Journal of the Korea Convergence Society
Vol. 9. No. 7, pp. 69-75, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.7.069

스마트 팩토리 엔터티를 위한 블록체인 기반의 효율적인 역할기반 접근제어

이용주, 이상호*
충북대학교 전자계산학과

Efficient RBAC based on Block Chain for Entities in Smart Factory

YongJoo Lee, Sang-Ho Lee*
Dept of Computer Science, Chungbuk National University

요 약 스마트 팩토리 내의 디바이스를 비롯한 다양한 엔터티 들은 보다 활동적이고 능동적으로 발전하고 있어서, 엔터티의 특성에 맞는 세분화된 접근제어가 필요하지만 기존의 디바이스에 대한 접근제어는 세분화된 접근제어가 부족하고, 사용자에 대한 접근제어는 절차가 복잡하고 가변적인 내용을 빠르게 적용하기에 어려움이 많다. 이 논문에서는 스마트 팩토리 엔터티에 최적화되어 효율성과 보안성을 유지할 수 있는 접근제어 방법을 제안한다. 기존에 PKC(Public Key Certificate)의 속성부여를 위해 정의되었던 AC(Attribute Certificate)를 PAC(Permission AC)로 확장하여 각 역할에 부여하여 통합관리가 용이한 RBAC(Role-basedAccessControl)를 제안한다. 또한 ACI(AC Issuer)의 디지털 서명된 PAC를 블록체인 기반의 모델에 적용하여 배포함으로써 수시로 바뀌는 엔터티의 역할에 대한 접근 및 권한 부여를 빠르고 정확하게 확인 및 반영할 수 있는 블록체인 기반의 RBAC-PAC 모델을 제안 한다. 기존연구와 효율성 측면에서 비교 분석하였고, 특히 엔터티 수가 많고 권한 갱신이 빈번할수록 효율성이 높아진 것을 확인하였다.

주제어 : 블록체인, 공인인증서, 사물인터넷, 스마트 팩토리, 역할기반접근제어

Abstract The key technology of Industry 4.0, Smart factory is evaluated as the driving force of our economic development hereafter and a lot of researches have been established. Various entities including devices, products and managers exist in smart factory, but roles of these entities may be continuous or variable and can become extinct not long after. Existing methods for access control are not suitable to adapt to the variable environment. If we don't consider certain security level, important industrial data can be the targets of attacks. We need a new access control method satisfying desired level of efficiency and security without excessive system loads. In this paper, we propose a new RBAC-PAC which extend AC defined for PKC to the authority attribute of roles. We distribute PACs for roles through block chain method to provide the efficient access control. We verified that RBAC-PAC is more efficient in the smart factory with large number of entities which need a frequent permission update.

Key Words : Block Chain, PKC, Internet of Things, Smart Factory, RBAC

1. 서론

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 가

*Corresponding Author : Sang-Ho Lee (shlee@cbnu.ac.kr)
Received May 30, 2018 Revised June 10, 2018
Accepted July 20, 2018 Published July 28, 2018

지는 지능적(intelligent)이고 스마트(smart)한 공장으로 정의하고 있으며, 핵심기술은 CPS(Cyber Physical System)와 IoT(Internet of Things)이다. 또한, 4차 산업혁명은 CPS를 기반으로 제조 단위가 제조 프로세스, 제품의 맞춤화(customization) 및 산출물의 규모와 범위 측면에서 더 높은 유연성을 가능하게 한다. 그리고 4차 산업혁명의 개념을 제조현장에 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 엔터티들이 존재하게 되며 스마트 팩토리 환경에 따라 수시로 변경될 수 있다[1, 2, 3].

이 논문에서는 이러한 고도로 네트워크화 된 환경에서 효율적으로 사용할 수 있는 PA(Permission Attribute)을 이용한 RBAC(Role-based Access Control)를 블록체인 기반으로 제안하여 보안성과 효율성을 제공하고자 한다. 2장에서는 이를 위해 필요한 기존 연구들을 정리하고, 3장에서는 이 논문에서 제안하는 RBAC를 설계하고, 4장에서는 시나리오로 검증하고 효율성을 비교하여 결론을 맺고자 한다.

2. 관련연구

2.1 스마트 팩토리

스마트 팩토리는 4차 산업혁명의 개념과 핵심기술이 통합된 형태를 의미하며, 공장의 생산설비를 기반으로 한 수직적 통합과 고객의 요구사항을 시작으로 제품개발 가치사슬의 수평적 통합이 구현되는 공장으로 정의할 수 있다. 수직적(생산시스템) 통합은 생산의 효율화를 위한 목표를 가지고 있으며 이를 위하여 제품이 생산되는 다양한 설비에서 센서 및 디바이스를 통하여 신호를 획득하고, PLC(Programmable Logic Controller) 및 HMI(human Machine Interface) 등의 제어기술을 통하여 설비의 제어를 수행하며, 생산 프로세스를 관리하기 위한 MES(Manufacturing Execution System)와 창고관리를 위한 WMS(Warehouse Management System)를 거쳐 상단의 ERP (Enterprise Resource Planning)까지 유기적으로 관리 될 수 있는 개념이다[4, 5]. 그리고 수평적 통합은 제품을 사용하는 고객(B2B에서의 기업고객 및 B2C에서의 개인고객을 모두 포함)이 원하는 요구사항을 도출하기 위한 시장조사 및 제품기획 단계를 거쳐, 고객의 요구사항을 충족시키기 위한 제품개발 단계 및 공정설계 후 제품을 생산하여 제품을 고객에게 전달하는 과정까지를 포함하고 있다[6].

2.2 블록체인

블록체인은 피어투피어(peer to peer) 환경에서 안전한 데이터 저장을 제공하는 기술이다. 블록체인 기술을 이용한 대표적인 응용이 암호 화폐인 비트코인이며 기존 서버-클라이언트 구조의 중앙 집중형 통화발행 및 관리 방식이 아닌 인터넷 환경에서 은행과 같은 제 3자의 개입이 없고, 사용자간 신뢰 관계가 없이 안전하게 암호 화폐 거래가 가능하도록 개발되었다. 즉 관리하는 중앙 기관 없이 피어투피어 네트워크 환경에서 사용자 간 직접적인 암호 화폐를 통한 안전한 거래를 제공한다. 이러한 기능을 가능하게 하는 블록체인의 특징은 크게 두 가지로 살펴 볼 수 있다[7,8].

첫째는 시간별로 블록이 정리되어진다. 한 블록에는 앞의 블록과 뒤의 블록을 연결하는 연결정보가 포함되어 있으며, 앞 블록의 내용을 변경하면 뒤에 이어지는 모든 블록을 다시 생성해야 한다. 따라서 과거 블록의 내용을 조작하는 것은 어렵다. 반대로 과거 시점의 거래 기록이 존재한다면 그것은 그 시점에 거래가 이루어졌다는 것을 객관적으로 알 수 있고 이러한 특징은 변조의 공격을 막아 무결성을 제공한다. 두 번째 중요한 특징은 분산 원장이다. 블록체인 네트워크에 참가한 모든 사람이 모든 거래 기록을 기록한 원장을 소유하기 때문에 거래의 투명성이 높다는 것이 특징 중 하나이며 거래를 관리하는 중앙 시스템이 없어 탈중앙화가 가능하다. 블록체인에 참여하는 사용자들은 거래를 작성하고 자신의 개인키로 거래에 서명한다. 작성된 거래들은 다른 사용자들에게 브로드 캐스팅하여 전달하고, 합의과정에서 특정 합의 알고리즘을 통해 거래들을 하나의 블록으로 생성한다. 생성된 블록은 기본 블록체인에 연결되게 되고, 블록의 정보는 다른 사용자들에게 브로드 캐스팅한다. 사용자들은 블록체인에 연결된 블록의 정보들을 바탕으로 중앙 시스템 없이 사용자들 간에 데이터의 신뢰성을 확인할 수 있다[9,10].

2.3 RBAC(Role-based Access Control)

RBAC는 역할(Role)에 따라 사용자의 교체나 일의 재

할당을 할 수 있어 전통적인 접근제어보다 관리가 쉽고 보다 효율적인 특징이 있다. RBAC에서 사용자는 OB(Object)에 접근이 허용된 권한을 가진 역할에 할당되었을 경우, 해당 OB에 접근할 수 있다. RBAC에서 역할의 개념은 조직의 기능적 역할과 유사하며 동시에, 어느 특정한 보안정책을 포함하는 대신 그 정책을 표현하는 방법이기도 하다. Fig 1에서와 같이 역할은 사용자와 OB의 중간자 위치에 있으며, 사용자가 아닌 역할에 따른 접근권한을 부여받게 된다. 예를 들어 OB가 파일이라면 역할에 따라 tran_a(읽기) 등이 부여된다[11,12].

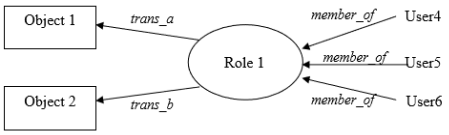

Fig. 1. Role Relationships

2.4 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[13, 14]. 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 반복해야 하며, ACR에 대한 추가적인 보안조치 또한 중요하여 조직의 특성과 역할의 중요성에 따라 가변적으로 적용해야 할 필요성이 있다[15,16].

2.5 RBAC-SC(Smart Contract)

J.CRUZ[15]는 블록체인 기반의 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.

3. RBAC-PAC

3.1 요구사항

이 논문에서 제안 하고자 하는 RBAC-PAC는 스마트 팩토리의 엔터티에 최적화된 접근제어 기법으로 다음 요구사항을 목표로 한다. 1) 인증 시 마다 반복되는 절차를 최소화 하여 엔터티 수가 늘어날수록 더욱 효율적이어야 한다. 2) 인증서 신청 및 갱신은 엔터티가 아닌 시스템관리자가 하도록 설계하여 수동적인 엔터티까지 접근제어 할 수 있도록 한다. 3) 역할에 대한 권한이 중복 정의되어 발생하는 혼란 및 충돌이 없어야 한다. 4) 인증서 보관 및 인증주체에 대한 추가적인 보안조치 없이 접근제어 제공이 가능해야 한다.

3.2 Role과 PAC의 관계 정의

이 논문에서는 기존의 PKC X.509 인증서와 연계하여 사용하기 위해 정의된 AC를 역할의 권한 속성을 정의하기 위한 PAC로 이용하여 스마트 팩토리 엔터티 들에 최적화된 역할기반 접근제어 모델을 설계하고자 한다. 이 논문에서 사용하는 PAC는 IETF의 RFC 5755[17, 18] 등에서 정의한 AC Profile을 기반으로 사용하며 PAC가 할당되는 주체는 User가 아닌 역할이며 각 역할은 계층적인 구조로 설계하여 자식 역할은 부모 역할의 PA를 상속

하게 된다. Fig 2은 계층적인 역할의 구조를 보여주고 있다.

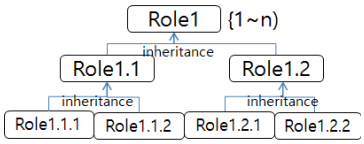

Fig. 2. Hierarchical Architectures of Roles

하나의 엔터티는 하나 이상의 역할을 가지고 있고, 각 역할은 부모 역할의 PA를 상속한다. 하나의 역할은 다수의 권한 속성을 가질 수 있으며, 인증서로 표현된 하나의 PAC Profile을 소유한다. Fig. 3는 이러한 관계를 보여주고 있다.

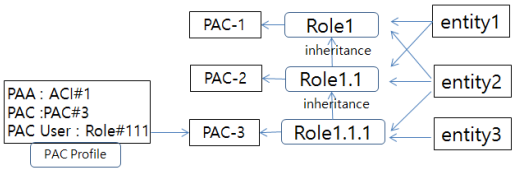

Fig. 3. PAC profiles for Roles and Entities

3.3 RBAC-PAC 메커니즘

이 논문에서 제안하는 접근제어를 제공하기 위해 아래의 절차로 나누어 설명한다.

- 준비 : ACI가 발급한 PAC가 ACI로부터 발급되었다는 점을 특별한 질의 없이 디지털 서명으로 확인시키기 위해 ACI는 공개키 쌍$(PubKey, PrvKey)$을 생성한 후 블록체인을 통해 공개키를 배포한다.
- PAC 발급/갱신요청 : 스마트 팩토리 관리자는 스마트 팩토리 내에 특정 Role에 대한 PAC의 발급 및 갱신을 요청한다.
- ACI의 PAC 발급 : ACI는 PAC를 발급하고 식(1)와 같이 자신의 비밀키로 서명한다. 스마트 팩토리 관리자는 서명된 트랜잭션을 블록체인에 등록한다.

$$EnPAC = encrypt(PAC)withPrvKey \quad (1)$$
$$Tran = EnPAC$$

- 블록체인 등록 : 트랜잭션을 등록하면 네트워크에 있는 모든 노드들에게 브로드 캐스트 되어 블록을 생성하기 위한 해답을 찾고 이 과정이 끝나면 새로운 블록은 모든 노드에 저장되어 무결성이 유지된다.
- PAC 확인: AC Verifier(속성 검증자)는 역할에 대한 PAC를 찾아서 미리 공개된 ACI의 공개키로 식(2)와 같이 복호화 한 후 접근제어에 사용한다.

$$PAC = decrypt(EnPAC)withPubKey \quad (2)$$

3.4 블록체인을 이용한 RBAC-PAC

Fig. 4는 3.2절에서 생성한 트랜잭션을 블록체인을 통하여 배포하고 사용하는 절차를 보여주고 있다. 인증 시 공개된 비밀키로 복호화 함으로써 PAC의 검증과 무결성 모두를 만족 시킬 수 있다. 블록체인에 의해 등록자의 디지털 서명이 된 트랜잭션이 블록체인을 통해 배포되면 브로드캐스트 기능을 통해 각 노드에 저장이 되므로 블록의 무결성이 유지된다. 즉, 어느 노드에서든지 필요한 트랜잭션을 추출하여 확인하여도 신뢰할 수 있는 PAC이므로 접근제어에 활용할 수 있다.

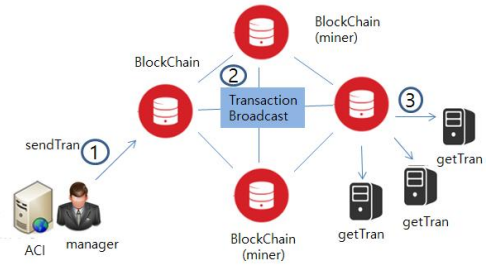

Fig. 4. Block Chain based RBAC-PAC

블록체인에 등록된 블록은 헤더와 페이로드로 구성되며 이전 블록의 해시 값, Nonce, DifficultyBit, 머클트리 루트 등으로 구성되며 Fig. 5와 같다.

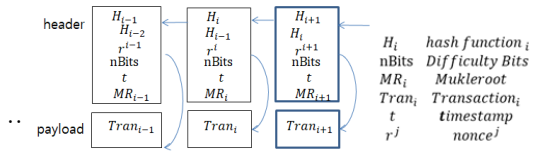

Fig. 5. Headers and Payloads in Blocks

4. 검증

4.1 Use Case 시나리오

이 논문에서 제안한 메커니즘을 검증하고자 스마트

팩토리의 디바이스 접근제어에 적용해 보고자 한다. 스마트 팩토리 내에는 활동성이 부여된 장비, 로봇, 생산 설비 등을 비롯하여 원자재, 완성품 등 센서 등이 부착된 다양한 엔터티 들이 존재한다. 각 엔터티는 이벤트 업, 다운로드 등을 포함하여 다양한 접근제어의 관리 대상이 되고 있지만 현재는 효율성의 문제들로 인해 시리얼넘버 등의 단순인증 만을 사용하고 있다. 이러한 디바이스를 예를 들어 효율적이고도 안전한 접근제어가 가능한 시나리오를 작성해 보고자 한다.

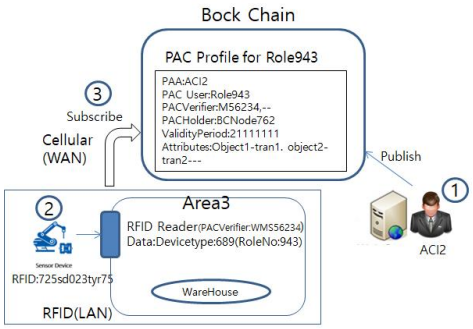

Fig. 6. Use Case Scenario for Smart Factory

스마트 팩토리 내에 디바이스 센서는 M2M (Machine2Machine)-RFID으로 연결되어 있고 Fig 6과 같은 대표속성을 가지고 있다고 가정한다. 스마트 팩토리 역할속성 부여 책임자는 각 역할에 대한 상세한 권한 속성을 ACI통하여 발급요청하고 블록체인에 등록한다. Fig 6에서 디바이스는 Area3에 있는 WareHouse(물류창고)에 접근 하려고 한다. 접근 요청을 하지 않아도 WM(WareHouse Manager)는 RFID 인식으로 해당 디바이스가 입장하려 한다는 것을 알고 있으며, 디바이스 타입과 RoleNo를 확인할 수 있다. 접근을 통제하는 ACVerifier(WMS56234)는 블록체인에 등록된 해당 RoleNo(role943)에 등록된 PAC를 검색하여 Area3에 대한 접근이 허가된 엔터티 인지 확인하고 접근제한을 해제한다. 공개된 ACI의 공개키로 복호화 된다면 PAC가 ACI에 의해 발급된 것인지 확인되기 때문에 추가적인 절차는 필요치 않으며 블록체인 내에 블록은 시간의 순서대로 정렬되어있기 때문에 가장 최근의 PAC를 가져올 수 있어 ValidityPeriod 필드의 유효성만 검증하면 되므로 추가적인 절차가 필요치 않아 간단한 절차로 모두 자동화가 가능하다. 이 시나리오는 간단한 사용 예이며, 보다 복잡하고 중첩적인 접근 제어도 정책(Policy)을 정의하여 모두 자동화 시스템으로 설계 및 구현이 가능하다.

4.2 효율성 분석

4.2.1 효율성 분석 환경

기존연구에서 제안한 RBAC-SC[15]와 이 논문에서 제안한 RBAC-PAC의 효율성을 비교하기 위하여 등록절차(Reg), 접근제어(A.Control), 권한갱신(P.Renewal)로 나누어 필요한 트랜잭션을 조사하였고, 엔터티 수(N.Entities)를 1과 300으로 분리하여 총 트랜잭션의 수를 Table 1로 나타내었다. RBAC-SC에서는 역할을 확인하기 위해 Role Issuer에게 질의하는 절차를 거치게 되어 A.Control 1회당 최소 6회의 트랜잭션이 필요하고, RBAC-PAC에서는 이러한 확인 절차를 디지털 서명으로 대체하여 3회의 절차가 필요하다. 또한 역할 갱신 시, RBAC-PAC에서는 역할 단위로 갱신을 하며, 하나의 역할에 할당된 엔터티의 수는 30개로 가정하였다.

Table 1. Transaction Comparison of Entities

	N.Entities	Reg	A.Control	P.Renewal	TotalTran
RBAC-SC	1	3	6	2	12
	300	900	1800	600	3600
RBAC-PAC	1	2	3	1	7
	300	600	900	10	1810

4.2.2 효율성 비교

Table 1을 기반으로 RBAC-SC와 RBAC-PAC의 효율성을 비교하기 위하여 첫 번째로는 하나의 엔터티가 등록, 접근제어, 권한갱신을 각 1회씩 했을 때 엔터티 수에 따른 효율성을 Fig 7의 A그래프에 나타내었다. Fig 7의 B는 하나의 엔터티가 1회 등록절차를 수행 후 10회 접근제어, 10회 권한 갱신을 했을 경우 엔터티 수에 따른 효율성을 비교한 것이다. A 그래프에서 엔터티의 수가 3만개 일 경우에 RBAC-PAC가 RBAC-SC의 50% 효율성 차이를 보였는데, B의 그래프에서 엔터티의 수가 3만개 일 경우에 39%로 줄어 든 것을 볼 수 있다. 즉 등록 후, 접근제어, 권한 갱신 등이 빈번하게 일어날수록 절차의 간소화와 역할 권한 갱신 단위의 효과로 효율성이 높아지는 것을 볼 수 있다.

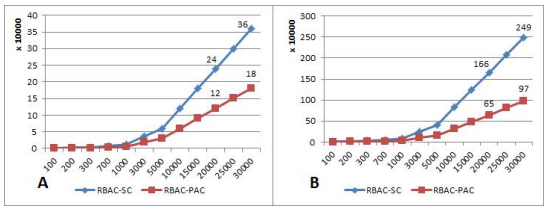

Fig. 7. Comparison of Efficiency

4.3 기존 연구와의 비교

기존 연구(RBAC-SC)에서는 각 역할의 주체가 역할 할당을 신청하였으며, Role Verifier(역할 검증자)는 직접 Role Issuer(역할 발행자)에게 매번 역할 발행 여부를 확인하는 절차를 거친다. 또한 역할 갱신 시 각 사용자 마다 신청하여야 한다. 이 논문에서 제안하는 RBAC-PAC는 역할 매니저가 역할의 발행을 신청하여 Role Issuer의 디지털 서명 후 블록체인을 통하여 등록하므로 Role Verifier는 역할 발행여부를 확인하지 않고, Role Issuer의 공개키로 복호하여 검증과정을 대체한다. 복잡한 절차를 간소화 할 수 있고, 권한 갱신 시 각 역할 단위로 갱신이 이루어지므로 엔터티 수가 많고 권한 갱신이 빈번한 대형 스마트 팩토리에서 더 높은 효율성을 가진다.

4.4 요구사항 평가 및 토의

이 논문에서 목표로 했던 요구사항에 대해서 평가하고자 한다. 1) 인증 시 마다 반복되는 절차를 최소화하기 위하여 Role Issuer의 디지털 서명을 추가하였으므로 역할 발행여부에 대한 확인절차 없이 인증이 가능하다. 2) 인증서 신청 및 갱신은 관리자가 신청하고 등록하므로 수동적인 엔터티 까지 관리할 수 있다. 3) 역할의 상속 기능을 통하여 역할을 계층화하여 정의하고, 하나의 Role에 하나의 PAC만 매치 되도록 설계하여 중복 정의로 인한 혼란 및 충돌을 사전에 제거하였다. 4) 블록체인을 통하여 배포하고 확인하므로 인증서를 보관하는 서버 등이 불필요하다. 이 논문에서 제안한 접근제어는 스마트 팩토리의 엔터티의 보안성과 효율성에 초점을 맞춘 것이므로, 스마트 팩토리에서 매우 중요한 역할을 담당하는 관리자나 보안 담당자에게는 추가적인 보안 조치가 필요하다. 또한 엔터티 수가 많지 않은 스마트 팩토리에서는 효율성의 차이가 크지 않으므로 대형화된 스마트 팩토리의 접근제어가 빈번한 자동화 시스템에 더욱 적합하다.

5. 결론 및 향후 과제

이 논문에서는 스마트 팩토리 내의 다양한 엔터티들의 속성을 정의한 PAC를 활용하는 접근제어 방식을 정의하였다. 이 논문에서 정의한 PAC는 수시로 변하는 엔터티 들의 속성을 효율적으로 변경하기 위해 계층적으로 설계하여 상속개념을 적용하였으며, 인증 및 허가 시에도 효율적으로 권한속성을 확인하고 접근제어에 활용할 수 있도록 ACI의 디지털 서명 후 블록체인을 이용하여 배포하였다. 이로 인해 각 엔터티들 마다 반복해서 수행해야 될 등록 및 관리 작업, 및 검증 작업을 단순화하여 효율을 높였으며, 이는 엔터티 들의 수가 많은 대형 스마트 팩토리의 경우에 더 큰 효율을 가져올 수 있다. 이로 인해 효율성이 중요한 스마트 팩토리 환경에서 새로이 배포되는 PAC를 적용하여 활용할 수 있게 됨으로써 보다 안전하고 효율적인 접근제어가 가능하게 되었다. 향후, 보다 다양하고 효율적이면서 보안성이 강조된 접근제어 기법 등이 연구되어야 할 것이다.

REFERENCES

[1] Y. J. Cho. (2017). National Smart Factory Strategy for The 4th Industrial Revolution. Joutnal of Korea Information Science society, 41.

[2] S. H. Hong. & H. J. Shin. (2017). Analysis of the Vulnerability of the IoT by the Scenario. Journal of the Korea Convergence Society, 18(9), 1-7.

[3] J. Park. & K. Lee. (2017). Realization of user-centered smart factory system using motion recognition. Joutnal of Convegence. &(6). pp.153-158.

[4] S. H. Lee. & D. W. Lee. (2016). A study on u-Health Fusion Field based on Internet of Thing. Journal of the Korea Convergence Society, 17(4), 19-24.

[5] I. S. Jeon. (2016). Curriculum Development for Smart Factory Informaton Security Awareness Training. Journal of KIISC, 26(5).

[6] O. Novo. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE IoT Journal, 5(2).

[7] S. H. Hong & S. H. Park. (2017). The Research on Blockchain-based secure IoT authentication. Journal of the Korea Convergence Society, 1 8(11), 57-62.

[8] S. K. Hong & C. R. Seo. (2018). Developing a Blockchain based Accounting and Tax Information in the 4th

Industrial Revolution. Joutnal of the Korea Convegence Society, 9(3), 45-51.
[9] K. Blockchains. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303.
[10] D. F. Ferraiolo. (2001). Proposed NIST Standard for Role-Based Access Control. A C M T r a non InfoSystemSecurity, 14(3), 224-274.
[11] Y. S. Jeong. (2018). User Privacy Security Scheme using Double Replication Key in the Cloud Environment. Journal of the Korea Convergence Society, 9(4), 9-14.
[12] R. Sandhu. & C. Youman. (1996). Role-Based Access Control Models. IEEE Computer, 29(2).
[13] H. Kim. & S. Pan. (2016). Technology Trends, Research and Design of AIM Framework for Authentication Information Management. Journal of Digital Convergence, 14(7), 373-383.
[14] N. H. Kim. (2018). Secure MQTT protocol based on Attribute-based Encryption Scheme. Journal of KIISE, 45(3), 195-199.
[15] Y. S. Jeong. & K. H. Han. (2017). A hierarchical property based multi-level approach method for improves user access control in a cloud environment. Journal of the Korea Convergence Society, 18(11), 67-73.
[16] J. P. Cruz. & Y. Kaji. (2018). Role-based Access Control using Smart Contract. IEEE Access, 6, 12240-12251.
[17] J. Jung & J. Kim, (2015). A study on Development of Certification Schemes for Cloud Security, Journal of Digital Convergence, 13(6). 81-89.
[18] S. Farrell. & T. C. Dublin. (2010). An Internet Attribute Certificate Profile for Authorization. IETF.:RFC 5755.

이 용 주(Lee, Yong Joo) [학생회원]

- 1999년 2월 : 청주대학교 정보통신공학과(학사)
- 2001년 2월 : 충북대학교 전자계산학과(이학석사)
- 2001년 1월 ~ 2009년 12월 : 한국전자통신연구원 선임연구원
- 2002년 3월 ~ 현재 : 충북대학교 전자계산학과 박사과정
- 관심분야 : IT융합, 블록체인, 정보보안, 스마트 팩토리
- E-Mail : silvianna817@naver.com

이 상 호(Lee, Sang Ho) [종신회원]

- 1972년 2월 : 숭실대학교 전자계산학과(학사)
- 1981년 2월 : 숭실대학교 전자계산학과(이학석사)
- 1989년 2월 : 숭실대학교 전자계산학과(이학박사)
- 1981년 3월 : ~ 현재 : 충북대학교 소프트웨어학과 교수
- 관심분야 : 컴퓨터네트워크, 통신보안, 중소기업정보화, IT융합, 스마트 팩토리
- E-Mail : shlee@cbnu.ac.kr