computer, Vol. 29, No. 2.

[6] NamHo Kim, (2018), Secure MQTT protocol based on Attribute-based Encryption Scheme, Journal of KIISE, Vol.45. No.3. pp195-199

[7] J, Cruz. (2018) “Role-based Access Control using Smart Contract”, IEEE Access, pp 12240-12251, VOL 6.