https://doi.org/10.33778/kcsa.2022.22.1.129

스마트 통합플랫폼 보안위협과 대응방안 연구★

유 승 재*

ABSTRACT

스마트플랫폼이란 기존 플랫폼과 첨단 IT기술을 결합함으로써 물리 및 가상공간을 초연결 환경으로 구현한 진화된 플랫폼이라 정의된다. 초연결로 언급되는 정보와 정보, 인프라와 인프라, 인프라와 정보, 공간과 서비스가 연결은 사용자의 삶의 질과 환경을 획기적으로 변화시켜 주는 고품질의 서비스 구현 및 제공을 가능하게 한다. 특히 스마트 정부와 스마트 헬스케어 구현으로 사회안전망과 개인건강관리 수준을 획기적으로 개선시킨 효과를 모두에게 제공하고 있다. 이 과정에서 생산되고 소비되는 수많은 정보들은 그 자체로서 혹은 빅데이터 분석을 통해 공공 및 개인의 기본권을 위협하는 요인으로 작용할 수 있다. 특히 스마트시티의 생태계를 형성하는 핵심기능으로서의 스마트플랫폼은 자연스럽게 지속적으로 확장되어 가기 때문에 그에 따르는 데이터의 처리운용과 네트워크 운영 상 커다란 보안 부담에 직면하고 있다. 이 논문에서는 스마트시티의 핵심 기능으로서의 플랫폼 구성 요소와 그에 대한 적절한 보안위협 및 대응 방안을 연구한다.

A Study on the Security Threat Response in Smart Integrated Platforms

Seung Jae Yoo*

ABSTRACT

A smart platform is defined as an evolved platform that realizes physical and virtual space into a hyper-connected environment by combining the existing platform and advanced IT technology. The hyper-connection that is the connection between information and information, infrastructure and infrastructure, infrastructure and information, or space and service, enables the realization and provision of high-quality services that significantly change the quality of life and environment of users. In addition, it is providing everyone with the effect of significantly improving the social safety net and personal health management level by implementing smart government and smart healthcare. A lot of information produced and consumed in these processes can act as a factor threatening the basic rights of the public and individuals by the informations themselves or through big data analysis. In particular, as the smart platform as a core function that forms the ecosystem of a smart city is naturally and continuously expanded, it faces a huge security burden in data processing and network operation. In this paper, platform components as core functions of smart city and appropriate security threats and countermeasures are studied.

Key words : Cyber Security, Smart Security Platform, Smart City

접수일(2022년 02월 28일), 게재확정일(2022년 03월 31일)

* 중부대학교 정보보호학과

★ This paper was supported by Joongbu University Research & Development Fund, in 2021

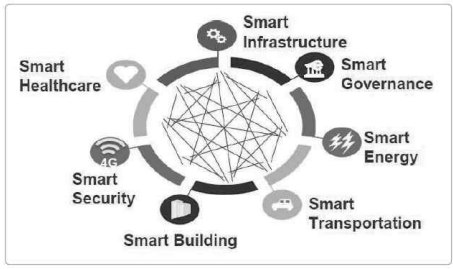
Ⅰ. 서론

스마트플랫폼이란 기존 플랫폼과 첨단 IT기술을 결합함으로써 물리 및 가상공간을 초연결 환경으로 구현한 진화된 플랫폼이라 정의된다. 초연결로 언급되는 정보와 정보, 인프라와 인프라, 인프라와 정보, 공간과 서비스가 연결은 사용자의 삶의 질과 환경을 획기적으로 변화시켜주는 고품질의 서비스 구현 및 제공을 가능하게 한다. 특히 스마트 정부와 스마트 헬스케어 구현으로 사회안전망과 개인건강관리 수준을 획기적으로 개선시킨 효과를 모두에게 제공하고 있다. 이 과정에서 생산되고 소비되는 수많은 정보들은 그 자체로서 혹은 빅데이터 분석을 통해 공공 및 개인의 기본권을 위협하는 요인으로 작용할 수 있다. 특히 스마트시티의 생태계를 형성하는 핵심기능으로서의 스마트플랫폼은 자연스럽게 지속적으로 확장되어 가기 때문에 그에 따르는 데이터의 처리운용과 네트워크 운영 상 커다란 보안 부담에 직면하고 있다.

이 논문에서는 스마트시티의 핵심 기능으로서의 플랫폼 구성 요소와 그에 대한 적절한 보안위협 및 대응방안을 연구하기 위해서 먼저 스마트플랫폼 유형과 현황을 조사하고, 그 운영과 서비스 구현을 위한 보안 요구사항을 검토한다. 그리고 보편적 사이버보안 위협의 유형별 대응방안과 함께 사이버 환경의 진화에 따른 스마트통합보안 플랫폼의 구현 필요성을 제언한다.

Ⅱ. 스마트플랫폼 현황

스마트시티는 인적자원과 환경, 에너지, 교통, 도시, 인프라 등 도시 관련 모든 자원에 첨단 ICT를 활용하여 지속적인 경제발전과 삶의 질 향상을 실현하는 미래형 도시로 정의된다. ICT와 인공지능 등 신기술 전반을 적용한 인프라와 서비스를 구현한 기능적인 플랫폼 도시이다. 스마트 시티는 도시, ICT, 공간정보 등의 인프라 그리고 IoT, 데이터 공유, 알고리즘, 도시 서비스 등의 구성요소를 바탕으로 형성되며[6], 도시 구조, 도시 운용 및 서비스 등에서 도시 전체가 하나의 플랫폼으로 연결되는 유기적이며 창의적인 도시이다. 고도화되고 인간 친화적인 IIoT 기반의 융·복합 기술의 발달로 인하여 교통, 방범, 에너지, 주차, 상하수도 등 생활밀착형 서비스 효과는 물론 에너지 효율화, 신도시 개발, 신기술 개발 등 추진목표에 따라 다양한 유형의 플랫폼 구성이 가능하다.



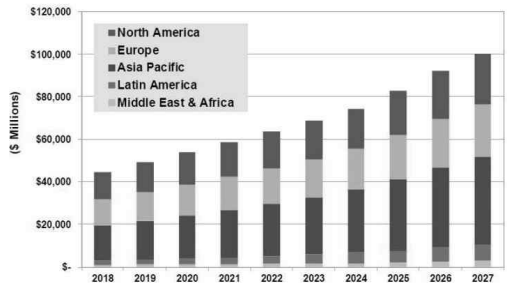
[그림1] 스마트시티 주요 분야 [14]

스마트시티의 주요구성은 위 [그림1]과 같이 제시되었는데, 여기서 스마트정부는 개념적으로 정보통신기술에 기반한 차세대 전자정부라 할 수 있다. 간섭없는 정보제공의 연속성과 인프라, 에너지, 교통, 헬스케어, 빌딩 등의 각종 구성요소에 대한 보안과 고품질 서비스를 제공하도록 구현된다. 여러 분야의 스마트시티의 구성요소들을 유기적이고 효율적으로 관리하기 위한 여러 핵심기술과 주요 어플리케이션들이 적용되고 있는데, 이를 통해 주목할 만한 수준의 도시비용절감, 생산성 향상 및 경제지표 개선의 효과를 기대할 수 있으며[7], 도시에서의 이동성, 보건 공공안전, 생산성 등에서 현저한 절약의 효과가 예상된다.[13]

[그림2] 2010~2030 스마트시티 국가별 투자규모 [8]

위 [그림2]는 해외 주요국 스마트시티 프로젝트 투자 예상규모이다. 이에 따르면 해외 주요국들은 교통혼

잡, 범죄·재난, 환경문제 등의 도시문제를 해결하고 시민편의를 제고하기 위하여 ICT 기술을 접목한 스마트시티 프로젝트 추진 중에 있으며, 2030년까지 총투자규모는 미국이 $6,850B, 중국 $7,450B 그리고 일본 $1,170B로 전망했다.[8] 또한 Markets and Markets은 2019년 전망보고서에서 연평균 18.4%의 성장을 통하여, 2023년 $617.2B 규모가 될 것으로 전망했으며, 아래 [그림3]과 같이 Navigant Research는 2027년 기준 $100B으로 전망하며 전 세계적 확산을 예측했다.



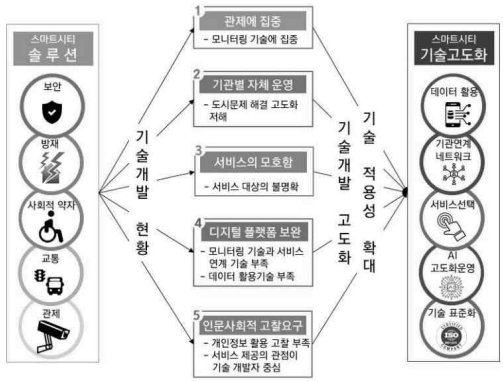
[그림3] 스마트시티 시장규모 예측[12]

스마트시티 구축과 서비스 운영을 위한 기반환경으로서 IEEE에서는 네트워크와 통신, 사이버물리시스템과 IoT, 클라우드와 에지컴퓨팅, 개방형 데이터 그리고 빅데이터와 데이터 분석 등의 5개 ICT 기술을 제시하였고, 스마트도시 핵심 기술로는 스마트그리드, 지능형 교통, 헬스케어, 에너지효율화, IoT, 5G, 사이버 안전, 전자 거버넌스, 스마트홈, 딥러닝 기술 등을 제시하였다. 또한 [그림4]와 같이 이들의 통합플랫폼 구축을 통해 스마트시티 서비스의 효율화를 추구하였다.

[그림4] 스마트시티 서비스분야 및 개발기술[9]

이를 기반으로 스마트시티 표준화와 서비스 분야 통합플랫폼 구축 및 고도화를 위한 지속적인 기술개발 연구와 지원체계 구축 이슈가 강조되고 있으며, 다양한 서비스 운영을 효율적으로 제공하고 관리하기 위한 표준화된 통합 플랫폼 기술개발이 고도화되고 있는 추세이다.[9]

아래 [그림5]는 통합플랫폼 기술개발의 필요성과 기술개발 핵심 키워드와의 관계를 설명한 것이다.



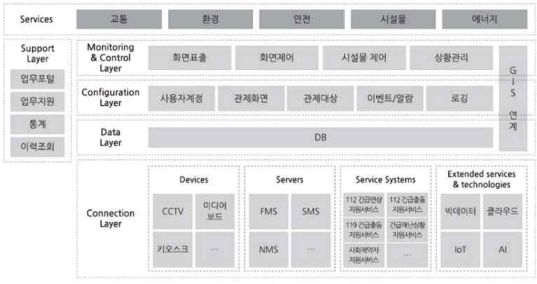
[그림5] 통합플랫폼 기술개발 핵심 키워드[9]

그러나 현재의 스마트시티 구축과 서비스 운영에는 여러 개선 필요 요구사항들이 있는 것으로 연구·보고되고 있는데 그 중 서비스 자체가 민간 영역과 밀접하여 현재 대부분 공공영역에만 집중되어 있는 부분, 제한적인 기술개발 상황 등이 있다. 또한 민감한 개선요구부분으로서, 데이터에 의한 플랫폼 대부분이 민간 사업자에 의해 개발되어 공공플랫폼과의 연동 어려움, 그리고 수집되는 데이터의 완전한 개방에 대한 정보 분류체계 및 제도적 장치의 미흡 등은 신속한 개선이 요구되는 부분이다. 이러한 한계점 개선을 위한 전략으로 우선 스마트 통합플랫폼 구축이 제시되고 있다. 공공영역 통합플랫폼과 민간영역 연계를 위한 기술개발 및 향후 미래지향적 설계(AI, 디지털 트윈, 개방형 데이터, 빅데이터 등의 주제를 중점으로 한 스마트시티 구축계획 수립 및 기술 방향성외 서비스 영역 확장 등)를 그 개선 방안으로 고려된다.

또한 급변하는 글로벌 기술 변화 트렌드 반영의 한계를 고려하여 미래지향적 원천기술의 개발을 중심으로 추진하는 것이 타당할 것이다.

Ⅲ. 스마트시티 구성기술요소 및 보안 요구사항

정보화 기반 도시인 U-City의 경우는 구성요소기술로써 ICT인프라 구축에 기반한 정보의 수집가공-활용에 주안점을 둔다면, 스마트시티는 스마트기술·인프라, 통합플랫폼기술 및 서비스솔루션기술을 기반으로 한 서비스에 주안점을 둔다고 할 수 있다. 도시와 공간을 연결하는 공간정보 및 통신인프라 등의 기반기술 환경 하에 에너지, 교통, 안전, 헬스케어 등 도시 공간 내에 구현된 다양한 스마트 서비스를 유기적이고 원활하게 운영하도록 하는 통합플랫폼 구축을 위해 AI등 수 많은 요소 세부기술들이 동작하고 있다.
기본적으로 스마트시티 요소 기술의 근간은 IoT, Cloud, BigData, Mobile기술임은 자명하며 여기에 AI와 그 응용기술들이 주요 핵심을 이루고 있다.
아래 [그림6]은 스마트시티 통합플랫폼 소프트웨어 구조를 구조화한 것인데 데이터, 각각의 레이어 구성요소마다 대부분 보안공격요소들로서 기능적 측면에 앞서 보안위협에 대한 검토와 선제적 대책마련이 동시에 제시되어야 할 것이다.



[그림6] 스마트시티 플랫폼 소프트웨어 참조모델[4]

스마트시티의 사이버보안 위협은 기존 네트워크 보안 위협과 IoT 보안위협을 망라하여 기밀성, 무결성, 가용성 및 인증 등 전반적인 영역에서 이슈화 될 것이다. 아래 [표1]은 전 세계의 사이버 보안에 관한 연구결과를 반영하여, 스마트시티 보안 위협요소들을 선정하고 아래 표와 같이 분류한 것이다.[1]
스마트시티 보안위협 확대의 근본 배경으로 디바이스, 연결성 그리고 데이터의 급격한 증가를 들 수 있다.

<표1> 스마트시티 사이버보안 위협요소[1]

스마트시티 사이버보안 요구사항		
멀웨어공격	원격활동공격	HW/SW비인가조작
비인가SW설치	데이터유출	정보조작
사회공학적공격	정보누설	감사도구악용
DDoS공격	개인정보탈취	비인가행위
Spam공격	가짜인증서	거짓정보
목표된공격	방출자료가로채기	정보가로채기
무차별공격	메시지재생공격	세션도용
승인남용	네트워크조작	워드라이빙
출처미상정보활용		

수많은 IoT디바이스와 플랫폼과 사람들 간의 상호 다자간 복합적 연결 및 서비스 운영에서 많은 위협지점들이 노출된다.[5] 보안성이 취약한 펌웨어로 인해 디바이스 자체에 대한 공격, 취약한 디바이스를 경유한 서비스플랫폼 공격, 이후 서비스플랫폼 해킹을 통한 디바이스 임의제어 등으로 이어지는 연쇄적인 공격으로 최악의 경우 도시 전체를 마비시킬 수 있음을 쉽게 예상할 수 있을 것이다.

[그림7] 스마트 통합보안 플랫폼 구조

스마트시티의 보안은 사이버보안영역에서 인프라, 서비스, 인프라, 공간 등 물리적 영역 포함 전 구성요소로 확대하여 사이버공격에대한 강한 내성을 갖춘 보안 면역체계 구축이 요구된다. 이로부터 중단 없는 서비스 체제를 유지하는 것이며 이를 위해 최초의 기획과 설계단계에서의 보안구축은 물론 운영상에서 IT와 물리를 망라한 융합보안 모니터링 및 대응 복구체계를 갖추는 것, 그리고 지속적으로 보안수준 유지를 위한 상시검점 체계를 갖추는 것이 필요하다. 이를 반영

한 아래 [그림7]은 스마트플랫폼의 통합보안 플랫폼 구성의 개요이다.

다음 [표2]에서는 스마트시티의 보안성유지를 위한 진단평가를 위해 설계된 보안모델의 구성을 정리한 것이다. 여기에는 보안관리, 서비스, 디바이스, 통합플랫폼, 인프라 등 5개 영역으로 구분하고, 총 27개 분야에 대해 57개 통제항목에 대한 132개의 이행지침을 보안모델로 제시하였다.

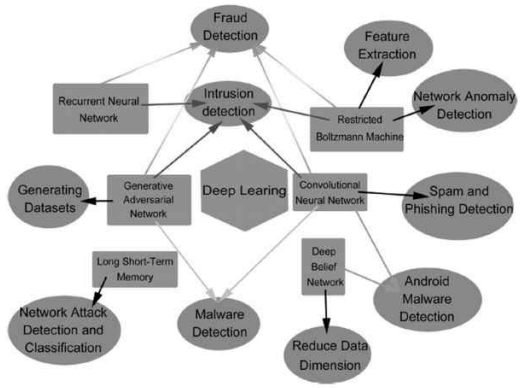
<표2> 스마트시티 보안모델[4]

구분 (분야수/항목수/이행지팀)	분야 (항목수/이행지침)
스마트시티 보안관리 (8/24/61)	정책, 조직, 자산관리 (4/11) 통합운영센터 보안 (3/5) 접근통제 (3/7) 네트워크보안 (2/6) 프라이버시 관리 (2/7) 기록 및 검토 (2/5) 서비스도입 및 개발보안 (6/14) 사고예방 및 대응 (2/6)
스마트시티 서비스 (2/3/10)	스마트시티서비스 (2/7) 데이터흐름관리 (1/3)
스마트시티 디바이스 (5/12/27)	인증관리 (2/4) 모니터링 (3/11) 연속성관리 (3/8) 디바이스보안관리 (3/12) 데이터흐름관리 (1/2)
스마트시티 통합플랫폼 (4/9/18)	인증관리 (2/4) 모니터링 (3/11) 연속성관리 (3/8) 데이터흐름관리 (1/5)
스마트시티 인프라 (4/9/26)	인증관리 (2/4)
	모니터링 (3/11)
	연속성관리 (3/8)
	데이터흐름관리 (1/3)
계 (23/57/132)	

스마트플랫폼에서는 인프라, 서비스 망론하고 수많은 보안상의 위협과 취약점이 노출될 수 있는데, 보안모델을 통해 진단·평가하여 개선하는 환류체계를 통해 그 보안성을 강화에 유용하게 활용될 것으로 기대된다. 실제로, 초고용량 네트워크 트래픽 관리문제, 폭발적 증가가 예상되는 단말기기 서비스 인증 처리문제, 수많은 이벤트로 발생되는 빅데이터 관리문제, 프라이버시와 금융정보 등 각종 유형의 개인정보침해 문제는 물론이고, 에너지나 교통망 등 기반시설에 대한 무수한 사이버공격 시도에 적절히 대응하기 위한 복합적이고 통합적인 보안체계의 구축이 요구된다.

이에 대해서 우선 고려사항으로 AI기술을 통한 사이버 보안 영역의 능동적 개선 가능성을 검토해 보면 대표적으로 사이버완화, 데이터보안 및 생체인증 등에서 강력한 성능을 기대할 수 있을 것이다.[10]

Mandiant.의 조사보고서[11]에 따르면 발생하는 전체 사이버공격 중 33%정도 차단, 26%는 탐지, 9%는 경보가 이루어지지만 나머지 53%는 아무 대응이나 감지조차 없이 벌어지고 있는 것으로 보고되는데, AI를 통한 사이버 위협 예측시스템을 통해 대규모 데이터 풀을 스캔하고 공격행동패턴을 분석 식별한다면 비탐지 비율을 현저히 줄일 수 있을 것이다.



[그림8] 스마트시티 딥러닝모델응용과 사이버보안[2,3]

데이터 보안적 측면에서 AI기술을 접목하여 폭발적인 증가추세의 데이터 관리의 난제를 해결함으로써 유출사고로 인한 손실 예방 등 데이터관리의 효율성을 높일 수 있을 것이다. 또한 AI기반기술을 악용할 경우 기존의 식별기술의 통제를 회피할 수 있는 위변조가 가능하기 때문에 [그림8]에서 보듯이 AI기반의 학습을 통해 정밀한 인식 성능을 갖춘 AI기반 생체인증 기술 적용으로 적절한 인증과 접근통제를 구현할 수 있을 것이다.

Ⅳ. Conclusions

스마트플랫폼을 위한 안전한 보안구축의 시작은 사이

버 환경의 진화를 인지하고 기존의 레거시 시스템에 대한 위협대책만으로는 감당할 수 없음을 인식함으로부터 시작된다.

점진적인 암호체계의 개선, 사회안전망 위협요소에 대한 규정과 대응을 위한 관리적 보안전략 및 기술적 보안시스템 개발을 필요로 한다. 인프라 안전대책으로서 통신 및 에너지 인프라에 대한 물리 정보보안 환경 관리가 수행되어야 한다. 각기 독립적으로 운영되면서 공공·민간 인프라 및 서비스에 대한 각종 위협상황과 대응정보 통합관리를 위한 지자체 하부단계부터 통합노력과 함께 범정부 차원의 기구설치운영으로 소·중·대규모 시스템별 위협유형 분석 및 대응을 위한 세분화·고도화된 인공지능기반의 분석·대응시스템 구축 및 확대운영을 추구해하 할 것이다. 사이버보안의 효율성을 제고하고 안전한 대응환경 구축을 위해서는 먼저 적정한 보안 기준선 설정과 함께 보안검증 과정의 자동화된 시스템의 구축이 요구된다. 이에 선행되어야 할 부분으로 효율의 최적화 유지와 보안환경의 변화에 대한 경계와 검토가 필요하다. 공격기술과 공격도구의 변화와 빠른 전파, 그리고 엔드포인트와 네트워크 등 적대적인 공격벡터의 증가로 인한 다발적 공격 우려 등 사이버위협의 진화에 대응하여 스마트 플랫폼 기반 요소인 네트워크 구성에 대한 내외부의 지속적인 모니터링과 자동화된 보안검증 프로세스의 구현·구축이 요구된다.

참고문헌

[1] 김성민 외2명, “프레임워크 기반 스마트시티 사이버보안 메트릭스”, 한국산업융합학회논문집, 제23권 제2호. 333-341, 2020.

[2] Chen. etl, “Cyber security in smart cities: A review of deep learning-based applications and case studies”, Sustainable Cities Soc. Vol. 66, 102655.

[3] Chen Ma, “Smart city and cyber-security; technologies used, leading challenges and future recommendations” Energy Reports7, 7999-8012, Elsevier, 2021.

[4] 스마트시티 보안모델, 한국인터넷진흥원 2020.

[5] 주성진, “스마트시티보안”, LGCNS Security Summit 2021.

[6] IoT 오픈 플랫폼 기반 스마트시티 분야 서비스 사례집, 정보문화진흥원 2016.

[7] 스마트시티 발전전망과 한국의 경쟁력 보고서, 한국정보화진흥원, 2016.

[8] SPRI, 산업 동향 https://spri.kr/posts/view/21846?code=industry_trend.

[9] AI·데이터 기반 스마트시티 통합플랫폼 모델 개발 및 실증을 위한 기획연구, 국토교통과학기술진흥원, 2020.

[10] Global Cybersecurity Outlook 2022, World Economic Forum.

[11] Deep Dive into Cyber Reality, Security Effectiveness Report 2020, Mandiant.

[12] Utility opportunities in smart cities, Navigant Research report, 2019.

[13] Smart Cities - What’s Init for Citizens?, Junifer Research, 2018.

[14] Frost & Sullivan, “Moving the Smart Cities Idea from Concept to Reality”, Progress of smart cities and market implications evaluated at Growth, Innovation and Leadership 2013.

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수
email : sjyoo@joongbu.ac.kr