JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 25, No. 5, pp. 1281-1290, May. 2024

Check for updates

프라이버시 보호를 위한 스마트 시티 보안모델 연구

김 시 정[1†] · 조 도 은[2†*]
[1†] 청주대학교 교양학부 교수
[2†] *목원대학교 SW교양학부 교수

Smart City Security Model for Privacy Protection

Si-Jung Kim[1‡] · Do-Eun Cho[2‡ *]

[1‡] Professor, Department of Liberal Arts, Cheongju University, Cheongju 363170, Korea
[2‡] *Professor, Department of SW Liberal Arts, Mokwon University, Daejeon 35349, Korea

[요 약]

스마트 시티 플랫폼을 기반으로 제공되는 서비스에는 사용자의 다양한 데이터 수집, 가공, 관리, 저장 등의 기술이 적용된다. 스마트 시티의 안전한 서비스 활용을 위해서는 사용자 프라이버시의 보안성이 보장되어야 한다. 본 논문은 스마트 시티 구성 요소들에 대한 보안 위협 요소를 분석하고, 서비스 제공을 위한 보안 요소를 도출하여 효과적인 사용자의 서비스 접근과 프라이버시 침해 대응을 위한 보안 서비스 모델을 제안하였다. 스마트 시티 서비스에 접근하는 사용자를 효율적으로 인증하고 관리하기 위해 제로 트러스트 보안 개념을 응용한 동적 인증 기법과 FIDO 방법을 적용하였다. 또한 사용자 식별 정보를 암호화하고 마스킹하여 프라이버시를 보호하고, 차분 프라이버시 기법을 적용하여 사용자의 데이터 접근제어를 함으로써 프라이버시 보호를 강화하였다. 제안 모델의 보안성을 STRIDE와 LINDDUN 위협 모델의 분류 기준을 적용하여 분석한 결과 충분한 보안성을 갖추고 있음을 확인하였다.

[Abstract]

The services provided based on the smart city platform utilize various technologies for data collection, processing, management, and storage. In order to safely utilize smart city services, the security of user privacy must be guaranteed. This paper analyzes security threats to smart city components, identifies essential security elements for service provision, and proposes a security service model to ensure effective user access to services and a robust response to privacy infringements. To efficiently authenticate and manage users accessing smart city services, dynamic authentication techniques and FIDO methods, incorporating the concept of zero trust security, were applied. Additionally, privacy was protected by encrypting and masking user identification information and further strengthened by applying a differential privacy mechanism to control users' data access. An analysis of the security of the proposed model, based on the classification criteria of the STRIDE and LINDDUN threat models, confirmed that it has sufficient security measures in place.

색인어 : 스마트 시티, 보안, 개인정보 보호, 보안 위협, 사용자 인증
Keyword : Smart City, Security, Privacy Protection, Security Threat, User Authentication

http://dx.doi.org/10.9728/dcs.2024.25.5.1281

Received 19 March 2024; **Revised** 02 April 2024
Accepted 17 May 2024

‡ These authors contributed equally to this work

***Corresponding Author; Do-Eun Cho**

Tel: +82-42-829-7649
E-mail: decho@mokwon.ac.kr

Ⅰ. 서 론

데이터 수집 및 분석 기술을 통해 도시의 문제를 해결하고 가치를 높이는 스마트 시티에 대한 관심이 높아지고 있다. 스마트 시티는 일상생활에서 편리한 공공 서비스를 제공하고, 생활에 필요한 많은 자원을 공유하며, 구성원의 삶의 질을 높이는 것을 목적으로 다양한 미래 지향적 서비스를 제공하고 있다. 스마트 시티(Smart City)의 정의는 여러 학자들과 기관 그리고 국가별로 다양하게 정의하고 있으나[1], 사회 인적 자원의 삶의 질을 향상 시키고 도시의 효과적인 운영을 통해 거주성(Livability), 업무 효율성(Workability), 지속가능성(Substantiality)을 개선하는 것을 지향하고 있다.

ISO(International Standards Organization)는 스마트 시티를 인적 자원의 삶의 질과 서비스를 변화시키기 위해 도시의 지속가능성과 회복력을 향상시키고, 도시가 시민사회에 어떻게 영향을 주는지, 협력적 리더십 수단들에 어떻게 적용되는지, 도시 운영 구성 요소들과 도시 시스템에서 어떻게 작동하는지, 데이터와 통합기술을 어떻게 사용하는지를 근본적으로 개선 시키는 것이라고 정의하고 있다[2],[3].

스마트 시티는 스마트 행정, 교통, 의료 및 복지, 환경, 안전, 교육 등 다양한 분야에 폭넓게 서비스를 제공한다. 이러한 스마트 시티 서비스를 위해서는 유무선 네트워크를 기반으로 한 다양한 디바이스 인증 및 사용자 인증을 위한 정보를 송수신하고 공유 및 저장 과정이 요구된다.

스마트 시티 서비스는 ICT와 IoT를 포함한 다양한 첨단 기술을 통해 실시간으로 대량의 데이터가 수집 및 활용된다. 이처럼 스마트 시티는 대량의 정보를 활용하는 서비스인 만큼 정보 해킹과 프라이버시 침해에 노출되어 있다[4]. 따라서 스마트 시티 서비스에서 사용되는 정보의 보안 정책과 프라이버시 보호 문제는 중요한 연구과제이다.

한국인터넷진흥원(KISA)에서는 안전한 스마트 시티 구축을 위해 필요한 보안 요구사항 및 보안 대책을 제시하고 있다[5]. KISA에서 제시한 스마트 시티 모델에서는 국내 스마트 시티 플랫폼 구축에 있어 효과적인 보안을 위해, 각 구성 요소별 보안 분야와 보안 항목에 대해 상세 내용을 제시하고 있으며, 내용에 대한 이행 지침을 제시하여 스마트 시티를 구축하고자 할 때 적용할 수 있도록 가이드 라인을 제시하고 있다.

본 논문에서는 KISA에서 제시한 스마트 시티 통합플랫폼 보안 모델 구축 지침을 통해 스마트 시티의 구성 요소별 보안 위협을 분석하여 프라이버시 보호를 위한 구체적인 보안 서비스 모델을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트 시티의 구성 요소별 보안 위협에 대하여 살펴보고, 프라이버시 보호를 위한 관련 기술을 살펴본다. 3장에서는 제안 모델의 보안 요구 사항과 스마트 시티의 프라이버시를 위한 보안 서비스 모델을 제안한다. 그리고 4장에서는 제안 모델의 보안성을 분석한다. 마지막으로 5장에서 결론 및 향후 연구 방향을 기술한다.

Ⅱ. 스마트 시티 보안 서비스

스마트 시티는 첨단 ICT 기술을 기반으로 도시의 인프라를 구성하는 서비스 플랫폼이며, 다양한 도시 문제에 해결 방안으로 제시되고 있다. 따라서 스마트 시티는 대량의 정보를 수집하고 이를 활용한 서비스를 제공함으로써 도시에 여러가지 편리성을 제공한다. 그러나 서비스를 위해 수집되는 대량의 데이터에 대한 사이버 공격, 프라이버시 침해에 대한 위협이 존재하며 이에 대한 보안 정책을 수립하는 것은 매우 중요한 요소이다[6]. 이를 위해 본 장에서는 스마트 시티의 구성 요소별 보안 위협과 적용가능한 보안 기술에 대해 분석한다.

2-1 스마트 시티 구성 요소별 보안 위협

스마트 시티는 서비스를 이용하는 사용자, 서비스 운영과 제공을 하는 운영 주체 및 유관기관, 데이터 수집을 위한 디바이스, 서비스를 구성하는 인프라, 수집한 데이터를 처리하거나 제공하는 플랫폼 그리고 다양한 서비스로 구성된다. 그림 1은 스마트 시티 프레임워크의 구성 요소를 나타낸 것이다. 스마트 시티에서의 데이터 보안 위협은 구성 요소인 디바이스와 인프라, 플랫폼을 연계하여 제공되는 각 단계에서 발생할 수 있다.

디바이스 단계의 보안 위협에는 도청, 위조, 데이터 및 통신 정보의 변조가 있다. 이는 일상생활에서 다양한 데이터를 수집하기 위한 디바이스와 센서로 구성되는 IoT 구성요소를 스마트 시티 인프라와 연결하는 과정과 각 디바이스 간 통신 도중 발생하는 위협으로 정의할 수 있다.

인프라는 전체 스마트 시티 서비스의 기반을 형성하는 구성 요소이며, 기존 통신 망의 보안 취약점이 보안 위협이 된다. 네트워크의 접근 차단, 우회 경로를 통한 정보 유출, 무단 사용자의 접근, 패킷 차단과 같은 DDoS 공격 등이 있다.

도시의 통합 운영 부분인 플랫폼에서의 보안 위협에는 서비스를 구현하는 소프트웨어 코드의 보안 취약점, 사용자 데이터의 생성 및 저장 과정에서의 데이터 유출, 대규모 인프라 및 통신 시설에 대한 사이버 위협 등이 있다.

스마트 시티 서비스의 사용자에 대한 보안 위협으로는 사

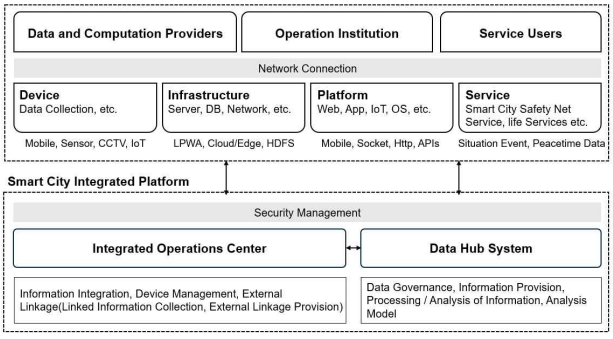

그림 1. 스마트 시티 프레임워크 구성 요소
Fig. 1. Smart city framework components

표 1. 스마트 시티 보안 위협 요소
Table 1. Smart city security threat

Configuration	Security Threat	Case
Configuration Devices	· Communication failure and service interruption due to DoS attacks · Malicious code penetration over the network · Malicious code transfer between devices through malicious programs · Exposing encryption keys, improper use of passwords due to weak encryption · Device usability corruption · Personal information leak · Personal information leakage due to counterfeiting of firmware	IoT Sensor, Control Device, N.W base Devices, CCTV
Infrastructure, Network	· Information eavesdropping and eavesdropping in the infrastructure · Accessing services with software installed by unauthorized users · Data leakage by sniffing · Data interception in network · Personal information leakage due to ID leakage	LAN, WiFi, LTE/5G, ZigBee, NFC, Platform
Platform Software	· Vulnerability to the security of the platform design itself · Security threats to software's own vulnerabilities · Modulation of transmission and reception data, such as session hijacking, sniping, etc · Inadequate access control and physical control · MITM(Man in the Middle) attack · Vulnerability to network server access control	OpenAPI, Public Service, Web Public Data Service
Smart City, Service	· Data loss flowing into smart cities · Data loss through service data modulation & falsification · Vulnerability in access management · Loss of information due to service users · Infringement of user privacy · Privacy infringement in sensor based big data integrated information system	Services linked to the platform, OpenAPI base IoT Service

용자의 신원 도용, 인증 우회, 서비스 제공을 위한 등록 정보에 대한 데이터 위변조 그리고 개인정보 유출 등이 있다[7],[8].

스마트 시티에서의 데이터 보안 위협은 각 구성 요소의 구현 단계마다 존재한다. 특히 사용자의 등록 또는 생성 정보에서 데이터 저장 및 활용 단계까지의 전 단계에서 프라이버시 침해에 대한 보안 위협은 매우 심각하다. 최근 인공지능 기반의 자동화된 생활 가전들이 네트워크 기반의 디바이스 구성 요소로 등장하면서 일상생활에서 무분별하게 수집되는 단편적 또는 종합적인 데이터들이 스마트 시티 통합 플랫폼으로 유입됨에 따라 심각한 프라이버시 침해로 이어질 수 있다.

표 1은 이러한 스마트 시티 구성 요소의 단계별 위협 요소를 나타낸 것이다.

2-2 프라이버시 보호 기법

프라이버시에 대한 취약성은 스마트 시티 구성 요소의 여러 단계에서 발생 될 수 있다. 먼저 프라이버시 침해에 대한 보안 요구사항을 정보의 생성 단계부터 적용, 보관, 활용 단계까지 전 단계에서 살펴보면, 스마트 시티의 기획 단계에서 서비스를 통해 처리되는 사용자의 개인정보를 식별하고 보안 통제를 적용하도록 설계하고, 운영단계에서는 스마트 시티 보안 체계와 각 정보를 활용하는 주체의 개별 정보보안 통제안을 적용하여 운영하는 것이 필요하다. 그리고 거버넌스가 주체가 되어 개인정보의 활용에 주체권을 사용자에게 보장해야 한다. 이를 위해 스마트 시티 서비스를 이용하기 위한 개인정보에 대한 식별 태그 정보 즉, 사용자 개인의 식별에 적용되는 프라이버시 정보를 적절한 암호화 과정을 거쳐 보관과 전송 그리고 활용이 이루어져야 한다. 다양한 정보 활용 서비스에 프라이버시 침해는 매우 중요한 보안 요소이므로 여러 방법이 대응 방안으로 적용되고 있다. 정보를 생성하는 사용자의 프라이버시 침해에 대응하면서 데이터베이스 내의 개인정보를 활용하는 방법을 두 가지로 구분할 수 있다[9].

첫째, 데이터의 프라이버시를 유지하면서 공개하는 방법인 PPDP(Privacy Preserving Data Publishing)은 데이터 저장 시 개인정보를 사용자에게 배포할 수 있는 새로운 비식별 정보로 처리하거나 합성한 정보로 가공하여 생성하는 것이다.

둘째, 프라이버시 보존형 데이터 마이닝 방법인 PPDM(Privacy Preserving Data Mining)은 데이터를 수집하고 이를 처리하는 과정에서 개인정보가 노출되지 않도록 보호한다. 이를 위해 데이터 마스킹, 랜덤화, 암호화 기반 방법 등을 사용한다.

스마트 시티 통합 플랫폼 운영에서 사용자의 프라이버시 침해에 대한 대응 방안을 위한 연구 방법을 살펴보면 전통적으로 암호화 기법을 기반으로 이루어졌다. 그리고 사용자의 개인 식별 정보를 가공하여 비식별화하는 방법이 활용된다[10]. 이러한 방법에는 별칭으로 변경하는 가명 처리(Pseudonymization), 수학 공식을 적용한 총계 처리(Aggregation), 식별에 활용되는 일부 데이터를 제거하는 데이터 값 삭제(Data Reduction), 특정 데이터 값이 속하는 범위로 표현하는 데이터 범주화(Data Suppression) 그리고 임의의 측정값을 추가하거나 공백을 추가하는 데이터 마스킹

(Data Masking) 등이 있다. 이러한 방법들은 생성된 데이터를 변경하여 데이터 활용 시 개인의 식별 또는 프라이버시 침해를 할 수 없도록 데이터를 가공하는 방법들이다. 이외에도 프라이버시 보호를 위해 개인 정보를 비식별화하는 방법으로 차분 프라이버시(Differential Privacy) 기술을 사용할 수 있다[11]. 차분 프라이버시의 주요 개념은 다음과 같다. 함수 f에 대해 D_1, D_2는 레코드 하나만 다른 데이터베이스로, t는 임의의 실수라고 하였을 때, 특정 $\epsilon > 0$에 대해 식 (1)이 항상 성립한다면 함수 f는 프라이버시 수준(level) ϵ으로 차분 프라이버시가 보호된다.

$$\Pr(f(D_1) = t) / \Pr(f(D_2) = t) \leq \exp(\epsilon) \quad (1)$$

차분 프라이버시에서 비식별화 함수 f를 위해 노이즈(Noise)를 추가하며, 민감도가 높은 데이터에는 더 많은 노이즈를 추가하고, 민감도가 낮은 데이터에 대해서는 더 적은 노이즈를 추가함으로써 프라이버시를 유지하는 동시에 데이터 분석이나 통계 처리시 유용하게 활용할 수 있다.

또한 동형 암호화(Homomorphic Encryption) 기술은 암호화된 데이터를 복호화하지 않고 연산하는 기술이다. 암호문들을 이용한 연산 결과는 새로운 암호문이 되며, 이를 복호화하여 얻은 평문은 암호화하기 전의 데이터의 연산 결과와 같다[12]. 예를 들어 데이터 소유자가 비밀키를 이용하여 동형 암호화하여 데이터를 저장하고, 데이터 사용자는 동형 암호 연산을 통하여 데이터 분석에 사용 할 수 있다. 이는 데이터의 암호화 상태를 유지함으로써 데이터 프라이버시를 유지하며, 각종 연산, 통계, 분석 등의 작업을 수행할 수 있다(그림 2).

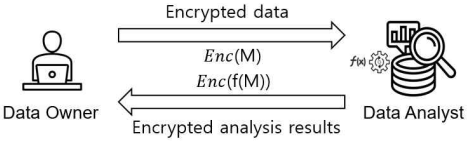

그림 2. 암호화된 상태에서의 데이터 분석[12]
Fig. 2. Analyzing data while encrypted[12]

이러한 기법은 스마트 시티에서 프라이버시를 유지하며 다양한 서비스에서 데이터를 안전하게 활용하는 방안으로 활용될 수 있다.

2-3 사용자 인증기법

스마트 시티에서 사용자 인증 방법은 다양한 요소들이 고려되어야 한다. 스마트 시티는 광범위한 서비스와 장치를 연결하고, 대량의 데이터를 처리하며, 다양한 사용자의 요구를 충족해야 한다. 따라서, 효율적이고 보안이 강화된, 그리고 사용자 친화적인 인증 방법이 필요하다.

- 멀티 팩터 인증(MFA): 사용자 이름과 비밀번호와 함께, 추가적인 인증 수단(예: 모바일 앱을 통한 인증, OTP, 생체 인식)을 사용하는 방식이다. 이는 보안을 강화하는 동시에 사용자에게 편리함을 제공한다.
- 생체 인식: 지문, 안면 인식, 홍채 스캔과 같은 생체 인식 방법은 높은 보안 수준을 제공하며, 사용자에게 매우 편리하다. 스마트 시티 환경에서는 공공장소 또는 서비스에 접근할 때 빠른 인증을 가능하게 한다.
- 모바일 기반 인증: 대부분 사용자가 스마트폰을 소지하고 있어 QR 코드 스캔, NFC, 블루투스 등 모바일 앱을 통한 인증은 매우 효과적이다.
- 디지털 ID: 스마트 시티 서비스에 접근하기 위해 디지털 신분증이나 전자 증명서를 사용할 수 있다. 이는 특히 공공 서비스 접근에 유용할 수 있다.
- 행동 인증: 사용자의 행동 패턴(예: 키 입력 방식, 걷는 방식 등)을 분석하여 인증하는 방법이다. 이는 지속적인 백그라운드 인증으로 활용될 수 있다.
- 단일 로그인(SSO): 여러 서비스나 애플리케이션에 걸쳐 하나의 인증 정보를 사용하는 것이다. 사용자가 매번 다른 서비스에 로그인할 필요 없이 한 번의 로그인으로 여러 서비스를 이용할 수 있게 한다.
- 블록체인 기반 인증: 투명성과 보안성을 제공하며, 사용자 데이터의 중앙집중화 위험을 줄일 수 있다.

표 2. 사용자 인증 기법
Table 2. User authentication methods

Classification	Content	Technology
Knowledge-based Authentication	· Siloed Identity : Creating and registering different information for each user's access service as a basic authentication method for online services · Federated Identity : Leverages integrated applicable information provided by IDP. SAML(Security Assertion Markup Language) & SSO(Single Sign on)	ID, Password, PIN
Ownership-based Authentication	· How to enhance user authentication based on the different types of information you have · Complement the shortcomings of centralized processing and massive data storage, and extend user authority over authentication	Security Card, OTP, User Key, Mobile Device
Bio information-based Authentication	· Provides authentication services based on user's own biometric information improves security and convenience compared to traditional ID and Password methods	Biometric Recognition Information

스마트 시티에서의 인증 방법 선택 시에는 보안성, 사용 편의성, 비용 효율성, 확장성 등을 고려해야 한다. 또한, 사용자의 프라이버시를 보호하고 법적 규제를 준수하는 것도 중요하다. 스마트 시티에서 사용자에 대한 인증은 대부분 원격 서버에서 시행되며, 사용자들에게 접속 권한이 부여된다. 이때 인증 과정은 식별(Identification), 인증(Authentication), 인가(Authorization)의 과정으로 진행된다. 표 2는 다양한 사용자 인증 기법을 나타낸 것이다[13].

최근 지식기반 인증 기술의 취약성이 가시화되면서 인증 기술에 대한 패러다임은 생체 인식 기반의 FIDO(Fast Identity Online)로 전환되고 있다. FIDO 인증은 사용자 기기의 안전한 영역에 저장된 개인키를 활용하여 인증 요청 메시지에 대한 서명을 생성하여 전달하며, 매칭된 공개키를 활용하여 서명을 검증하는 형태로 인증 과정을 수행한다.

이와 같은 과정은 강력한 디바이스 바인딩(Device Binding)을 통해 사용자의 프라이버시를 보호하고, 편의성을 제공한다. FIDO 구조는 클라이언트와 서버 그리고 프로토콜로 구성되며 역할은 다음과 같다[14],[15].

- Client : FIDO 인증 토큰과 인증 토큰 API의 추상화 단계에서 연동 역할 수행, 서버와 안전하게 정보를 송수신하며 등록, 인증, 조회 서비스 제공
- Server : 클라이언트와 송수신하며 클라이언트가 제시하는 인증토큰을 검증 및 등록 그리고 인증된 사용자의 접근을 승인
- Protocol : 디바이스에 있는 인증토큰을 조회하고 검증하며, 메시지는 '도전(Challenge)-응답(Response)' 형태로 프로토콜을 수행하여 사용자의 신원을 인증

2-4 데이터 접근 제어 및 모니터링 기법

KISA에서 제시한 모델에서는 보안 위협을 위한 스마트 시티 보안 모델 구축 지침이 명시되어 있으나[5], 공급망 보안과 제로 트러스트(Zero-Trust)와 관련된 보안 요구사항은 부족한 실정이다. 스마트 시티는 다양한 기기와 시스템이 상호 연결되어 있어 다수의 사이버 보안 취약점이 발생할 수 있다. 이러한 환경에 제로 트러스트 모델을 적용하면 모든 사용자와 장치가 신뢰할 수 있는지 지속적으로 검증하고, 접근 권한을 최소화하여 외부 위협뿐만 아니라 내부 위협에서도 정보를 보호할 수 있다.

제로 트러스트는 사이버 보안에서 사용되는 보안 모델로 네트워크 내부 또는 외부에 위치한 모든 사용자와 디바이스의 신뢰를 기본적으로 부여하지 않는다는 원칙에 기반한다. 따라서 모든 네트워크 트래픽을 잠재적 위협으로 간주하고 모든 접근 시도를 검증하는 것을 목표로 한다[16]. 따라서 제로 트러스트를 통해 스마트 시티의 데이터의 접근을 엄격히 제어하고, 모든 접근 시도를 로깅하여 감사 및 모니터링을 강화함으로써 법적 규제 준수를 지원할 수 있다. 또한 모든 접근 요청과 트래픽을 검증하고 로깅함으로써 네트워크 운영의 투명성을 제공하고, 비정상적인 행동이나 잠재적인 보안 위협을 보다 쉽게 식별할 수 있다.

그림 3. 제로 트러스트 접근 과정[16]
Fig. 3. Zero trust access process[16]

그림 3은 제로 트러스트에서 정책 결정 포인트(PDP)와 정책 시행 시점(PEP)을 통해 데이터에 대한 접근을 허용하는 것을 나타낸다[16]. PDP는 보안 정책 및 요청 컨텍스트(예: 장치 보안 상태, 사용자 자격 증명 및 동작 속성)를 기준으로 각 액세스 요청을 평가한다. PEP는 PDP에 의해 인증되고 승인된 사용자만 리소스에 액세스할 수 있도록 제어할 수 있다.

제로 트러스트에 장치 에이전트/게이트웨이 기반 배포(Device Agent/Gateway-Based Deployment) 모델을 적용하면 그림 4와 같다[16]. 장치 에이전트가 액세스 요청을 정책 관리자(Policy Administrator)에게 전송한다. 정책 관리자는 정책 엔진(Policy Engine)을 통해 액세스 요청을 평가하고, 접근을 승인하거나 거부한다. 접근이 승인되면, 정책 관리자는 게이트웨이에 통신 경로를 설정하라고 지시한다. 장치 에이전트와 게이트웨이는 이 설정을 바탕으로 연결을 시작하며, 사용자는 승인된 범위 내에서 자원을 사용할 수 있다.

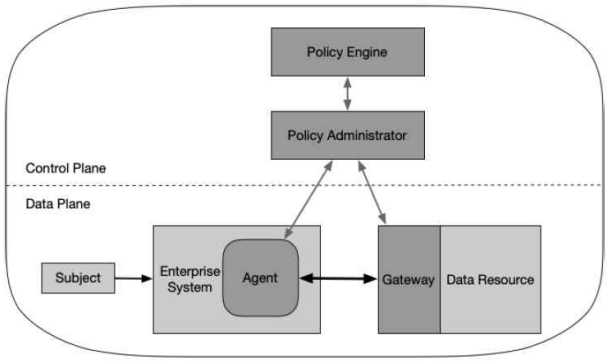

그림 4. 장치 에이전트/게이트웨이 기반 배포 모델[16]
Fig. 4. Device Agent/Gateway-based deployment[16]

Ⅲ. 프라이버시를 위한 보안 서비스 모델

3-1 보안 서비스 모델의 요구사항 분석

본 논문에서 제안하고자 하는 모델의 보안 요구 사항을 마이크로소프트에서 제안한 STRIDE 위협 모델의 분류에 기반하여 도출하였다. STRIDE는 보안 위협 모델링을 위해 사용되는 프레임워크로, 공격자의 관점에서 보안 위협을 식별하고

분석하여 적절한 보안 조치를 취할 수 있게 한다. STRIDE는 위장(Spoofing identity), 변조(Tempering with data), 부인(Repudiation), 정보 노출(Information disclosure), 서비스 거부(Denial of service), 권한 상승(Elevation of privilege)의 6가지 카테고리로 위협을 분류하고 있다[17]. STRIDE는 IT 관련 위협에 초점을 맞추어 설계 단계에서 다양한 종류의 보안 위협을 식별하고, 발생 가능한 위협과 취약점을 분류하는데 효과적인 기법이다. 표 3은 STRIDE 분류를 이용한 스마트 시티 보안 모델의 보안 요구 사항을 나타낸 것이다. 스마트 시티는 다양한 사이버 보안 위협에 대응하기 위해 종합적인 방안이 필요하다. 이에는 강력한 인증 시스템을 통한 데이터 보호와 사용자 행동의 추적 및 검증이 필요하다. 민감한 데이터 보안을 위한 로그 관리 및 감사 시스템, 접근 제어 시스템의 적용이 필요하며, 서비스의 연속성을 보장하고 권한 상승을 방지하기 위한 조치도 요구된다.

표 3. STRIDE 분류에 의한 보안 요구 사항
Table 3. Security requirements by STRIDE classification

STRIDE Element	Smart City Security Requirements
Spoofing identity(S)	Implementation of robust authentication systems to prevent identity forgery
Tempering with data(T)	Application of encryption and integrity verification systems to ensure data integrity
Repudiation(R)	Establishment of log management and audit trailing systems for action tracking
Information disclosure(I)	Encryption and access control systems for the protection of personal and sensitive data
Denial of service(D)	Deployment of defense mechanisms and strategies to ensure service continuity and availability
Elevation of privilege(E)	User rights management and adherence to the principle of least privilege to prevent unauthorized privilege escalation

표 4. LINDDUN 분류에 의한 보안 요구 사항
Table 4. Security requirements by LINDDUN classification

LINDDUN Element	Smart City Privacy Requirements
Linkability(L)	Implementation of anonymization and data segregation to minimize linking of user activities
Identifiability(I)	Strong data protection and encryption to prevent exposure of personal identifiers
Non-repudiation(N)	Log management and audit systems for tracking and verifying user actions
Detectability(D)	Security monitoring systems for detecting unauthorized access and data breaches
Disclosure of information(D)	Managing data access rights to prevent exposure of sensitive information
Unawareness(U)	Enhancing privacy awareness through user education and policy transparency
Non-compliance(N)	Ongoing audits and compliance checks to adhere to laws and policies

또한 스마트 시티의 프라이버시 보안을 위해 LINDDUN 위협 모델의 분류 기준을 이용하여 요구사항을 도출하였다.

LINDDUN은 프라이버시 침해 가능성을 식별하고, 프라이버시 위협을 분석하고 평가하기 위한 모델이다. LINDDUN은 연결(Linkability), 식별(Identifiability), 부인 방지(Non-repudiation), 검출(Detectability), 정보 유출(Disclosure of information), 내용 몰인식(Unawareness), 정책 및 동의 불이행(Non-compliance)의 7가지 카테고리로 프라이버시 위협을 분류하고 있다[18]. 이 위협 모델의 분류를 이용하여 스마트 시티 서비스의 프라이버시 요구사항을 도출하였다. 표 4는 LINDDUN 분류를 이용한 보안 요구 사항을 나타낸 것이다. 스마트 시티 프라이버시 보호를 위한 요구사항은 데이터의 연결성과 식별 가능성을 최소화하기 위해 익명화 및 데이터 분리 처리가 필요하다. 사용자 행동의 부인 방지를 위해 로그 관리 및 감사 시스템을 구축하고, 탐지 가능성을 높이기 위한 보안 모니터링 시스템 적용이 필요하다. 또 민감한 정보의 무단 공개를 방지하기 위해 데이터 접근 권한 관리와 이에 따른 시스템의 정책 수립이 중요하다.

3-2 제안하는 프라이버시 보안 모델

제안하는 스마트 시티를 위한 보안 서비스 모델은 그림 5와 같다. 제안 모델은 일반적인 스마트 시티 프레임워크에 에이전트(Agent), 인증 서버(Authentication Server), 정보 서버(Info Server), 모니터링 시스템(Monitoring System)을 추가하였다.

에이전트(Agent)는 네트워크 연결 및 서비스 제공, 인증 세션을 통제하는 서버이다. 스마트 시티 서비스에 접속하는 사용자의 인증을 요청받고, 인증 서버에 해당 사용자의 인증 및 접근 권한을 요청한다. 이때 사용자의 연결 환경(위치, 기기 유형, 네트워크 상태 등)에 따라 일시적 사용자와 지속적

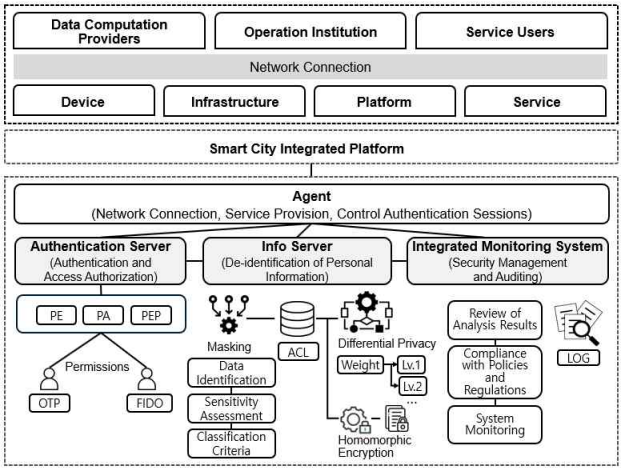

그림 5. 제안하는 프라이버시를 위한 보안 모델
Fig. 5. A proposed security model for privacy

사용자로 구분하는 적응형 인증 방법을 사용한다. 인증 서버에 인증 요청 시 임시적 사용자 경우 인증 서버에 OTP 인증 또는 SMS 인증을 요청하며, 지속적 사용자 경우 FIDO 인증을 요청하게 된다.

인증 서버(Authentication Server)는 사용자 인증 및 접근 권한을 부여하며, 사용자의 접근을 통제하는 서버이다. 인증 서버는 정책엔진(PE), 정책관리자(PA), 정책시행시점(PEP)로 구성된다. PE는 사용자의 접근 권한을 부여하며, PA는 사용자의 세션별 인증 및 인증 토큰 또는 자격 증명을 생성한다. PEP는 사용자 요청 시 인증 정보를 통해 세션을 관리한다. 이는 제로 트러스트 보안 개념을 사용자의 동적 접근 제어에 응용 하였다.

모니터링 시스템(Monitoring System)은 사용자 인가 여부, 정보 보호구역 통제, 사용자 로그 관리와 감사 기능을 하는 시스템이다. 정기적인 감사를 통해 접근 제어 정책의 준수 여부를 확인하고, 비정상적인 접근 시도를 모니터링하여 보안 위반 사항을 즉시 탐지한다.

그림 6은 인증 서버의 사용자 인증 과정을 나타낸 것이다. 사용자 인증을 요청받았을 때 인증 서버는 임시 사용자에게 일시적 인증코드를 전송하고, 사용자는 해당 코드를 입력하여 인증을 완료한다.

지속적 사용자인 경우 인증 서버로부터 FIDO 인증 요청을 받게 되며, 사용자는 인증 수단(지문, 얼굴인식, PIN번호 등)을 사용하여 인증을 완료하면, 해당 정보는 암호화되어 인증

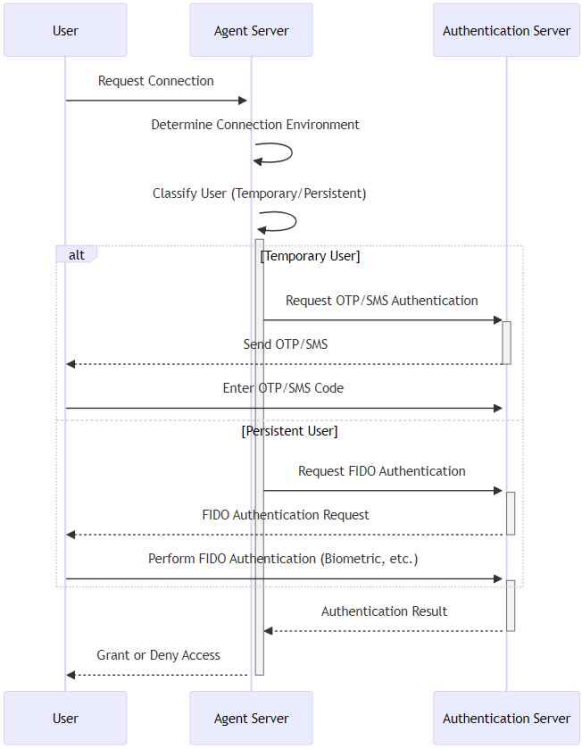

그림 6. 제안하는 모델의 사용자 인증 과정
Fig. 6. User authentication process for the proposed model

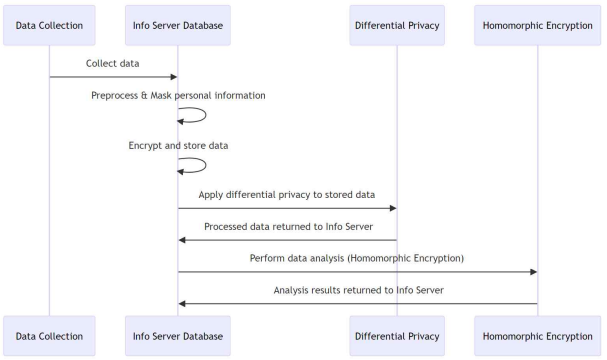

그림 7. 제안하는 모델의 프라이버시 처리 과정
Fig. 7. The privacy process of the proposed model

서버로 전송된다.

인증 서버는 전송된 인증 정보를 검증한 후, 인증 결과에 따라 사용자에게 필요한 서비스나 정보에 대한 접근 권한을 부여하게 된다. 이때 PE는 요청한 사용자의 정보에 따라 데이터 접근을 제한할 수 있으며, PEP을 통해 권한을 동적으로 부여할 수 있다.

그림 7은 프라이버시를 위한 데이터 저장과 처리 과정을 표현한 것이다. 스마트 시티의 데이터를 저장하는 정보 서버(Info Server)는 스마트 시티의 다양한 정보를 저장한다.

수집된 데이터는 저장 전 전처리 과정을 거치며, 이때 개인정보 검출 및 마스킹 모듈을 이용하여 개인정보가 포함된 이미지나 데이터를 마스킹한다. 마스킹 처리된 데이터는 정보 서버에 암호화되어 안전하게 저장된다.

전처리 과정에서 데이터의 항목을 식별하여 데이터의 유형(개인 식별 정보, 공공 데이터, 익명화된 데이터 등)을 분류한다. 각 데이터 유형의 민감성과 중요성을 평가하여 적절한 보안 수준을 설정한다. 저장된 데이터는 접근 제어 목록(ACL)을 통해 데이터에 접근 가능한 사용자나 접근 권한의 목록을 관리한다.

데이터 사용을 위해 데이터는 차분 프라이버시 처리를 통해 추가적인 개인정보 보호 조치를 하게 된다. 데이터는 사용 범위와 시스템 정책에 따라 수준별로 분류되며, 데이터 민감도에 따라 가중치(노이즈 값)를 부여하여 각 수준에 따라 차분 프라이버시가 적용되어 데이터 프라이버시 수준이 결정된다. 또한 일부 데이터는 동형 암호화 방법을 적용하여 암호화된 개인정보가 식별되지 않은 상태에서도 검색 가능하도록 하여 세부적인 데이터는 엄격한 접근 제어하에 제공될 수 있도록 한다.

프라이버시 처리 과정을 거친 결과는 모니터링 시스템에서 보안 감사를 실행하여, 데이터 분석 결과의 프라이버시 보호 수준을 평가하고, 이행되는 프라이버시 조치들이 표준과 규정을 준수하는지 검토를 자동화한다. 또한 모든 데이터 분석 및 검토 활동에 대한 감사 로그를 생성하고 보관한다. 이는 데이터에 대한 접근 시도와 접근 유형을 지속적으로 모니터링하여, 비정상적인 접근 패턴이나 무단 접근 시도를 감지한다.

Ⅳ. 제안 모델의 보안성 평가

본 논문에서 제안한 모델은 스마트 시티 프레임워크에 제로 스트러트 개념을 응용한 시스템 구조로 동적 사용자 접근을 제어하고, 차분 프라이버시와 동형 암호화 방법을 적용하여 프라이버시 보호를 강화하였다. 제안 모델의 보안성 평가를 위하여 STRIDE와 LINDDUN의 분류 기준에 따라 도출한 보안 요구사항을 만족하는지 분석하였다. 표 5는 제안 모델의 인증기법을 STRIDE 분류 기준에 따라 보안성 만족도를 나타낸 것이다. 제안 모델의 사용자 인증 기법에서 일시적 사용자 인증 방법인 OTP 인증은 합법적인 사용자만 접근할 수 있는 고유 코드를 제공하여 스푸핑 공격을 방지할 수 있으며, OTP는 일시적인 특성으로 인해 조작이나 재사용이 어려우므로 오용 위험이 줄어든다. 지속적 사용자 인증 방법인 FIDO 인증은 생체 인식 또는 하드웨어 토큰을 사용함으로써 높은 수준의 보호기능을 제공하며 데이터 변조가 어렵고, 고유한 자격 증명으로 인해 사용자의 작업 기록 추적이 가능하다.

표 5. 보안 모델의 STRIDE 보안성 분석
Table 5. STRIDE security analysis of security models

Technology/ Process	S	T	R	I	D	E
Authentication (OTP/SMS, FIDO)	●	○	●	○	○	○
Authentication Server Validation (PE, PA, PEP)	●	◐	●	●	◐	●
Encryption of Authentication Data	○	●	◐	●	○	○
Agent Access Control	◐	◐	◐	○	◐	●
System Monitoring	◐	●	●	●	●	◐

※ ● : High, ◐ : Medium, ○ : Weak

또한 제로 트러스트 개념을 응용한 인증 서버의 접근 제어 및 동적 접근 권한 부여는 민감한 데이터에 대한 사용자의 데이터 접근을 엄격하게 통제하며, 사용자에게 최소한의 필요한 정보만이 제공되므로 정보 유출의 가능성을 최소화한다. 모니티링 시스템을 통한 지속적인 검증은 권한 상승 시도를 방지하며, 데이터에 대한 모든 활동은 로그로 기록되어 관리 및 분석되어 부인 방지의 역할을 수행한다. 이러한 인증 방법은 STRIDE에서 식별된 다양한 보안 위협에 대해 데이터를 보호하는데 중요한 역할을 하며, 스마트 시티 프레임워크 내에서 안전한 인증 시스템을 보장한다.

표 6은 프라이버시 보안 기법을 LINDDUN의 분류 기준에 따라 보안성을 분석하여 나타낸 것이다. 수집된 데이터를 저장 전 전처리를 통해 개인정보 검출 및 마스킹 처리하며, 이를 암호화하여 저장하는 과정은 개인정보 식별 가능성과 무단 정보 공개를 방지하는데 매우 효과적인 방법이라 할 수 있다. 또한 차분 프라이버시 처리 과정을 통해 개인정보 연결성과 식별 가능성을 크게 줄여 데이터 분석이 개인의 프라이버시를 침해하지 않도록 보장한다. 동형 암호화 기법은 암호화된 데이터를 처리할 수 있게 함으로써 유용한 데이터 분석을 가능하게 하면서 프라이버시를 유지한다.

표 6. LINDDUN 분류에 의한 프라이버시 보안성 분석
Table 6. Privacy security analysis by LINDDUN classification

Technology/ Process	L	I	N	D	D	U	N
Personal Information Detection & Masking	◐	●	○	◐	●	◐	◐
Data Encryption	○	●	◐	○	●	●	○
Differential Privacy Processing	●	●	○	●	●	◐	●
Homomorphic Encryption	●	◐	○	●	●	○	○
Data Classification & Weighting	◐	◐	○	◐	◐	◐	●
System Monitoring	◐	◐	●	●	●	○	◐

※ ● : High, ◐ : Medium, ○ : Weak

차분 프라이버시 기법에서 시스템 정책에 맞추어 가중치를 적용하여 데이터 수준에 따라 보안 등급을 결정하는 방안은 정보의 유출과 프라이버시 위험을 효과적으로 관리하고 준수한다. 또한 보안 감사 및 모니터링을 통해 부인 방지와 정책 및 동의 불이행 위협에 대해서도 효과적으로 대응할 수 있다.

Ⅴ. 결 론

최근 스마트 시티에 대한 관심이 증가하고 있으며, 이는 도시 문제를 해결하고 데이터 수집 및 분석 기술을 통해 도시 운영의 효율성을 높이는 데 초점을 두고 있다. 스마트 시티의 보안 위협은 각 구성 요소의 구현 단계마다 존재하고 있으며, 특히 스마트 시티 서비스를 위해 ICT와 IoT를 비롯한 다양한 첨단 기술을 통한 대량의 데이터가 실시간 수집 및 분석되면서 프라이버시 침해 문제가 대두되고 있다. 따라서 스마트 시티 구성 요소의 보안을 강화하고, 프라이버시를 보호하는 체계적인 접근 방법이 요구된다.

본 논문에서는 스마트 시티 서비스에 있어서 효과적으로 사용자 접근을 제어하고 프라이버시 보호를 위한 보안 서비스 모델을 제안하였다. 이를 위해 스마트 시티 각 구성 요소별 다양한 보안 위협과 프라이버시를 위한 보안 기술 및 사용자 인증 기법에 대해 살펴보았다. 또한 제안 모델은 STRIDE와 LINDDUN 모델의 분류 기준을 사용하여 보안 요구사항을 도출하고, 프라이버시 보호 방법을 체계적으로 분류함으로써 스마트 시티 서비스가 직면할 수 있는 주요 보안 위협에 대응하는 구체적인 보안 모델을 제시하였다. 제안된 모델은 스마

트 시티 서비스에 접근하는 사용자를 효율적으로 인증하고 관리하기 위해 적응형 인증 기술 및 FIDO 방법을 사용하며, 제로 트러스트 개념을 적용한 에이전트와 인증 서버, 모니터링 시스템을 추가하였다. 이는 사용자의 동적 접근 제어를 가능하게 하며, 비정상적인 접근을 모니터링하여 보안 위반 사항을 탐지한다. 또한 데이터 저장 전 처리과정에서 데이터 보안 정책에 따른 사용자 식별 정보를 암호화하고 마스킹하여 프라이버시를 보호하며, 데이터 활용 단계에서 데이터 접근 제어 메커니즘을 강화하기 위하여 차분 프라이버시와 동형 암호화 기법을 적용하여 프라이버시를 강화하였다. 제안 모델의 보안성을 분석한 결과 STRIDE와 LINDDUN 모델의 분류 기준에 따른 위협에 대응할 수 있는 보안 요소를 충분히 갖추고 있음을 확인하였다.

제안 모델은 스마트 시티의 설계와 운영단계에서 프라이버시를 중심으로 한 보안 접근 방식을 채택함으로써 사용자의 프라이버시를 강화하고, 디지털 신뢰를 구축한다. 향후 제안 모델을 구현하여 스마트 시티 환경에 적용하였을 때, 그 효과를 평가함으로써 스마트 시티의 프라이버시와 보안 강화를 위한 구체적이고 실용적인 가이드 라인을 제공할 수 있도록 모델을 개선해 나갈 예정이다.

참고문헌

[1] J. Lee and J. Lee, “The Future after Digital Transformation Smart City Trends in 2023,” *Smart City Top Agenda 2023,* pp. 282-294, February 2023.

[2] S. M. Park, H. M. Choi, and S. I. Choi, “Examining Smart City Paradigm Shift : A Focus on Global Indices and Major Cities Case Studies,” *Journal of the Korea Academia-Industrial Cooperation Society*, Vol. 25, No. 2, pp. 270-279, February 2024. https://doi.org/10.5762/KAIS.2024.25.2.270

[3] H. Lee and K. Son, “A Study on a Smart City Supply Chain Security Model Based on Zero-Trust,” *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 32, No. 1, pp. 123-140, February 2022. http://dx.doi.org/10.13089/JKIISC.2022.32.1.123

[4] H. J. Kim and T. S. Shon, “A Study on Cyber Security Threat Intelligence(CTI) Utilization for Smart City Security,” *Journal of Digital Contents Society*, Vol. 20, No. 6, pp. 1173-1180, June 2019. http://dx.doi.org/10.9728/dcs.2019.20.6.1173

[5] Korea Internet & Security Agency. Smart City Security Model [Internet]. Available: https://www.kisa.or.kr/2060205/form?postSeq=13&lang_type=KO.

[6] F. Loukil, C. Ghedira-Guegan, and K. Boukadi, “Privacy-Preserving IoT Data Aggregation Based on Blockchain and Homomorphic Encryption,” *Sensors*, Vol. 21, No. 7, 2452, April 2021. https://doi.org/10.3390/s21072452

[7] Y.-J. Shin, “The Improvement Plan for Personal Information Protection for Artificial Intelligence(AI) Service in South Korea,” *Journal of Convergence for Information Technology*, Vol. 11, No. 3, pp. 20-33, March 2021. https://doi.org/10.22156/CS4SMB.2021.11.03.020

[8] J. S. Jang, “A Study on the Highly Trust Network for Personal Information Protection of IoT Environment,” *Journal of Digital Contents Society*, Vol. 21, No. 3, pp. 609-616, March 2020. http://dx.doi.org/10.9728/dcs.2020.21.3.609

[9] R. P. Romansky and I. S. Noninska, “Challenges of the Digital Age for Privacy and Personal Data Protection,” *Mathematical Biosciences and Engineering*, Vol. 17, No. 5, pp. 5288-5303, August 2020. http://dx.doi.org/10.3934/mbe. 2020286

[10] Y. C. Kim, J. H. Hong, and Y. G. Kim, “Establishment of a Service Operation Platform Based on Information Linkage to Improve Stability,” *Journal of Digital Contents Society*, Vol. 24, No. 7, pp. 1583-1589, July 2023. http://dx.doi.org/10.9728/dcs.2023.24.7.1583

[11] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating Noise to Sensitivity in Private Data Analysis,” in *Proceedings of Third Theory of Cryptography Conference*, pp. 265-284, March 2006. http://dx.doi.org/10.1007/11681878_14

[12] Homomorphic Encryption Standardization. Homomorphic Encryption [Internet]. Available: https://homomorphicencryption.org/.

[13] G. Y. Kim, M. J. Shin, and I. C. Euom, “Privacy Exposure Corresponding Framework of Artificial Intelligence System Considering the Life Cycle of Personal Information,” *Journal of Information Technology and Architecture,* Vol. 18, No. 3, pp. 255-264, 2021. http://dx.doi.org/10.22865/jita.2021.18.3.255

[14] H. G. Yeo, M. G. Kang, and S. I. Sonh, “A Study on the DID Based Smart Remocon and FIDO Transaction Certification for Home-Shopping,” *Smart Media Journal*, Vol. 9, No. 1, pp. 60-66, 2020.

[15] M. Kang, “FIDO Platform of Passwordless Users based on Multiple Biometrics for Secondary Authentication,” *Journal of Internet Computing and Services*, Vol. 23, No. 4, pp. 65-72, August 2022. https://doi.org/10.7472/JKSII.2022.23.4.65

[16] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 2020, “Zero Trust Architecture,” National Institute of Standards and Technology, NIST Special Publication 800-207, August 2020. https://doi.org/10.6028/NIST.SP.800-207

[17] R. McRee, “Microsoft Threat Modeling Tool 2014:

Identify & Mitigate," *ISSA Journal*, pp. 39-42, May 2014.
[18] Linddun. Privacy Threar Knowledge Support [Interent]. Available: https://linddun.org/threats

김시정(Si-Jung Kim)

1990년 : 한밭대학교(공학학사)
1995년 : 한남대학교 대학원 (교육학석사)
2002년 : 한남대학교 대학원 (공학박사-컴퓨터응용)

2013년～2018년: ㈜에이티엔티 연구소 소장
2019년～2019년: 우송대학교 SW융합대학 초빙교수
2020년～현 재: 청주대학교 교양학부 교수
※관심분야 : 정보보호(Personal Information), 컴퓨터교육(Coumputer EDU), 스마트 시티플랫폼(SmartCIty)등

조도은(Do-Eun Cho)

2008년 : 충북대학교 대학원(공학박사)

2008년～현 재: 목원대학교 SW교양학부 교수
※관심분야 : 정보보호(Personal Information), 센서네트워크(Sensor Network), 공학교육(Engineering Education) 등