Gichan Lee

Youngeun Ahn

Access Control Solution for IoT-based Smart Environments

2017년 6월 21일

**Technical Documentation For IoT Project**

본 고는 seLab에서 진행하는 ‘IoT기반 스마트 환경을 위한 접근제어 솔루션’ 프로젝트를 효과적으로 진행하기 위한 문서이다. 현재의 프로젝트 진행상황을 주기적으로 기록하는 것을 주 목적으로 하며 향후 연구실에서 새로이 프로젝트에 진입하는 학생들이 빠르게 프로젝트를 이해할 수 있도록 인사이트를 제공한다. 이 문서는 참여자들에 의해 언제든지 수정, 재배포될 수 있으며 연구노트로써의 목적 또한 수행될 수 있다.

**A. 연구의 개요**

본 연구는 인터넷에 접속되는 사물이 급속도로 증가하는 사물인터넷 환경에서의 접근 제어 솔루션을 제공함에 목적이 있다. 인터넷 기반의 분산 컴퓨팅 시스템에서 이미 접근 제어 기술은 DAC, MAC, RBAC, ABAC와 같은 철학을 중심으로 발전되어 왔음에도 불구하고 사물인터넷 환경에 적합한 접근 제어 기술은 아직까지 큰 성과를 확보하지 못하고 있다. 가트너의 조사에 따르면 2020년 IoT 기기는 250억개에 육박할 것이라 전해지며 이러한 수많은 기기들이 모두 클라우드 상에 존재하는 사물 인터넷 시대에 이 기기들을 효과적으로 제어하기 위한 접근 제어 기술은 반드시 필요한 요구사항이다. 하지만 현재의 일반적인 시스템에서는 소수의 관리자가 시스템 상에서 제어해야하는 주체들과 관련된 모든 접근 제어 요구사항을 전반적으로 관리하고 있는 것이 대부분이다. 접근 제어 변동 사항을 실시간으로 추적, 감시하고 그에 맞춰 유동적으로 권한을 부여, 제거하는 방식의 접근 제어는 기존과 비교해 그 주체의 수가 매우 많고 그 관계가 매우 뒤섞여있을 것이라 예상되는 사물인터넷 환경에서 그대로 적용되기에는 분명한 한계가 존재한다. 두 가지 예를 든다면 첫째로, 앞서 언급했듯 접근 제어를 해야하는 자원의 수, 자원에 접근하는 주체의 수가 매우 많은 사물 인터넷 환경은 주체 및 자원들의 복잡한 관계를 필연적으로 요구하며 이는 기존 방식의 접근 제어가 제 역할을 하지 못하게 한다. 기존 방식에서 대표적이라 할 수 있는 RBAC와 ABAC의 룰은 주체의 많은 수로 인해 역할 폭발 등이 일어나 적용될 수 없는 공통적인 문제가 발생하며 이로 인해 RBAC, ABAC, 하이브리드 ABAC를 기반으로 하는 모든 접근 제어 방법이 같은 이유로 적용하기 어려운 한계에 봉착한다.  
둘째로는 접근 제어를 위해 작성되는 정책에 대한 정확성 검증 및 신뢰성 보장에 관한 연구가 아직 미흡하여 정책이 보안 요구사항을 충족하지 못하거나 정책 작성자가 의도한 방식과 다르게 동작하는 경우에 대한 대처가 충분하지 않다. 정책이 다른 정책과 의미상으로 충돌하여 정책 작성자의 작성 의도에서 동떨어진 행동을 시스템이 수행하게 될 경우 보안적으로 매우 위험한 의도치 않은 행동의 결과가 나타날 수 있다. 접근 제어의 범위가 매우 넓고 사물 인터넷 자원을 다루기 위한 정책이 기하급수적으로 증가하리라 예상되는 미래에 사물 인터넷 자원에 대한 정책 작성을 손쉽게 하고 정책 사이의 충돌을 사전에 탐지하여 예방할 수 있다면 향후 사물 인터넷 환경 구축 시 필수요소인 ‘보안’ 기술 중 정확성 및 신뢰성이 보장된 접근제어 솔루션을 확보할 수 있다.  
이를 위해 본 연구는 3년에 걸친 연차별 연구 목표를 달성함으로써 결과 솔루션을 획득하고자 한다.  
1차 년도 : IoT 기반 스마트환경에 적합한 XACML 접근제어 기술 개발과 실험 환경 구축  
2차 년도 : XACML 정책의 정확성 및 신뢰성의 검증과 실험을 통한 최적화  
3차 년도 : XACML 정책 관리자를 위한 토털 솔루션 개발, 테스트 및 분석

**B. 연구의 배경지식**  
B에서는 프로젝트의 이해를 위해 필요한 사전지식을 설명한다. 신진연구\이기찬\AccessControlOnIoT\IoT backgrounds 디렉토리를 확인하면 다음과 같은 목차로 분류되어 있으며 제목을 통해 주제를 구분지었다.

Index

1. IoT Insight

2. 한국 IoT 동향 분석(ETRI, TTA) 등

3. Policy Conflict Papers

4. XACML Technology

5. IoT Platform Standard

**B-1. IoT Insight**

B-1-1. Research Directions For The Internet Of Things

2014 Invited Paper로 IoT가 현재까지 어떤 방식으로 연구개발 되어왔고 무엇이 모자란지 어떤 방향의 연구가 진행되어야하는지에 대한 구체적인 방향을 제시한다. 이 논문을 통해 IoT 영역에서 어떠한 연구들이 중점적으로 작용하는지에 대해 전체적인 뷰를 확보할 수 있으며 배경지식을 위하여 확인하도록 한다.

B-1-2. Authentication and Access Control in the Internet of Things

현대의 IoT 환경에서 Authentication과 Access Control의 중요성, 시도되고 있는 여러 방식에 대해 언급한 논문으로 이 논문을 통해 IoT 영역에서 Security 및 Privacy를 확보하기 위한 어떤 노력이 진행되고 있는지 확인하도록 한다. 2012년 논문이기는 하나 IoT의 Authentication 부문 기본적인 개념을 확인할 수 있으므로 확인하도록 한다.

B-1-3 Internet of Things for Smart Cities

이 논문은 Padova City의 공공정보부문 온도, 습도, 광량, 벤젠 지수 등의 데이터를 모아 도시의 환경을 개선하는데 활용한 공공정보 이용시스템을 적용한 IoT platform의 구체적인 케이스를 제공한다. IoT 기술이 아주 구체적이고 넓은 스펙트럼으로 도시에 적용된 사례로써 IoT 기술의 구현이 어떤 식으로 진행되는지 확인하도록 한다.

B-1-4 Middleware for Internet of Things – A Survey

IoT 시대를 열기 위해서 반드시 필요한 여러 미들웨어 기술의 요구사항을 구체적으로 조사한 논문으로써 아웃라인을 잡고 향후 연구 방향에 참고하는데 참조하도록 한다.

B-1-5 privacy\_iot

Privacy 문제를 해결하기 위해서 IoT 영역에서 반드시 보장해야할 요구사항들을 언급한 매거진 칼럼으로, IoT Privacy 영역에서 기술적으로 좀 더 발전이 이루어져야하는 여러 가지 이슈에 대한 인사이트를 제공한다. IoT Security가 중요한 이유에 대한 백업을 제시하므로 확인하도록 한다.

**B-2. 한국 IoT 동향 분석(ETRI, TTA) 등**

B-2에서 처음 oneM2M과 OCF에 대한 개요를 확인함과 동시에 IoT 환경을 제어하고자 하는 IoT 플랫폼 동향에 대한 참고 자료를 확인하도록 한다. oneM2M과 OCF는 현재 IoT 플랫폼 표준을 주도하는 두 국제기관으로써 현재 한국의 여러 기업 및 연구기관에서 주도적으로 표준화를 진행하기 때문에, 얻을 수 있는 정보도 많거니와 향후 프로젝트에서 개발할 솔루션을 표준에 맞추어 개발할 수 있도록 반드시 동향을 추적할 수 있어야한다. 계속해서 릴리즈될 표준에 맞춰 솔루션을 개발하고 현재 아직까지 연구 개발이 미흡한 접근 제어 영역을 우리 솔루션을 통해 구체화, 표준화 후 제시할 수 있도록 하는 것을 목표로 한다. 디렉토리 및 파일 제목 그대로 주제를 포함하고 있으며 참고자료로써 확인할 수 있도록 한다.

**B-3 Policy Conflict Papers**

정책 충돌 문제는 비단 IoT 환경만의 문제가 아니었고 다양한 분야 및 시스템에서 이를 해결하기 위한 많은 노력이 있어왔다. 이와 관련된 여러 논문을 통해 제시된 여러 해결 방법을 확인하여 불필요한 노력을 미연에 방지하고 의미있는 연구 방법을 좀 더 심층적으로 파고듦으로써 향후 솔루션을 개발하는데 참고할 수 있도록 한다. 정책 충돌은 어떤 시스템에서 발생하던지 간에 일정한 문제의 공통분모가 존재함을 확인하고 IoT 환경에서 이 문제가 어떻게 심화될 것이며 어떻게 해결할 것인지에 대해 유념하면서 논문들을 확인할 수 있도록 한다. 각 논문은 편의상 13-28에 이르는 인덱스가 지정되어있는데 변경하여도 상관없다.

**Paper Index**

13. Research on QOS Policy Conflict Detection and Resolution Technology

14. Dynamic Policy Conflict Analysis for Collaborative Web Services

15. Study on the Policy Conflict Detection in the Security Management Model

16. A Study on Policy Conflicts Analysis of Multi-Domain Access Control in Clouds

17. A device-centric policy conflict in IoT

18. A Prototype for Solving Conflicts in XACML-based e-Health Policies∗

19. A Static ABAC Policy Conflict Resolution Algorithm

20. Policy Conflict Management using XACML

21. A conflict detection approach for XACML policies on hierarchical resources

22. A Privacy Policy Conflict Detection Method based on Sub-graph Isomorphism

23. Analysis of Adaptive Policy-based Approach to Avoid Policy Conflicts

24. Knowledge-based Policy Conflict Analysis in Mobile Social Networks

25. Privacy preserving access control policy and algorithms for conflicting problems

26. Detecting Conflicts in ABAC Policies with Rule-reduction and Binary-search Techniques

27. Conflicts Analysis and Resolution for Access Control Policies

28. A CAUTIONARY NOTE ABOUT POLICY CONFLICT RESOLUTION

[13]에서는 네트워크 관리 시스템에서의 QoS 관리 정책 충돌을 탐지, 해결하고자 하였으며 웹 서비스간의 Collaborative한 환경에서의 서비스 간의 정책 충돌을 탐지하거나[14] security management model에서의 정책 충돌을 해결하기 위해 충돌 유형을 분류별로 라이브러리에 저장하고 이를 이용하는 시도를 하였다[15]. [16]에서는 클라우드 기반 멀티 도메인 RBAC 시스템에서의 충돌 분석을 제시하였고 [17]의 경우 WoT 시스템 상에서 디바이스의 지속가능하고 안전한 활용을 위한 정책 충돌 분석을 서술하였다. [18]의 경우 XACML 기반의 E-Health 정책 충돌을 해결하기 위해서 Combining Algorithm을 확장하는 시도를 하였고 [19]에서는 정책의 condition attribute의 중요도를 판별하는 조건부 확률 공식과 Bayesian formula를 활용하여 Static하게 정책 충돌을 해결하고자 하였다. 한편 OCF의 Technical specification에서 사용했던 ACL을 XACML로 변환하여 Combining Algorithm으로 문제를 일부 해결하고자 했던 [20]도 존재하였으며 수학적으로 정책의 구성요소를 쪼개 그래프로 만들어 해결하고자 했던 [21], [22]와 같은 시도들도 다수 존재하였다. 기존의 프레임워크(PobMC)에서 발생하는 충돌을 패턴별로 분석하여 해결하거나[23] 모바일 네트워크 환경을 반영하여 정책의 모델을 Knowledge-based로 새로 정의하고 그에 맞추어 충돌을 탐지하는 로직을 세운 프레임워크의 개발[24]도 시도되었다. 의도치 않은 접근 제어 결정으로 인한 프라이버시 노출을 방지하기 위해서 모델 정의 및 충돌 패턴 분석을 실시한 [25], ABAC 모델에서의 정책 모델에서 rule reduction, binary search 등의 방법을 동원해 충돌 탐지를 시도한 [26], 그리고 정책 충돌을 Modality, Redundancy, Potential 세 분류로 특정하고 각각 그에 맞춘 알고리즘을 제시한 [27]과 같은 ACP 자체에 대한 의미있는 분석을 시도한 경우도 존재하였다. 2006년에 쓰여진 [28]은 자동화된 정책 충돌 탐지 및 충돌 해소 알고리즘이나 프레임워크를 도입해도 정책을 다시 분석하고 재수립해야한다면, 즉 유저가 어차피 정책을 관리할 책임을 지니고 있다면 유저가 주의깊게 정책을 분석하고 재작성할 수 있도록 하는 정책 구조와 재작성 원칙들을 가이드라인으로 제시하자고 제안하였는데 꽤 오래된 논문이지만 우리의 프로젝트 방향성과 부분적으로 일치하는 특성을 보여 반드시 읽어둬야할 논문이다. 인덱스가 되어있지 않은 2개의 논문은 각각 정책 분석의 가시화 방법과 WCRP를 활용한 정책 충돌 해결방법에 대해 제시하고 있는데 각각 향후 솔루션이 개발됨에 따라 참고할 수 있는 논문들이기에 차후 확인할 수 있도록 한다. 이 외에도 IEEE / ACM에서 확인할 수 있는 여러 논문들이 있다. 새로운 연구 및 접근이 있을 경우 참고가 필요하다면 인덱스를 업데이트할 수 있도록 한다.

**B-4 XACML Technology**

XACML(eXtensible Access Control Markup Language)는 접근 제어만을 위해 개발된 오아시스 표준의 접근 제어 언어 및 아키텍처를 의미한다. 이 XACML을 활용하여 접근 제어 솔루션을 개발할 예정 중에 있으나 현재 XACML에 대하여 연구 역량이 아직까지 집중되지 못하고 있으며 OCF, oneM2M 표준에서 선택 가능한 옵션으로 제안되는 수준에 불과하다. 따라서 이 XACML을 학습하고 활용하기 위한 리서치를 진행해야 하며 현재는 XACML의 코어를 개발한 연구자가 소속되어있는 Axiomatics([www.axiomatics.com](http://www.axiomatics.com)) 회사에서 많은 정보를 습득할 수 있다. Axiomatics의 blog & white paper를 통해 XACML에 대해 학습하고 오아시스 표준 문서를 참고하여 부족 내용을 보충해 활용하도록 한다. 스터디 후 각각 Study, XACML standard, 논문으로 구성되어있는 디렉토리에 내용을 보충할 수 있도록 한다.

**B-5 IoT Platform Standard**

B-5에서는 OCF와 oneM2M의 최근 릴리즈 Technical Specification를 정리해 모아두었다. 향후 최신 릴리즈가 발행되면 업데이트한다. OCF는 전신인 OIC에서 제안된 TS를 그대로 이어받았으나 ACL을 이용한 접근 제어정도에 머물러있고 oneM2M은 비교적 구체적으로 아키텍쳐와 함께 제안하고 있기 때문에 oneM2M의 spec을 분석하고 표준에서 제안하고 있는 것과 한계를 명확히 파악할 수 있어야 한다. 또한 프로젝트 솔루션이 oneM2M 표준 인증을 받을 수 있도록 세부적인 요구사항에도 주의를 기울일 수 있어야 한다.

**C. Proceedings about IoT project.**

C에서는 현재까지 진행된 프로젝트의 진행사항에 대해 공유한다. 2016년 3-4분기에는 프로젝트의 실험 환경을 구축하기 위한 기자재를 구입하고 접근 제어와 XACML 기술에 대한 배경 조사 및 사전지식을 습득하였으며 2017년 1-2분기에는 관련 논문 출판 및 학회 참석, 프로젝트 솔루션의 프로토타입 아키텍쳐를 설계하였다.

신진연구\이기찬\AccessControlOnIoT\Project outputs\Design에서 현재 UML(Deployment Diagram)로 작성된 아키텍쳐를 확인할 수 있으며 향후 리서치미팅을 통해 관련 내용을 공유한다. 현재 Proceeding에 관한 정리가 요구되며 GitHub Wiki에 마이그레이션 후 진행사항을 주기적으로 업데이트할 수 있도록 한다.