이기종 사물인터넷 플랫폼 간의 상호운용 가능한 속성기반 접근제어 프레임워크

강길욱[1,2], 구자훈[1], 김영갑[1,2,†]
[1]세종대학교 정보보호학과
[2]세종대학교 지능형드론융합전공
giluk1027@sju.ac.kr, sigmao91@sju.ac.kr, alwaysgabi@sejong.ac.kr

Interoperable Attribute-based Access Control Framework for Heterogeneous IoT Platforms

Giluk Kang[1], Jahoon Koo[2], Young-Gab Kim[1,†]
[1]Dept. of Computer and Information Security, and Convergence Engineering for Intelligent Drone, Sejong University
[2]Dept. of Computer and Information Security, Sejong University

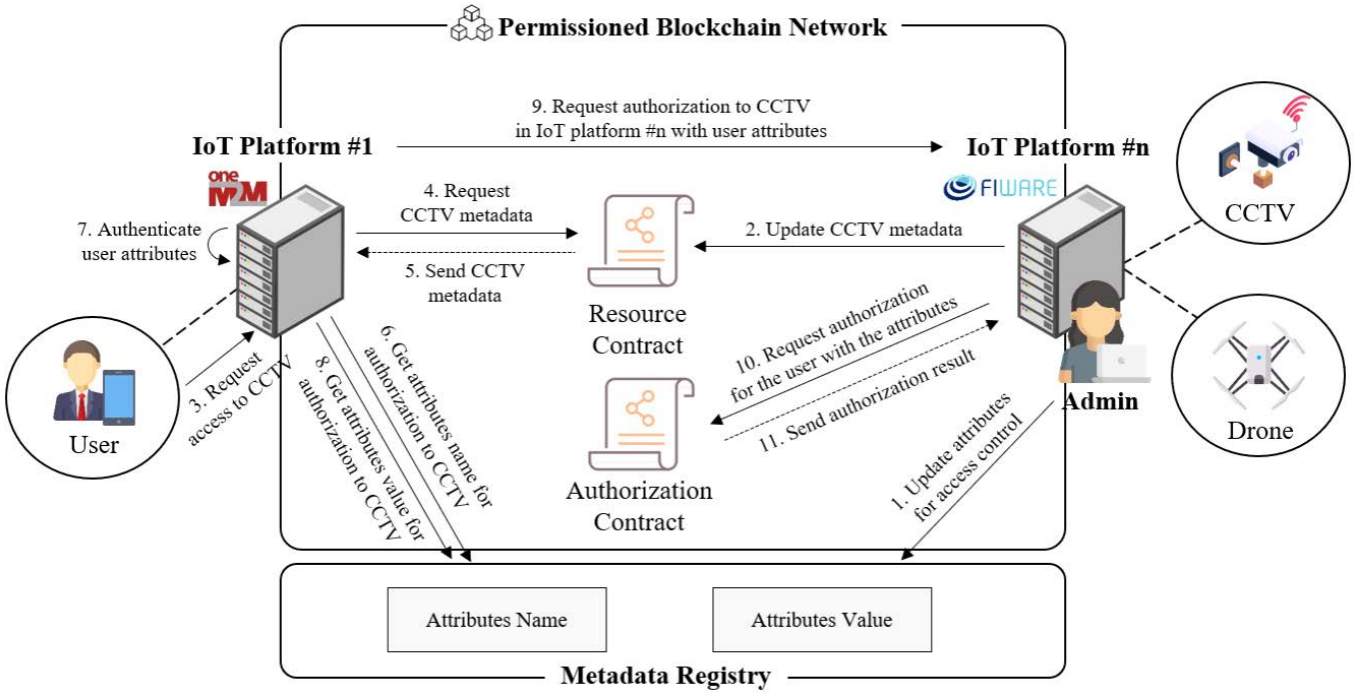
요 약

현재 사물인터넷 플랫폼이 활발히 개발됨에 따라, 이를 기반으로 사용자에게 많은 서비스가 제공되고 있다. 그러나 플랫폼들이 독자적으로 개발되고 있어 상호운용이 보장되지 못하고 있는 상황이다. 특히, 플랫폼마다 리소스를 표현하는 방식이 서로 불일치하여 리소스가 공유되더라도 이기종 플랫폼의 사용자는 리소스를 사용할 수 없는 문제가 있다. 더욱이 각각의 플랫폼들이 다양한 접근제어 모델을 사용함에 따라, 이기종 플랫폼의 사용자가 리소스 접근을 요청하더라도 인증/인가를 수행할 수 없는 상황이다. 결과적으로, 이러한 상호운용성 문제는 사물인터넷의 주요 목적인 초연결성을 달성하는 데 한계를 가져오고 있다. 이에, 본 논문에서는 이기종 사물인터넷 플랫폼 간의 상호운용이 가능한 속성기반 접근제어 프레임워크를 제안하고자 한다. 본 프레임워크는 MDR(Metadata Registry)를 기반으로 속성기반 접근제어를 위한 속성 불일치 문제를 해결하고 허가형 블록체인을 이용하여 속성기반 접근제어를 사용하지 않는 플랫폼이라도 접근제어에 대한 상호운용을 달성할 수 있도록 한다.

1. 서론

사물인터넷(Internet of Things; IoT)은 사물들이 인터넷을 기반으로 네트워크, 기기, 애플리케이션 등의 제약 없이 초연결되어 사용자에게 다양한 서비스를 제공하는 것으로 스마트 시티, 스마트 팩토리, 스마트 헬스케어 등 여러 분야에 적용되어 개발되고 있다. 특히, 최근에는 이러한 사물인터넷 기기(예: 센서, 액추에이터) 간의 연결을 지원하고 사용자에게 서비스를 제공할 수 있는 사물인터넷 플랫폼을 개발하는 기업이 증가하고 있다. 사물인터넷 플랫폼은 다양한 사물인터넷 기기들의 관리를 포함하여 액세스 포인트, 보안 등을 제공하는 소프트웨어로써 Oliot, Waston IoT, Azure 등이 대표적으로 개발되고 있다 [1]. 그러나 다양한 기업들이 사물인터넷 플랫폼을 독자적으로 개발함에 따라, 이들 간에 상호운용이 이뤄지지 않아 사물인터넷의 주요 목적인 초연결성을 제공하지 못하는 상황이다. 특히, 플랫폼마다 동일한 리소스일지라도 이를 표현하는 방법이 달라 리소스 교환이 이뤄지더라도 이해를 할 수 없는 상황이다. 더 나아가, 사물인터넷 플랫폼의 보안 기능을 위해 제공되는 접근제어 모델의 경우에 ACL(Access Control List), RBAC(Role-based Access Control) 등과 같이 다양한 모델이 사용되고 있다. 이는 동일한 접근제어 모델과 보안 정책의 형식을 다른 플랫폼이 사용하지 않으면 리소스에 접근할 수 없는 문제를 야기하고 있다. 예를 들어, 특정 플랫폼의 사용자가 다른 플랫폼의 서비스를 이용하고자 할 때, 접근제어 방식이 달라 다른 플랫폼이 해당 사용자를 인증할 수 없을 뿐만 아니라 동일한 접근제어 모델과 형식을 사용하더라도 리소스의 표현 방식이 달라 인가를 수행할 수 없다. 따라서, 본 연구에서는 이기종 사물인터넷 플랫폼 간의 상호운용 가능한 속성기반 접근제어 프레임워크를 제안한다. 본 프레임워크는 접근제어를 위해 독자적인 인증/인가 시스템을 활용하는 것이 아닌 플랫폼에서 자체적으로 지원하는 시스템을 활용할 수 있도록 한다. 또한, 속성기반 접근제어를 지원하지 않는 플랫

† 교신저자



(그림 1) 이기종 플랫폼 간의 상호운용 가능한 속성기반 접근제어 프레임워크

폼에 대해서는 허가형 블록체인(Permissioned Blockchain) 내에 스마트 계약(Smart Contract)을 사용하여 리소스를 소유한 플랫폼에서 인가가 수행될 수 있도록 지원한다. 본 논문의 구성은 다음과 같이 구성된다. 2장에서는 사물인터넷 플랫폼과 관련된 연구를 분석한다. 3장에서는 이기종 플랫폼 간의 상호운용 가능한 속성기반 접근제어 프레임워크를 제안한다. 마지막으로, 4장에서는 결론과 향후 연구에 관해 서술한다.

2. 관련 연구

Koo and Kim [1]은 이기종 사물인터넷 플랫폼 내 장치 및 서비스 식별자에 대한 의미론적/구문론적 상호운용성을 달성할 수 있는 프레임워크를 제안했다. 특히, 표준화 기구 기반 사물인터넷 플랫폼(예: oneM2M, FIWARE)들에 대해 리소스 식별자를 구성하는 메타데이터를 맵핑하여 서비스 URL과 같은 경로를 해당 플랫폼에 맞게 변환한다. 그러나, 그들은 프레임워크 내에서 접근제어를 고려하진 않았다. Deshmukh et al. [2]은 이기종 사물인터넷 플랫폼 간 상호운용성을 보장하기 위해 통합 플랫폼인 Data Spine을 제안했다. 해당 플랫폼은 데이터 변환, 메시지 브로커 등의 기능을 제공하여 데이터 형식, 접근제어 등에 대해 상호운용성 제공할 수 있다. 그러나, 접근제어가 통합 플랫폼에서만 이뤄져 중앙집중화의 문제점이 있다. Oh and Kim [3]은 OAuth(Open Authorization)을 활용하여 이기종 사물인터넷 플랫폼 간의 상호운용 가능한 인가 프레임워크를 제안했다. 특히, 상호운용할 수 있는 OAuth 토큰을 개발하여 이기종 플랫폼이더라도 리소스에 대한 인가가 가능하게 했다. 그러나, 그들은 접근제어를 위한 인증은 고려하지 않은 한계가 있다. Rosa et al. [4]은 의료 및 사회 시스템 분야에서 민감한 데이터를 관리하는 플랫폼 간의 상호운용을 위한 Parser를 제안했다. 특히, Parser는 XACML과 자연어 간의 변환을 통한 보안 정책의 구문 분석에 중점을 두고 있다. 그러나, 이는 XACML에 의존적으로 다른 형식의 접근제어 정책은 변환할 수 없는 한계가 있다.

3. 제안 프레임워크

그림 1은 제안하는 프레임워크로, MDR과 허가형 블록체인을 기반으로 이기종 사물인터넷 간에 접근제어 모델이 불일치하더라도 다른 플랫폼의 사용자가 리소스 접근을 시도하면 속성기반 접근제어가 수행될 수 있도록 한다. 이를 위해, 본 프레임워크는 크게 블록체인 네트워크, MDR로 구성된다. 블록체인 네트워크 내에서는 사물인터넷 플랫폼들이 피어(Peer)로 참여하고 있으며, 두 개의 스마트 계약인 Resource Contract와 Authorization Contract가 구성

돼 있다. Resource Contract는 리소스에 대한 메타데이터들을 관리하는 스마트 계약으로써 리소스 이름, IP, 리소스 경로 등이 포함되어 있다. 또한, 속성기반 접근제어를 위한 속성 리스트도 가지고 있어 타 플랫폼의 사용자가 리소스에 접근할 때 어떤 필요 속성들이 있는지를 확인할 수 있도록 한다. Authorization Contract는 리소스의 인가를 위한 스마트 계약으로써 속성기반 접근제어 모델을 사용하지 않는 사물인터넷 플랫폼들이 본 스마트 계약을 통해 인가를 수행할 수 있도록 한다. 더불어 MDR은 이기종 사물인터넷 플랫폼 간 인증에 필요한 리소스 표현 불일치 문제를 해결하기 위해 구성된 것으로써 사용자의 속성과 값을 리소스를 가진 플랫폼의 형식으로 변환할 수 있도록 돕는다. 이들을 통해 접근제어가 수행되는 간략한 과정은 다음과 같다. 첫째, 리소스를 가진 플랫폼 B의 관리자는 MDR에 접근제어에 필요한 속성과 값에 대한 맵핑을 수행하고, Resource Contract에 리소스에 대한 메타데이터를 등록한다. 둘째, 플랫폼 A의 사용자가 소속된 플랫폼을 통해 플랫폼 B의 리소스 접근을 요청하면 플랫폼 A는 Resource Contract를 통해 요청된 리소스 메타데이터를 가져온 후, 메타데이터 내에 있는 속성 리스트를 MDR을 통해 자신이 이해할 수 있는 표현 형식으로 변경한다. 셋째, 플랫폼 A는 사용자가 인가에 필요한 적합한 속성이 있는지를 판단하고, 있다면 사용자의 속성값을 인증하고 MDR을 통해 플랫폼 B의 형식으로 변환한다. 넷째, 플랫폼 A는 메타데이터에 있던 속성과 인증된 사용자의 속성값을 플랫폼 B에 전달하고 인가를 요청한다. 다섯째, 전달받은 플랫폼 B은 전달받은 속성값을 기반으로 인가를 결정한다. 이때, 플랫폼 B가 속성기반 접근제어 모델을 사용하지 않으면 Authorization Contract를 통해 인가를 수행하고 결과를 반환받아 인가를 결정하게 된다.

4. 결론 및 향후 연구

사물인터넷이 발전하게 되면서, 이를 기반에 둔 서비스들을 사용자가 손쉽게 제공받을 수 있도록 하는 사물인터넷 플랫폼이 급격히 증가하고 있다. 하지만, 이러한 플랫폼들은 독자적인 형태로 개발되고 있어 상호운용성이 보장되지 못하는 문제가 발생하고 있다. 특히, 특정 플랫폼의 리소스에 대해 다른 플랫폼의 사용자가 접근을 시도하더라도 접근제어 모델이 서로 상이하여 접근할 수 없다. 이를 해결하기 위해, 본 논문에서는 이기종 사물인터넷 플랫폼 간에 속성기반 접근제어가 달성되도록 하는 허가형 블록체인 및 MDR 기반 접근제어 프레임워크를 제안했다. 본 프레임워크는 사물인터넷 플랫폼이라면 손쉽게 수집할 수 있는 센싱 데이터를 사용자의 인증 요소로 사용하는 속성기반 접근제어를 통해 접근제어 모델이 불일치하더라도 플랫폼 내에서 속성을 검증하여 인증을 수행할 수 있도록 했다. 또한, MDR을 이용해 속성 이름과 값을 이기종 플랫폼에 적합하게 변환하여 리소스를 가진 플랫폼에서 인가를 수행할 수 있도록 했다. 향후 연구에서는 리소스 접근을 위한 이기종 사물인터넷 플랫폼 간의 상호운용 가능한 속성기반 접근제어를 넘어 리소스 공유가 가능하도록 하여 이기종 사물인터넷 플랫폼 간의 완전한 상호운용성을 보장하고자 한다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2012635)

참고문헌

[1] Koo, J., and Kim, Y. -G., “Resource identifier interoperability among heterogeneous IoT platforms,” Journal of King Saud University-Computer and Information Sciences, Vol. 34, Issue 7, pp. 4191-4208, 2022.

[2] Deshmukh, R. A., Jayakody, D., Schneider, A., and Damjanovic B. V., “Data spine: A federated interoperability enabler for heterogeneous iot platform ecosystems,” Sensors, Vol. 21, Issue 12, Art. No. 4010, 2021.

[3] Oh, S. -R., and Kim, Y. -G., “AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth,” International Journal of Distributed Sensor Networks, Vol. 16, Issue 2, pp. 1-15, 2020.

[4] M. Rosa, J. P. Barraca, and N. P. Rocha., “ Access control for social care platforms using fast healthcare interoperability resources,” In Proceedings of World Conference on Information Systems and Technologies, Springer, pp. 94 - 104, 2019.