Journal of Next-generation Convergence Information Services Technology Vol.15, No.3, June (2026), pp.435-448
ISSN 2384-101X(p) 2672-1163(e) *http://dx.doi.org/10.29056/jncist.2026.06.12*

키워드 네트워크와 BERTopic 모델링을 통한 디지털 트윈 기반 정보보안 연구동향 분석

Analysis of Digital Twin-based Information Security Research Trends through Keyword Networks and BERTopic Modeling

이동은[1], 한주연[2], 김문구[3], 박민재[4]*

DongEun Lee[1], Jooyeon Han[2], MunGoo Kim[3], MinJae Park[4]*

요 약

본 연구는 계량서지학 네트워크 분석과 BERTopic 토픽 모델링을 활용하여 디지털 트윈 기반 정보보안 연구의 동향을 분석하였다. Scopus 데이터베이스에서 디지털 트윈과 보안 관련 검색어를 활용하여 수집한 308편의 학술지 논문을 대상으로 출판 및 인용 현황, 주요 저널 분포, 국가 간 협력 네트워크, 키워드 공출현 네트워크, 그리고 연구 주제의 의미 구조를 살펴보았다. 관련 논문은 2018년에 처음 발표된 이후 2025년까지 CAGR 약 93.07%로 빠르게 성장한 것으로 나타났다. 인용 수 기준 상위 저널 상당수가 IEEE 계열 학술지로 확인되어 해당 분야가 공학 및 정보통신 기술 영역과 밀접하게 연관되어 있음을 보여준다. 국가 간 협력 네트워크에서는 중국과 미국이 중심적 위치를 차지하였으며, 중국은 논문 수에서, 미국은 국가 간 연결 매개 역할에서 두드러지는 것으로 나타났다. 키워드 네트워크 분석에서는 디지털 트윈과 사이버보안이 핵심 키워드로 확인되었으며, 블록체인, IoT, CPS, AI 등이 주요 클러스터를 형성하였다. 도출된 9개 클러스터는 스마트 시티, ICS, 헬스케어, 에너지 인프라 등 적용 분야별로 연구 주제가 세분화되고 있음을 보여준다. BERTopic 분석에서는 스마트 그리드 보안, CPS 및 ICS 사이버 위협, 헬스케어 데이터 프라이버시, 자율 시스템 보안, 차량 네트워크 보안 등 11개 토픽이 도출되었다. 이러한 결과는 디지털 트윈 기반 정보보안 연구가 다양한 산업 분야에서 디지털 트윈이 적용되는 과정에서 기술적 취약점 탐지, 위협 관리, 정책적 대응을 아우르는 방향으로 발전하고 있음을 시사한다.

핵심어 : 디지털 트윈, 정보보안, 사이버보안, 계량서지학 분석, BERTopic, 키워드 네트워크

1 Department Science Technology Policy, Ajou University, Gyeonggi, Korea [Graduate Student]
e-mail: eastgrace@ajou.ac.kr
2 Department Science Technology Policy, Ajou University, Gyeonggi, Korea [Graduate Student]
e-mail: bistella@ajou.ac.kr
3 Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea [Senior Researcher]
e-mail: mkkim@etri.re.kr
4 Department Business Analytics, Ajou University, Gyeonggi, Korea [Professor]
e-mail: geglove@ajou.ac.kr (Corresponding author)

* 이 논문은 2026년 아주대학교 학술연구조성비의 지원으로 작성되었습니다.

Received(April 21, 2026), Review Result(1st: May 14, 2026), Accepted(June 13, 2026), Published(June 30, 2026)

Abstract

This study analyzes research trends in digital twin-based information security through bibliometric network analysis and BERTopic topic modeling. A total of 308 journal articles indexed in Scopus were collected using search terms related to digital twin and security, and their publication and citation trends, journal distribution, country-level collaboration networks, keyword co-occurrence networks, and topic structures were examined. Related publications first appeared in 2018 and grew rapidly through 2025, recording a CAGR of approximately 93.07%. Most highly cited journals were IEEE publications, reflecting the field's close ties to engineering and information and communications technology. In the collaboration network, China and the United States held central positions, with China leading in publication volume and the United States acting as the primary mediator of cross-national connections. Keyword analysis identified digital twin and cybersecurity as the core keywords, with blockchain, IoT, CPS, and AI forming key surrounding clusters, and the 9 clusters suggest that research topics are increasingly differentiated by application domain such as smart cities, ICS, healthcare, and energy infrastructure. BERTopic modeling yielded 11 distinct topics covering smart grid security, CPS and ICS cyber threats, healthcare data privacy, autonomous system security, and vehicular network security. These findings indicate that the field is moving toward technical vulnerability detection, threat management, and policy responses as digital twins are applied across various industries.

Keyword : digital twin, information security, cybersecurity, bibliometric analysis, BERTopic, keyword network

1. 서론

디지털 트윈(digital twin)은 현실의 물리 시스템을 가상 환경에 구현하고 양측의 데이터를 교환하여 시스템 상태를 분석하고 관리하는 기술이다. IoT, 인공지능(AI), 데이터 분석 기술과 결합해 산업 시스템의 운영 효율성과 의사결정을 지원하는 핵심 기술로 주목받으며 [1], 제조업 중심에서 에너지, 의료, 교통, 스마트 시티 등으로 확대되고 [2]. 디지털 트윈 환경에서는 물리 시스템과 가상 시스템이 네트워크로 상시 연결되어 데이터가 오가므로 데이터 위변조, 서비스 거부 공격, 중간자 공격 등의 위험이 크다. 특히 사이버-물리 시스템(cyber-physical systems, CPS)에서는 공격이 시스템 오작동과 물리적 피해로 이어질 수 있고 [3], 다양한 장치와 네트워크가 결합된 구조로 인해 데이터 보안과 개인정보 보호가 중요한 연구 주제로 논의된다 [4]. 이에 보안 위협과 대응 전략에 관한 논의도 늘고 있다. 다양한 사이버 공격에 대응할 보안 기술과 위협 대응 체계의 필요성이 제시되는 한편 [5], 디지털 트윈으로 시스템 동작을 가상 환경에서 분석해 취약점을 사전에 파악하는 방안 [6], AI 및 머신러닝(ML)을 활용한 대응 전략 [7]도 제시되고 있다.

디지털 트윈 환경의 정보보안에 대한 관심이 높아지면서 동향을 정리하는 서지분석 연구도 이루어지고 있다. Ravi Prakash et al. [8]은 블록체인 기반 사이버보안, Ganji and Afshan [9]은 IoT 정보보안, Pourmadadkar et al. [10]은 CPS 기반 중요 인프라 보안, Purnama et al. [11]은 머신러닝(machine learning, ML) 기반 사이버보안 연구를 각각 분석하였다. 반면 디지털 트윈 자체를 중심에 둔 분석은 매우 제한적이다. Achuthan et al. [12]은 디지털 트윈과 사이버보안의 주요 응용 분야와

보안 메커니즘을 제시했으나, 연구 협력 구조나 핵심 키워드 간 관계 등 구조적 특성은 다루지 않았다. 또한 계량서지학 연구는 출판 추세나 키워드 빈도 분석 중심이어서 연구 주제 간 의미적 관계를 심층 파악하는 데 한계가 있다 [13].

이에 본 연구는 Scopus에 수록된 디지털 트윈 기반 정보보안 논문을 대상으로 계량서지학 네트워크 분석과 의미 기반 토픽 모델링을 결합하여 출판 및 인용 현황, 국가 간 협력 구조, 핵심 키워드 네트워크, 연구 주제의 의미 구조를 분석하였다. 연구 질문은 다음과 같다. 첫째, 출판 및 인용 현황, 주요 저널 분포, 국가 간 협력 네트워크는 어떤 특성을 보이는가? 둘째, 키워드 네트워크의 구조와 중심 키워드는 무엇인가? 셋째, 도출되는 주요 연구 토픽과 의미 구조는 무엇인가?

2. 연구배경

2.1 디지털 트윈과 정보보안

디지털 트윈은 현실의 물리적 객체나 시스템을 가상 환경에 구현하고, 양측 데이터를 양방향으로 교환하여 시스템 상태를 실시간으로 모니터링하고 분석하는 기술이다. 제조, 에너지, 의료, 교통 등 다양한 산업에서 운영 효율성 향상과 의사결정 지원에 중요한 역할을 한다. Fuller et al. [1]은 이를 IoT, AI, 데이터 분석 기술과 결합해 예측 유지보수와 운영 최적화를 가능하게 하는 핵심 기술로, Kritzinger et al. [2]은 물리 시스템과 가상 시스템 간 상호 연결 구조로 보며 제조업을 중심으로 여러 산업으로 확산되고 있다고 설명하였다.

활용이 확대되면서 정보보안의 중요성도 높아지고 있다. 물리 시스템과 가상 시스템이 네트워크로 상시 연결되어 데이터 수집, 전송, 저장 전 과정에서 보안 위험이 발생할 수 있으며, 특히 IoT 센서, 네트워크 인프라, 클라우드 플랫폼이 결합된 환경에서는 데이터 위변조, 서비스 거부 공격, 접근 권한 침해가 일어날 수 있다. Humayed et al. [3]은 CPS 환경에서 중간자 공격이나 서비스 거부 공격이 시스템 오작동과 물리적 피해로 이어질 수 있음을, Wang et al. [4]은 다양한 물리 장치와 네트워크가 연결되는 구조적 특성으로 인해 보안 취약성과 개인정보 보호가 주요 연구 과제로 부상하고 있음을 지적하였다.

한편 디지털 트윈은 보안 위험을 높이는 기술일 뿐 아니라 보안 관리 도구로도 활용될 수 있다. Suhail et al. [5]은 가상 환경을 활용한 보안 분석과 위협 대응 방안을, Eckhart et al. [6]은 시스템 상태를 반복 시뮬레이션하여 취약점을 사전에 분석하고 대응 전략을 수립하는 활용 가능성을 제시하였다. 이러한 논의는 정보보안이 단순한 기술적 보호 수단을 넘어 시스템 설계 단계에서부터 고려되어야 할 요소임을 시사한다.

2.2 관련 선행연구 고찰

디지털 트윈 기술은 IoT, CPS, AI, 블록체인 등 다양한 디지털 기술과 연결되며 발전하고 있고, 이 연결성은 동시에 새로운 정보보안 위험을 낳는 요인이 되기도 한다. 이에 따라 디지털 트윈과 밀접한 개별 기술 영역을 중심으로 정보보안 연구의 흐름을 정리하려는 서지분석과 체계적 문헌고찰이 이루어져 왔다.

대표적으로 IoT 환경의 정보보안 [9], CPS 기반 중요 인프라 보안 [10], 머신러닝 기반 사이버보안 [11], 블록체인 기반 정보보안 [8] 등이 있으며, 이들은 개인정보 보호, 침입 탐지, 분산 신뢰 구조 등 각 영역의 핵심 주제를 제시하였다.

이처럼 기존 연구는 개별 기술 영역 중심으로 발전 양상을 분석하는 데 초점을 두었으나, 디지털 트윈 자체를 중심에 두고 지식 구조와 주제 변화를 살펴본 연구는 아직 제한적이다. Achuthan et al. [12]은 디지털 트윈과 사이버보안 연구의 주요 응용 분야와 보안 메커니즘을 제시한 점에서 의미가 있으나, 산업 분야별 적용 사례와 기술적 활용 가능성에 초점을 두어 협력 구조나 핵심 키워드 간 관계 등 구조적 특성은 체계적으로 분석하지 않았다. 또한 계량서지학 연구는 출판 추세나 키워드 빈도 분석 중심이어서 연구 주제 간 의미적 관계를 심층 파악하는 데 한계가 있다 [13].

따라서 디지털 트윈 기반 정보보안 연구를 대상으로 연구 협력 구조와 연구 주제의 의미적 관계를 함께 분석하는 접근이 필요하다.

3. 연구 방법

3.1 데이터 수집

본 연구는 디지털 트윈 기반 정보보안 연구의 동향을 분석하기 위해 Scopus에서 관련 학술 논문을 수집하였다. Scopus는 다양한 분야의 국제 학술지 논문을 포함하며 계량서지학 연구에서 널리 활용되는 대표적 데이터베이스이다 [14].

검색어는 "digital twin*", "digital-twin*", "securit*"으로 설정하고 검색 범위는 논문 제목과 저자 키워드로 한정하였다. 검색식은 다음과 같다. (TITLE (("digital twin*" OR "digital-twin*") AND "securit*") OR KEY (("digital twin*" OR "digital-twin*") AND "securit*")) AND DOCTYPE (ar) AND LANGUAGE (english)

문서 유형은 학술지 논문, 언어는 영어로 제한하였고 검색은 2026년 1월 15일에 수행하였다. 이후 제목과 초록을 검토해 디지털 트윈과 정보보안을 동시에 다루지 않는 논문을 제외하여, 최종 308편을 분석 대상으로 확정하였다.

3.2 분석방법

본 연구는 디지털 트윈 기반 정보보안 연구의 지식 구조와 주제를 분석하기 위해 계량서지학 분석, 키워드 네트워크 분석, 토픽 모델링 분석을 순차적으로 수행하였다.

계량서지학 분석(bibliometric analysis)은 서지 정보로 특정 분야의 발전 과정과 구조를 파악하는 방법이다 [15]. 본 연구에서는 연도별 출판 현황, 주요 학술지 분포, 국가별 논문 수와 인용 수를 분석해 분야의 전반적 특성을 파악하였다.

이어서 공동 저자 정보를 기반으로 국가 간 협력 네트워크를 구성하였다. 3회 이상 논문을 출판한 국가의 공저자(co-authorship) 네트워크를 구축해 협력 구조를 시각화하고, 각 국가의 구조적 위치를 파악하기 위해 중심성 분석(centrality analysis)을 수행하였다 [16]. 지표는 연결 중심성(degree centrality, 연결 수), 매개 중심성(betweenness centrality, 중개 역할), 근접 중심성(closeness centrality, 접근 속도), 고유벡터 중심성(eigenvector centrality, 영향력 높은 국가와의 연결 정도) 네 가지이며, 분석은 VOSviewer와 GEPHI로 수행하였다.

다음으로 저자 키워드 기반 공출현 네트워크 분석을 수행하였다. 모든 키워드를 소문자·단수형·약어로 통일하고 오탈자를 수정하는 전처리를 거친 뒤, 3회 이상(전체 논문의 1% 이상) 등장한 키워드를 선정하였다. 공출현 네트워크는 두 키워드가 같은 논문에 함께 등장하는 빈도를 연결 강도로 표현해 어떤 주제들이 함께 다루어지는지를 보여준다. 선정된 키워드로 네트워크를 구성하고 클러스터링 분석과 중심성 분석을 수행해 핵심 키워드와 주제 군집을 도출하였다.

마지막으로 연구 주제의 의미 구조를 분석하기 위해 BERTopic 기반 토픽 모델링을 수행하였다. 토픽 모델링은 대규모 텍스트에서 주요 주제를 식별하고 문서 간 의미적 관계를 분석하는 방법이다. 널리 쓰이던 LDA는 단어 빈도 중심이어서 문맥적 의미를 충분히 반영하기 어렵다 [17]. 반면 BERTopic은 문장 임베딩(sentence embedding)으로 유사 문서를 그룹화한 뒤 대표 토픽을 도출하여 문맥적 의미를 더 잘 반영하는 개선된 방법으로 평가된다 [18]. 본 연구에서는 논문의 제목과 초록을 입력으로 NetMiner를 활용해 분석하였다.

본 논문의 연구 설계, 데이터 분석, 결과 해석, 논문 작성은 모두 저자가 수행하였으며, 문장 표현 개선을 위해 생성형 AI 도구인 ChatGPT(4.5 버전 AUTO)를 일부 활용하였다.

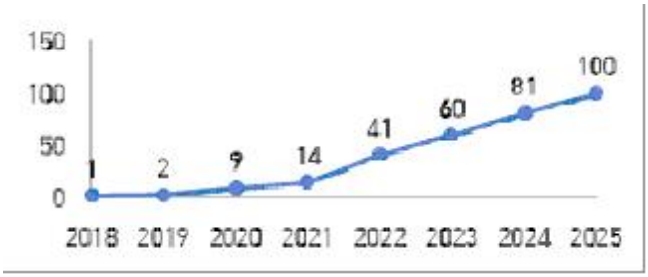
4. 연구 결과

4.1 논문 출판, 인용, 국가간 협력관계 분석

4.1.1 연도별 출판 현황

[그림 1]은 디지털 트윈 기반 정보보안 연구의 연도별 출판 현황을 보여준다. 관련 논문은 2018

년 처음 발표된 이후 꾸준히 증가해 2025년 100편이 출판되었다. 2018년부터 2025년까지의 연평균 복합 성장률(compound annual growth rate, CAGR)은 약 93.1%로, 짧은 기간에 빠르게 성장한 분야임을 알 수 있다. 특히 2020년 이후 논문 수가 두드러지게 증가하는데, 이는 디지털 트윈의 적용 범위가 다양한 산업으로 확대되면서 관련 보안 연구 관심도 함께 높아지고 있음을 시사한다.



[그림 1] 연도별 출판현황

[Fig. 1] Publication Status by Year

4.1.2 출판 및 인용 상위 저널

[표 1]은 논문 수와 인용 수 기준 상위 저널을 분석한 결과이다.

[표 1] 출판과 인용의 상위 10위권 저널

[Table 1] Top 10 journals in publication and citation

순위	논문 출판			인용		
	저널	n	%	저널	n	%
1	IEEE Access	19	6.2%	IEEE Internet of Things Journal	806	9.3%
2	IEEE Internet of Things Journal	15	4.9%	IEEE Communications Surveys and Tutorials	757	8.8%
3	Sensors	14	4.5%	IEEE Access	639	7.4%
4	IEEE Transactions on Intelligent Transportation Systems	10	3.2%	IEEE Transactions on Intelligent Transportation Systems	573	6.6%
5	IEEE Transactions on Consumer Electronics	8	2.6%	IEEE Transactions on Industrial Informatics	503	5.8%
6	Applied Sciences, Future Internet, IEEE Journal on Selected Areas in Communications, IEEE Network	6	1.9%	Buildings	274	3.2%
7				Future Generation Computer Systems	253	2.9%
8				IEEE Network	242	2.8%
9				Computers in Industry	237	2.7%
10	Computers and Electrical Engineering, IEEE Internet Computing, IEEE Transactions on Vehicular Technology, International Journal of Information Security	5	1.6%	IEEE Communications Standards Magazine	212	2.5%

논문 수 기준으로는 IEEE Access(19편, 6.2%)가 가장 높았고 IEEE Internet of Things Journal(15편, 4.9%), Sensors(14편, 4.5%)가 뒤를 이었다. 인용 수 기준으로는 IEEE Internet of Things Journal(806회, 9.3%)이 가장 높았다.

두 기준 모두에서 상위권에 오른 저널은 IEEE Internet of Things Journal, IEEE Access, IEEE Transactions on Intelligent Transportation Systems로, 게재 건수뿐 아니라 연구 영향력 측면에서도 해당 분야를 주도하고 있음을 보여준다. IEEE 계열 외에 Sensors, Future Generation Computer Systems, Computers in Industry, Buildings 등에서도 관련 연구가 발표되어, 이 분야가 IoT, 산업 정보화, 지능형 교통 시스템, 건축 환경 등 공학 및 정보통신 분야의 여러 세부 영역과 밀접하게 연관되어 있음을 보여준다.

4.1.3 출판과 인용의 상위 국가 분석

[표 2]는 논문 수와 인용 수 기준 상위 국가 분석 결과이다. 논문 수와 인용 수 모두에서 중국과 미국이 가장 높은 비중을 차지하였다. 상위 국가의 지역 분포를 살펴보면 아시아(중국, 인도, 한국, 파키스탄), 북미(미국, 캐나다), 유럽(영국, 스웨덴), 중동(UAE, 사우디아라비아) 등 다양한 지역의 국가들이 포함된 것으로 나타났다. 이는 디지털 트윈 기반 정보보안 연구가 특정 지역에 집중되기보다는 여러 지역에 걸쳐 수행되고 있음을 시사한다.

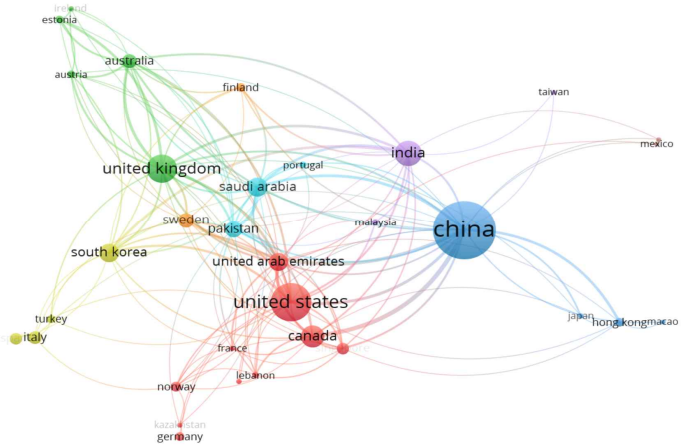
[표 2] 출판과 인용의 상위 10위권 국가
[Table 2] Top 10 countries for publishing and citation

순위	논문 출판			인용		
	국가	n	%	국가	n	%
1	중국	110	35.7%	중국	3228	37.3%
2	미국	60	19.5%	미국	1703	19.7%
3	영국	39	12.7%	영국	1432	16.6%
4	인도	34	11.0%	캐나다	1204	13.9%
5	캐나다	28	9.1%	UAE	1173	13.6%
6	사우디 아라비아	23	7.5%	한국	1002	11.6%
7	한국	22	7.1%	스웨덴	738	8.5%
8	UAE	21	6.8%	인도	667	7.7%
9	파키스탄	18	5.8%	파키스탄	619	7.2%
10	스웨덴	16	5.2%	호주	483	5.6%

4.1.4 국가간 협력관계 분석: 클러스터링과 중심성 분석

[그림 2]는 3회 이상 논문을 출판한 국가의 공저자 기반 협력 네트워크를 구성하고 클러스터링

한 결과로, 총 8개 클러스터가 도출되었다. 가장 규모가 큰 클러스터 1은 미국을 중심으로 캐나다, 프랑스, 독일, 싱가포르 등이 연결된 다지역 구조를 보였다. 그 외에는 영국 중심의 유럽·영연방 그룹, 중국 중심의 동아시아 그룹, 한국 중심 그룹, 북유럽 그룹 등 대체로 지역적 인접성을 바탕으로 형성되었다. 다만 클러스터 1처럼 지리적으로 떨어진 국가가 함께 묶인 경우도 있어, 연구 주제의 유사성 역시 협력 관계 형성에 영향을 미칠 수 있음을 시사한다.



[그림 2] 국가간 협력 클러스터링 결과

[Fig. 2] Results of inter-country cooperation clustering

[표 3]은 중심성 분석 결과를 보여준다. 중국은 가중 연결 중심성(83)과 고유벡터 중심성(1.0000)에서 가장 높아 공저 규모와 영향력 측면에서 네트워크의 핵심 위치를 차지하였다. 미국은 매개 중심성(0.2335)과 근접 중심성(0.6265)에서 가장 높아, 공저 규모에서 두드러지는 중국과 달리 국가 간 연결을 매개하는 역할에서 중심적이었다. 캐나다는 연결 중심성(18)이 상위 국가보다 낮으나 매개 중심성(0.1797)이 두 번째로 높아 일정 수준 이상의 중개 역할을 하였다. 한국은 연결 중심성 8위(16)이며, 고유벡터 중심성(0.7976)은 캐나다(0.7994)와 유사한 수준이었다.

종합하면, 국가 간 협력 네트워크는 중국과 미국이 각각 공저 규모와 중개 역할에서 중심적 위치를 차지하는 가운데 아시아, 북미, 유럽, 중동 등 다양한 지역의 국가가 참여하는 구조를 보였다.

[표 3] 연결 중심성 기준 상위 10권 국가

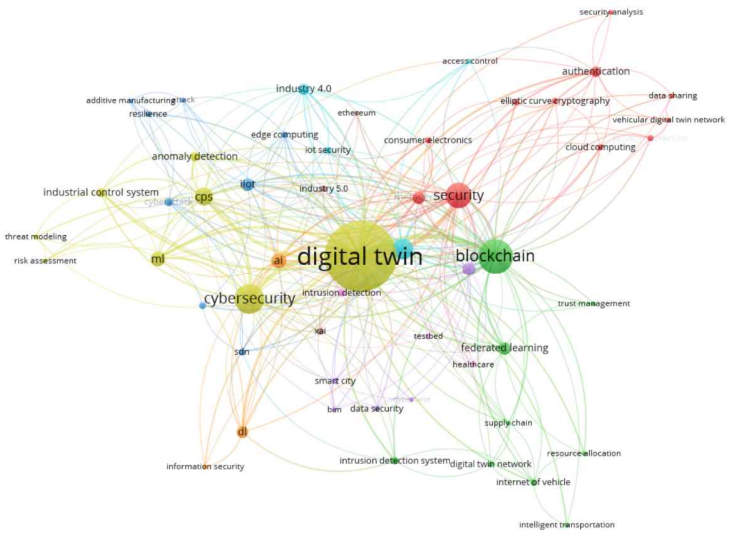
[Table 3] Top 10 countries based on connectivity centrality

순위	국가	연결 중심성	가중 연결 중심성	매개 중심성	근접 중심성	고유벡터 중심성
1	중국	24	83	0.1413	0.6047	1.0000
2	미국	24	60	0.2335	0.6265	0.9931
3	영국	23	67	0.1355	0.6047	0.9728

4	파키스탄	20	44	0.0766	0.5714	0.9170
5	UAE	20	47	0.0579	0.5652	0.9372
6	캐나다	18	45	0.1797	0.5714	0.7994
7	인도	18	49	0.0645	0.5591	0.8549
8	한국	16	35	0.0894	0.5652	0.7976
9	호주	15	40	0.0184	0.5200	0.7602
10	사우디 아라비아	14	42	0.0495	0.5417	0.7174

4.2 키워드 네트워크 및 중심성 분석

VOSviewer로 3회(전체 논문의 1%) 이상 등장한 저자 키워드의 공출현 네트워크를 구성하고 클러스터링 분석을 수행하였다. [그림 3]의 분석 결과 총 9개 클러스터가 도출되었다. 이 가운데 클러스터 4는 디지털 트윈, 사이버보안, CPS, ML, ICS, 이상 탐지, 위협 모델링 등으로 구성되어 핵심 주제가 집약된 중심 클러스터로 확인되었다. 나머지는 인증 및 접근 보안(클러스터 1), 블록체인·FL 기반 분산 보안(클러스터 2), IIoT 및 엣지 컴퓨팅 환경의 사이버 공격 대응(클러스터 3), 스마트 시티 데이터 보안 및 프라이버시(클러스터 5), IoT 및 industry 4.0 보안(클러스터 6), AI 기반 정보보안(클러스터 7)으로 구분되었고, industry 5.0(클러스터 8)과 헬스케어(클러스터 9)는 소규모로 나타났다. 전반적으로 클러스터는 스마트 시티, ICS, 헬스케어, 에너지 인프라 등 디지털 트윈의 주요 적용 분야를 중심으로 구분되었으며, 각 영역에 특화된 보안 기술 키워드가 분포하였다.



[그림 3] 저자 키워드 네트워크와 클러스터링

[Fig. 3] Author Keyword Network and Clustering

이어서 키워드 네트워크의 구조적 특성을 파악하기 위해 중심성 분석을 수행하였으며, 결과는 [표 4]에 제시하였다. 디지털 트윈은 연결·매개·근접·고유벡터 중심성 모든 지표에서 가장 높은 값을 보여 해당 분야의 핵심 키워드로 확인되었다. 사이버보안은 연결 중심성과 고유벡터 중심성에서 두 번째로 높았고 블록체인이 그 뒤를 이었다. IoT, CPS, AI는 중간 수준의 연결 구조를 형성하였으며, 침입 탐지, ML, 프라이버시, 인증, FL 등 세부 보안 기술 키워드도 상위권에 포함되었다.

종합하면, 키워드 네트워크는 디지털 트윈과 사이버보안을 중심축으로 블록체인, IoT, CPS, AI 등이 연결된 구조를 보이며, 스마트 시티, ICS, 헬스케어, 에너지 인프라 등 주요 적용 분야를 중심으로 보안 연구 주제가 세분화되는 경향이 나타났다.

[표 4] 연결 중심성 기준 상위 10권 저자 키워드

[Table 4] Keywords for the top 10 authors based on connectivity centrality

순위	키워드	연결 중심성	가중 연결 중심성	매개 중심성	근접 중심성	고유벡터 중심성
1	digital twin	63	455	0.3888	0.9846	1.0000
2	cybersecurity	48	249	0.1681	0.8000	0.8432
3	blockchain	44	173	0.1295	0.7619	0.8075
4	IoT	29	104	0.0380	0.6465	0.6248
5	CPS	26	68	0.0322	0.6275	0.5559
6	AI	21	58	0.0177	0.5981	0.4950
7	intrusion detection	18	39	0.0128	0.5818	0.4255
8	machine learning	16	42	0.0065	0.5714	0.4398
9	privacy	16	52	0.0064	0.5714	0.4206
10	authentication	15	31	0.0092	0.5664	0.3653
	federated learning	15	29	0.0055	0.5664	0.3981
	industry 4.0	15	34	0.0068	0.5664	0.3868
	metaverse	15	45	0.0057	0.5664	0.4053

4.3 BERTopic 토픽 모델링 분석

BERTopic 분석 결과 총 11개 토픽이 도출되었으며, 노이즈로 분류된 48편(15.6%)을 제외한 260편(84.4%)이 각 토픽에 할당되었다. 세부 내용은 [표 5]에 제시하였다. 가장 비중이 큰 토픽 0(무선 네트워크 환경에서의 객체 보안, 13.6%)은 카메라·센서 등 물리적 객체를 디지털 트윈으로 구현하고 그 환경의 트래픽 및 영상 데이터 보안을 다루는 연구로 구성되었다.

산업 인프라 보안은 두 토픽으로 나타났다. 토픽 1(스마트 그리드 및 전력 인프라 사이버보안, 10.4%)은 전력망과 에너지 시스템에 대한 사이버 공격 대응을, 토픽 2(CPS 및 ICS 사이버 위협, 9.7%)는 산업제어시스템 환경의 위협 분석을 다룬다. 두 토픽 모두 물리 인프라와 가상 시스템이

연결된 환경의 보안 위협을 다룬다는 점에서 디지털 트윈 기반 정보보안의 핵심 영역에 해당한다.

이어 토픽 3(헬스케어 데이터 보안 및 프라이버시, 9.1%)은 의료 데이터와 환자 정보 보호를, 토픽 4(드론·위성 기반 자율 시스템 보안, 7.5%)는 드론·위성·무인 차량의 통신 및 운용 보안을, 토픽 5(엣지 컴퓨팅 환경에서의 자원 관리 및 인증 보안, 7.1%)는 엣지 컴퓨팅의 자원 할당과 인증 문제를 다룬다.

IoT 기기 보안은 토픽 7(IIoT 기기 보안 및 업데이트 관리, 5.5%)과 토픽 10(IoT 기기 보안 정책 및 접근 제어, 4.9%)으로 나타나 펌웨어 업데이트와 FL 기반 보안, 접근 권한 관리를 포함하며, 토픽 6(산업·금융 환경에서의 이상 거래 탐지 및 보안, 5.8%)은 사기 및 이상 거래 탐지를 다룬다.

토픽 8(차량 네트워크 보안, 5.5%)은 VDT를 핵심 키워드로 하여 차량 디지털 트윈이 독자적 연구 영역으로 발전하고 있음을, 토픽 9(내부자 위협 탐지 및 이상 행위 분석, 5.2%)는 외부 공격뿐 아니라 내부자 위협까지 연구 대상에 포함됨을 보여준다.

종합하면, 11개 토픽은 디지털 트윈이 적용되는 다양한 산업 영역의 보안 연구를 반영하며, 스마트 그리드, CPS·ICS, 헬스케어, 자율 시스템, 차량 네트워크 등 적용 분야별로 특화된 주제가 형성되어 있다. 아울러 내부자 위협 탐지, IoT 보안 정책, FL 기반 보안 등 기술적·관리적 대응을 다루는 토픽도 독립적으로 도출되어, 해당 연구가 특정 기술이나 영역에 국한되지 않고 기술적·정책적 측면을 아우르며 발전하고 있음을 보여준다.

[표 5] 토픽별 분포와 핵심 키워드

[Table 5] Distribution by Topic and Key Keywords

토픽	토픽명	n	%	핵심 키워드
Topic 0	무선 네트워크 환경에서의 객체 보안	42	13.6	dt, wireless, object, video, traffic
Topic 1	스마트 그리드 및 전력 인프라 사이버 보안	32	10.4	cyber, grid, power, energy, cyber physical
Topic 2	가상물리시스템 및 산업제어시스템 사이버 위협	30	9.7	cyber, CPS, ICS, risk, cyber attack
Topic 3	헬스케어 환경에서의 데이터 보안 및 프라이버시	28	9.1	healthcare, health, patient, metaverse, medical
Topic 4	드론·위성 기반 자율 시스템 보안	23	7.5	UAV, vehicle, satellite, terrestrial, drone
Topic 5	엣지 컴퓨팅 환경에서의 자원 관리 및 인증 보안	22	7.1	task, organization, computation, delay, authentication
Topic 6	산업·금융 환경에서의 이상 거래 탐지 및 보안	18	5.8	fraud, organization, industry, shopping, online shopping
Topic 7	산업용 사물인터넷 기기 보안 및 업데이트 관리	17	5.5	IIoT, client, update, FL, Internet of Things
Topic 8	차량 네트워크 보안	17	5.5	vehicle, vehicular, VDT, authentication, vehicular digital

Topic 9	내부자 위협 탐지 및 이상 행위 분석	16	5.2	feature, dataset, insider, IDS, insider threat
Topic 10	사물인터넷 기기 보안 정책 및 접근 제어	15	4.9	IoT, product, policy, IoT device, access control

5. 결론

5.1 연구요약과 시사점

본 연구는 ScOPUS 308편의 논문을 대상으로 계량서지학, 네트워크 분석과 BERTopic 토픽 모델링을 수행하여 디지털 트윈 기반 정보보안 연구 동향을 분석하였다. 주요 결과는 다음과 같다.

첫째, 이 분야는 짧은 기간에 빠르게 성장하였다. 관련 논문은 2018년 이후 증가해 2025년 100편이 발표되었고 CAGR은 약 93.1%였다. 이는 디지털 트윈의 적용 확대와 함께 보안 연구 관심도 높아짐을 반영하며, 연구자에게는 새로운 기회를, 실무자에게는 선제적 대응 필요성을 시사한다.

둘째, 이 분야는 공학 및 정보통신 분야와 밀접하다. 출판·인용 상위 저널 상당수가 IEEE 계열이었고, 특히 IEEE Internet of Things Journal, IEEE Access, IEEE Transactions on Intelligent Transportation Systems가 두 기준 모두 상위권으로 IoT, 지능형 교통 시스템, 산업 정보화 등 공학 기반 영역과의 긴밀한 연결을 보여준다. 반면 보안 정책, 규제 설계, 사용자 행동 등 사회과학적 접근의 비중은 낮아, 기술 중심 연구와 정책·제도적 관점 간 접점을 넓히는 확장이 향후 고려될 수 있다.

셋째, 국가 간 협력 구조에서는 중국과 미국이 중심적 위치를 차지하였다. 중국은 공저 규모와 영향력에서, 미국은 연결을 매개하는 역할에서 두드러졌으며, 아시아·북미·유럽·중동 등 다양한 지역이 포함되어 연구가 특정 지역에 한정되지 않음을 보여준다. 한국은 논문 수와 인용 수 모두 상위권이나 연결·매개 중심성은 상위 국가보다 낮아, 국제 공동연구 네트워크 확장이 향후 과제로 제기된다.

넷째, 키워드 네트워크에서 디지털 트윈과 사이버보안이 핵심 키워드로 확인되었고 블록체인, IoT, CPS, AI가 뒤를 이었다. 9개 클러스터는 디지털 트윈 기반 사이버보안 핵심 주제를 중심으로 블록체인·FL 기반 분산 보안, IIoT 및 엣지 컴퓨팅 환경의 사이버 공격 대응, IoT 및 industry 4.0 보안, 스마트 시티 데이터 보안 및 프라이버시, AI 기반 정보보안 등으로 형성되었다. 침입 탐지, ML, 프라이버시, 인증, FL 등 세부 기술 키워드도 상위권에 포함되어, 이 분야가 단일 기술을 넘어 다양한 산업 영역과 보안 기술을 아우르며 발전하고 있음을 보여준다.

다섯째, BERTopic 분석에서 11개 토픽이 도출되어 키워드 네트워크 분석과 상호 보완적으로 의미 구조를 확인할 수 있었다. 스마트 그리드 및 전력 인프라 사이버보안(10.4%), CPS 및 ICS 사이

버 위협(9.7%), 헬스케어 데이터 보안 및 프라이버시(9.1%), 드론·위성 기반 자율 시스템 보안(7.5%), 차량 네트워크 보안(5.5%) 등 적용 분야별 특화 주제가 형성되었고, 내부자 위협 탐지 및 이상 행위 분석, IoT 기기 보안 정책 및 접근 제어, FL 기반 보안 등 기술적·관리적 대응 토픽도 독립적으로 도출되었다. 이는 해당 연구가 기술적 취약점 탐지를 넘어 설계 단계의 보안 내재화, 운용 과정의 위협 관리, 정책적 제도 보완 등 다층적 접근이 필요함을 시사한다. 특히 산업 영역별 특화 주제가 형성되는 만큼, 향후 개별 산업 환경의 특성을 반영한 맞춤형 보안 체계와 정책 방향을 함께 논의하는 것이 중요하다.

5.2 연구한계 및 후속연구 방향

본 연구는 다음과 같은 한계를 가지며, 이는 후속연구의 방향이 된다.

첫째, 시계열적 주제 변화 분석이 이루어지지 않았다. 2018년부터 2025년까지의 논문을 하나의 분석 단위로 처리하여 연도별 토픽 변화나 키워드 트렌드를 동적으로 살펴보는 데 제한이 있다. 계량서지학 연구에서는 특정 시점을 기준으로 기간을 구분하거나 일정 단위로 분절하여 주제 변화를 추적하기도 한다. 향후 시기별 분석을 통해 주제 변화 양상을 보다 구체적으로 파악할 수 있을 것이다. 둘째, 주요 국가별 비교 분석이 충분하지 않았다. 국가 간 협력 네트워크 구조는 분석하였으나 국가별 연구 주제의 차이나 특정 국가의 집중 영역 비교까지는 나아가지 못하였다. 국가별 연구 우선순위나 산업 환경의 차이가 주제 분포에 영향을 미칠 수 있는 만큼, 향후 한국을 포함한 주요 국가의 연구 주제 및 키워드 분포를 비교하여 국가 간 연구 특성의 차이를 세밀하게 살펴볼 수 있을 것이다.

References

[1] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108952-108971, May 2020, doi: 10.1109/ACCESS.2020.2998358.

[2] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, "Digital Twin in manufacturing: A categorical literature review and classification," IFAC-PapersOnLine, vol. 51, no. 11, pp. 1016-1022, June 2018, doi: 10.1016/j.ifacol.2018.08.474.

[3] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security-A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, May 2017, doi: 10.1109/JIOT.2017.2703172.

[4] W. Wang, Z. Su, S. Guo, M. Dai, T. Luan, and Y. Liu, "A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 14965-14987, Apr. 2023, doi: 10.1109/JIOT.2023.3263909.

[5] S. Suhail, R. Jurdak, and R. Hussain, "Security Attacks and Solutions for Digital Twins," Feb. 2022, arXiv:2202.12501, doi: 10.48550/arXiv.2202.12501.

[6] M. Eckhart et al., "Security-enhancing digital twins: Characteristics, indicators, and future perspectives," *IEEE Security & Privacy*, vol. 21, no. 3, pp. 64-75, May 2023, doi: 10.1109/MSEC.2023.3271225.

[7] M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," *Artificial Intelligence Review*, vol. 57, Art. no. 201, Jul. 2024, doi: 10.1007/s10462-024-10805-3.

[8] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, Art. no. 100112, Nov. 2022, doi: 10.1016/j.jjimei.2022.100112.

[9] K. Ganji and N. Afshan, "A bibliometric review of Internet of Things (IoT) on cybersecurity issues," *Journal of Science and Technology Policy Management*, vol. 16, no. 6, pp. 984-1002, Feb. 2024, doi: 10.1108/JSTPM-05-2023-0071.

[10] M. Pourmadadkar, M. Lezzi, and A. Corallo, "Cyber Security for Cyber‐Physical Systems in Critical Infrastructures: Bibliometrics Analysis and Future Directions," *IEEE Transactions on Engineering Management*, vol. 71, pp. 15405-15421, Oct. 2024, doi: 10.1109/TEM.2024.3489273.

[11] Y. Purnama, Y. Nugroho, and H. Prasetyo, "Machine Learning for Cybersecurity: A Bibliometric Analysis from 2019 to 2023," *Journal of Wireless Mobile Networks*, vol. 5, no. 4, pp. 243-258, Dec. 2024, doi: 10.58346/JOWUA.2024.I4.016.

[12] K. Achuthan, B. B. Gupta, and R. Raman, "Bridging cybersecurity with digital twin technology: A thematic analysis," *International Journal of Information Security*, vol. 24, Art. no. 207, Sep. 2025, doi: 10.1007/s10207-025-01115-y.

[13] B. Borsi, Z. Vida, and S. Soós, "Keyword standardization and restructuring: The impact on analysing network-based science maps in innovation management research," *Scientometrics*, vol. 130, pp. 593-617, Feb. 2025, doi: 10.1007/s11192-025-05232-2.

[14] P. Mongeon and A. Paul-Hus, "The journal coverage of Web of Science and Scopus: a comparative analysis," *Scientometrics*, vol. 106, no. 1, pp. 213-228, Oct. 2015, doi: 10.1007/s11192-015-1765-5.

[15] H. P. F. Peters and A. F. J. van Raan, "Co-word-based science maps of chemical engineering. Part I: Representations by direct multidimensional scaling," *Research Policy*, vol. 22, no. 1, pp. 23-45, Feb. 1993, doi: 10.1016/0048-7333(93)90031-C.

[16] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215-239, 1978-1979, doi: 10.1016/0378-8733(78)90021-7.

[17] S. Sia, A. Dalmia, and S. J. Mielke, "Tired of Topic Models? Clusters of Pretrained Word Embeddings Make for Fast and Good Topics too!," in *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, Online, Nov. 16-20, 2020, pp. 1728-1736, doi: 10.18653/v1/2020.emnlp-main.135.

[18] M. Grootendorst, "BERTopic: Neural topic modeling with a class-based TF-IDF procedure," Mar. 2022, arXiv:2203.05794, doi: 10.48550/arXiv.2203.05794.