KNOM Review '17-02 Vol.20 No.02
https://doi.org/10.22670/knom.2017.20.2.44

매쉬업 프레임워크를 이용한 화학실험실 안전관리 매쉬업 서비스 개발

이응기◆, 김현우*, 주홍택°

Development of Mash-up Service for Chemical Laboratory Safety Management using Mash-up Framework

Eunggi Lee◆, Hyunwoo Kim*, Hongtaek Ju°

요 약

최근 발생하는 화학실험실 내의 사고사례들을 살펴보면 다양한 원인으로 인해 안전사고가 발생한다. 이러한 화학실험실 내의 안전사고를 예방하고 피해를 줄이기 위해서는 자동화된 안전관리 서비스가 필요하다. 그러나 자동화된 안전관리 서비스를 구현하기 위해서는 몇 가지 문제가 해결되어야 한다. 본 논문에서는 이 문제들을 해결하기 위하여 매쉬업 프레임워크(Mash-up Framework)를 이용한 화학실험실 안전관리 매쉬업 서비스를 개발하였다.

본 논문은 화학실험실 안전관리 매쉬업 서비스를 개발하기 위하여 서비스 시나리오, 구성도, 시퀀스 다이어그램을 설계하였다. 본 논문은 이러한 설계를 바탕으로 매쉬업 프레임워크와 다양한 외부 서비스들을 이용하여 화학실험실 안전관리 매쉬업 서비스를 구현하였다. 그리고 이를 검증하기 위해 앞서 설계한 서비스 시나리오에 적용하여 각각의 시나리오에 따른 결과들을 확인하였다.

Key Words : Mash-up Framework, Open IoT Platform, Open API

ABSTRACT

Recent data on careless accidents in laboratories show that they have various causes. Therefore, automated safety management services are needed to prevent accidents and reduce damage in chemical laboratories. However, developing automated safety management services has some problems. In this paper, to solve these problems, we developed Mash-up Service for Chemical Laboratory Safety Management using Mash-up Framework. We designed service scenario, architecture, and sequence diagram to develop Mash-up Service for Chemical Laboratory Safety Management. Based on these designs, this paper implemented the Mash-up Service using Mash-up Framework and a variety of external services. In order to validate this implementation, we applied the service scenario designed before, and confirmed whether the results are appropriate for each scenario.

※ 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업이며(2015R1D1A1A01059786), 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2015-0-00274, (ICBMS-2 세부) ICBMS 플랫폼 간 정보모델 연동 및 서비스 매쉬업을 위한 스마트 중재 기술 개발)
◆ First Author : Keimyung University Department of Computer Engineering, leggod1004@stu.kmu.ac.kr
° Corresponding Author : Keimyung University Department of Computer Engineering, juht@kmu.ac.kr
* Keimyung University Department of Computer Engineering, hwkim84@kmu.ac.kr
논문번호 : KNOM2017-02-08, Received December 1, 2017; Revised December 13, 2017; Accepted December 17, 2017

Ⅰ. 서 론

1.1. 연구 배경 및 문제정의

최근 발생하는 화학실험실 내의 안전사고에 대한 자료들을 살펴보면 대부분의 사고들이 화학 실험자의 부주의로 인해 발생하는 것을 볼 수 있다[1,2]. 이외에도 허가되지 않은 화학물질 사용이나 도난에 의한 화학 안전사고도 적지 않게 발생한다. 또한 이렇게 발생한 화학 안전사고가 사고원인 파악과 초동조치가 늦어지는 바람에 2차 사고로 이어져 더 큰 피해를 낳게 된다[3]. 그래서 여러 기관들이나 실험실에서는 화학 안전사고로 인한 인명, 재산 피해를 줄이기 위하여 화학 안전사고 발생 방지를 위한 교육 및 지침서들을 마련하여 실시하고 있으나, 이는 정보 공유나 교육 목적으로 개발되어 사고에 직접적인 대처를 할 수 없다.

위와 같은 화학 안전사고가 발생할 시 직접적인 대처를 위해서는 자동화된 안전관리 서비스가 필요하다. 자동화된 안전관리 서비스에는 다음과 같은 기능 요구된다. 우선, 화학 실험자가 위험 화학물질을 다룰 때 화학물질에 대한 정보와 주의사항을 실험자에게 전달해줘서 실험자의 부주의로 인한 사고를 예방해야한다. 그리고 위험 화학물질이나 위험 실험기구에 접근을 제어하여 도난에 의한 사고를 예방해야 한다. 그리고 화학 안전사고가 발생했을 때 이를 감지하고 관리자와 주변 사람들에게 대피하도록 알려 빠른 초동조치와 2차 사고를 방지할 수 있어야 한다.

그러나 이러한 자동화된 안전관리 서비스를 마련하려면 몇 가지 문제점들이 있다. 첫째, 화학물질 정보안내를 위한 방대한 양의 화학물질 정보를 구축해야 된다. 화학물질은 그 종류가 매우 다양할 뿐만 아니라 혼합물들의 정보까지 포함할 경우 그 수는 헤아릴 수 없다. 둘째, 하나의 자동화된 안전관리 서비스는 여러 개의 실험실에, 여러 위치의 다양한 종류의 센서들을 효율적으로 관리해야 한다. 화학 안전사고를 탐지하는 센서들은 다양한 상황에서 발생하는 화학 안전사고를 놓치지 않고 탐지해야 하기 때문에, 센서의 위치나 분포정도가 탐지능력에 큰 영향을 끼친다. 또한 센서의 작동상태를 지속적으로 확인하여 서비스의 지속성을 확보해야한다. 셋째, 화학실험실이나 보관 장소에 권한이 없는 비허가자의 위장출입을 방지해야한다. 출입 제어 기술에 보편적으로 사용되고 있는 ID카드나 비밀번호를 이용한 출입제어 방식은 ID카드와 비밀번호 도용에 의해 쉽게 보안이 위협될 수 있다.

1.2. 연구목표 및 해결방안

본 논문의 연구목표는 화학실험실에서 발생할 수 있는 안전사고를 예방하고, 사고발생 시 신속한 조치를 취할 수 있도록 하는 자동화된 안전관리 서비스를 설계하고 개발하는 것이다. 이 절에서는 이러한 연구목표를 달성하기 위해 이전 절에서 제시한 안전관리 서비스 자동화의 문제점들에 대한 해결방안을 제시한다.

첫째, 방대한 양의 화학물질에 대한 정보를 제공하기 위해서는 '공공데이터포털[4]' 에서 제공하는 MSDS(Material Safety Data Sheet, 물질 안전 보건 자료) Open API를 사용한다. MSDS는 화학물질에 대한 정보를 위험성, 취급방법, 주의사항, 사고 시 대처방안 등의 항목으로 세분화하여 정리함으로써 화학물질로 인한 사고가 발생하지 않도록 하기 위한 자료이다. MSDS는 현재 공공데이터 포털에서 누구든지 접근할 수 있게 Open API로 제공되고 있다. 이 MSDS Open API를 사용하면 방대한 양의 화학물질에 대한 정보를 직접 구축하지 않고도 화학물질 정보를 쉽게 활용할 수 있다.

둘째, 화학 안전사고를 탐지하기 위한 다양한 종류의 센서들을 효율적으로 관리하기 위해서 Open IoT 플랫폼인 IoTivity[5]를 사용한다. IoTivity는 다수의 IoT 디바이스들을 운영체제나 네트워크 프로토콜에 구애받지 않고 연결할 수 있는 Open IoT 플랫폼이다. 현재 IoTivity는 에디슨, 아두이노와 같은 하드웨어뿐만 아니라, 우분투, 타이젠, 안드로이드와 같은 소프트웨어 플랫폼도 지원하고 있으며 지속적으로 그 지원범위를 넓혀가고 있다. 그렇기 때문에 다양한 종류의 센서 디바이스를 연결해야하는 서비스를 개발하기 위해서라면 IoTivity를 사용해서 개발하는 것이 적합하다.

셋째, 화학실험실이나 화학물질 보관 장소에 권한이 없는 비허가자의 위장출입을 막기 위해서는 안면인식 Open API를 활용하여 2단계 인증방법을 사용한다. 기존 출입제어 시스템에 많이 사용되던 비밀번호나 ID카드는 비밀번호가 유출되거나 ID카드가 분실될 경우 보안에 큰 위협이 될 수 있다. 그렇기 때문에 최근 출입제어 시스템 시장에는 생체인식을 이용한 출입제어 시스템이 많이 사용되고 있다. 생체인식은 사람마다 각기 다른 생체 정보를

이용한 인식방법으로 복제나 분실의 위험이 없기 때문에 높은 수준의 보안을 요구하는 시스템에서 많이 사용된다. 생체인식 방법으로는 홍채, 망막, 지문, 손금, 안면, 음성 등이 있다. 홍채나 망막을 이용한 생체인식 방법은 정확도는 높으나 센서의 가격이 비싸고, 사회적 수용성이 낮다. 지문이나 손금을 이용한 생체인식 방법은 정확도도 높고 가격도 저렴한 편이며 사회적 수용성도 높다. 하지만 심한 노동으로 지문이 닳거나 피부의 건습도, 상처, 이물질 등의 요인으로 인식이 어려운 경우가 많다. 안면을 이용한 생체인식 방법은 정확도는 다소 떨어지지만 사회적 수용성이 높고 서비스를 제공하는데 가격도 저렴하다. 하지만 안면을 이용한 생체인식 방법은 환경이나 목적에 따라 안면인식을 위한 데이터를 학습시켜야하며 이를 개발하기 위한 비용이 많이 든다. 이때 안면인식 서비스를 Open API를 이용하면 학습이나 개발에 필요한 비용을 절감할 수 있다. 그래서 본 논문에서는 가격대비 성능이 우수하고 사회적 수용성이 높은 안면인식 Open API를 사용하면서 동시에 ID카드를 사용하여 안면인식의 단점인 정확도를 높이고자 한다. 이렇게 하면 ID카드를 이용하여 출입권한 인증을 하고 안면인식 Open API를 이용하여 ID카드의 소지자와 출입자가 동일인물인지 비교함으로써 ID카드 도난으로 인한 위장출입을 방지할 수 있다.

1.3. 연구내용

이 절에서는 이전 절에서 제시한 문제점과 해결방안을 바탕으로 어떻게 자동화된 안전관리 서비스를 설계하고 개발할지에 대한 방향에 대해 설명 한다.

이전 절에서는 화학실험실 안전관리 서비스 자동화의 문제점을 해결하기 위해서 MSDS Open API와 얼굴인식 Open API 그리고 IoTivity Open IoT Platform를 이용하는 방법을 제시했다. Open API는 서비스 개발자가 개발하고자하는 서비스의 기능을 구현하기 위한 특수한 기술이 없더라도 손쉽게 서비스를 구현할 수 있도록 지원해주는 프로그램이다. 그래서 Open API를 사용하면 서비스 개발에 필요한 비용과 인력을 절감할 수 있다. Open IoT Platform 또한 IoT 서비스를 개발하는데 필요한 다양한 기능을 제공하여 개발 비용을 절감할 수 있게 해준다. 그러나 이러한 Open API나 Open IoT Platform들은 해당 서비스를 제공해주는 기관이나 회사마다 메시지의 형식이나 프로토콜이 제각각이라서 이러한 서비스들을 연계해서 새로운 서비스를 개발하기 위해서는 메시지를 통합하고 연계하기 위한 추가적인 노력이 필요하다. 개발비용을 줄이기 위한 이점이 오히려 개발비용을 증가시키는 단점이 될 수 있는 것이다.

그래서 본 논문에서는 자동화된 화학실험실 안전관리 서비스를 개발하기 위해 매쉬업 프레임워크(Mash-up Framework)를 이용하여 Open API들을 효율적으로 사용하고자 한다. 매쉬업 프레임워크는 2가지 이상의 서로 다른 서비스들을 조합하여 새로운 서비스를 만들 수 있도록 하는 프레임워크로서, 여러 개의 어댑터(Adaptor)와 이 어댑터들 간의 메시지를 중계해주는 메시지 라우터(Message Router), 프레임워크의 보안을 관리하는 Security Manager, 사용자와 프레임워크사이의 인터페이스인 Mash-up Framework Open API로 구성된다. 이 매쉬업 프레임워크를 사용하면 서로 다른 메시지 형식과 프로토콜을 사용하는 서비스들을 연계하여 새로운 서비스를 개발할 수 있다.

그래서 본 논문에서는 화학실험실 안전관리 서비스를 자동화하기 위해 Open API와 Open IoT Platform을 이용하고 이들을 연계하기 위해 매쉬업 프레임워크를 이용하여 화학실험실 안전관리 매쉬업 서비스를 개발하고자 한다.

이후 본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해서 설명한다. 3장에서는 화학실험실 안전관리 매쉬업 서비스를 개발하기 위한 시나리오, 구조도 설계, 시퀀스 다이어그램에 대해 설명한다. 4장에서는 화학실험실 안전관리 매쉬업 서비스의 구현에 대한 방법과 기술에 대해 설명하고 이를 검증한다. 마지막으로 5장에서는 결론 및 향후 연구에 대해서 논의한다.

Ⅱ. 관련 연구

이 장에서는 화학실험실 내의 안전사고 사례와 안전관리 시스템, 출입제어 시스템, 매쉬업 프레임워크에 관련된 기존 연구들에 대해 논의한다.

2.1. 화학실험실 사고 사례

장유리 등[1]은 기존 가스 누출에 의한 피해 분석 연구들은 플랜트나 충전소와 같이 사용하는 화학물질의 양이 많은 대상을 위주로 연구하여 일반 실험실의 피해 영향과는 차이가 있음을 지적했다. 그래서 장유리 등은 실험실에서 주로 사용하는 화학 물

질들을 선정하여 이 물질들이 누출 되는 시나리오를 가지고 피해 정도를 예측하여 위험성에 대한 평가를 하였다.

이태형 등[2]은 기존 실험실에서 발생한 사고 관련 연구들은 화재나 폭발과 같은 안전사고의 예방이나 대책을 위한 연구에 초점이 맞추어져있어 화학사고의 발생 유형이나 원인 등과 관련된 연구는 미진함을 지적하였다. 그래서 이태형 등은 2013년부터 2015년까지 국내 화학실험실에서 발생한 화학사고의 유형, 원인, 기관현황, 사고 물질 등을 분석하여 화학사고 예방대책 수립을 위한 기초자료를 제공하고자 하였다.

정경삼과 백은선[3]은 유해화학물질 취급장에서 발생하는 화학사고의 발생 원인에 대해 관련 제도나 안전관리 실태 등으로 다양한 방면에서 문제점을 분석하였다. 그래서 해당 논문에서는 유해물질 화학사고 발생을 방지하기 위한 제도개선, 취급시설 개선, 안전관리 개선 등의 방법을 제시하여 설명한다.

화학실험실 안전사고 사례에 관련된 기존 연구들[1-3]은 사업장과 같은 대상 뿐 아니라 규모가 작은 실험실에서 발생하는 화학사고의 경우에도 관련 연구도 좀 더 활발히 진행되어야함을 강조하였다. 그리고 화학실험실 사고 발생의 가장 큰 원인인 실험자의 부주의에 대한 대응책의 필요성과, 사고발생 시 초기대응의 중요성에 대해서도 설명하고 있다.

2.2. 안전관리 서비스

김범수 등[6]은 산업현장에서 유해화학물질 누출 사고 발생 시 누출 사업장의 환경과 화학물질의 정보 등을 파라미터로 하여 수학적 모델에 적용 하여 화학물질 확산 시뮬레이션을 개발하였다. 이 시뮬레이션 프로그램은 기존 소프트웨어 보다 저렴한 비용으로 사용할 수 있도록 개발하는데 초점을 맞추고, 비전문가도 사용하기 쉽도록 간단한 UI와 3D 도면으로 개발하여 실제 사업장 외에도 학교나 연구기관에서 교육목적으로도 사용이 가능하도록 개발하였다.

장하용 등[7]은 국내의 위험유해물질 사고관련 대응 업무가 다양한 부처에 분산되어있고 네트워크 기반의 통합관리체계가 구축되어있지 않고, 각 부처의 데이터들은 사고 대응데이터 중심으로 비표준, 비정형 상태로 유지되고 있어 사고발생시 신속하고 정확한 사고대응이 어려움을 지적하였다. 그래서 장하용 등은 국내의 위험유해물질관련 사고데이터를 고품질화 및 표준화하여 화학사고 발생 시 신속하고 합리적인 대응을 결정하도록 지원하고, 여러 부처 간의 체계적인 사고관리가 가능한 사고이력관리 시스템(HATS)을 개발하였다.

Ryu 등[8]은 과거 국내에서 발생한 위험유해물질 사고들의 사례를 분석하여 다음과 같은 국내 사고 대응시스템의 문제점을 지적하였다. 첫째, 유해물질 사고에 특화된 시스템이나 장비가 없다. 둘째, 사고 대응 매뉴얼은 신속하고 정확한 의사를 결정하는데 꼭 필요하다. 셋째, 위험유해물질 사고대응시스템은 통합관리 돼야 한다. Ryu 등은 이러한 문제점을 바탕으로 국내에 위험유해물질 통합 관리 시스템 개발이 고려되어야 한다고 설명했다.

안전관리 서비스에 관련된 기존 연구들[6-8]은 화학 사고에 대응하기 위한 안전관리 서비스의 통합 및 자동화의 필요성에 대해 설명하고 이를 구현하고자 하였다. 안전관리 서비스의 자동화는 사고 대응에 대한 결정에 신속하고 정확한 판단을 유도하여 인명 및 재산 피해를 최소화 할 수 있기 때문이다.

2.3. 매쉬업 프레임워크

Kim 등[9]은 두가지 이상의 서비스를 매쉬업하여 새로운 서비스를 만들 때 여러 서비스를 효율적이고 쉽게 연계하기 위한 매쉬업 프레임워크를 설계하였다. 매쉬업 프레임워크는 한두 개의 서비스를 연계하여 서비스를 만들 때 보다는 많은 서비스들이 연계된 복잡한 매쉬업 서비스를 생성하는데 개발비용을 줄여주는 프레임워크이다. Kim 등은 제안한 매쉬업 프레임워크의 타당성을 평가하기 위해 CSMMS(Campus Safety Management Mash-up Service)에 대한 시나리오를 설계하여 검증하였다.

김현우 등[10]은 출입자 관리 서비스를 개발하기 위한 매쉬업 프레임워크를 EIP(Enterprise Integration Patterns)을 기반으로 하여 설계하였다. 매쉬업 서비스에서 연계하는 다양한 서비스들을 EIP의 엔드포인트(Endpoint)로 표현하여 이 엔드포인트들 간에 주고받는 메시지를 변환, 라우팅 등 다양한 기법을 통해 처리하고자 하였다.

2.4. 출입자 제어 서비스

Lee 등[11]은 매쉬업 프레임워크를 이용한 출입자 제어 서비스를 개발하였다. 이 출입자 제어 시스템은 ID 카드와 얼굴인식 기술을 이용한 2단계 인증 방법을 사용함으로써 도용카드를 이용한 위장출입자

를 방지 하고자 하였다. 또한, 얼굴인식 기술 중 식별(Identification) 기능만을 사용하여 출입자를 인증하는 방법과 검증(Verification)기능과 ID카드를 연계하여 인증하는 방법을 비교하여 검증 기능을 이용한 방법이 응답속도와 신뢰도에 있어 이점이 있음을 보였다.

Kwon 등[12]은 컨테이너(Container) 기반의 출입자 제어 매쉬업 서비스의 테스트베드를 설계하고 개발하였다. 해당 논문에서는 출입자 제어 매쉬업 서비스의 메시지 라우터와 어댑터 등을 컨테이너 기반으로 개발하여 모듈화 하였다. 그래서 이 컨테이너들을 출입자 제어 매쉬업 서비스의 테스트베드를 한 번에 빌드, 실행, 테스트, 로그모니터 할 수 있도록 스크립트를 설계함으로써 컨테이너들을 통합 관리 하고자 하였다.

매쉬업 프레임워크를 설계한 기존 연구들[9-12]은 여러 가지 서비스를 연계하여 개발할 때 발생하는 메시지의 복잡성 문제나, 개발비용의 문제를 해결하기 위하여 매쉬업 프레임워크를 설계하였다. 그리고 이 매쉬업 프레임워크를 이용하여 매쉬업 서비스를 개발한 기존 연구들은 기존의 단일 서비스가 가지는 문제점들을 서비스 매쉬업을 통해 해결하고자 하였다.

본 논문에서는 화학 사고를 예방하고 사고 발생 시 신속하고 정확한 대응을 할 수 있도록 하는 자동화된 화학실험실 안전관리 매쉬업 서비스를 개발하고자 한다. 이 화학실험실 안전관리 매쉬업 서비스는 여러 가지 기능들을 Open API 서비스를 이용하여 개발함으로써 개발비용을 줄이고, 여러 가지 서비스를 연계할 때 생기는 복잡성의 문제를 매쉬업 프레임워크를 이용하여 개발함으로써 해결하고자 한다.

Ⅲ. 서비스 설계

이 장에서는 화학실험실 안전관리 매쉬업 서비스의 시나리오, 요구사항, 시스템 구성도 설계에 대해서 설명을 한다. 화학실험실 안전관리 매쉬업 서비스를 구현하기 위해서 먼저 서비스 시나리오를 설계하고 기능 요구사항을 도출했다. 도출된 서비스 기능 요구사항을 바탕으로 시스템 구성도 설계를 하였다.

3.1. 서비스 시나리오 설계

화학실험실 안전관리 매쉬업 서비스 시나리오는

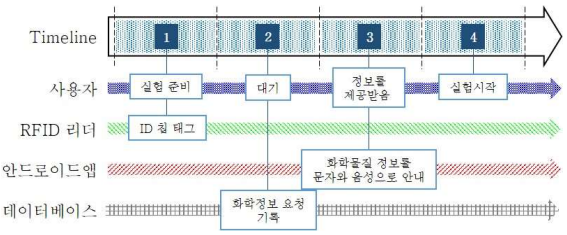

그림 1. 화학물질 정보 안내 시나리오 타임라인
Fig. 1. Chemical Information Guide Scenario Timeline

화학물질 안내 시나리오, 화학사고 감지 및 알람 시나리오, 출입자 제어 시나리오 세 가지가 있다.

그림 1은 화학물질 안내 시나리오는 화학 실험자의 부주의로 인한 사고를 줄이기 위하여 화학물질 사용직전에 화학물질에 대한 정보를 실험자에게 안내하여 화학물질의 유해성이나 위험성에 대해 다시 한 번 상기시키기 위한 시나리오이다. 타임라인 1에서 사용자는 사용하고자 하는 시약병에 붙은 RFID 태그를 흄후드나 실험대에 위치한 RFID 리더기에 인식시켜 이벤트를 발생시킨다. 타임라인 2에서 이 벤트는 화학실험실 안전관리 매쉬업 서비스에 의해 처리되고, 타임라인 3에서 안드로이드 어플리케이션을 통해서 음성과 글로 사용자에게 전달된다. 사용자에게 전달되는 정보에는 화학물질에 관한 정보, 유해성, 주의사항, 응급조치요령 등이 포함되어있다. 타임라인 4에서는 사용자가 전달받은 정보를 가지고 주의하며 실험을 시작한다.

그림 2는 같이 화학사고 감지 및 알람 시나리오는 화학사고가 발생하거나 위험이 감지될 시에 관리자와 사용자들에게 사고사실을 알려 초동조치가 가능하도록 하기 위한 시나리오이다. 타임라인 1에서 실험대나 화학물질 보관함에 위치한 화학사고 감지 센서에 화학사고가 감지되면 이벤트가 발생한다. 타임라인 2에서 이벤트는 화학실험실 안전관리 매쉬업 서비스에 의해 처리되고, 타임라인 3에서 사고가 발생한 장소의 관리자나 실험 담당자에게 문

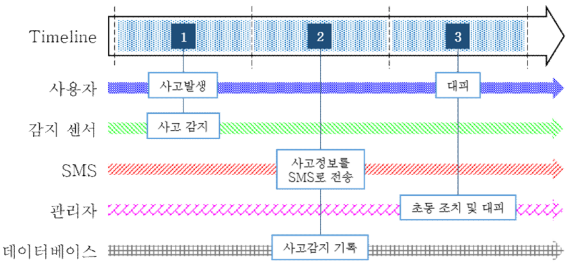

그림 2. 화학사고 감지 및 알람 시나리오 타임라인
Fig. 2. Chemical accident detection and alarm scenario timelien

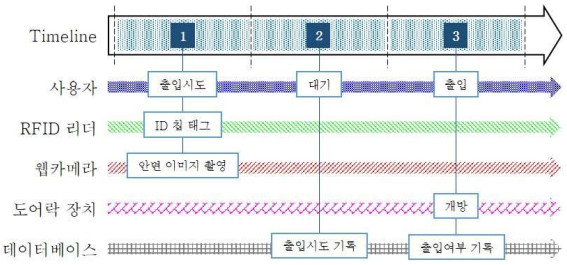

그림 3. 출입자 제어 시나리오 타임라인
Fig. 3. Access control scenario timeline

자 메시지로 사고 내용을 알린다. 동시에 사고 장소에는 경보기가 울려 주변에 사고가 났음을 알리고, 관리자는 초동조치를 실시한다.

그림 3은 출입자 제어 시나리오는 고위험 화학물이 보관된 장소나 위험한 실험을 하는 실험실의 출입을 제어함으로써 권한이 없는 사용자의 접근을 차단하고, 화학물질의 도난을 예방하여 화학사고의 발생을 예방하는 시나리오이다. 타임라인 1에서 사용자가 출입을 하기 위해서는 RFID칩이 내장된 카드를 RFID 리더기에 태그를 해야 한다. RFID 칩이 태그 됨과 동시에 카메라를 통해 출입자의 안면 이미지가 촬영된다. 타임라인 2에서 RFID 칩의 ID값과 출입자의 안면 이미지는 화학실험실 안전관리 매쉬업 서비스에 의해 출입자의 출입권한을 확인한다. 타임라인 3에서 출입권한 결과에 따라 출입문의 잠금장치가 열리거나 잠겨 사용자의 출입을 통제한다. 출입 거부 시 출입 시도 사실은 관리자에게 문자 메시지로 전달이 된다.

3.2 서비스 시스템 구성도 설계

이전 절에서 도출된 서비스 요구사항을 기반으로 그림 4와 같은 화학실험실 안전관리 매쉬업 서비스의 구조도를 설계했다. 이 구조도는 이승기 등[13]에서 설계한 화학실험실 안전관리 매쉬업 서비스를 이전 절에서 도출한 시나리오와 요구사항에 따라 필요한 기능들을 추가 및 변경하고, 메시지 중계와 Route 설정을 위해 매쉬업 프레임워크를 적용하여 재설계 하였다.

매쉬업 서비스는 크게 외부서비스, 어댑터, 메시지라우터로 나누어진다. 외부서비스는 IoTivity와 Non-IoT Device, MongoDB[14], Cool SMS[15], Face++[16], OKTA[17], MSDS 총 7가지를 사용한다. IoTivity는 1장에서도 설명했듯이 IoT 디바이스를 효율적으로 관리하기 위한 Open IoT Platform이

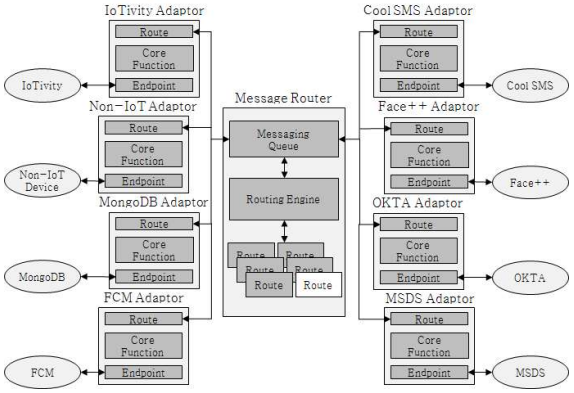

그림 4. 화학실험실 안전관리 매쉬업 서비스 구성도
Fig. 4. Chemical laboratory safety management mash-up service architecture

다. Non-IoT Device는 IoTivity에서 지원하지 않는 Device를 제어하기 위한 어댑터이다. 본 논문에서는 출입자의 안면 이미지를 촬영하는 카메라를 제어하기 위해서 Non-IoT 어댑터를 사용한다.

MongoDB는 NoSQL 데이터베이스로 분류되는 문서지향 데이터베이스로서 화학실험실 안전관리 매쉬업 서비스에서 발생하는 모든 이벤트들을 기록할 뿐만 아니라, 여러 가지 서비스들로부터 처리되어 나온 메시지들도 모두 기록을 하기 위한 데이터베이스이다. 본 논문에서는 다양한 종류의 외부 서비스들과 서비스마다 다양한 기능이 사용되기 때문에 기록하고자 하는 메시지들의 형식이나 포맷이 달라서 하나의 테이블의 스키마로 정의하기가 어렵다. 또한 외부 서비스들의 업데이트로 메시지 형식이 바뀔 수 있기 때문에 일반 관계형 데이터베이스를 쓰기에는 부적합하다. 그래서 본 논문에서는 매쉬업 서비스의 다양한 메시지들을 기록하기 위하여 문서지향 데이터베이스인 MongoDB를 사용했다.

Cool SMS는 문자 메시지 전송을 위한 서비스로서 Open API를 통해 SMS를 전송할 수 있다. 본 논문에서는 화학 안전사고 발생 시 관리자나 사용자들에게 사고내용을 전달하기 위해 사용되었다.

Face++는 얼굴인식 관련 기능을 제공하는 Open API 서비스이다. Face++에서는 Face Recognition, Detection, Comparing, Searching 등 다양한 기능을 제공하고 있다. 본 논문에서는 출입자의 안면 이미지와 ID카드 소지자의 안면 이미지를 비교하기 위하여 Face Comparing 기능을 이용하였다.

OKTA는 사용자 관리, 그룹관리, 권한 관리 등을 위하여 사용하는 Open API 서비스이다. 본 논문에서 제안하는 서비스에서는 출입자의 권한을 관리하

고 출입자의 출입 권한을 확인하기 위하여 사용되었다. Cool SMS와 OKTA Open API는 매쉬업 프레임워크를 사용하는 이점을 최대로 발휘하기 위해 문자메시지 전송기능과 사용자 권한 관리 기능을 직접 구현하지 않고 Open API를 사용하여 구현했다.

MSDS는 '공공데이터포털'에서 제공하는 물질 안전 보건 자료로서 Open API를 이용하여 화학 물질의 정보를 요청할 수 있다. 본 논문에서 제안하는 서비스에서는 사용자에게 화학 물질을 사용하기 전 화학물질에 대한 정보를 확실하게 숙지하고 실험을 할 수 있도록 하기 위한 화학물질의 정보를 조회하기 위해 사용된다. FCM(Firebas Cloud Messaging)은 안드로이드나 iOS 모바일 디바이스로 메시지를 전송하기 위한 서비스이다. 본 논문에서 제안하는 서비스에서는 MSDS에서 조회한 화학물질에 대한 정보를 사용자에게 안드로이드 어플리케이션을 통해 전달하기 위해 사용 된다.

어댑터는 크게 Route와 Core Function, Endpoint로 분류된다. Route는 각 어댑터에서 제공하고자 하는 서비스들의 기능들을 분류하여 다른 어댑터나 사용자가 요청하여 사용할 수 있도록 하는 역할을 한다. Route가 요청되면 해당되는 서비스의 기능을 실행하기 위한 처리를 Core Function에서 처리한다. 이 Core Fuction은 서비스의 기능마다 입출력 데이터가 다르므로 각각의 어댑터들은 메시지를 처리하는 알고리즘이 서로 다르다. Endpoint는 각각의 서비스에 맞는 프로토콜에 따라 서비스와 통신하여 메시지를 분석하는 역할을 한다.

메시지 라우터는 Messaging Queue, Routing Engine, Route로 구성되어 미리 정의된 Route에 따라 매쉬업 서비스의 이벤트가 처리되도록 어댑터들 간의 메시지를 연계해주는 역할을 한다. Messaging Queue는 어댑터들로부터 오는 메시지나 어댑터로 보내는 메시지들의 통로 역할을 한다. Routing Engine은 이렇게 메시지 라우터로 온 메시지들을 메시지의 출발지와 도착지, 목적에 따라 분류하여 정해진 Route에 따라 실행될 수 있도록 하는 역할을 한다. Route는 매쉬업 서비스에서 제공하는 기능들을 수행하는데 필요한 외부서비스의 기능을 연계하여 정의해둔 집합이다.

3.3 서비스 시퀀스 다이어그램 설계

이 절에서는 이전 절에서 설계한 화학실험실 안전관리 매쉬업 서비스의 구성도에 따른 모듈들이

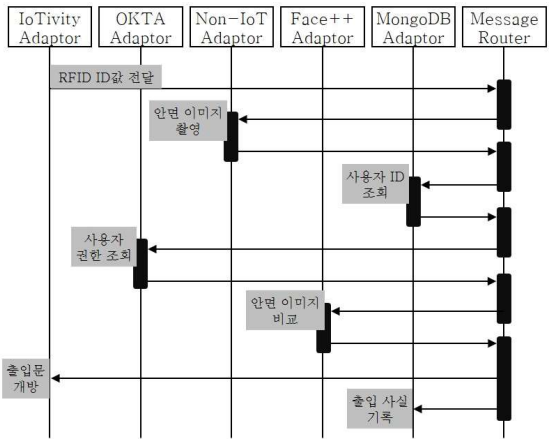

그림 5. 출입자 제어 시나리오 시퀀스 다이어그램
Fig. 5. Access control scenario sequence diagram

어떻게 동작하는지 시퀀스 다이어그램을 통해 설계를 검증한다.

그림 5는 본 논문에서 제안하는 매쉬업 서비스의 출입자 제어 시나리오의 시퀀스 다이어그램이다. 최초 IoTivity에 연결된 RFID 리더기로부터 RFID ID 카드가 태그되면 ID값은 메시지 라우터로 전달된다. 이때, 메시지 라우터로 출입자 제어 이벤트가 발생했으므로 그에 맞는 Route를 실행하게 된다. 메시지 라우터는 바로 Non-IoT 어댑터로 메시지를 보내 출입자의 안면이미지를 촬영하도록 한다. 촬영된 이미지의 저장경로는 메시지 라우터로 전달된다. 메시지 라우터는 RFID의 ID값으로 사용자 ID를 조회하기 위해 MongoDB 어댑터에 조회를 한다. 조회된 사용자 ID는 OKTA 어댑터로 전달되어 출입자의 권한을 질의한다. 이때, 만약 출입자의 권한이 없을 경우 Route는 종료되고 출입문은 개방되지 않는다. 하지만 출입자의 권한이 있을 경우 이전에 촬영된 출입자의 안면이미지와 ID 카드 소지자의 안면이미지 비교를 위해 Face++ 어댑터로 메시지가 전달된다. Face++로부터 두 이미지가 동일인물이라는 결

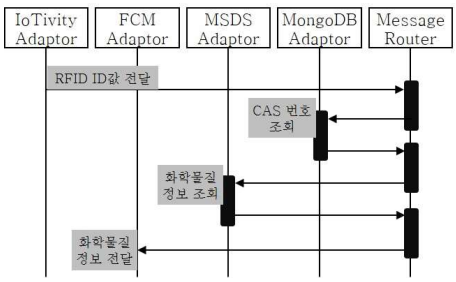

그림 6. 화학물질 정보 안내 시나리오 시퀀스 다이어그램
Fig. 6. Chemical information guide scenario sequence diagram

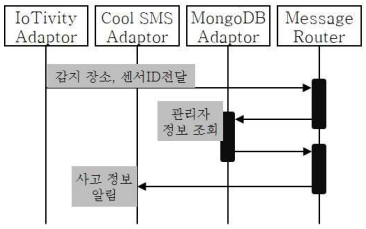

그림 7. 화학사고 감지 및 알림 시나리오 시퀀스 다이어그램
Fig. 7. Chemical accident detection and alarm scenario sequence diagram

과가 나올 경우 메시지 라우터는 IoTivity 어댑터로 메시지를 전달하여 출입문을 개방하도록 한다. 동시에 메시지 라우터는 MongoDB 어댑터로 메시지를 전달하여 출입자의 출입 사실을 기록한다.

그림 6은 본 논문에서 제안하는 매쉬업 서비스의 화학물질 정보 안내 시나리오의 시퀀스 다이어그램이다. 최초 사용자가 RFID 칩이 부착된 시약병을 리더기에 태그하면 이벤트가 발생한다. 태그된 RFID의 ID값은 메시지 라우터로 전달되어 알맞은 Route를 실행한다. 화학물질의 정보를 MSDS에 조회하기 위해선 CAS 번호나 화학물질의 이름을 알아야 하므로 MongoDB 어댑터로 전달되어 CAS 번호를 조회한다. 조회된 MSDS 화학물질 정보는 FCM 어댑터로 전달되어 사용자의 스마트 디바이스에 푸시 메시지를 전달하게 된다.

그림 7은 본 논문에서 제안하는 매쉬업 서비스의 화학사고 감지 및 알림 시나리오의 시퀀스 다이어그램이다. 화학실험실이나 화학약품 보관 장소에 배치된 센서들에 화학사고가 감지되면 해당 센서의 정보가 메시지 라우터로 전달되며 이벤트가 실행된다. 메시지 라우터는 감지된 화학사고의 정보를 관리자에게 전달하기 위해서 MongoDB 어댑터로 메시지를 전달하여 관리자의 정보를 조회한다. 조회된 관리자의 정보와 감지된 화학사고의 정보를 Cool SMS 어댑터로 전달하여 관리자에게 문자메시지를 전송하도록 한다.

Ⅳ. 구현 및 검증

이 장에서는 3장에서 설계한 화학실험실 안전관리 매쉬업 서비스를 어떻게 구현하였는지 설명하고, 사용자 인터페이스를 통해 서비스를 사용하는 방법을 설명함으로써 구현한 기능들을 검증한다.

4.1. 구현

4.1.1. 개발환경

화학실험실 안전관리 매쉬업 서비스의 메시지 라우터와 어댑터들은 도커(Docker)[18] 컨테이너 위에서 실행된다. 도커는 컨테이너 기반의 오픈소스 가상화 플랫폼으로 기존의 가상화 방식과는 다르게 프로세스를 격리시키는 리눅스 컨테이너 기술을 자동화 하여 쉽게 사용할 수 있게 하는 프로젝트이다. 도커에는 이미지라는 개념이 있는데, 이미지는 컨테이너를 실행하기 위한 모든 파일과 설정 값을 가지고 있는 것으로, 이 이미지를 실행(run)하면 컨테이너가 실행된다. 그런데 이렇게 실행된 컨테이너에 상태가 바뀌어도 이미지는 변하지 않고 유지되어 또 다른 컨테이너를 여러 개 실행시킬 수 있다. 또한 변경된 컨테이너는 변경된 파일이나 설정 값들을 가진 채로 새로운 이미지를 생성할 수 있다.
이러한 도커의 기능을 활용해서 하나의 이미지로 실행한 여러 컨테이너마다 각각 하나의 어댑터만 실행되도록 하여 각각의 어댑터를 개발할 때 동일한 환경에서 개발할 수 있게 하고, 개발 후 어댑터가 실행되는 컨테이너를 이미지화 하였다. 이렇게 이미지화 된 어댑터는 특정 어댑터로 트래픽이 몰려 과부화의 위험이 있을 경우 동일한 해당 어댑터의 이미지로 새로운 컨테이너를 실행하여 트래픽을 분산시켜 서비스를 유지시켜 준다.

4.1.2 IoTivity

IoTivity는 크게 Client와 Server로 구분된다. Client는 Server에 있는 자원(Resource)들을 GET, PUT, OBSERVE와 같은 명령을 통해 관리할 수 있다. GET 명령어는 Server가 가지고 있는 자원을 요청할 때 쓰는 명령어이고, PUT은 Client가 Server

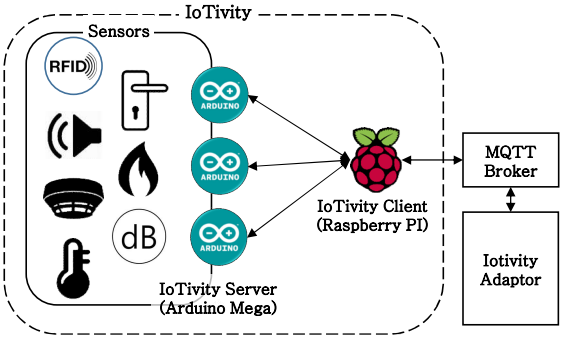

그림 8. IoTivity 개발 구조도
Fig. 8. IoTivity development structure

로 값이나 정보를 전달하여 Server의 상태를 변경하고자 할 때 사용한다. OBSERVE는 GET과 유사하나 한 번의 요청으로 지속적인 응답을 받음으로써 Server의 상태를 지속적으로 모니터링 하기 위한 명령어이다. IoTivity의 Client와 Sever는 항상 연결되어 있는 상태가 아니다. Client는 Server에게 요청 메시지를 전송하고 싶을 때 브로드캐스트 방식을 이용하여 Server를 찾아낸 후에 메시지를 전송한다. 이러한 특징 때문에 Server와 Client는 보통 같은 로컬네트워크 내에 위치하게 되어 통신한다.

본 논문에서 개발한 매쉬업 서비스의 IoTivity는 그림 7과 같은 구조로 개발되었다. 해당 구조도는 이응기 등[19]의 IoTivity 구조도를 재설계하여 발전시킨 것이다. Client는 Raspberry PI에서 실행된다. Raspberry PI의 운영체제는 Ubuntu Mate를 사용하였다. Ubuntu Mate는 Ubuntu에서 공식 파생된 버전으로 Raspberry PI처럼 작은 하드웨어 성능에서도 잘 실행될 수 있게 변형된 버전이다. IoTivity가 Ubuntu를 지원하고 있기 때문에, Raspberry PI에서 IoTivity Client를 사용하기 위해 Ubuntu Mate를 사용하였다. 덕분에 Raspberry PI에서 IoTivity 개발과 동시에 Client 실행파일을 바로 실행할 수도 있었다.

Server는 Arduino Mega 2560에서 실행된다. Arduino Mega 2560에는 여러 종류의 센서와 작동기가 연결되어있다. 화학물질 안내 시나리오에서 화학물질 시약병의 RFID 칩을 읽을 때와 출입자 제어 시나리오에서도 출입자의 ID카드에 RFID 칩을 읽기 위하여 RFID 리더 센서를 사용했다. 또 출입자 제어 시나리오에서 출입자의 권한에 따라 출입문을 개폐하기 위해 전기정 스트라이크를 사용했는데, 전기정 스트라이크가 DC 12V로 작동을 해서 아두이노용 5V 릴레이를 사용하여 제어했다. 화학사고 감지 및 알림 시나리오에서는 화학 사고를 감지하기 위해서 가스 센서와 온습도 센서, 불꽃 센서, 마이크 센서를 사용했다. 해당 센서들은 특정 임계값을 넘으면 화학사고 이벤트를 발생하도록 했다. 그리고 화학사고가 났음을 알리기 위해서 피에조 부저를 사용하여 사고 발생 시 피에조 부저에서 경고음이 반복되도록 하였다.

이러한 IoTivity Server와 Client는 공유기를 이용한 NAT환경에서 Private IP로 같은 로컬네트워크에 구성되어있다. 이러한 IoTivity Client와 IoTivity 어댑터가 서로 메시지를 주고받을 수 있게 하기 위해서 COAP(Constrained Application Protocol)와

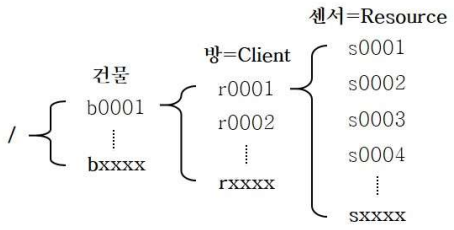

그림 9. 화학 실험실 안전관리 매쉬업 서비스의 MQTT 토픽 트리
Fig. 9. MQTT topic tree of chemical laboratory safety management mash-up service

MQTT(Message Queue Telemetry Transport) 프로토콜을 고려하였는데, 결과적으로 본 논문에서 개발한 화학실험실 안전관리 매쉬업 서비스에서는 MQTT 프로토콜을 사용했다. COAP와 MQTT 프로토콜은 둘 다 하드웨어 자원이 제한적인 IoT 환경에서 주로 사용되는 경량화된 메시징 프로토콜이라는 공통점이 있다. 하지만 COAP 프로토콜은 HTTP 프로토콜과 같은 요청(Request) & 응답(Response) 형태의 일대일 통신 프로토콜로 본 논문에서 개발한 서비스의 IoTivity처럼 NAT 환경의 노드(IoTivity Client)와는 통신을 하려면 포트포워딩과 같은 특별한 공유기 설정을 해야 한다는 문제가 있다. MQTT 프로토콜의 경우 발행(Publish) & 구독(Subscribe)형태의 다대다 통신 프로토콜로서 브로커(Broker) 서버를 통해 토픽(Topic)을 구독함으로써 노드간 통신이 가능하다. 그렇기 때문에 COAP와 달리 NAT 환경의 노드(IoTivity Client)가 있어도 브로커 서버의 IP만 알면 두 노드(IoTivity Client와 IoTivity 어댑터)는 서로 통신이 가능하다. 또한 MQTT는 3단계 QoS를 지원하고 있어 상황에 따라 신뢰성 있는 메시지 전송이 가능하다. 그래서 본 논문에서 개발한 화학실험실 안전관리 매쉬업 서비스의 IoTivity 어댑터는 MQTT 프로토콜을 이용하여 IoTivity Client와 통신한다.

화학 실험실 안전관리 매쉬업 서비스의 MQTT 토픽 트리는 루트(/)부터 건물(Building), 방(Room), 센서(Sensor) 순으로 구성된다. 센서들이 위치한 방에는 IoTivity Client가 각각 하나씩 배치되어있기 때문에 방의 번호가 곧 Client의 번호와 동일하다. 센서 역시 하나의 센서는 하나의 자원과 연결되므로 동일하게 봐도 무방하다. 이렇게 구성된 토픽 트리는 센서들을 장소에 따라 통합 관리하기 위해서 그림 8과 같이 구성했다.

4.1.3 Apache Camel

Apache Camel은 메시지 통합 프레임워크로 일반 어플리케이션에 내장이 가능한 라이브러리 형태로 제공되는 오픈소스 이다. Apache Camel에서 메시지를 송수신하는 대상을 엔드포인트(Endpoint)라고 부르는데 Apache Camel은 이 엔드포인트들 사이에서 라우팅, 변환, 중개, 검증, 로깅 등 다양한 기능을 제공해준다. 이러한 기능들은 모두 EIP(Enterprise Integration Patterns)로 정의가 가능하다. 또한 Apache Camel은 JAVA DSL(Domain Specific Language)를 지원하고 있어 메시지 통합에 있어 복잡한 과정들을 직관적이고 간결하게 나타낼 수 있다.

본 논문에서 개발한 화학실험실 안전관리 매쉬업 서비스는 이러한 Apache Camel의 장점을 활용하여 개발되었다. 메시지 라우터의 입장에서 어댑터들은 각각 하나의 Endpoint가 되어 연계됨으로써 다양한 루트(Route)를 만들 수 있다.

4.2. 검증

이 절에서는 본 논문에서 개발한 화학실험실 안전관리 매쉬업 서비스가 3장에서 설계한 세 가지 시나리오와 시퀀스 다이어그램대로 동작하는지 검증을 한다. 검증 방법은 이벤트 발생 시 메시지 라우터와 어댑터를 통해 외부 서비스들 간에 메시지가 정상적으로 연계되어 사용자가 원하는 출력 결과가 시나리오에 맞게 출력되는지 확인하여 검증한다.

4.2.1. 화학물질 안내 시나리오

화학물질 안내 시나리오는 사용자가 화학물질 시약병에 부착된 RFID 칩을 리더기에 태그하면 해당

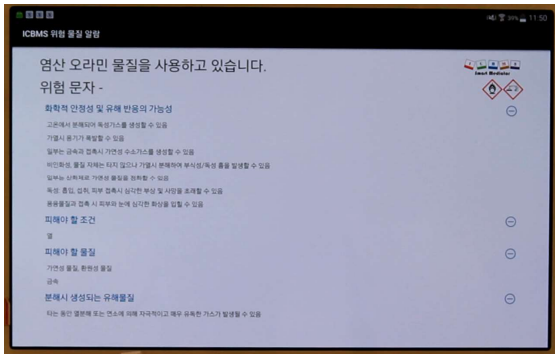

그림 10. 화학물질 정보 안내 시나리오 안드로이드 어플리케이션
Fig. 10. Chemical information guide scenario Android application

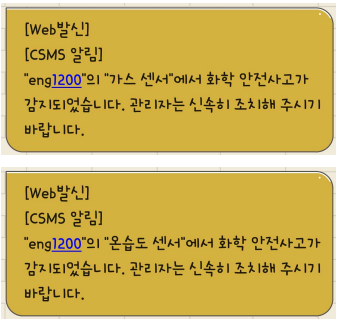

그림 11. 화학사고 감지 및 알림 시나리오 문자메시지
Fig. 11. Chemical accident detection and alarm scenario SMS

RFID 칩의 ID가 화학물질의 CAS번호로 변경되어 공공데이터 포털의 MSDS 정보를 조회한 후 해당 정보를 안드로이드 어플리케이션을 통해 사용자에게 텍스트와 음성으로 안내를 해야 한다. 그림 8은 안드로이드 어플리케이션에 염산 오라민의 정보가 출력되어 사용자에게 안내하고 있는 장면이다. 해당 정보는 텍스트로 표시됨과 동시에 안드로이드의 TTL(Text-To-Speech) 기능을 통하여 사용자에게 음성으로 안내되었다.

4.2.2. 화학사고 감지 및 알림 시나리오

화학사고 감지 및 알림 시나리오는 화학사고가 감지되면 사고 발생 장소의 관리자에게 SMS로 사고 정보를 알려야 한다. 그림 9는 'eng1200'의 가스 센서와 온습도 센서로부터 화학사고가 감지되어 SMS를 통해 관리자에게 사고사실을 알려주는 장면이다.

4.2.3 출입자 제어 시나리오

출입자 제어 시나리오는 사용자가 RFID 칩이 내장된 ID카드를 RFID 리더기에 태그하면 카메라로 사용자의 안면이미지를 촬영하고 2단계 인증을 통

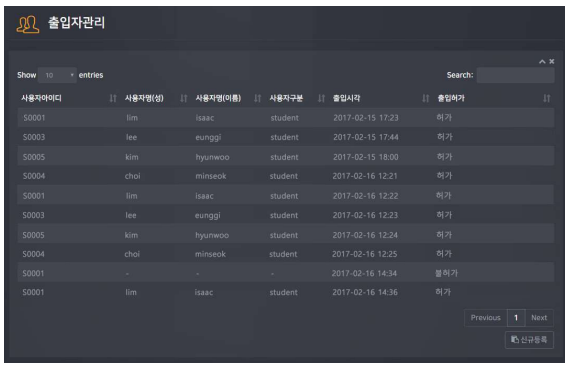

그림 12. 출입자 제어 시나리오 웹 인터페이스
Fig. 12. Access control scenario web interface

해 출입을 시도하는 사용자가 ID카드에 등록된 소지자와 동일인물인지 판단하여 출입권한과 동시에 위장출입 여부를 확인하여 출입문 개폐를 결정한다. 그림 4-4는 출입자들의 출입기록을 보여주는 웹페이지다. 10번째 기록을 보면 ID 'S0001'은 출입 장소에 대한 권한이 있음에도 불구하고 9번째 출입기록에서 사용자의 출입카드를 타인이 도용하여 출입시도를 하여 출입 불허가가 났음을 확인할 수 있다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 화학실험실의 안전사고를 예방하고 사고발생 시 신속한 초동조치를 할 수 있도록 하는 화학실험실 안전관리 매쉬업 서비스를 개발하였다. 먼저 화학실험실에서 발생하는 안전사고의 원인으로부터 화학실험실 안전관리 서비스의 컴퓨터 자동화의 필요성을 도출했다. 그리고 화학실험실 안전관리 서비스를 자동화에 대한 세 가지 문제점을 제시했다. 첫째, 방대한 양의 화학물질 정보 구축의 어려움. 둘째, 다양한 종류의 센서 제어 및 관리의 어려움. 셋째, 위험 화학물질에 대한 위장 출입자의 접근 문제이다.

본 논문은 이러한 화학실험실 안전관리 서비스 자동화의 문제점을 Open API와 Open IoT Platform을 이용하여 해결하고자 하였다. 첫째, 공공데이터 포털의 MSDS Open API를 이용하여 방대한 양의 화학물질에 대한 정보를 손쉽게 얻고자 하였다. 둘째, Open IoT Platform인 IoTivity를 이용하여 다양한 종류의 센서 자원을 쉽게 관리하고자 하였다. 셋째, ID카드와 얼굴인식 Open API를 이용한 2단계 인증방법을 통하여 위장출입자의 출입을 막고자 하였다.

본 논문은 이러한 해결방안들을 하나의 안전관리 서비스로 구현하기 위하여 매쉬업 프레임워크를 사용하였다. 그리고 매쉬업 프레임워크의 이점을 최대한으로 발휘하기 위하여 얼굴인식과 화학물질 정보 Open API 이외에도 단문문자메시지, 사용자 권한관리, 안드로이드 메시지 푸시 기능도 직접 구현하지 않고 외부 서비스를 사용하였다. 그래서 본 논문에서는 화학실험실 안전관리 매쉬업 서비스를 개발하고자 하였다.

본 논문은 화학실험실 안전관리 매쉬업 서비스를 개발하기 위하여 서비스 시나리오, 요구사항, 구성도, 시퀀스 다이어그램을 설계하였다. 서비스 시나리오는 화학물질 정보 안내, 화학사고 감지 및 알람, 출입자 제어와 같이 세 가지 시나리오로 설계하였다. 서비스 요구사항 설계는 서비스 시나리오를 바탕으로 시스템 요구사항, 기능 요구사항, 인터페이스 요구사항으로 나누어 설계하였다. 서비스 구성도는 앞서 설계한 시나리오와 요구사항을 바탕으로 설계하였다. 서비스 시퀀스 다이어그램은 서비스 구성도의 모듈들 이 어떻게 동작하는지 시나리오별로 나누어 설계하였다.

이렇게 설계된 시나리오를 바탕으로 화학실험실 안전관리 매쉬업 서비스를 구현하였다. 메시지 라우터와 어댑터들은 각각 도커의 Container 위에서 개별적으로 동작을 하고 있고, 각각의 어댑터의 Container는 이미지로부터 실행될 수 있어 배포가 용이하고 트래픽 과부화시 추가로 이미지를 실행해서 트래픽 분산이 가능하다. IoTivity 어댑터는 7가지 센서와 작동기를 제어하기 위해 IoTivity Server는 Arduino Mega 2560을 사용하고, IoTivity Client는 Raspberry PI를 사용했다. 그리고 IoTivity Client와 어댑터 사이에 MQTT 프로토콜을 사용하여 서로 통신할 수 있도록 하였다. 어댑터들은 Apache Camel을 이용하여 구현되었으며, 각각이 Camel의 Endpoint가 되어 메시지 라우터에서 Route에 정의되어 이벤트 발생 시 해당 Route에 따라 메시지를 처리하도록 구현하였다.

이렇게 구현된 화학실험실 안전관리 매쉬업 서비스는 설계한 서비스 시나리오별로 검증을 하였다. 각각의 시나리오들은 특정 이벤트가 발생할 때마다 알맞은 외부 서비스들을 연계하여 상황에 맞는 결과물을 출력함으로써 매쉬업 서비스가 설계된 시나리오에 맞게 동작하는 것을 확인할 수 있었다. 또한 이러한 화학실험실 안전관리 매쉬업 서비스를 자동화하기 위해 매쉬업 프레임워크를 이용하여 다양한 기능들을 외부 서비스를 연계하여 개발함으로써 개발비용의 절감 효과가 있을 수 있었다.

References

[1] Y. Jang, S. Jung, K. Park, "Consequence Analysis for Accidental Gas Release in Labs," Journal of the Korean Institute of Gas, vol. 19, no. 4, pp. 29-34, Aug. 2015.

[2] T. H. Lee, D. J. Lee, J. D. Park, C. H. Shin, "Study fo the Characteristics Analysis of Laboratory Chemical Accidents," Fire Science and Engineering, vol. 30, no. 3 pp. 110-116,

June. 2016.

[3] G. S. Jeong, E. S. Baik, “A Study on the Improvement of Safety Management of Hazardous Chemicals Handling in the Workplace,” Fire Science and Engineering, vol. 28, no. 1, pp. 12-19, Feb. 2014.

[4] 공공데이터포털, Retrieved Dec. 18. 2017, from https://www.data.go.kr/.

[5] IoTivity, Retrieved Dec. 18. 2017, from https://www.iotivity.org/.

[6] B. S. Kim, B. T. Ryu, M. S. Kim, C. B. Jang, J. W. Ko, “A Study on the development of Safety Management System for Harmful Chemical Substance Accident,” Korean Journal of Hazardous Materials, vol. 1, no. 1, pp. 33-38, June. 2013.

[7] H. Y. Jang, M. J. Ha, H. S. Jang, J. H. Yoon, E. B. Lee, M. J. Lee, “Design and Implementation of an HNS Accident Tracking System for Rapid Decision Making,” Journal of the Korean Society of Marine Environment & Safety, vol. 23, no. 2, pp. 168-176, Apr. 2017.

[8] J. W. Ryu, J. M. Kim, S. M. Shin, H. K. Park, “The need of early response system to HNS accident based on case analysis,” in Proc. the 3rd International Conference on Civil, Offshore and Environmental Engineering. (ICCOEE 2016), pp. 143-146, Kuala Lumpur, Malaysia, Aug. 2016.

[9] T. Kim, H. Kim, D. Kwon, K. Ok, I. Im, E. Lee, H. Je, N. Rakhmatov, D. An, H. Ju, “Design of an Effective Framework for Mash-up Service Development,” in Proc. 2016 International Conference on Information Networking. (ICOIN 2016), pp. 357-359, Kota Kinabalu, Malaysia, Mar. 2016.

[10] H. Kim, D. Kwon, H. Ju, “Design of a Mash-up Framework based on Enterprise Integration Patterns for Access Management Service,” in proc. Korean Network Operations and Management Conference 2016. (KNOM 2016), pp. 111-112, Chuncheon, Korea, May. 2016.

[11] E. Lee, I. Lim, H. Kim, K. Ok, D. Kwon, D. An, H. Ju, “Development of gate security system based on mash-up framework,” in Proc. 2017 Third Asian Conference on Defence Technology (ACDT 2017), pp. 70-74, Phuket, Thailand, Mar. 2017.

[12] D. Kwon, H. Kim, D. An, H. Ju, “Container Based Testbed for Gate Security Using Open API Mashup,” 8th International Conference on Advances in Information Technology, Procedia Computer Science. (IAIT 2016), pp. 19-22, Macau, China, Dec. 2016.

[13] E. Lee, H. Kim, D. Kwon, I. Lim, H. Ju, “Design of Laboratory Safety Management Mash-up Service to Prevent of Chemical Accident in College,” in proc. Korean Network Operations and Management Conference 2017. (KNOM 2017), pp. 37-38, Jeonnam, Korea, June. 2017.

[14] MongoDB, Retrieved Dec. 18. 2017, from https://www.mongodb.com/.

[15] Cool SMS, Retrieved Dec. 18. 2017, from https://www.coolsms.co.kr/.

[16] Face++, Retrieved Dec. 18. 2017, from https://www.faceplusplus.com/.

[17] OKTA, Retrieved Dec. 18. 2017, from https://www.okta.com/.

[18] Docker, Retrieved Dec. 18. 2017, from https://www.docker.com.

[19] E. Lee, H. Kim, H. Ju, “IoTivity-based Access Control Method,” in proc. Korean Network Operations and Management Conference 2016. (KNOM 2016), pp. 63-64, Chuncheon, Korea, May. 2016.

이 응 기 (Eung-gi Lee)

2016 2년 : 계명대학교 컴퓨터공학과 학사

2016 3월~현재 : 계명대학교 컴퓨터공학과 석사과정

<관심분야> IoT 관리, 네트워크, 스마트 중재기

김 현 우 (Hyeonwoo Kim)

2010년 2월 : 계명대학교 컴퓨터공학과 학사
2012년 2월 : 계명대학교 컴퓨터공학과 석사
2012년 3월~현재 : 계명대학교 컴퓨터공학과 박사과정
<관심분야> IoT 관리, 방화벽 정책 추론 및 관리, 네트워크 관리 및 보안, 스마트 중재기

주 홍 택 (Hongtaek Ju)

1989년 8월 : 한국과학기술원 전자계산학과 학사
1991년 8월 : 포항공과대학교 컴퓨터공학과 석사
1997년 8월 : 대우통신종합연구소 선임연구원
2002년 2월 : 포항공과대학교 컴퓨터공학과 박사
2002년 9월~현재 : 계명대학교 컴퓨터공학부 교수
<관심분야> 네트워크 및 시스템 관리, IoT 관리, SDN 네트워크 관리, 인터넷 침입 예측, 네트워크 보안