https://doi.org/10.33778/kcsa.2024.24.2.031

토픽모델링과 시계열 분석을 활용한 클라우드 보안 분야 연구 동향 분석 : NTIS 과제를 중심으로★

윤 선 영*, 조 남 욱**

요 약

최근 클라우드 서비스 사용이 확산하면서 클라우드 보안의 중요성이 증가하였다. 본 연구의 목적은 클라우드 보안 분야의 최근 연구 동향을 분석하고 시사점을 도출하는 것이다. 이를 위해 2010년부터 2023년까지 국가과학기술지식정보서비스(NTIS)에서 제공하는 R&D 과제 데이터를 활용하여 클라우드 보안 연구 동향을 분석하였다. LDA 토픽모델링과 ARIMA 시계열 분석을 통해 클라우드 보안 연구의 핵심 토픽 15개를 도출하였으며, AI를 활용한 보안 기술, 개인정보 및 데이터보안, IoT 환경에서의 보안 문제 해결이 연구에서 중요한 영역임을 확인했다. 이는 클라우드 기술의 확산과 기반 시설의 디지털 전환으로 인해 발생할 수 있는 보안 위협에 대응하기 위해 관련 연구가 필요함을 시사한다. 도출된 토픽들을 기반으로 클라우드 보안 분야를 네 가지 범주로 나누어 기술참조모델을 정의하였으며, 전문가 인터뷰를 통해 해당 기술참조모델을 개선하였다. 본 연구는 클라우드 보안 발전의 방향을 제시하며 학계 및 산업계에 미래 연구와 투자에 대한 중요한 지침을 제공할 것으로 기대된다.

Analysis of Research Trends in Cloud Security Using Topic Modeling and Time-Series Analysis: Focusing on NTIS Projects

Sun Young Yun*, Nam Wook Cho**

ABSTRACT

Recent expansion in cloud service usage has heightened the importance of cloud security. The purpose of this study is to analyze current research trends in the field of cloud security and to derive implications. To this end, R&D project data provided by the National Science and Technology Knowledge Information Service (NTIS) from 2010 to 2023 was utilized to analyze trends in cloud security research. Fifteen core topics in cloud security research were identified using LDA topic modeling and ARIMA time series analysis. Key areas identified in the research include AI-powered security technologies, privacy and data security, and solving security issues in IoT environments. This highlights the need for research to address security threats that may arise due to the proliferation of cloud technologies and the digital transformation of infrastructure. Based on the derived topics, the field of cloud security was divided into four categories to define a technology reference model, which was improved through expert interviews. This study is expected to guide the future direction of cloud security development and provide important guidelines for future research and investment in academia and industry.

Key words : Cloud Security, NTIS, LDA, ARIMA, Technical Reference Model

접수일(2024년 05월 14일), 수정일(1차: 2024년 06월 06일), 게재확정일(2024년 06월 30일)

이 논문은 2024년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0017123, 2024년 산업혁신인재성장지원사업).

* 서울과학기술대학교 IT정책전문대학원 박사과정(주저자)

** 서울과학기술대학교 산업공학과 교수(교신저자)

1. 서 론

COVID-19 팬데믹이 전 세계적으로 확산하면서 원격 근무와 온라인 활동이 증가했고, 이에 따라 클라우드 서비스 활용도가 높아졌다. 이에 따라 개인정보 및 기업의 지적 재산과 고객 데이터를 보호하는 클라우드 보안의 중요성이 강조되고 있다. 클라우드 보안 연구는 이러한 핵심 정보를 보호하고 클라우드 서비스의 안정성을 높이는 데 기여한다.

본 연구의 목적은 클라우드 보안 분야의 최근 연구 동향을 분석하고 시사점을 도출하는 것이다. 이를 위해 국가과학기술지식정보서비스(NTIS, National Science & Technology Information Service)가 제공하는 R&D 과제 데이터를 분석에 활용하여 2010년부터 2023년까지 클라우드 보안 분야 연구 동향을 분석하고자 한다. LDA 토픽 모델링과 ARIMA 시계열 분석을 활용하여 연구 주제의 시간 변화와 발전을 추적하고, 월별 토픽 변화 추이를 분석함으로써 클라우드 보안의 핵심 분야를 식별하고 이를 기반으로 기술참조모델을 정의하고자 한다.

(그림 1) NTIS 개요 [1]

본 연구는 NTIS에서 수집한 R&D 과제 데이터를 기반으로 정량적 분석을 수행한다. 기술참조모델을 정의한 후, 전문가 인터뷰를 통해 해당 모델을 검증하고 보완한다. 이와 같이 정량적 방법론과 정성적 방법론을 모두 활용함으로써 연구의 타당성을 강화했다.

2. 관련 연구

본 절에서는 클라우드 보안 연구와 연구 동향 분석 연구를 중심으로 관련 연구를 살펴보고자 한다.

2.1 클라우드 보안 연구

이선우와 이재우(2022)는 BIGKinds에서 뉴스 데이터를 수집하여 토픽모델링 분석을 수행했다. 해당 연구에서는 COVID-19 대유행 전후의 클라우드 보안 동향 변화를 분석하고, COVID-19 이후 국내에서 클라우드와 클라우드 보안에 관한 관심이 증가한 것을 확인했다[2].

구동영(2020)은 클라우드 관련 시스템의 보안 위협과 취약점을 분석하였다. 연구 결과, 중앙 집중형 클라우드뿐만 아니라 개인 시스템에도 보안 대응이 필요함을 확인했다. 또한, SLA(Service Level Agreement) 체결 시 정보의 기밀성과 무결성 보장이 중요함을 강조했다[3].

신대민 외(2023)는 금융 분야에서 클라우드 전환 사례를 조사하여 전환 동향, 요인, 업권별 특징 및 규제 변화를 분석하고 향후 클라우드 이용 환경의 변화를 예측했다. 연구 결과, 클라우드 규제가 점차 완화됨에 따라 규제 정책에 의해 통제되던 금융정보가 클라우드 기반 서비스로 활용되고, 이와 관련된 보안 조치가 필수적임을 확인했다[4].

2.3 연구동향 분석 연구

양명석 외(2021)는 NTIS가 제공하는 인공지능 관련 국가연구과제를 대상으로 LDA 토픽모델링 기법을 활용해 국가 연구개발 사업의 연구 주제와 투자 방향을 분석했다. 이를 통해 정부는 기초 기

술 연구를 포함하여 다양한 산업 분야에서 각 부처의 특성에 맞추어 인공지능 기술의 활용을 확대하고 있음을 확인했다[5].

박건철과 이치형(2019)은 스마트시티의 개념을 정의하고, SCOPUS와 Springer를 통해 "Smart City"를 포함하는 논문을 수집하여 연구 동향을 분석했다. 연구를 통해 핵심 토픽 8개와 관련 키워드를 도출하였으며, "시민 중심 스마트시티 추진을 통한 지속가능성의 확보"라는 주제가 주로 언급된 것으로 나타났다. 또한 데이터와 프라이버시 관련 연구의 중심성을 연관관계 분석을 통해 확인했다[6].

이수지와 정호현(2023)은 국내외 독과점 규제 관련 논문 초록을 수집하고 LDA 토픽모델링을 통해 주요 토픽 15개를 추출했다. ARIMA 시계열 분석으로 향후 3년간의 연구 중요도를 예측한 결과, 국내에서는 '온라인 거래' 관련 연구의 중요도가 증가할 것으로 나타났다[7].

기존 연구에서는 LDA 토픽모델링과 ARIMA 시계열 분석이 연구 동향 파악에 주로 활용되었다. 본 연구는 이러한 방법론을 클라우드 보안 데이터 분석과 기술참조모델 정의에 적용하여 해당 분야의 연구 동향을 파악하고자 한다. 이 과정을 통해 클라우드 보안 기술의 발전 방향과 연구 필요성을 명확하게 제시하며, 향후 연구의 기초를 마련할 것으로 예상된다.

3. 연구 방법

3.1 분석 대상 데이터

본 연구에서는 2010년부터 2023년까지 NTIS에서 제공하는 클라우드 보안 관련 R&D 과제 데이터 중 '계속과제여부구분'이 '신규'로 지정된 1,540건의 데이터를 수집하였다. 제공된 77개 항목 중 '과제명(국문)', '연구 목표', '연구 내용' 등 5개를 선별하여 분석에 활용하였으며, 해당 항목은 <표 1>에 제시하였다.

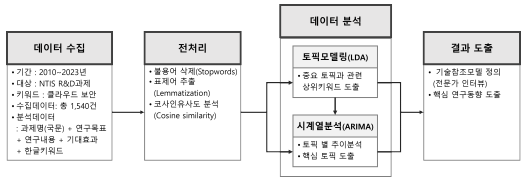
<표 1> 수집 대상 항목(NTIS)

항목	상세 설명
과제명(국문)	연구 세부 과제의 국문명
연구 목표	해당 과제의 연구 목표 요약
연구 내용	해당 과제의 연구 내용 요약
기대효과	해당 과제의 기대효과 요약
한글 키워드	연구를 대표하는 한글 키워드

3.2 연구 프레임워크

본 연구의 프레임워크는 데이터 수집, 전처리, 분석, 결과 해석의 4단계로 구성되어 있으며, 전체적인 프레임워크는 (그림 2)에 제시하였다. 데이터 수집 단계에서 NTIS에서 클라우드 보안 관련 R&D 과제 데이터를 수집한다. 전처리 단계에서 수집된 데이터를 정제하고 표준화하는 작업을 수행하여 분석을 준비한다.

분석 단계에서 데이터는 LDA 토픽모델링을 사용해 클라우드 보안 연구 과제의 주요 주제를 식별하고, ARIMA 시계열 분석을 통해 주제의 시간 추이를 파악한다. 결과 도출 단계에서 분석 결과를 토대로 연구 주제를 그룹화하고 클라우드 보안 분야의 기술참조모델을 정의한다. 해당 모델은 클라우드 보안 연구의 핵심 분야를 보여주고, 향후 연구 방향을 결정하는 데 기준점을 제공한다.



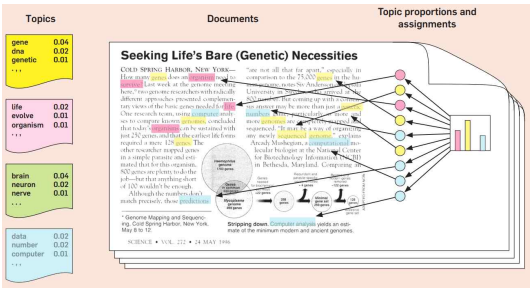
(그림 2) 연구 프레임워크

3.3 데이터 분석

3.3.1 LDA 토픽모델링

LDA(Latent Dirichlet Allocation) 토픽모델링은 텍스트 데이터 집합에서 주제를 추출하는 통계적 방법론이다. 이 모델은 문서가 여러 주제 혼합으로 구성될 수 있다고 가정하고, 각 주제가 특정 단어들로 표현될 확률을 계산하여 주제를 도출한

다. 이 방법론을 사용하여 클라우드 보안 연구와 관련된 대량 문서 데이터에서 중요한 주제와 키워드를 식별하고, 주제별 연구 동향을 파악할 수 있다[8].



(그림 3) LDA 토픽모델링(Blei, 2012) [8]

3.3.2 ARIMA 시계열 분석

ARIMA(Autoregressive Integrated Moving Average) 모델은 자기회귀(AR, Autoregressive)와 이동평균(MA, Moving Average)을 통합하고 비정상 시계열의 차분을 포함하여 개발된 모델로, 기존 ARMA 모델을 확장한 형태이다. 이 모델은 추세나 계절성을 포함하는 비정상 시계열 데이터를 분석하기 위해 설계되었다. ARIMA는 비정상적 변동성을 보이는 사회경제적 또는 비즈니스 관련 시계열 데이터 분석에 유용하다. 데이터의 차분을 통해 비정상성을 제거하고 시계열의 구조적 특성을 파악할 수 있어 복잡한 시계열 데이터를 처리하는 데 사용된다[9].

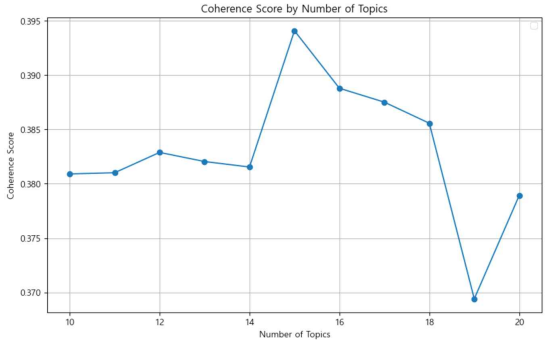
4. 연구 결과

4.1 LDA 토픽모델링 결과

데이터 분석을 위해 불용어(Stopwords) 제거, 표제어 추출(Lemmatization), 코사인 유사도(Cosine similarity) 분석 등의 전처리를 수행하였다. 전처리 과정 후 빈도수가 4번 이상인 단어를 추출하고 Python의 NLTK 라이브러리를 사용해 토큰화를 수행하였다.

LDA 토픽모델링은 Python의 Gensim 라이브러리에서 제공하는 'LdaMulticore' 함수를 적용하였다. 'LdaMulticore'는 여러 프로세서 코어를 활용하여 병렬 처리를 지원하므로 학습 속도를 향상할 수 있다. 반복 횟수(Passes)는 1,000회로 설정하였고, α와 β는 'auto'로 지정하여 데이터에 따라 최적의 값을 적용하도록 하였다.

토픽 수는 토픽 개수별 응집도 지수(Coherence Score)를 확인하여 가장 높은 15개로 결정하였으며, 해당 결과를 (그림 4)에 제시하였다.



(그림 4) 토픽 개수별 응집도 지수

LDA 토픽모델링을 통해 15개 토픽을 도출했으며, <표 2>에 결과를 제시했다. 분석 결과 클라우드 보안 연구는 신기술 접목 분야(Intelligent CCTV, Smart City, Open Banking 등)와 클라우드 운영 환경에 적합한 보안 기술(Document Security, Virtual Network Security, Quantum Cryptography 등)에 중점을 두고 진행된 것을 확인할 수 있었다. 이 결과를 통해 AI 활용 보안 기술, 개인정보 및 데이터보안, IoT 환경에서 보안 문제 해결이 핵심 연구 영역임을 알 수 있었다.

<표 2> 토픽모델링 분석 결과(LDA)

토픽 명		중요키워드	비중(%)
1	Intelligent CCTV	영상, 인공지능, 카메라, 처리, 자동화, 설계, CCTV, 인식	4.34
2	Quantum	암호, 엣지, 설계,	9.64

	Cryptography	양자, 분산, 모델, 프라이버시, 효율	
3	Content Syndication	콘텐츠, 서버, 모델, 디지털, 네트워크, 제공, 모바일, 게임	4.51
4	BigData Platform	구축, 빅데이터, 인공지능, 사업, 체계, 정보, 기업, 운영	11.20
5	Smart City	정보, 검색, 스마트, 스마트시티, 품질, 컨테이너, 인공지능, 평가	4.23
6	Document Security	인증, 서버, 모바일, 사용자, 기업, 제공, 문서, 솔루션	12.58
7	Virtual Network Security	네트워크, 탐지, 공격, 가상화, 정보, 가상, 소프트웨어, 인프라	13.32
8	Smart Sensor	센서, 사물인터넷, 설계, 수집, 모듈, 스마트, 실시간, 구축	11.25
9	Open Banking	모바일, 구현, 서버, 정보, API, 설계, 블록체인, 금융	4.67
10	Smart Port	운영, 인공지능, 예측, 터미널, 항만, 구축, 제공, 스마트	2.77
11	Blockchain Platform	소프트웨어, CDM, 블록체인, 솔루션, 구축, 하이브리드, 구현, 스마트	2.50
12	Healthcare Information	의료, 환자, 병원, 건강, 구축, 정보, 표준, 인공지능	5.14
13	Autonomous Vehicle Security	차량, 자율, 주행, 콘텐츠, 포렌식, 통신, 인증, 실시간	3.67
14	Untact Service	무인, 구축, 목표, 감시, 점포, 서버, 고도화, 제작	2.08
15	Smart Grid	사물인터넷, 설계, 에너지, 스마트, 블록체인, 기기, 소프트웨어, 안전	8.10

도출된 토픽들은 모두 대량의 데이터를 활용하거나 대규모 IoT 디바이스 네트워크를 통합하여 사용하는 기술들이다. 이런 기반 기술들은 안전성과 효율성을 유지하기 위해 클라우드를 활용하고 있다. 이들 토픽에서는 대량의 데이터를 클라우드에 전송하거나 분석하고, 클라우드 보안기술을 통해 사용자 데이터의 프라이버시와 보안을 보장받는다. 연구 결과에 따르면, 클라우드 기술의 확산과 기반 시설의 디지털 전환은 보안 위협을 증가시킬 수 있으며, 이에 대응하기 위한 연구가 필요함을 알 수 있다. 클라우드 기술이 확산함에 따라 보안 문제는 더욱 복잡하고 다층적으로 대두될 것으로 예상된다.

4.2 ARIMA 시계열 분석 결과

ARIMA를 사용하여 각각 토픽의 시계열분석을 수행하였다. ARIMA 알고리즘은 자기 회귀모델의 차수(p), 차분(d), 이동평균(q) 파라미터를 정의해야 한다. 이러한 파라미터는 Python의 pmdarima 라이브러리에서 제공하는 'auto_arima' 함수를 적용하여 최적의 값을 적용하도록 했다.

<표 3>은 ARIMA 분석을 통해 각 토픽의 중요도를 3년 후까지 예측한 결과이다. 각 토픽에 대해 도출된 ARIMA 모델과 AIC, LB Test, JB Test 값을 표시하였다. AIC(Akaike Information Criterion)는 ARIMA 모델의 파라미터(p, d, q)와 모델의 적합도를 평가하는 값으로 낮을수록 모델이 데이터를 더 잘 설명한다. Ljung-Box 검정(LB Test)은 잔차가 백색잡음인지 확인하며, P-value가 0.05보다 클 경우 잔차가 독립적임을 의미한다. Jarque-Bera 검정(JB Test)은 잔차의 정규성을 검정하며, P-value가 0.05보다 클 경우 잔차가 정규분포를 따른다고 볼 수 있다.

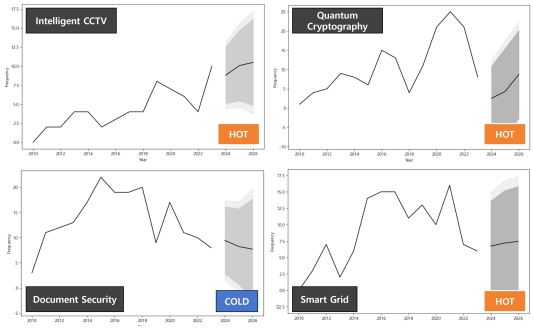
지표를 통해 모델 성능을 분석한 결과 대부분의 토픽이 적합하지만, 일부 토픽(Topic 3, 4, 10, 13)의 경우 데이터를 재선별하는 등의 보완이 필요한 것으로 확인되었다.

<표 3> 토픽 별 시계열분석 결과(ARIMA)

토픽 번호	모델 (p, d, q)	AIC	P-value	
			LB Test	JB Test
1	(1, 2, 1)	61.1447	0.464	0.666
2	(2, 0, 0)	94.1054	0.656	0.604
3	(1, 0, 1)	81.3391	0.712	0.002

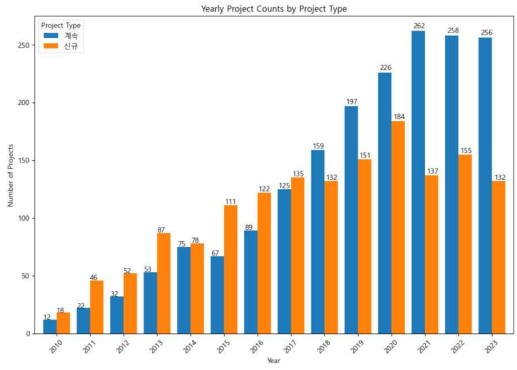
4	(0, 1, 1)	87.6362	0.210	0.628
5	(0, 0, 0)	76.2493	0.965	0.200
6	(1, 1, 2)	82.5754	0.587	0.580
7	(0, 0, 0)	97.1767	0.263	0.806
8	(0, 1, 0)	77.7365	0.450	0.992
9	(2, 1, 0)	59.5776	0.251	0.792
10	(0, 0, 0)	75.4499	0.312	0.001
11	(1, 0, 0)	70.2894	0.578	0.278
12	(2, 1, 0)	74.8797	0.247	0.836
13	(1, 1, 2)	58.3596	0.601	0.013
14	(0, 0, 1)	70.9578	0.880	0.458
15	(1, 0, 0)	86.1003	0.682	0.797

ARIMA 시계열 분석 결과, 'Intelligent CCTV', 'Quantum Cryptography', 'Smart Grid' 토픽은 클라우드 보안 연구 분야에서 'Hot' 토픽으로 분류됐다. 이 결과는 클라우드와 결합 된 IoT 기기들이 클라우드 서비스에서 활용되며, 클라우드 보안 연구에 중요한 역할을 하고 있음을 보여준다. 반면 'Document Security'는 'Cold' 토픽으로 분류돼 연구 활동이 줄어드는 추세를 보였다. 이는 해당 기술이 이미 성숙기에 접어들었거나, 다른 신흥 기술에 비해 관심이 낮아진 것을 의미한다.



(그림 5) 시계열 분석 결과(ARIMA)

(그림 5)의 분석 결과, 2022년부터 Frequency가 감소하고 있으나, 이는 연구 활동 감소를 나타내지 않는다. (그림 6)에서 볼 수 있듯이, 2018년부터 '계속' 과제 수가 '신규' 과제 수를 초과하였음을 확인할 수 있다. '계속' 과제와 '신규' 과제는 내용이 중복되므로 LDA 토픽모델링 분석에서 제외했다. 따라서 나타난 감소 추세는 분석 선택 결과이며, 실제 연구 활동은 감소하지 않았음을 의미한다.

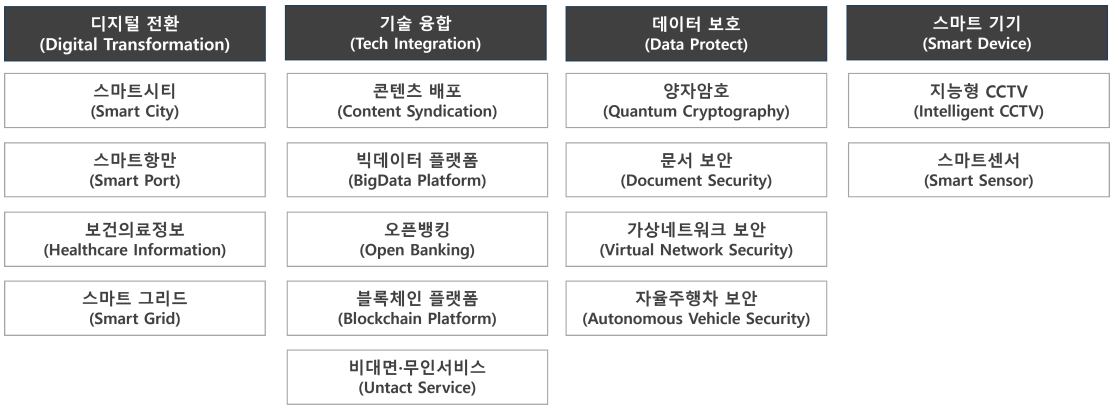


(그림 6) 연도별 과제 수 분포

4.3 기술참조모델

분석을 통해 도출된 토픽들로 클라우드 보안 분야의 연구를 네 가지 범주로 구분하고 기술참조모델을 정의하였다. 기술참조모델을 개선하기 위해, 본 연구는 15명의 전문가와 인터뷰를 진행하였다. 인터뷰에 앞서 연구 내용과 과정, 데이터 분석 방법에 관해 설명하였고, 이를 토대로 전문가들의 의견을 수렴하였다. 인터뷰를 통해 기술참조모델에 반영된 범주와 토픽들이 클라우드 보안 분야의 연구 동향을 적절히 반영하는지 검증하고 모델을 보완하였다.

LDA 토픽모델링으로 식별된 15개의 토픽을 '디지털 전환', '기술 융합', '데이터 보호', '스마트 기기' 네 가지 분야로 분류하였다. '디지털 전환'은 기반 기술에 클라우드와 신기술이 통합된 형태를 나타내며, '기술 융합'은 클라우드와 신기술을 결합한 플랫폼 서비스를 의미한다. '데이터 보호'는 개인정보와 핵심 데이터를 보호하기 위한 기술이며, '스마트 기기'는 클라우드 기반 서비스에 연결되어 데이터를 수집 및 처리하는 기기를 지칭한다.



(그림 6) 클라우드 보안 분야 기술참조모델

이 기술참조모델은 클라우드 보안 연구의 방향성을 정립하고 연구 분야에서 중요한 이슈를 식별하는 데 활용될 수 있다. 또한, 연구자들에게 클라우드 보안의 다양한 시사점을 제공하고 미래 연구 및 개발을 위한 전략적 계획 수립에 도움을 줄 것으로 기대된다.

5. 결론

본 연구는 NTIS에서 제공하는 R&D 과제 데이터를 활용하여 2010년부터 2023년까지의 클라우드 보안 분야 연구 동향을 분석하였다. LDA 토픽 모델링과 ARIMA 시계열 분석을 사용하여 클라우드 보안 관련 핵심 토픽 15개를 식별하고 기술참조모델을 정의하였다.

LDA 토픽모델링 분석 결과, 클라우드 보안 연구는 신기술 접목 분야와 클라우드 운영 환경에 적합한 보안 기술에 중점을 두고 진행되었음을 확인하였다. 이를 통해 AI 활용 보안 기술, 개인정보 및 데이터보안, IoT 환경에서 보안 문제 해결이 핵심 연구 영역임을 알 수 있었다. ARIMA 시계열 분석 결과, 'Intelligent CCTV', 'Quantum Cryptography', 'Smart Grid' 토픽은 클라우드 보안 연구 분야에서 'Hot' 토픽으로 분류되었으며, 이는 클라우드와 결합한 IoT 기기들이 클라우드 서비스에서 활용되며 클라우드 보안 연구에 중요한 역할을 하고 있음을 나타냈다. 기술참조모델을 '디지털 전환', '기술 융합', '데이터 보호', '스마트 기기'의 네 가지 범주로 정의하였고, 전문가 인터뷰를 통해 해당 모델에 반영된 범주와 토픽들이 클라우드 보안 분야의 연구 동향을 적절히 반영하는지 검증하고 모델을 보완했다.

본 연구를 통해 클라우드 기술의 확산과 기반 시설의 디지털 전환은 보안 위협을 증가시킬 수 있으며, 이에 대응하기 위한 연구가 필요함을 알 수 있었다. 연구에서 정의한 기술참조모델은 클라우드 보안 연구의 방향성을 제시하고 각 연구 분야에서 중요한 이슈를 식별하는 데 활용될 수 있다. 또한, 이 모델은 연구자들에게 클라우드 보안의 다양한 시사점을 제공하며, 미래 연구 및 개발을 위한 전략적 계획 수립에 도움을 줄 것으로 기대된다.

참고문헌

[1] NTIS, https://www.ntis.go.kr/ThAbout.do

[2] 이선우, 이재우, “뉴스 데이터 토픽 모델링을 활용한 COVID-19 대유행 전후의 클라우드 보안 동향 파악”, 융합보안논문지, 제22권, 제2호, pp. 67-75, 2022.

[3] 구동영, “클라우드 컴퓨팅 보안 기술 동향”, 정보보호학회지, 제30권, 제6호, pp. 101-106, 2020.

[4] 신대민, 김지윤, 유일선 “국내 금융권 클라우드 전환 동향 및 보안”, 정보보호학회지, 제33권, 제5호, pp. 57-68, 2023.

[5] 양명석, 이성희, 박근희, 최광남, 김태현, “LDA 토픽 모델링을 활용한 인공지능 관련 국가R&D 연구동향 분석”, 인터넷정보학회논문지, 제22권, 제5호, pp. 47-55, 2021.

[6] 박건철, 이치형, “토픽 모델링을 활용한 스마트시티 연구동향 분석”, 인터넷정보학회논문지, 제20권, 제3호, pp. 119-128, 2019.

[7] 이수지, 정호현, “토픽모델링과 시계열 분석을 활용한 국내외 독과점 산업 연구 동향 분석”, 한국데이터분석학회지, 제25권, 제5호, pp. 1683-1699, 2023.

[8] David M. Blei, "Probabilistic Topic Models", Communications of the ACM, Vol. 55, No. 4, pp. 77-84, 2012.

[9] Ratnadip Adhikari and R. K. Agrawal, "An Introductory Study on Time Series Modeling and Forecasting", LAP Lambert Academic Publishing, Germany, 2013.

〔저자소개〕

윤 선 영 (Sun-young Yun)
2020년 8월 동국대학교 국제정보보호대학원 사이버포렌식 석사
2022년 03월 ~ 현재 서울과학기술대학교 IT정책전문대학원 박사과정
email : itpe.yunsy@gmail.com

조남욱 (Nam-Wook Cho)
1994년 2월 서울대학교 산업공학과 학사
1996년 2월 서울대학교 산업공학과 석사
2001년 5월 Purdue대학교 산업공학과 박사
2003년 3월~현재 서울과학기술대학교 산업공학과 교수
email : nwcho@seoultech.ac.kr