사물인터넷 디바이스의 계정 관리 시스템

최창원[1*], 정현철[2]
[1]한신대학교 컴퓨터공학부 교수, [2]㈜온솔아이티 대표이사

An Account Management System on IOT Devices

Changwon Choi[1*], Hyuncheol Chung[2]
[1]Professor, Division of Computer Engineering, Hanshin University
[2]CEO, ONSOLIT Co. LTD

요 약 사물인터넷의 발달에 따라 IOT 장비의 보안 중요성도 더욱 가중되고 있다. 특히 사물인터넷의 특성 상 수십, 수백 개에 이르는 IP 카메라, 홈 IOT 장비, 다양한 측정 장비 등의 계정 관리는 시스템 관리자나 사용자들이 필수적으로 수행해야 하는 번거로운 작업이 되었다. 본 논문에서는 사물인터넷 상에 사용될 수 있는 다양한 장비들의 계정 관리를 체계적으로 설계하여 사용자에게 업무 효율을 높일 수 있는 시스템을 제안한다. 계정 관리의 주요 기능을 6 가지 기능으로 나누어 제공하고 기존의 시스템들보다 개선된 기술들을 적용하였다. 제안 시스템은 권위있는 기관의 인증 테스트를 성공적으로 통과하여 현재 실무 현장에 활용되고 있으며 향후 AI 기술을 적용한 스마트 계정 관리 시스템으로 개발 중이다.

주제어 : 계정관리 시스템, 사물인터넷 디바이스 보안, 스마트 관리 시스템

Abstract As the IOT technology has developed, it becomes more big issues about IOT device security. An account management is a nerve-in-the-box routine job for the system administrator and users who manage the several hundreds IOT devices(IP camera, Home IOT, the various measuring equipment). This study is to propose the account management system by the hierarchical design and it is efficient for the user to manipulate the account management. The designed system supports 6 functions for the account management and apply the advanced technologies for the existed system. After the performance of the designed system is validated successfully by the authoritative test, the designed system is applied for the relative fields. And it is on going for the development of the smart account management system by applying the AI technique.

Key Words : Account Management System, IoT Devices Security, Smart Management System

1. 서론

1.1 연구 배경 및 목적

사물인터넷의 발달에 따라 IOT 장비의 보안 중요성도 더욱 가중되고 있다. 특히 사물인터넷의 특성 상 수십, 수백 개에 이르는 IP 카메라, 홈 IOT 장비, 다양한 측정 장비 등의 계정 관리는 시스템 관리자나 사용자들이 필수적으로 수행해야 하는 번거로운 작업이 되었다. IT 분야에서 보안 이슈는 과거부터 현재까지 계속 IoT 디바이스의 70%가 암호화되지 않은 네트워크를 통해 데이터를 전송하는 것으로 조사되었다[1].

SANS Institute에 따르면 보안전문가 391명 대상 설

*교신저자 : 최창원(won@hs.ac.kr)
접수일 2021년 1월 24일 수정일 2021년 2월 27일 심사완료일 2021년 3월 20일

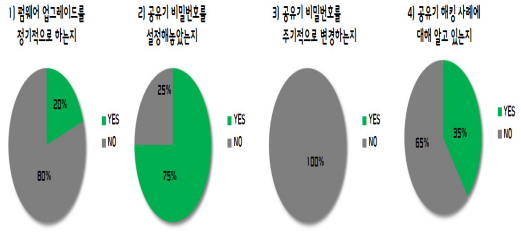
문조사 결과 2/3가 IoT 보안에 대해 우려하고 있다고 답변하였다. 또한 가트너의 조사에 따르면 22%의 기업이 IoT로 인해 새로운 위험에 직면할 것이라고 경고하였다[1]. 400만대(공공용 36만대·민간용 350만대)의 CCTV가 설치되어 있는 경우 이로 인해 수도권 시민은 9초에 한 번씩(하루 평균 80~110회 정도) CCTV 카메라에 포착된다고 우려하였다[2].

IoT 장비 검색 엔진인 'Shodan'을 사용하면 키워드 검색만으로 다양한 CCTV의 IP주소를 얻을 수 있으며, 그에 따른 부가적인 정보 또한 쉽게 얻을 수 있다. 〈Table 1〉 3은 "Shodan"에서 얻을 수 있는 다양한 보안 사고 사례이며 IP 노출로 인해 이러한 부가적인 정보까지 손쉽게 얻을 수 있다는 것이므로 IP 노출에 대한 피해가 더욱 커질 수 있다[4].

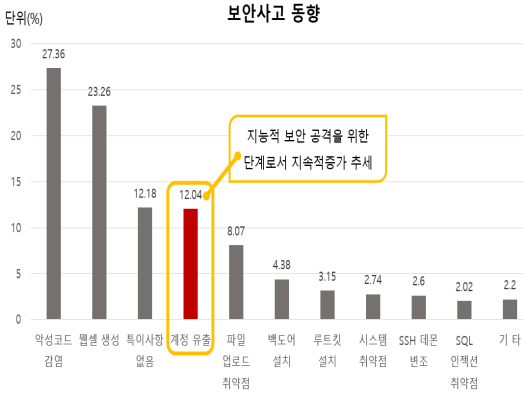
〈Table 1〉 Security Accident Cases

유형	사고 사례	비고
트렌드넷의 유아 관찰용 CCTV	트렌드넷(TRENDnet)의 CCTV 제품 시큐어뷰(SecurView)소프트웨어의 결함으로 인해 인터넷 주소만 알면 누구든 보안을 우회해 온라인으로 영상과 음성을 도감청. 2013년 9월 미 연방통상위원회(FTC)로부터 제재 조치 받았음. 조사 결과, 인터넷 상 약 700개의 CCTV에서 촬영중인 실시간 영상 링크가 유포됨.	
IoT 기기 대상 악성 코드 **미라이 (Mirai)**	대상 : **기본패스워드가 설정된 IoT 기기** 공격방법 : **관리자 계정설정이 취약한(공장 초기 설정대로 운영되는 장비) 임베디드기기(무선공유기, CCTV, 스마트 전구, NAS 등) 스캐닝·접속** → 악성코드 감염 → 취약한 他기기 검색·감염으로 좀비 확보 → 디도스 공격(DDoS), 미국 동부 지역 인터넷 마비.	
ID/PW 출고 설정값 사용	보안업계에서 **'기본 암호'**로 통하는 3가지 종류의 **비밀번호(암호 없음, 12345678, 4321)**를 1,132곳의 계정에 대입한 결과 44.0%에 해당하는 498곳의 CCTV 관리자 계정이 열림	
CCTV ID/PW 관리 소홀로 인한 2차 금융정보 유출 피해 우려	국내 시중 은행들이 영업점 현금자동입출금기(ATM) 부스 천장에 CCTV를 설치해 예금을 입출금하는 **고객의 비밀번호 등 개인 정보를 촬영**. 농협, 국민, 기업은행 등 대부분의 제1금융권 은행은 물론 제2금융권과 특수은행들도 천장형 CCTV를 운영 중이며, 전국 은행에 설치된 ATM기는 올해 9월 말 현재 5만 1,097대	
관리자 계정 관리 소홀	관리자가 카메라가 설치된 곳이 아닌 외부에서 영상을 확인하고 카메라를 제어할 수 있는 기능을 내장. 문제는 관리자만 쓸 수 있는 기능에 **비밀번호를 설정하지 않은 채**로 내버려 둘 경우 인터넷이 연결된 곳이면 누구나 스마트폰이나 PC를 통해 영상을 훔쳐보고 카메라를 조작할 수 있음	
특정 IP 차단 미흡 및 ID/PW 출고 설정값 사용	2014년 러시아 해커가 IP가 노출된 CCTV 73,000여개를 해킹, 해킹 방법은 인터넷에 노출되어 있는 수많은 IP주소를 수집하여 그 중에 CCTV로 사용되는 IP를 찾고, 아이디·패스워드가 없거나 **'admin-1234', 'admin-admin'**등과 같은 기본으로 주어진 아이디/패스워드를 가지고 있는 CCTV에 접속하여 권한을 얻은 후 CCTV 화면을 획득하는 방법을 사용.미국,프랑스,일본,네덜란드,이탈리아, **한국**,스페인,독일 등의 순으로 피해.	

정부와 공공 기관들의 공공 와이파이 구축이 증가되면서 이에 따른 보안 정보 노출 문제도 커지고 있다. [Fig. 1]은 '공공 와이파이 관리자들의 보안 의식에 대한 조사' 결과이며 많은 관리자들이 계정 관리를 소홀히 하는 것으로 나타났다.



[Fig. 1] Security Consciousness Survey for the Public WiFi Administrators



[Fig. 2] Security Accidents Types

[Fig. 2]는 보안 사고의 형태와 동향이며 계정 관리 문제가 증가 추세이며 이에 대한 중요성을 강조하고 있다[1]. 따라서 계정 관리를 체계적으로 다룰 수 있는 시스템의 개발이 필요하며 본 논문에서는 다양한 기능을 제공하며 기존의 방식과는 보안 차별성을 제공할 수 있는 시스템을 설계하고 개발한다.

1.2 연구 내용

패스워드 관리는 해당 제품의 제조사/모델별 상이한 환경을 가지고 있어 개별적인 프로토콜 연동 개발이 필요하여 고객사별 개발 프로젝트의 성격이 뚜렷한 성향을 나타낸다. 이에 따라 개발 기간의 소요와 비용이 많이 발생하는 문제점이 노출되어 보안 관리 활동에 많은 제약을 주고 있다. 본 논문에서는 이러한 문제점을 극복하고자 현재 국내에서 판매 중인 IOT 장비의 주요 제품의 모델별 사전 개발을 통해 패스워드 관리 S/W를 모델별 모듈화하고 개별 운영 기관에는 이를 네트워크를 통해 원격 다운로드하여 패스워드 관리 시스템을 구축하도록 한다.

2 장에서는 제안 시스템의 구성 방식과 제공되는 주요 기능들을 모듈별로 설명한다. 3 장에서는 개발된 시스템의 안정성 및 효율성을 제고하기 위한 성능 평가의 결과를 제시하며 4 장에서 연구 결과와 향후 보완 사항들을 기술한다.

2. 제안 시스템 주요 설계

2.1 제안 시스템 기능

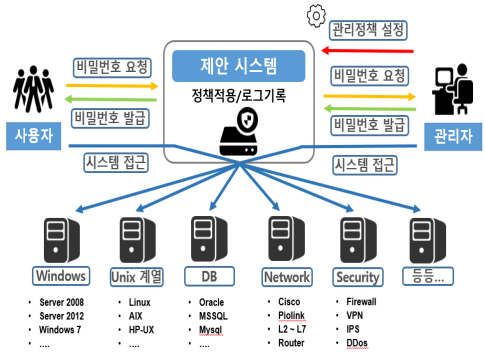
제안 시스템은 효율적인 계정 관리를 위해 여섯 개의 기능을 관리자나 사용자에게 제공하도록 설계되었다.

- 시스템 비밀번호 관리 기능(루트, 사용자 계정)
- 그룹별(부서별, 사용 시스템별, 사용자별) 보안 정책 적용 기능
- 애플리케이션 비밀번호(하드코팅 비밀번호 포함) 관리 기능
- 사용자 인증 기능
- 업무 결재 지원 기능
- 보고서 제공 기능

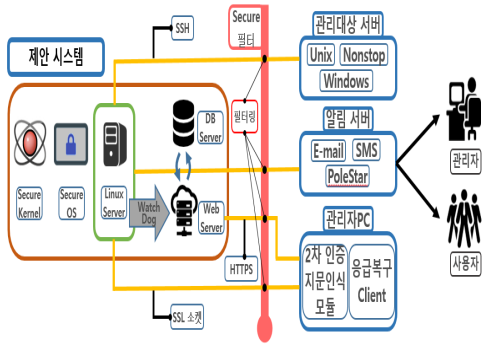
2.2 제안 시스템 구성

제안 시스템은 효율적인 계정 관리를 위해 관리자와 일반 사용자(외부 사용자 포함)들이 비밀 번호를 요청하면 각 기관별로 설정한 정책에 따라 비밀 번호를 발급한다. 발행되는 비밀 번호는 다양한 운용 시스템에 적합하도록 커스터마이징된다[Fig. 3].

[Fig. 4]는 제안 시스템의 구성 요소들과 이들의 상호작용을 나타내며 2 종의 서버와 2차 인증을 위한 시스템을 제공하고 각 트랜잭션들을 이상 행위 감지 기능을 통해 필터링된다[10,13].

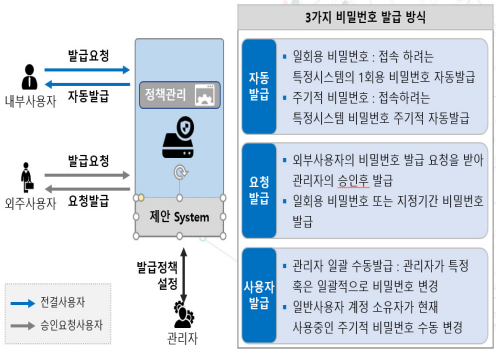


[Fig. 3] System Process Flow



[Fig. 4] System Design Map

2.3 비밀번호 관리 기능



[Fig. 5] Password Issue

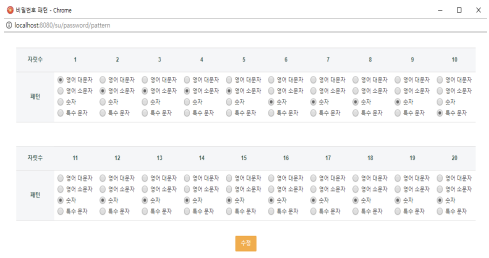
비밀 번호는 자동발급, 요청발급, 사용자발급의 3 가지 방식으로 발급되며 비밀 번호의 유형은 다음과 같다.

1) 일회용 비밀번호
   - 패턴 정책에 따른 형태의 One-Time 비밀 번호를 생성
2) 기간제 비밀번호

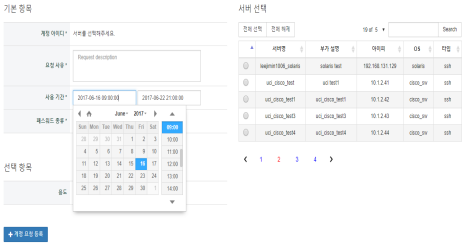
- 사전에 사용 기간을 정하고 사용하는 비밀번호
- 사용 기간이 만료되면 대상 사용자의 권한을 상실시켜 부정 사용을 방지

3) 주기적 비밀번호
- 일정기간 동안 사용할 수 있는 주기적 비밀번호
- 시간, 일, 월 단위 등으로 정책에 따라 변경
- 비밀번호 유효 기간을 임의로 지정 가능

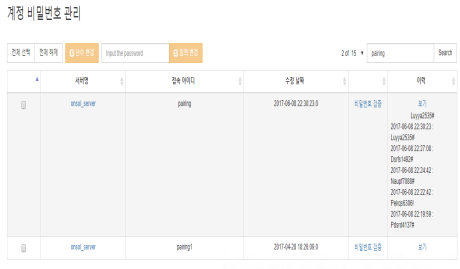
4) 임의적 비밀번호
- 사고 발생 또는 급히 비밀번호를 변경해야 할 때 관리자가 직접 변경
- 선택에 따라 일괄 변경 및 부분 변경 가능
- 자동 생성 비밀번호 또는 관리자가 입력한 비밀번호로 변경
- 긴급한 돌발상황에도 업무의 연속성 보장



[Fig. 6] Password Pattern Setup



[Fig. 7] Periodic Password



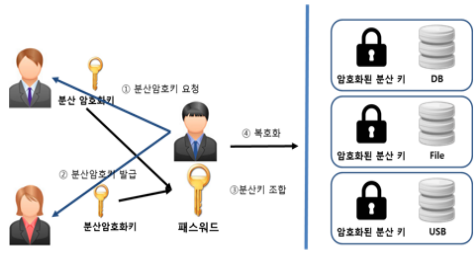
[Fig. 8] Random Password

기관별로 업무에 활용하는 다양한 애플리케이션들이 증가되면서 애플리케이션별로 계정 관리 기능도 필요하게 되었다. [Fig. 9]은 애플리케이션의 비밀 번호를 관리하는 것으로 애플리케이션 특성에 따라 2 가지의 형태로 발급한다.

- Push 방식 : API를 제공하여 애플리케이션에 직접 전달
- Pull 방식 : 하드코딩된 비밀번호 파일을 파싱및 수정 하여 비밀번호를 전달(C, C++, C#, JAVA, VB, Delphie등) [10-16].

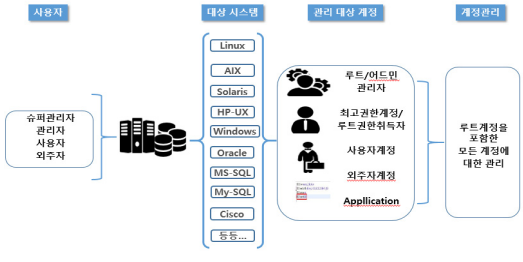
[Fig. 9] Application Password

사용자의 계정을 안전하게 관리하기 위해 키 분산 알고리즘을 개발하고 이를 제안 시스템에 적용하였다.



[Fig. 10] Key Distribution Process

2.4 시스템 계정 관리 기능

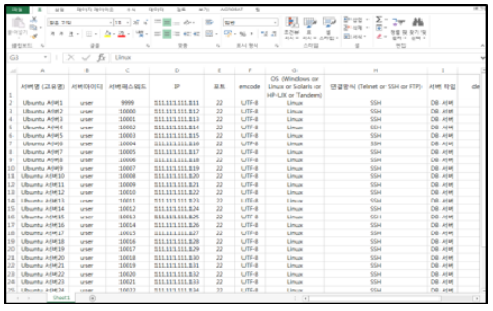


[Fig. 11] System Account Management

시스템 계정 관리 기능은 다양한 사용자들을 대상으로 관리 대상 계정을 구분하고 대상 시스템별로 체계적으로 관리하는 기능이다[Fig. 11]. 계정의 등록 및 삭제, 작업

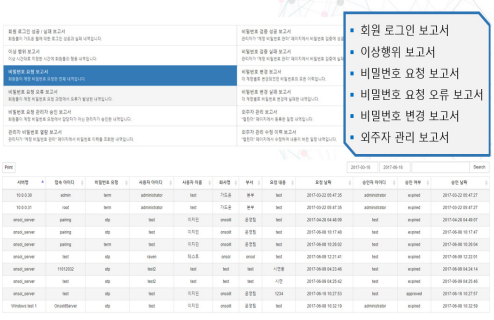
내용 로그, 신규 계정의 동기화 기능 등을 제공한다 [12,14,15,16,18].

[Fig. 12] Account Registration



[Fig. 13] Data Migration Template

2.5 보고서 제공 기능



[Fig. 14] Reporting

설계된 계정 관리 시스템은 다양한 형태의 보고서를 제공하여 안정되고 일관된 계정 관리 시스템을 운영하도록 하였다.

〈Table 2〉는 설계된 시스템을 실무 업무에 적용하기 위한 단계적인 내용들로 IoT 보안 서비스 터미널 제작, 계정관리 Master 임베디드 S/W 개발, 제조사 및 모델별 PW관리 S/W 모듈, 원격 시스템 구축 순으로 개발하였다.

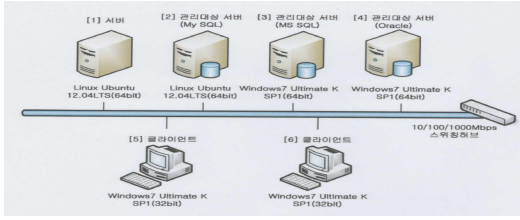
〈Table 2〉 System Customizing Stage

Modules	Description	Stage
IoT security service terminal development	CCTV, Wifi 등 IoT account management service service terminal	Embedded terminal H/W
Account management Master Embedded S/W	Customizing for account management service terminal	Customizing
PW mana- gement S/W module for each vendor models	PW mana- gement S/W module for each major vendor models -) module for updating	Customizing
Build-up remote system	Remote download system development Remote Maintenance system	management & maintenance

3. 성능 평가

제안 시스템의 성능 평가는 정보통신기술협회 소프트웨어 시험인증연구소에서 수행하였으며 안정되고 효율적인 평가 결과를 도출하였다.

3.1 실험 환경



[Fig. 15] Performance Evaluation Model

3.2 시나리오 및 측정 항목

1) 시나리오 1

10초간 일회용 비밀번호(OTP) 발급 시 서버와 클라이언트의 자원 효율성 측정

2) 시나리오 2

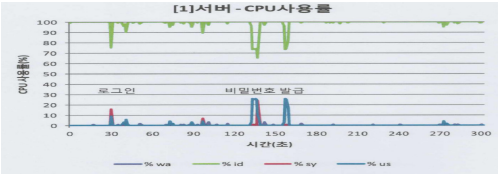
각 관리대상 서버(My SQL, MS SQL, Oracle)별 접속 정보 조회 시 서버와 클라이언트의 자원 효율성 및 클라이언트의 시간 효율성 측정

〈Table 3〉 Performance Test Item

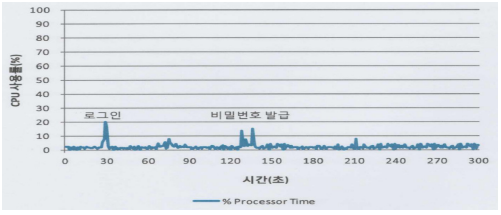
Item	Unit	Description	
CPU Usage	%	%Processor Time	Time Ratio for executing non-idle thread
		%usr	Time Ratio for executing threads in user mode
		%sys	Time Ratio for executing threads in system mode
		%wio	Wait Time Ratio until I/O ends
		%idle	Time Ratio during the system is idle
Memory Amount	MB	Private Mbytes	Average memory amount in the system
Response Time	sec	Time from executes a command to return the results	

3.3 성능 평가 결과

1) 시나리오 1



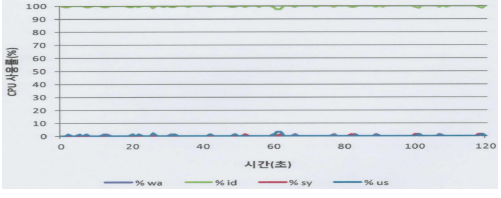
[Fig. 16] CPU Usage Ratio(Server)



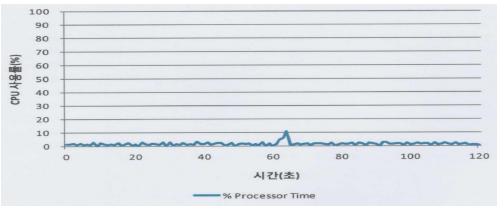
[Fig. 17] CPU Usage Ratio(Client)

서버와 클라이언트 모두 제안 시스템의 운영 시 안정적인 CPU 사용률을 보였다. 비밀번호 발급 시 CPU 사용률이 일시적으로 증가되지만 전반적으로 시스템 운영에 미치는 영향은 미비하다.

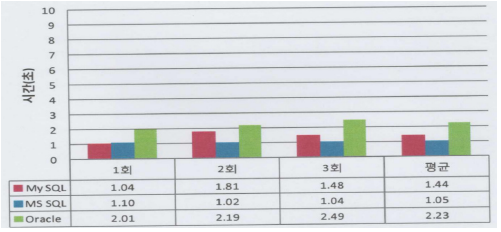
2) 시나리오 2



[Fig. 18] CPU Usage Ratio(Server)



[Fig. 19] CPU Usage Ratio(Client)



[Fig. 20] Response Time(Client)

시나리오 1보다 서버와 클라이언트 모두 제안 시스템의 운영 시 안정적인 CPU 사용률을 보였다. 클라이언트에서의 각 서버별 응답 시간도 평균 1-2 초의 결과를 도출하였으며 제안 시스템의 운영에 따른 영향은 거의 없다고 볼 수 있다.

〈Table 4〉는 기존의 주요 계정 관리 시스템과 제안한 시스템을 주요 기능별로 비교한 결과이다. 비밀번호 일괄 변경과 동기화 기능 및 웹을 이용한 관리 기능들은 공통적으로 제공하지만 다채널 비밀번호 발급 기능, 외주자 스케쥴링 및 접근 관리 기능 등은 제안된 시스템에서만 제공 가능한 기능들로 계정 관리 시스템을 보다 효율적으로 운영할 수 있다.

〈Table 4〉 Comparison with the major vendor S/W

Function	The major vendor S/W	The designed S/W
Batch process for password changing	O	O
Sync. for the management system with the password	O	O
Web Management	O	O
Multi-channel the password Issue	X	O
Visitor scheduling	X	O
Visitor Access Management(OTP Issue)	X	O

4. 결론

사물인터넷의 발달에 따라 IOT 장비의 보안 중요성이 높아지고 있으며 다수의 IP 카메라, 홈 IOT 장비, 다양한 측정 장비 등의 계정 관리는 IOT 보안의 기본적인 영역이 되었다.

본 논문에서는 사물인터넷 상에 사용될 수 있는 다양한 장비들의 계정 관리를 체계적으로 설계하여 사용자에게 업무 효율을 높일 수 있는 시스템을 제안한다. 실무에서 광범위하게 활용될 수 있는 기능을 6 가지로 도출하고 이에 대한 체계적인 설계를 수행하였다.또한 개발된 결과는 적용 업무나 상황에 맞도록 커스터마이징하여 활용되고 있다. 제안 시스템의 안정성과 보안성을 검증하기 위해 권위있는 기관의 인증 테스트를 실시하였으며 각 시나리오 별로 다양한 평가 항목에서 모두 안정적인 결과를 보였다.

앞으로 IOT 보안 위해 요소들을 유기적으로 감시하고 대처할 수 있는 AI 기술을 적용한 스마트 계정 관리 시스템을 개발하는 것이 향후 연구 과제이다.

REFERENCES

[1] IoT Proliferation Strategy, Government-related Ministry Joint Report, 2015.12.

[2] “Analyzing the domestic CCTV industry environment through CCTV system technology and marketability analysis,” CCTV News interview, Park Se-hwan (Korea Institute of Science and Technology Information), 2015.08.

[3] Internet of Things(Concepts, Implementation and Business), H. Kim, Hongrung Publishing, 2018.

[4] C. Lee. C. Choi, A Simple Cost Analysis of Host ID-LOC Separating protocol using SDN Features, JKIOTS, Vol.2, No.4, pp.41-47, 2016.

[5] K. Lee, A Design on Learning Model using Triz on Project-based Learning in IOT, JKIOTS, Vol.5, No.3, pp.29-35, 2019.

[6] S. Lee, An Analysis of Software Development Process Based on Software Engineering in IOT Environment, JKIOTS, Vol.6. No.1, pp.25-31, 2020.

[7] A. Montazerolghaem, M. Yaghmaee, Load-balanced and QoS-aware Software-defined Internet of Things

[8] H. Lim C. Choi, A Design on Error Tracking System for Enhanced-Reliable IOT Service, JKIOTS, Vol.6. No.3, pp.15-20, 2020.

[9] https://www.opennetworking.org

[10] JavaScript(https://ko.wikipedia.org/wiki/JavaScript)

[11] TypeScript(https://ko.wikipedia.org/wiki/TypeScript)

[12] React.js(https://ko.wikipedia.org/wiki/React.js)

[13] Node.js(https://ko.wikipedia.org/wiki/Node.js)

[14] JSX(https://ko.wikipedia.org/wiki/React.js)

[15] GraphQL(https://ko.wikipedia.org/wiki/GraphQL)

[16] MariaDB(https://ko.wikipedia.org/wiki/MariaDB)

[17] Docker(https://ko.wikipedia.org/wiki/Docker)

[18] Git(https://ko.wikipedia.org/wiki/git)

최 창 원(Chang-Won Choi) [종신회원]

- 1990년 2월 : 고려대학교 전산과학과 졸업(학사)
- 1992년 2월 : 고려대학교 전산과학과 졸업(석사)
- 1995년 2월 : 고려대학교 전산과학과 졸업(박사)
- 1996년 ~ 현재 : 한신대학교 컴퓨터공학부 교수

〈관심분야〉
유무선 네트워크, 시스템 분석, 사물인터넷

정 현 철(Hyeon Cheol-Jeong) [정회원]

- 1993년 2월 : 동국대 경영학과 졸업(학사)
- 1993년 3월 : 현대
- 2002년 3월 : 한국핫빗트
- 2007년 3월 ~ 현재 : 온솔아이티 대표이사
- 교육 : 네트웍, 보안, 솔루션 등

〈관심분야〉
보안, 시스템 분석, 사물인터넷, 솔루션