2022년도 기본사업 세부(협약)과제 연차보고서

보안등급
일반[ ], 보안[△]

부처명	과학기술정보통신부	사업명	한국전자통신연구원 연구운영비지원 (기본사업)	
전문기관명	한국전자통신연구원			
과제유형	□ 기초 ■ 응용 □ 개발 □ 기타			
대과제 과제명	국가지능화 융합기술 개발로 혁신성장 동인 마련			
대과제 과제책임자	김 형 준	소속 및 부서	지능화융합연구소	
		전화번호	042-860-6576	
세부(협약)과제 과제명 국문	지능형 사이버보안 및 신뢰인프라 기술 연구			
세부(협약)과제 과제명 영문	Research on Intelligent Cyber Security and Trust Infra			
세부(협약)과제 과제책임자	김 익 균	소속 및 부서	정보보호연구본부	
		전화번호	042-860-5442	
과제수행기간 총 과제수행 기간	2020. 1. 1 - 2023. 12. 31 (4년 0개월)			
과제수행기간 단계 1단계	2020. 1. 1 - 2021. 12. 31 (2년 0개월)			
과제수행기간 단계 2단계	2022. 1. 1 - 2023. 12. 31 (2년 0개월)			
과제수행기간 당해 연도	2022. 1. 1 - 2022. 12. 31 (1년 0개월)			

연구개발비 (단위:천원)		정부출연금	민감부담금		합계		
			현금	현물	현금	현물	계
총계		19,670,000	-	-	19,670,000	-	19,670,000
1단계	1년차	4,864,000	-	-	4,864,000	-	4,864,000
	2년차	4,992,000	-	-	4,992,000	-	4,992,000
2단계	3년차	4,907,000	-	-	4,907,000	-	4,907,000
	4년차	4,907,000	-	-	4,907,000	-	4,907,000
당해 연도		4,907,000	-	-	4,907,000	-	4,907,000

참여인력(M/Y)	총 참여인력	157명 (78.2M/Y)	1단계 ('20~'21)	1년차	40명(21.0M/Y)
				2년차	40명(19.9M/Y)
			2단계 ('22~'23)	3년차	37명(17.5M/Y)
				4년차	37명(17.5M/Y)
			당해 연도		37명(17.5M/Y)

공동연구개발기관 등 (해당 시 작성)	기관명	책임자	직위	휴대전화	전자우편	비고 역할	비고 기관유형
공동연구개발기관							
위탁연구개발기관	부경대학교	신상욱	교수		shinsu@pknu.ac.kr	위탁	대학
	계명대학교	박요한	교수		yhpark@kmu.ac.kr	위탁	대학
	상명대학교	서대희	교수		daehseo@smu.ac.kr	위탁	대학
	(사)국제사이버보안연구원	김광조	원장		kkj@kaist.ac.kr	위탁	기타
	한국과학기술원	강민석	교수		minsukk@kaist.ac.kr	위탁	대학
	경북대학교	박영호	교수		parkyh@knu.ac.kr	위탁	대학
연구개발기관 외 기관							

ETRI 실무담당자	성명	조 남 수	소속 및 부서	정보보호연구본부
			전화번호	042-860-1860

이 연차보고서에 기재된 내용이 사실임을 확인하며, 만약 사실이 아닌 경우 관련 법령 및 규정에 따라 과제 중단, 협약 해약, 제재처분 등의 불이익도 감수하겠습니다.

2022년 11월 24일

세부과제책임자 : 김 익 균 (인)

대과제책임자 : 김 형 준 (인)

한국전자통신연구원장 귀하

세부(협약)과제 연차보고서 요약문

대과제명	국가지능화 융합기술 개발로 혁신성장 동인 마련								
세부(협약)과제명	지능형 사이버보안 및 신뢰인프라 기술 연구	과제 유형	기초[ ] 응용[√] 개발[ ] 기타[ ]	TRL	시작	2			
					종료	6			
1 세세부과제명	데이터 안심사회를 위한 트러스트 데이터 커넥톰 원천기술 개발	과제 유형	기초[ ] 응용[√] 개발[ ] 기타[ ]	TRL	시작	2			
					종료	6			
2 세세부과제명	시스템 펌웨어 보안강도 분석 및 검증 연구	과제 유형	기초[ ] 응용[√] 개발[ ] 기타[ ]	TRL	시작	2			
					종료	6			
3 세세부과제명	제로데이 보안체계 기술 검증 연구	과제 유형	기초[ ] 응용[√] 개발[ ] 기타[ ]	TRL	시작	2			
					종료	6			
국가과학기술 표준분류	EE0301. 공통보안기술	50%	EE0302. 네트워크 시스템 보안	30%	EE0304. 산업보안/융합보안	20%			
총 과제수행 기간	2020. 1. 1 - 2023. 12. 31 (4년 0개월)		해당 단계 과제수행 기간		2022. 1. 1 - 2023. 12. 31 (2년 0개월) (1차년도)				
당해연도 과제수행 기간	2022. 1. 1 - 2022. 12. 31 (1년 0개월)								

총연구개발비	연구개발비 (단위:천원)		정부출연금	민감부담금	합계
총 19,670,000 천원 * 정부출연금 : 19,670,000 천원 * 민간부담금 : 0 천원	총계		19,670,000	-	19,670,000
	1단계	1년차	4,864,000	-	4,864,000
		2년차	4,992,000	-	4,992,000
	2단계	1년차	4,907,000	-	4,907,000
		2년차	4,907,000	-	4,907,000

과제수행 목표 및 내용	최종 목표		○ 기존 TTP 기반 환경에 의존하지 않고 데이터 주권과 안전한 교환을 보장하는 트러스트 데이터 커넥톰 원천기술 개발 ※트러스트 데이터 커넥톰 (TDC) : 초연결 지능사회에서 사람, 사물(공간, 생물, 정보, 비즈니스)등이 유기적 상호작용으로 생성한 데이터에 대해 데이터 주권 및 안전한 교환을 제공하는 TTP-free 데이터 거래/활용 신뢰인프라 ○ 정교화·자동화 해킹을 원천차단하는 사이버보안 핵심 기술 개발
	1단계	목표	TTP-free 키교환 및 분산 자율거래 신뢰 플랫폼 주요 ICT 인프라 해킹대응 솔루션 (보안과제)
		내용	- 트러스트 데이터 커넥톰 구조 설계 - 신경망 학습 기반 인증된 키교환 기술 설계 - TTP-free 데이터 프라이버시 보호 기술 연구 - TTP-free 트러스트 데이터 거래 프로토콜 연구
	2단계	목표	트러스트 데이터 거래 실증 서비스 분산 개인 주권/안전성 보장 데이터 거래 실증 국방 ICT 인프라 해킹 대응 서비스 (보안과제)
		내용	- 트러스트 데이터 거래 실증 서비스 PoC - TTP-free 부인방지/접근 권한 세분화 기술 연구 - 트러스트 데이터 거래 책임성 추적 기술 개발 - TDC 통합 시스템 구축 및 PoC
	당해 연도	목표	- 트러스트 데이터 커넥톰 서비스 개발 - 트러스트 데이터 커넥톰 서비스 PoC 시스템 구축 - TTP-free 데이터 프라이버시 강화 기술 연구 - TTP-free 트러스트 데이터 거래 확장 기술 연구
		내용	○ 트러스트 데이터 커넥톰 구조 및 서비스 연구 • 트러스트 데이터 커넥톰 서비스 개발 및 시스템 구축 - 트러스트 데이터 커넥톰 서비스 개발 - 트러스트 데이터 커넥톰 서비스 PoC 시스템 구축 ○ TTP-free 트러스트 데이터 생성 기술 연구 • 데이터 시큐리티 강화 기술 설계 - 학습 기반 인증된 키교환 기술에 대한 수학적 안전성 모델 정립 - 키/알고리즘 정보 비공유 환경에서 데이터 암복호화 기술 설계

			- 제어가능 프라이버시 제공 기술 설계 - 데이터 접근 권한 세분화 관리 기술 설계 ㅇ TTP-free 트러스트 데이터 커넥팅 기술 연구 • 트러스트 데이터 블록체인 네트워킹 기술 개발 - 블록체인 네트워킹(트랜잭션캐스팅&블록캐스팅) 라이브러리 개발 - 블록체인 네트워킹 테스트넷 구축 및 시험 • 트러스트 데이터 거래 확장 기술 개발 - 트러스트 데이터 거래 책임성 추적 기술 개발 - 트러스트 데이터 거래 플랫폼 구축
과제 수행과정 및 내용			**ㅇ 과제 수행과정** - TTP에 의존하지 않는 참여자 사이의 독자적 시큐리티 및 프라이버시 보장 기술 · 기존 암호 체계로는 TTP-free 환경의 시큐리티 보장이 불가능, 신경망 학습 기반 암호 기술 등 새로운 접근 방법 발굴을 통한 데이터 중심의 새로운 안전성 모델 정립 및 기반 기술 확보 · 특정 TTP에 의존하지 않는 암호데이터 중복제거, 거래 부인방지 및 세분화된 권한 제어 기술 및 서비스 환경의 프라이버시 보호 기술 고도화 통해 데이터 거래 환경에서의 프라이버시 보장 - 데이터 소유자 중심의 실시간 데이터 안전 거래 지원 기술 · 실시간 거래가 필수인 데이터 비즈니스 분야에 적용될 수 있는 실시간 데이터 안전 거래 지원을 위한 네트워킹 환경 주소 및 ID 체계 확립 · 차세대 데이터 거래 기술로서 현 블록체인 등 구조의 확장성, 효율성 이슈를 개선한 데이터 안전 거래 구조 제시 및 데이터 거래 책임성 보장 기술 확보 **ㅇ 과제 수행내용** - 신경망 학습 기반 암호 기술 안전성 모델 설계 · 신경망 학습 기반 키교환 기술에 적용 가능한 계산기반 안전성 검증 모델 제시 · 주기적인 신경망 동기화를 통한 학습 기반 데이터 암복호화 기술 설계 - TTP-free 환경의 프라이버시 강화 핵심 기술 연구 · 탈중앙화된 데이터 거래 환경에서 데이터 유효성 검증 모델 개발 · 중앙신뢰기관 비의존적 사용자 중심 데이터 접근권한 세분화 기술 연구 · 프라이버시 강화를 위한 인증 및 키분배 프로토콜 연구 - 트러스트 데이터 블록체인 네트워킹 기술 개발 · 새로운 블록체인 파티셔닝 공격 및 해결 방안 연구 * 이더리움 소프트웨어 취약점 1건 공식 보고 완료 * NDSS2023 최우수학회 논문 진행중 (Major revision 단계) · 거래 참여자 프라이버시 보호를 위한 탈중앙 Web PKI (doTLS) 데이터 모델 설계 - TDC 접근제어 및 책임성 기술 개발 · TTP-free 분산 환경에서 사용자 중심의 키/데이터 관리 기능 및 암호화된 상태에서 데이터 검색 기능 제공 · 거래 데이터 책임성 보장을 위한 Bloom Filter 기반의 데이터 키워드 검증 기술개발 - TDC 거래 플랫폼 개발 · NFT 기반 거래 책임성 추적 가능한 데이터 일괄거래 및 구독거래 프로토콜 개발 · 사용자 프라이버시 보호를 위한 doTLS 기반 데이터 거래 기밀성 보장 통신 기능 개발 - TDC 서비스 모델 연구 · 차량데이터 기반 서비스 모델 2건 설계 및 데이터 생성 모듈 구현 · Healthcare Assistant 서비스 모델 설계 및 거래 검증 도구 제작 · 서비스 실증 적용을 위한 데이터 수집 및 관리 모델 개발 및 관련 SW 개발
과제 수행결과 및 목표달성도			**ㅇ 과제 수행결과**

<table>
<tr><th>구분</th><th>2021년도 (성과)</th><th>2022년도 (성과)</th></tr>
<tr><td>정량</td><td>
<table>
<tr><th colspan="2">논문</th><th colspan="4">특허</th><th colspan="2">기술이전</th></tr>
<tr><th rowspan="2">SCI(건)</th><th rowspan="2">비SCI(건)</th><th colspan="2">해외(건)</th><th colspan="2">국내(건)</th><th rowspan="2">건수</th><th rowspan="2">금액(백만원)</th></tr>
<tr><th>출원</th><th>등록</th><th>출원</th><th>등록</th></tr>
<tr><td>8건</td><td>3건</td><td>3건</td><td>-</td><td>4건</td><td>-</td><td>-</td><td>-</td></tr>
</table>
※논문 목표(2건) 대비 400% 달성
※국내/국제 특허 목표(2건/2건) 대비 각 200%, 150%달성
•(사업화) 해당사항없음
•(표준화) 해당사항없음
•(기타) 해당사항없음</td><td>
<table>
<tr><th colspan="2">논문</th><th colspan="4">특허</th><th colspan="2">기술이전</th></tr>
<tr><th rowspan="2">SCI(건)</th><th rowspan="2">비SCI(건)</th><th colspan="2">해외(건)</th><th colspan="2">국내(건)</th><th rowspan="2">건수</th><th rowspan="2">금액(백만원)</th></tr>
<tr><th>출원</th><th>등록</th><th>출원</th><th>등록</th></tr>
<tr><td>10건</td><td>3건</td><td>3건</td><td>1건</td><td>3건</td><td>2건</td><td>-</td><td>-</td></tr>
</table>
※논문 목표(3건) 대비 333% 달성 (상위20% 3건 포함)
※국내/국제 특허 목표(2건/1건) 대비 각 150%, 300%달성
•(사업화) 해당사항없음
•(표준화) 해당사항없음
•(기타) 해당사항없음</td></tr>
<tr><td>정성</td><td>•특정 TTP에 의존하지 않은 multi-domain 환경에서 프라이버시 보장 기술 제공
- multi-domain 환경에서 다중 TTP 기반 유연한 데이터 권한 관리 모델 제시
- 기밀성, 인증 및 데이터 권한 부여를 제공하는 토큰 기반 multi-domain 인증 모델 설계</td><td>•기존 특정 수학적 난제에 의존하는 증명가능 안전성 모델 적용이 불가능한 신경망 학습 기반 암호 기술에 대한 계산 기반 안전성 모델 제시 및 이를 적용한 안전성 검증 수행
- 우수 국제 학회 IEEE S&P 논문 제출</td></tr>
</table>

○ 과제 수행 목표달성도

가. 과제 수행 목표달성도 (기술개발 성과지표)

전략목표5 국가지능화 융합 기술 개발로 혁신성장 동인 마련			
계획 및 목표달성도	계획 (2단계 2022-2024)	목표달성도 (2단계 2022-2024)	
전략목표 로드맵	**공공.국민생활 문제해결형 국가지능화 융합 핵심기술 개발**	**공공.국민생활 문제해결형 국가지능화 융합 핵심기술 개발**	
성과목표 5-5	지능형 사이버보안 및 신뢰인프라 융합 기술	지능형 사이버보안 및 신뢰인프라 융합 기술	
달성목표	• 트러스트 데이터 거래 실증 서비스 PoC • TTP-free 부인방지/접근권한 세분화 기술 연구 • 트러스트 데이터 거래 책임성 추적 기술 개발 • 트러스트 데이터 커넥톰 통합 시스템 구축 및 PoC	• 트러스트 데이터 거래 실증 서비스 PoC 발굴 • TTP-free 부인방지/접근권한 세분화 기술 연구 • 트러스트 데이터 거래 책임성 추적 기술 개발 • 트러스트 데이터 커넥톰 통합 시스템 개발을 위한 핵심 모듈 개발	달성도 60% ('23년 달성예정)
위 목표의 달성 지표 및 평가 기준	연구개발 달성목표	연구개발 달성실적	달성도
	① 키교환 안전성 모델 제시	• 키교환 기술에 대한 안전성 모델 제시 및 이를 통한 안전성 검증 결과 제출 *'21년 SCIE 논문 게재를 통한 검증 완료, '22.12 개선안 논문 제출 (IEEE S&P)	100%
	② TTP-free 트러스트 데이터 커넥톰 응용 (응용 서비스 실증)	•트러스트 데이터 커넥톰 응용 서비스 발굴	30% ('23년 달성예정)

나. 공통지표

구분	기본지표				심화지표			
	지표명	총사업 연도	'21년도	'22년도 (달성도)	지표명	총사업 연도	'21년도	'22년도 (달성도)
과학적 성과	SCI(E) 논문	10	2	3 / (10)	표준화된 IF 상위 20% SCI 논문(건)	2	-	- / (3)
기술적 성과	국내특허(출원)	8	2	2 / (3)	특허활용률 (기술이전건수/ 특허등록보유건수)	-	-	-
	국내특허(등록)	3	-	- / (2)				
	국제특허(출원)	6	2	1 / (3)	국제표준승인표준 기고서(건)	-	-	-
	국제특허(등록)	2	-	- / (2)				
경제적 성과	기술이전(건)	-	-	-	3극 특허(건)	1	-	-
	기술료(억원)	-	-	-	연구비 대비 기술료 수입(%)	-	-	-

관련 분야에 대한 기여

○ 관련 분야 과학적·기술적·경제적·사회적 기여

과학적	• 총 SCIE 논문 10편 게재, 국내/국제학술대회 3편 발표 - 분산 환경에서 사용자 프라이버시 보호를 위한 보안취약점 분석 및 데이터 수집 기반 기술 연구 (SCIE 상위20% 저널, IEEE IoT(IF10.2), IEEE TDSC(IF6.8), IEEE TNSE(IF5.3) 게재) - 신경망 학습 기반 키교환 안전성 모델 연구 결과 제출 (우수 국제 학회 IEEE Security and Privacy)
기술적	• 국제특허 출원(3건), 국내특허 출원(3건) 및 핵심 기술에 대한 SW구현 완료 - TTP-free한 환경에서 안전하게 사용자주도 데이터 거래가 가능한 플랫폼 구현 - 탈중앙화 데이터 거래를 위한 영지식 증명 기반 데이터 유효성 검증 방법 설계 (3극 특허 출원을 통한 IPR 확보 추진중)
경제적	• 혁신적인 패러다임의 데이터 교환 플랫폼 구현으로 대규모 플랫폼 사업자에 집중된 데이터 비즈니스 생태계 변화에 기여 • 트러스트 데이터 커넥톰 PoC 구현을 통한 다양한 개인데이터 중심 신규 서비스 모델 개발을 통한 관련 산업 확장에 기여
사회적	• 개인 데이터 주권 및 프라이버시 보장을 통해 기존 중앙 집중적인 데이터 수집/가공/활용 기반의 데이터 산업으로 제공하기 어려웠던 개인 데이터 관련 新서비스 분야 창출에 기여 • 공공 데이터 인프라, 산업 인터넷, 스마트 시티 등 데이터 인프라의 신뢰 제고를 위한 기반 신뢰 인프라 플랫폼으로 활용

○ 후속 과제에 도움을 줄 수 있는 연구 결과

- 본 과제를 통해 확보된 신경망 학습 기반 암호화 기술 설계 노하우 및 신경망 학습 고도화 기술을 바탕으로, 향후 양자 컴퓨터 등 새로운 위협에 대응 가능한 新암호기술 설계에 활용 가능
- 본 연구과제를 통해 확보된 TTP-free 환경의 자율적이고 안전한 데이터 거래 플랫폼 핵심 원천 기술을, 향후 국가 정책으로 추진되는 개인데이터의 안전한 활용을 위한 마이데이터 기반 기술 및 융합 프라이버시 보호 분야 R&D에 활용 가능 (※개인정보보호위원회 R&D 로드맵 '21.11.)

<table>
<tr><td>성과관리 및 활용계획</td><td>ㅇ 성과관리 현황
– (데이터 생산 및 관리) 블록 및 트랜잭션 로그 수집을 위해 수정된 비트코인 코어 클라이언트, 이더리움 클라이언트, 이오스 클라이언트로부터 출력된 로그 파일을 일별로 클라우드 노드의 VM에 저장, VM의 하드디스크에 저장된 일별 로그 파일을 주기적으로 연구소 내의 저장 공간으로 이동
– (연구데이터 저장 및 보존) 연구데이터는 연구소 내에 설치된 NAS(Network Assisted Storage)에 저장 관리 중
– (데이터 공동활용) 2단계 연구개발을 통한 통합PoC 구축 결과를, ETRI 지능화융합연구소에서 추진중인 원내 지능화융합 오픈 소스 플랫폼에 향후 SW 라이브러리 형태로 제공을 통해 공유 활용 지원 예정
ㅇ 성과활용 계획
– (기술적) TTP에 모든 시스템의 안전성을 의존하는 현재의 시큐리티 기반 기술의 한계를 극복하여 미래의 예측하기 어려운 보안위협으로부터 데이터 시큐리티를 보장하는 TTP-free 시큐리티 보장을 위한 기반 기술로 활용
- (사회문제해결) 개인 데이터 주권 및 프라이버시 보장을 통해 기존 중앙 집중적인 데이터 수집/가공/활용 기반의 데이터 산업으로 제공하기 어려웠던 개인 프라이버시 데이터 관련 서비스 분야로 확산
- (확보된 기술의 사업화 전략) 과제 결과로 도출된 응용 서비스에 대한 실증 서비스 검증을 통한 상용화 가능성을 확인하여, 국가 공공 서비스에 先적용 후 민간 서비스로 확장하여 신 서비스 산업 창출 기반 조성</td></tr>
<tr><td>향후 과제 수행계획</td><td>ㅇ 다음 연도 연구개발계획
1) 연구개발 목표 및 내용
(성과목표 5-5)
- 트러스트 데이터 커넥톰 통합 검증
- 트러스트 데이터 커넥톰 응용 서비스 실증 및 고도화
- 트러스트 데이터 생성 및 전달 기술 고도화
- 정교화·자동화 해킹을 원천차단하는 사이버보안 핵심 기술(보안과제)
(연구내용)
- 트러스트 데이터 커넥톰 요소 기술 통합 검증
- 트러스트 데이터 커넥톰 서비스 실증 및 기능 개선
- TTP-free 키교환 및 암복호화 모듈 개발
- TTP-free 트러스트 네트워킹 고도화

2) 국내외 분야 환경변화
- 개인데이터 활용에 대한 법적/제도적 장치가 마련되는 시점으로 새롭게 변화하는 데이터 활용 환경에 맞는 서비스 발굴 및 데이터 거래 환경 개발이 요구됨

3) 연구개발 추진전략
- 한국전자통신연구원 주도로 TTP에 의존하지 않고 데이터 주권과 안전한 교환을 보장하는 트러스트 데이터 커넥톰 원천기술 연구 추진, 국내 학계와 협력을 통해 최신 연구 동향 교환 및 의견 수렴 및 국내 표준화 전문가와 연계를 통해 연구 결과에 대한 표준화 논의 추진

4) 연구개발 일정 및 기대 성과
- 2단계 연구개발 일정: 2022.1.1 ~ 2023.12.31
- (기대성과) 과제로 도출된 응용 서비스에 대한 실증 서비스 검증을 통한 상용화 가능성 확인, 국가 공공 서비스에 先적용 후 민간 서비스로 확장하여 신 서비스 산업 창출 기반 조성 및 기존 중앙 집중적인 데이터 산업으로 제공이 어려운 개인 프라이버시 데이터 관련 서비스 분야로 확산

5) 다음 연차 연구개발비 사용계획
<table>
<tr><th colspan="2">구 분</th><th>인건비</th><th>직접비</th><th>간접비</th><th>민간부담금</th><th>합계</th></tr>
<tr><td>2단계</td><td>2년차</td><td>1,634,000</td><td>2,883,000</td><td>390,000</td><td>0</td><td>4,907,000</td></tr>
</table>
</td></tr>
<tr><td>국문핵심어
(5개 이내)</td><td>마이데이터</td><td>프라이버시</td><td>데이터 주권</td><td>신경망암호</td><td>블록체인</td></tr>
<tr><td>영문핵심어
(5개 이내)</td><td>MyData</td><td>Privacy</td><td>Data Sovereign</td><td>Neural Cryptography</td><td>Blockchain</td></tr>
</table>

목 차

1 과제 개요

1. 과제 수행계획

가. 과제 수행의 필요성

□ 정부정책 및 기술수요

❍ 미래부는 관계부처합동으로 마련한 '지능정보사회 중장기 종합대책'의 핵심과제로 '미래 경쟁력 원천인 데이터 자원의 가치 창출'과 '데이터·서비스 중심의 초연결 네트워크 환경 구축'을 제시 (2017.01)

❍ 과기정통부의 중점 추진과제 중 '실체가 있는 4차 산업혁명 기반 구축'에서 자유로운 데이터 흐름 촉진으로 데이터 생태계 전반 활성화하기 위해 '양질의 데이터 구축과 데이터 유통 촉진'과 이를 지원하기 위한 '데이터 재산권 강화'를 위한 법 제도 개선 등을 발표함(2017.09)

□ 산업동향 및 시장 기술수요

❍ 초연결 네트워크의 진화와 사물인터넷(IoT)의 확산으로 데이터 발생량은 폭발적으로 증가하고 있으며, 특히 개인이 생산한 데이터의 프라이버시와 주권에 대한 관심이 높아지고 있음

※ [redacted]

※ OECD 및 세계경제포럼(WEF)에서는 개인 데이터를 개인과 관련된 모든 데이터로 정의

❍ 수집된 초기 데이터(raw data)를 분석·재가공으로 만들어진 21세기 디지털 원유로 불리는 데이터가 새로운 가치를 창출하므로 데이터의 수집·가공·분석과 안전한 교환에 대한 다양한 연구개발 진행 중

❍ 현재 데이터 활용에 대한 연구 개발은 공공 데이터로 부터 수집된 빅데이터 분석과 데이터 거래에 초점을 맞추고 있음

❍ 대부분의 초연결 네트워크에 연결되는 장치는 "스마트 장치"로 전환되어 실시간으로 가치있는 데이터를 생산해 낼 것으로 예측

❍ 개인 데이터의 중요성이 점차 증대되며 개인이 생산한 데이터는 개인의 자산으로서 거래가 이루어지는 환경 도래

- 마치 태양광 발전기를 통해 발생한 전기를 한전에 팔 듯 내가 소유한 장치가 발생하는 데이터는 데이터를 활용하여 새로운 비즈니스를 창출하고자하는 사업자에게 팔릴 것임
- 대표적인 예로, 나의 혈압 및 맥박수를 측정하여 약국, 병원, 또는 제약회사 등 의료 데이터가 요구되는 회사에 판매하거나, 사용자가 선택한 건강 분석 기관에 의뢰하는 환경이 예상됨

❍ 개인 데이터의 거래를 위해 안전하고, 경제적이고, 빠르고, 확장성이 있으며, 사용자

친화적인 데이터 거래 플랫폼이 필요

- 현재의 데이터 비즈니스의 모델은 중앙 집중화된 플랫폼에 대한 전적인 신뢰가 요구되고, 데이터로 부터 이익이 창출되는 과정에 대한 투명성이 결여되어 사용자는 데이터 사용권을 집중화된 기관에 넘겨주고 데이터 사용에 대한 제한된 권한만을 행사
- 데이터의 소유권 및 주권을 데이터의 생성자에게 줄 수 있는 데이터 경제 민주화를 위한 플랫폼 필요

❍ 데이터 생산자이면서 소비자인 개인에 대한 데이터 주권 보장과 데이터의 안전한 교환을 보장을 요구하고 있으나, 현재는 TTP에 의존한 채 프라이버시 보호 및 데이터 생성자의 주권이 보장되지 않고, 책임 소재를 밝히기 쉽지 않는 형태의 정보교환 및 디지털 거래 환경임

- 구글, 아마존, 페이스북 등은 소비자가 생산한 데이터를 분석·가공 후 개인 맞춤형 서비스를 제공하고 있으며, 공유경제의 대표 기업인 우버, 에어비엔비 등은 중간 거래자로서 디지털 비즈니스를 주도하고 있으며, 알리바바는 중간자로서 온라인 거래 시장을 선도
- 구글 등 선도적 기업을 중심으로 미래 컴퓨팅 환경의 변화에 대비하기 위한 새로운 데이터 트러스트 기반 기술 확보를 추진하고 있음
- 최근 블록체인기반의 데이터 활용 기술은 기존 중앙 집중적인 데이터 활용 환경에서 벗어나 자유롭게 데이터를 사용하려고 하지만, 데이터 주권과 프라이버시 보호 기술은 기존 TTP-의존적인 기술을 사용하고 있음

❍ 양자 컴퓨팅의 출현 등의 변화와 컴퓨팅 성능의 급격한 향상에 따라 TTP에 의존하는 기존의 데이터 거래 방식의 안전성도 위협을 받고 있어, TTP 비의존적이며 데이터 주권을 보장할 수 있는 형태의 데이터 거래에 대한 요구가 증대될 것으로 예측

❍ 분산 노드간의 자율적인 신뢰 구축이 가능한 블록체인 개념은 4차 혁명의 핵심기술로서 다양한 연구가 시도되고 있으나, 실시간 데이터 거래 및 제어에 근본적 한계

- IDC보고에 따르면 2021까지 블록체인을 이용한 95%의 데이터 관리 프로젝트는 성능 및 기술의 부적절한 활용에 의해서 실패할 것으로 예측
- 현재의 블록체인 기술은 블록 크기(비트코인은 1MByte Block size)의 한계로 대용량 데이터의 실시간 교환·제어는 현재 기술로 불가
- 블록에 일단 저장된 데이터는 제거가 쉽지 않아 강력한 데이터 조작 방지 등의 장점을 제공하는 반면 불법 데이터 또는 예외 사항에 의한 데이터 추가시 삭제할 수 없는 이슈에 대한 해결 필요
- 참여자에 대한 인센티브에 기반하는 시스템 특성 및 공격을 방지하기 위해 실행코드에 기반한 수수료 부과가 이루어지는 스마트 컨트랙트의 효율성 문제

□ ETRI 연구개발 추진 당위성

❍ TTP가 없는 환경에서도 데이터 주권과 안전한 거래를 보장하는 트러스트 데이터 교환 기술은 전 세계적으로도 아주 초기 단계의 기초원천에 해당되므로 국가 주도의 연구소에서 연구 · 개발하는 것이 타당함

❍ ETRI는 다수의 연구 과제 수행을 통해 암호/프라이버시 원천 기술 및 네트워크 기술 등 정보보호와 고신뢰 네트워크 핵심 기술 역량 확보

□ ETRI R&R 및 경영성과계획서와의 연관성

❍ ETRI R&R 전략목표5 '국가 지능화 융합기술 개발로 혁신성장 동인 마련'중 성과목표5-5 '정교화·자동화 해킹을 원천차단하는 지능형 사이버보안 핵심기술' 개발을 담당

❍ ETRI 경영성과 달성을 위하여 본 과제에서도 상위20% IF SCIE 저널 중심의 연구성과 발표, 국내/국제 지식재산권 도출 및 3극특허 확보를 성과목표로 설정

□ 사업추진의 시급성

❍ 4차 산업혁명 시대의 국가 경쟁력은 다양한 종류의 데이터를 연계하여 새로운 지식과 가치를 창출하며, 더 나은 정책의 수립 및 집행할 수 있는 능력에 의해 결정될 것으로 판단

❍ 유무선 네트워크가 가장 잘 구축되었지만 데이터 산업에서는 미흡한 국내 ICT 환경에서 미래 지능정보사회의 데이터 생산자 중심의 데이터 산업을 선점하는 트러스트 데이터 교환 기술의 연구개발은 국가 경쟁력 확보를 위해 시급

- 데이터 생산자가 믿을만한 중간자가 없는 환경에서도 자율적으로 안전한 거래하는 플랫폼의 원천기술 확보는 미래 데이터 경제 기술 세계선도의 견인차가 될 것으로 기대됨
- 특히 기존의 TTP에 의존하지 않고 안심하고 데이터를 활용하기 위한 기반기술 연구는 현재 초기 단계이므로 선도적 연구에 의해 핵심 기술과 IPR을 선점할 수 있는 분야임

나. 과제 수행의 중요성

❍ 데이터 플랫폼은 선발-후발기업간 기술격차로 인해 플랫폼 선점 기업의 승자독식이 발생하므로 'Fast Follower' 전략은 한계가 크며 'First Mover' 전략 채택을 통한 기술 선점 및 시장 보호 필요

❍ 現 데이터 비즈니스 모델은 ① 중앙 집중화된 플랫폼에 대한 전적인 신뢰가 요구되고, ② 데이터로부터 이익 창출 과정에서 투명성 결여, ③ 생산자는 데이터 사용권을 클라우드 사업자에게 허용하는 문제를 안고 있음

❍ 데이터의 소유권 및 주권을 데이터의 생산자가 행사하는 데이터 경제 민주화에 대한 요구가 증대되고 있으며, 이를 위한 플랫폼 기술 선점을 통한 "데이터 産油國" 도약 마련 필요

❍ TTP-free 보안체계와 네트워킹 서비스는 기존 데이터 경제 패러다임을 탈피한 혁신적이며 도전적인 목표로 향후 데이터 산업의 근간으로 활용될 것으로 전망

다. 과제 수행의 제약요인

❍ 막강한 자본력을 바탕으로 클라우드 기반의 중앙집중화된 플랫폼은 당분간 꾸준한 성장하며, 시장을 선도할 것으로 예측되므로 본 데이터 생태계 구축은 초기에 가시적인 성과를 내기에는 다양한 도전에 직면할 것으로 보임

❍ 분산 환경에서 TTP에 비의존적인 데이터 시큐리티를 보장하는 데이터 교환기술은 국내는 물론 국제적으로 연구 초기 단계로 초기 학습 과정이 필요한 상황으로 꾸준한 투자와 인내로 지원되어야 함

라. 과제 수행결과 기대효과

□ 기술적 기대효과

❍ 정보의 생성·전달·유통 전 영역의 고신뢰화를 위한 새로운 기술 패러다임인 트러스트 데이터 커넥톰 기술은 모든 산업 환경에서 핵심 기술로 활용 가능

❍ 멀티 도메인간 데이터 유통이 필수적인 초연결 통신 환경에 대한 핵심원천기술 선제적 확보로 국가 기술 경쟁력 제고 기대

- 데이터에 대한 공격/방어의 경쟁에서 TTP에 모든 안전성을 의존하는 현재 기술을 탈피하여 혁신적인 데이터 시큐리티 기술 변화 선도
- 완전 분산 P2P 기술로 산재된 IoT 등 초연결 환경에서 혁신적인 신뢰 네트워킹 기술 확보
- 데이터 거래의 완전 분산화를 통한 초연결 초신뢰 데이터 거래 보증 기술 선도

□ 산업적 기대효과

❍ 혁신적인 패러다임의 데이터 교환 플랫폼으로 기존 대규모 플랫폼 사업자에 집중화된 데이터 비즈니스 및 데이터를 이용한 신규 비즈니스 시장 형성 기여

□ 경제적 기대효과

❍ 국내 데이터 산업 발전은 국가 경제 성장 동력원으로서 국가 산업경제의 핵심적 역할을 수행

❍ 데이터 산업은 사물인터넷, 인공지능 등 기술의 진화와 함께 소비자 중심의 서비스 확대 등으로 [redacted] 이를 것으로 전망

❍ 트러스트 데이터 커넥톰 기술은 전체 데이터 산업 전반에서 기존 중앙 집중화된 형태의 플랫폼을 일시에 대체하기는 힘들지만 점차 시장 확대를 위한 기반을 제공

□ 활용 방안

❍ 공공 데이터 인프라, 산업 인터넷, 스마트 시티 등 데이터 인프라의 신뢰 제고를 위한 기반 신뢰 인프라 플랫폼으로 활용

❍ 프라이버시 및 데이터 주권을 보장하는 데이터 교환 기술은 데이터를 근간으로 하는 다양한 新산업에 활용

❍ TTP-free 데이터 생성 기술은 TTP 비의존적인 정보보호 기술로 데이터 중심 산업 뿐 아니라 범용 정보보호 기반 기술로 확대되어 활용

2. 현황 및 접근방법

가. 국내·외 현황

1) 국내·외 기술동향 및 수준

□ 데이터 공유경제의 활성화와 개인 데이터 거래에 대비한 데이터 공유 및 거래의 신뢰성에 대한 요구 증대로 트러스트 데이터 교환 플랫폼 필요성 제시되고 있으나 연구개발은 미진한 상태임

❍ 가상화폐 기술로 금융 분야에서 출발한 블록체인 기술은 물류, 공공 서비스 등 다양한 분산 네트워크 환경에서 정보의 무결성을 보장하며 탈중앙화를 시도하고 있으나, 검증된 신원 확인을 위해서는 기본적으로 TTP에 의존적인 한계 보유

❍ “블록체인은 효율성을 버리고 자율성을 얻은 시스템”으로 새로운 데이터가 블록체인에 추가되기 위해서는 참여자 사이의 합의 절차가 요구되어 빠른 거래가 필수인 비즈니스 분야에 적용되기에는 효율적이지 못함

- 시간이 흐르며 일방적인 추가만 가능한 블록체인의 데이터 관리 방식은 데이터 용량이 커짐에 따라 비효율적이 되며, 이는 곧 네트워크 오버헤드를 발생
- 네트워크 스토리지로 운영되는 관계형 데이터베이스 개념 적용을 통한 효율성 향상이 요구됨

❍ 현재의 블록체인 스크립팅 언어(스마트 컨트랙트)는 복잡 다양한 비즈니스 프로세스를 자동화 할 정도의 완성도가 부족

- 버그나 취약성 문제, 또는 코딩 실수 등에 대비한 예외 처리가 지원되는 ‘계약 취소 기능’ 등에 대한 마련 필요
- 이는 현재의 블록체인의 ‘조작 불가능’성을 가정할 때 최악의 보안 버그가 존재해도 이를 고칠 수 없는 상황으로 전개됨
- 실행코드(Opcode)기반의 가스 수수료 부과(예, 이더리움 가스)시스템은 코드 사이즈에 따른 가치를 부과하고 있으며, 공격을 막을 수 있으나 사용자 입장에서는 비용 부담이 크게 작용

❍ 또한 현재 블록체인 기술은 범용 데이터 거래를 위한 확장성 부족, 노드 수 제한 등의 이슈를 지니고 있음

❍ 독일 프라운호퍼 주도의 산업 연합체인 IDS (Industrial Data Space)는 산업 도메인간 데이터의 안전한 교환을 위한 표준 모델을 정립하고 있으나 관리 주체가 명확한 도메인간 데이터 교환 모델을 제공하고 있음

□ 데이터를 신뢰성 있게 저장하기 위하여 블록체인에 데이터를 분산하여 보관 및 관리하는 플랫폼 개발이 국외를 중심으로 이루어지고 있으나 아직 초기 단계임

- ❍ IOTA는 기존 블록체인의 구조와 달리 DAG (Directed Acyclic Graph) 기반의 Tangle 구조를 사용하여 수수료 없는 거래를 지향함
- ❍ BigchainDB는 데이터베이스에 블록체인의 특성을 추가하여 기존 데이터베이스가 제공하는 Query 언어와 높은 처리 속도를 지원함과 동시에 블록체인이 갖는 무결성, 분산 관리 등의 장점을 갖춤
- ❍ BitClave는 블록체인을 이용한 검색 데이터 보호 솔루션으로 사용자가 분산 검색 엔진을 사용하여 원하는 정보를 찾고 검색 기록에 대한 보상을 받음
- ❍ Storj는 이더리움 기반의 분산 클라우드 저장 공간으로 리소스를 대여해주는 Farmer와 리소스를 사용하는 Renter로 역할을 나누어 네트워크 피어 사이에 데이터 전송, 검색, 계약 등을 지원함
- ❍ IPFS는 버전 관리가 가능한 분산 파일 시스템으로 IPNS라는 네이밍 시스템을 사용하여 파일을 검색하는 기능을 제공하며 궁극적으로 웹을 대체하는 비전을 가짐

□ 세계 각국에서는 개인 데이터를 공유하기 위한 아키텍쳐 및 플랫폼을 프로젝트로 진행하고 있지만 아직 초기 단계임

- ❍ EU의 CARRE 프로젝트 중 'Personal Sensor Data Aggregator'는 개인 데이터를 하나로 모아 분석하기 용이한 구조를 제시하였지만 데이터를 서로 거래할 수 있는 구체적인 방법은 제시하지 않음
- ❍ openPDS는 프라이버시 보호를 위해 외부에 Raw데이터를 직접 제공하지 않고 요청에 대한 anonymous answer를 제공
- ❍ MyData는 GDPR 준수와 같은 개인 프라이버시 문제를 해결하기 위한 동의(consent) 구조와 인터페이스 프레임워크를 설계하는 프로젝트임
- ❍ CKAN(the Comprehensive Knowledge Archive Network)은 오픈 데이터 저장 및 배포를 위한 오픈소스 형태의 웹 기반 관리 시스템으로 미국, 유럽, 호주 등 여러 국가의 전자 정부에서 채용하고 있으나 개인 데이터 관리에 특화된 플랫폼은 아님
- ❍ Personium은 일본 Fujitsu사를 중심으로 개발되고 있는 공개 PDS 프로젝트로 분산 클라우드 기반의 PDS이나 시스템 구동의 오버헤드가 크고 IoT 환경이나 저작권 보호 등이 필요한 경우 적합하지 않음
- ❍ WWW(World Wide Web)의 창시자 Tim Berners-Lees는 사용자들의 개인정보를 자신이 직접 통제할 수 있도록 하는 Solid 프로젝트를 창안하였으나 아직 초기 단계로 확산에는 다소 많은 시일이 걸린 것으로 예상됨

□ 데이터를 거래하기 위한 플랫폼은 소수 진행 중이나, 대부분 IoT와 같은 센서 데이터에 특화되어있고 신뢰성있는 거래를 제공하기 위한 장치가 부족함

- ❍ IBM이 주축이 되어 진행 중인 Open Horizon은 IoT와 같은 지속적인 센서 데이터의 거래에 특화된 플랫폼이며 블록체인 등을 활용한 신뢰성있는 거래 계약 등이 미흡함
- ❍ DataHub는 다양한 데이터를 강력한 시각화 툴을 이용하여 검증 및 배포하는 플랫폼이지만 데이터를 검색하거나 거래 기록을 관리하는 등의 기능이 미흡함
- ❍ IOTA Data Marketplace는 IOTA 블록체인을 이용한 IoT 데이터 거래를 위한 플랫폼이며, IoT 데이터에 특화된 tangle을 사용하는 IOTA에 의존적임
- ❍ Digi.me는 데이터 제공자 중심의 개인 데이터 거래 플랫폼 중 하나로, 개인이 생성하는 모든 개인 데이터를 개인 데이터 저장소에 보관하고 제공자의 명시적 동의하에 서비스들이 개인 데이터에 접근할 수 있는 구조를 가짐
- ❍ UBDI 서비스는 개인이 개인데이터를 바탕으로 설문조사 형식의 연구에 참여하여 수익이 발생할 때 이를 개인에게 돌려주는 서비스임
- ❍ Cozy는 개인 클라우드 서비스 (Personal Cloud Service)로 개인 데이터의 안전한 저장공간을 제공하고, 그러한 공간에서 데이터를 활용할 수 있는 서비스를 제공

□ 개인 데이터 제공자들이 자신이 제공하는 데이터에 대한 보상을 어떻게 받는지에 대한 가치화 및 이해관계자의 신뢰도를 평가할 수 있는 모델연구가 진행되고 있으나, 초기 상태임

- ❍ ITU-T Recommendation Y.3052 “Overview of trust provisioning for ICT infrastructures and services”에서는 신뢰를 “측정가능 한 믿음”으로 과거로부터 축적된 가치, 미래에 예상되는 가치(value)로 정의하고, 이를 수치화하여 비교/평가할 수 있는 신뢰지수에 관한 개념을 제시함
- ❍ 2018년 5월 25일을 기점으로 강화된 개인정보 보호법인 GDPR 시행 이후 개인정보를 수집, 처리, 활용하는 객체들의 신뢰도 평가에 객관적 변수에 해당되던 요소들 또한 함께 포함되어야 하며, GDPR에서 요구하는 항목들의 충족 여부와 정보 제공자의 주관성을 능력(ability), 관계성(benevolence), 일관성(integrity), 경험(experience), 그리고 평판(reputation)으로 알맞게 나누어 신뢰도를 평가할 방법이 필요하게 됨
- ❍ Zhao 등은 “Machine-learning based privacy-preserving fair data trading in big data market” 연구를 통해 데이터 공급자와 데이터 구매자 간의 atomic exchange를 통한 지불 형평성 및 안정성 문제 해결을 제시
- ❍ SDTE: A secure blockchain-based data trading ecosystems 연구에서는, 기존의 데이터 거래 플랫폼에서는 구매자와 데이터 중개인의 도덕적 무결성을 가정하고 있

어 부정직한 구매자/데이터 중개인이 존재하는 실제 거래 환경에서의 문제점을 해결하고자 하는 연구를 진행

❍ 상기 선행연구들에서는 블록체인의 특징을 활용하기 때문에 블록체인에 참여한 데이터 브로커 또한 그 행동을 검증할 수 있어 incentive-compatible한 데이터 브로커의 행위를 방지할 수 있다고 가정하고 있음

❍ 하지만, 데이터 브로커의 외부 상호작용이 모두 블록체인에 적용되더라도 데이터 브로커는 (의도하던지 혹은 의도치 않던지) 데이터 판매자 및 구매자와 진행한 데이터 중개 계약을 위반할 수도 있으며. 이를 해결하는 원천 기술 연구가 필요함

□ 개인 데이터 거래를 위한 신뢰성있고 분산화된 원장을 제공하는 블록체인은 자체적으로 높은 보안성을 가진데에 반해, 데이터 거래가 이루어지는 블록체인 노드의 보안성은 여전히 낮고 연구가 이루어지지 않고 있음

❍ 블록체인이 가지는 원장 자체의 보안성은 다양한 공격의 발견과 이를 해결하기 위한 연구를 통해 높은 수준으로 발전함

- 이중 지불 공격(Double-spending attack), 채굴 공격(Mining attack), 네트워크 분할 공격(Partitioning attack) 등의 공격이 발견되고 이를 해결하기 위한 연구가 진행되었음
- 2018년 이후로 새로운 형태의 공격이 학계에서 발견되지 않고 있으며 기존 공격의 고도화만 이루어지고 있음

❍ 이에 반해 블록체인 네트워크를 구성하고 블록체인 원장에 접근하기 위해 필수적인 블록체인 노드는 보안성에 대한 검증이 이루어지지 않고 있음

- 블록체인 노드 소프트웨어는 다양한 개발 주체에 의해서 개발이 되고 있음. 예를 들어, 이더리움 블록체인의 경우 이더리움 재단에서 개발하는 Go Ethereum 뿐만 아니라, OpenEthereum, Nethermind, Besu, Trinity 등 사용하는 환경, 언어에 따라 다양함
- 또한 블록체인 노드는 다양한 네트워크 및 컴퓨팅 환경 (클라우드, 엔터프라이즈 등)에서 운영되고 있어 보안성의 검증이 일관되게 이루어지기 어려움
- 블록체인 노드 소프트웨어에 대한 보안성 검증은 개발자들에 의한 자발적 테스트와 바운티 프로그램(취약점을 보고하면 보상하는 제도)에 의존하고 있음

❍ 블록체인 노드의 보안성을 검증하기 위해 블록체인 네트워크에서 교환되는 트랜잭션 및 블록 정보의 측정을 통한 실제 네트워크 기반 분석을 통해 블록체인 노드의 공격 벡터를 확인하고 이를 해결할 수 있는 연구가 필요함

□ 데이터 중심의 네트워킹 아키텍처는 미국과 유럽을 중심으로한 미래 네트워크 프로젝트로 연구가 되고 있지만 TTP에 의존적인 구조적인 한계점을 가지고 있음

❍ NDN(Named Data Networking)은 미래 인터넷 아키텍처로 ICN 연구 프로젝트인 CCN(Content-Centric Network)을 계승한 이름을 기반으로 한 분산 데이터 네트워킹 구조이나 이름에 대한 사용 권한은 중앙화된 CA(Certificate Authority)로부터 비롯되어 TTP 의존적임

❍ DONA(Data Oriented Network Architecture)는 정보의 지속성, 인증 및 가용성을 제공하는 플랫한 이름을 이용하는 계층적 네트워크 구조를 가지지만 DONA 식별자는 사람이 판독 가능한 형태가 아니므로 변환하는 방법을 별도로 제공해야 함

❍ PURSUIT(Publish Subscribe Internet Technology)은 유럽의 FP7 프로그램의 일환으로 Publish-Subscribe 모델을 기반으로한 ICN 구조를 제시하여 다수-대-다수 통신에 유리하지만 DONA와 같은 식별자의 가독성 문제를 가지고 랑데부 노드의 SPOF(Single Point Of Failure) 문제를 가짐

□ 일본 제어기기 업체 오므론 등 100개의 일본 회사가 2020년에 IoT로 축적된 데이터를 거래하는 유통시장을 만들기로 합의 (니혼게이자이신문, '17.05.23)

□ 제3 신뢰자(Trusted Third Party, TTP)에 의존하지 않고 자체적으로 데이터 시큐리티를 보장하는 기술은 현대 암호학의 한계점을 뛰어넘는 도전적인 기술로 최근 일부 연구 시작

❍ TTP에 기반하지 않고 신경망 학습을 통해 키를 공유하고 데이터 시큐리티를 보장하는 암호 기술인 '신경망 암호(neural cryptography)'에 대한 국내 연구는 전무한 상황

❍ 인공신경망 및 신경망 학습 모델은 학계에서 꾸준히 연구되어온 연구 주제이지만, 최근까지 암호 분야에는 적합하지 않다는 인식이 지배적이었으며 주어진 데이터에서 추출된 데이터를 바탕으로 위협 탐지, 보안시스템 취약점 분석 등 제한적으로 활용됨

❍ 2000년대 초반부터 유럽을 중심으로 신경망 암호 연구가 수행 중이며, '02년 Tree Parity Machine 학습 모델 기반의 신경망 동기화를 통해 비밀 키 교환이 가능함을 최초로 제시

❍ '16년 기계학습으로 데이터 암복호화 알고리즘 설계에 대한 가능성이 최초로 발표되어, 기존 수학적 난제 기반의 암호 알고리즘의 한계를 뛰어넘는 양자 컴퓨터 대응 기술로 연구가 되고 있음

- 하지만, 현재까지 신경망 학습 기반의 키 교환 기술에 대한 정형화된 암호학적 안전성 모델은 부재하여 안전성 모델 확립 및 효율성 개선이 핵심 이슈로 연구될 것으로 예측됨

□ 데이터 중심 사회로의 변화에 따라 데이터 프라이버시 보호에 대한 필요성이 강조되면서 다양한 데이터 프라이버시 보호 기술이 개발되고 적용되고 있으나, TTP 기반의 기술 적용으로 여전히 데이터 소유자에 대한 권한 보장은 이루어 지고 있지 않음

❍ 데이터가 집중되는 클라우드 환경에서의 데이터 프라이버시 보호 기술이 다수 개발되고 있으나 클라우드 관리자 중심의 기술 개발이 주를 이루고 있으며, 데이터 소유자의 권한 보장을 위한 기술 개발은 상대적으로 미진함

- 분산 클라우드 환경에서 안전하게 컴퓨팅 및 스토리지 자원을 공유하기 위한 기술 연구가 진행
- Cross-Cloud 환경에서 데이터 신뢰성 확보를 위한 위협 분석 연구 및 안전성 제공을 위한 연구가 진행
- 클라우드 스토리지 환경의 가용성을 높이기 위한 데이터 중복처리 기술에 대한 확장성 효율성 개선 연구도 다수 진행되고 있음

❍ 인공지능, 사물인터넷, 자율주행차, 빅데이터 기술로 대표되는 4차 산업혁명에서 프라이버시 보호 기술에 대한 중요성은 점차 증대됨

- 기계학습 기술에 필수적인 대량의 데이터를 활용하는 과정에서 프라이버시 보호 기술과 더불어, 인공지능을 활용한 개인 프라이버시 관리 도구 개발 진행
- 사물인터넷 프라이버시 문제 핵심은 사물에 대한 사용자 접근을 인증하고 승인하기 위한 'ID'로, 사물인터넷의 발달에 따라 ID는 개인 식별도구의 기능을 넘어 객체 그 자체로 확대되고 있음
- '15년 발표된 유럽 자동차 제조사협회는 커넥티드카의 데이터 보호원칙에는 데이터 수집 등의 투명성 보장, 고객에게 선택권 제공, 데이터 보안 유지, 데이터 익명·가명·비식별 처리, 이용목적 달성 시 익명처리 또는 삭제 등 포함
- '16년 미국 도로교통안전국은 자율주행차 안전기준 지침에는 자율주행차 고객의 개인정보 관리를 위해 데이터 수집의 투명성, 선택권, 보안, 책임에 관한 내용이 포함됨

❍ 분산화된 원장을 기반으로 신뢰성을 제공하는 블록체인 기반 기술이 발전하면서 블록체인 기반의 사용자의 데이터 프라이버시 보호 기술에 대한 연구 진행

- 비트코인 등의 퍼블릭 블록체인은 익명성 보장을 통한 프라이버시를 제공하지만 제한적임
- 블록체인을 통한 스마트 컨트랙트 활용 단계에서 계약 당사자들의 민감 정보에 대한 개인정보 침해 우려가 높음
- 블록체인에서 높은 수준의 프라이버시 구현을 위해 링 서명(Ring Signature), 동형 암호화(Homomophic Encryption), 다자간 컴퓨팅(Multi Party Computation), 영지식 증명(Zero-knowledge Proof), 비밀 분산(Secret Sharing) 등의 다양한 암호 기반 기술 적용에 대한 연구가 진행 중

2) 국내·외 표준화 현황(또는 향후 기술 발전 추세)

❍ ITU-T에서 사물인터넷 및 스마트시티 표준화 연구를 총괄하고 있는 SG20은 데이터 상호운용성 표준 개발의 필요성을 인식하고, '17년 3월 SG20 회의에서 Focus Group on Data Processing and Management(FG-DPM)을 신설하고 IoT환경에서의 블록체인, 블록체인을 이용한 데이터 교환 및 공유, 블록체인을 이용한 데이터 관리 등에 사전 표준 작업을 시작

- 포커스 그룹이 활동을 종료 후 기술적 산출물은 ITU-T SG20을 비롯한 관련 연구반으로 전달되어 표준화 예정

❍ 블록체인의 합의 알고리즘 및 트랜잭션 처리 가속 기술 등이 다양한 기업에 의해 경쟁적으로 개발되고 있는 상태로 ISO, ITU-T 등에 의한 표준화가 시작됨

- ITU는 분산원장 기술(DLT: Distributed Ledger Technology) 응용 분야의 미래를 논의하기 위한 포커스 그룹 신설 ('17년 10월)
- 포커스 그룹이 활동을 종료 후 기술적 산출물은 ITU-T SG17을 비롯한 관련 연구반으로 전달되어 표준화 예정

❍ TTP에 의존하지 않는 데이터 시큐리티 보장 기술에 대한 기술 개발은 초기 단계로 일부 기술에 대한 연구가 관련 기업을 통해 시작되는 정도로 표준화에 대한 논의는 없음

❍ 데이터 프라이버시 보호 표준 및 정책은 유럽을 중심으로 활발하게 진행중

- 개인 식별정보에 대해 사용자의 데이터 통제권 보장, 이용자의 동의없는 광고 목적 활용 금지, 이용자 정보의 처리와 저장의 투명성 확보, 독립적인 제3자로부터의 준수사항 감사 실시 등을 포함하는 클라우드 환경에서 프라이버시 보호를 위한 국제 표준 ISO/IEC 27018를 '14년 발표
- 유럽의 경우 개인정보보호규정(GDPR, General Data Protection Regulation)을 '16년 제정, '18년 5월 일반 데이터 보호 법규(General Data Protection Regulation) 발효 예정
- P3P(개인정보보호정책, Platform for Privacy Preferences)는 인터넷 사용자에게 웹 사이트의 프라이버시 보호정책을 전달하는 기준을 제공함

3) 동일, 유사내용에 대하여 국내·외 관련자들의 수행내용

❍ 산업도메인간 안전한 데이터 교환에 관한 연구는 프라운호퍼 주도의 유럽 산업 연합체인 IDS(industrial data space)에서 수행중
- 참여 주체가 명확하게 정의되어 있고 TTP를 통해 인증된 산업 도메인들 간 디지털 주권, 안전한 데이터·서플라이 체인, 심플한 데이터 접속, 데이터 이코노미, 신뢰 보호, 분산형 데이터 격납, 데이터 거버넌스 등을 목표로 연구를 진행 중이며, 참여사 간 소스 공개를 하고 있음

❍ ETRI는 블록체인 구조 및 블록체인의 ICT 적용 등 블록체인 기반 신뢰 ICT 구조 설계를 진행 중

❍ AI 또는 신경망 학습 기반의 동기화를 통한 TTP-free 키 교환 기술
- 유럽에서는 '02년 TPM(Tree Parity Machine) 모델 기반의 뉴럴 네트워크 동기화를 통한 키 교환 기법이 최초 제안되었으나, 체계적인 암호학적 안전성 모델에 대한 연구 및 키 공유 참여자인증을 통한 인증된 키 교환에 대한 연구는 없음
- 미국 Google은 '16년 10월에 사전에 공유된 키를 가지고 있는 AI 엔진들이 기계학습을 통해 스스로의 암호화 알고리즘을 생성하는 연구 결과를 발표했으나, 16비트 기반 알고리즘에 성공률이 30% 수준의 연구 시작 단계임

❍ 데이터 프라이버시 보호 기술은 대량의 데이터를 수집 관리하는 중앙 집중방식의 기술 개발이 주도적이며 TTP-free 기반의 프라이버시 보호 기술에 대한 체계적인 연구는 현재 진행되지 않음
- Google은 크롬 웹 브라우저를 통해 수집한 데이터에 대해 프라이버시 보호 기술을 적용한 통계 처리 연구를 수행 중
- Apple은 자사의 수집 데이터 기반의 인공지능 서비스를 개발 중이며 수집된 데이터에 차등 프라이버시 기술 적용을 통해 프라이버시를 보호하는 기술을 도입
- 국내의 경우 데이터 프라이버시 보호를 위한 '포맷보존 암호 TTA 표준화(국보연)', '순서보존암호 적용 DB보안(한컴시큐어)' 등의 일부 관련 기술이 개발되었으며, 익명화, 개인정보 비식별화, 차등 프라이버시 등 연구가 진행되고 있음

4) 동일, 유사내용과 관련하여 제안자가 이미 수행한 사업 또는 연구개발과제

과제명	주 요 내 용	연구기간	비 고
암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천 기술 개발	데이터 유출의 원천적인 방지를 위해 데이터베이스가 암호화된 상태로 데이터 저장, 열람 및 검색이 가능한 암호 원천 기술 개발 - 암호데이터 중복 처리 및 소유권 검증 기술 개발 - 암호데이터 검색 기술 개발	2015.01. ~ 2017.12.	-
분산 초연결 신뢰 ICT 인프라 구조 기술 개발	블록체인 구조 및 블록체인의 ICT 적용 등 블록체인 기반 신뢰 ICT 구조 설계 진행	2017.06. ~ 2018.12.	-

5) 국내·외 경쟁기관 현황

❍ 프라운호퍼 주도의 유럽 산업 연합체인 IDS(industrial data space)는 산업 도메인간 안전한 데이터 교환에 관한 연구 수행중

- 산업 도메인에서의 ①디지털 주권, ②안전한 데이터·서플라이 체인, ③심플한 데이터 접속, ④데이터 이코노미, ⑤신뢰 보호, ⑥분산형 데이터 격납, ⑦데이터 거버넌스 등을 표방하고 있으나 분산 네트워크환경에서 TTP에 의존한 방법 제시

❍ MIT의 openPDS(open personal data store)는 개인이 생성한 데이터를 한 곳에 모으고 데이터의 활용을 위한 분석 등을 개인에게 부여할 수 있는 개인 데이터 활용 생태계 아키텍쳐 제시

❍ 암호 화폐로 시작된 블록체인 기술은 현재 금융권/비금융권, 정부기관 등 다양한 영역으로 확대되어 다양한 블록체인 기반 프로젝트가 진행 중에 있으나, 범용 데이터 거래를 위한 블록체인은 아직 초기 단계임

- 이더리움은 스마트 컨트랙트를 블록체인에 접목시키면서 기본적인 거래 장부 기록 외에 완전 튜링 컴퓨팅 기능과 그 기능을 이용하여 프로그램을 실행할 수 있는 환경을 제공함
- R3CEV는 금융권을 위한 현재 가장 큰 규모의 블록체인 컨소시엄으로, 금융권에서 필요한 복잡한 거래들과 기능들을 블록체인을 이용해 단순화하기 위해 만들어졌으며, 오픈 소스 기반의 Corda 프로젝트를 발표
- ZeroCash는 영지식 증명 기법을 사용한 거래내역 은닉형 블록체인으로, 금융 거래 당사자와 거래 금액 등의 정보에 대한 암호화를 통한 프라이버시 보호 기능을 제공하지만, 수식화가 어려운 데이터에는 적용이 어려움
- 리눅스 재단의 HyperLeger Fabric v1.0 에서는 개인정보 보호를 위해 트랜잭션 발행자의 익명화 뿐 아니라 동일한 사용자가 발행한 여러 트랜잭션 사이의 연결성 제거 시도를 진행하고 있음
- 네트워크에 블록체인을 적용하려는 시도는 Nokia Bell Labs 등을 필두로 초기 단계 진행

중임

❍ TTP-free 시큐리티 및 프라이버시

- TensorFlow와 알파고로 유명한 Google Brain은 2016년 10월 기계학습 환경에서의 학습을 통한 데이터 암복호화 알고리즘 생성 가능성 발표
- MS Research는 신경망 학습을 이용한 안전한 다자간 계산에 대한 연구를 진행
- 애플은 차등 프라이버시 기술이 적용된 인공지능 서비스 개발을 위해 기존 스타트업 인수, 인재 영입 등의 투자를 확대하고 있음

※ 개인의 얼굴 이미지를 저장하지 않고도 얼굴 표정을 인식하여 최대 10만 가지 얼굴 표정을 수집하고 분석하는 기술과 특허를 보유한 이모션트(Emotient)를 '15년 1월에, 프라이버시 보호를 위해 스마트폰에서 아주 적은 데이터를 기반으로 딥러닝을 이용한 이미지 인식 프로그램 기술 업체인 '퍼셉티오(Perceptio)를'15년 10월에 인수함

6) 국내·외 지식재산권 현황

❍ 데이터 교환 기술에 일부 적용이 가능한 블록체인 기술은 현재 금융 등 타 산업 분야에 집중되어 출원이 이루어지고 있으나, 데이터 산업 분야에 점차 특허 출원이 늘어날 것으로 예상됨

- 연도별 출원 현황을 보면 '13년 3건, '14년 5건으로 2년간 8건에 불과하였으나 이후 '15년 24건, '16년 94건, '17년 1~8월 114건으로 최근 출원이 급증
- 산업분야별로 출원 동향을 살펴보면 e-커머스(57.5%), 통신(28.3%), 컴퓨터(11.7%) 같은 ICT 분야에서 특허출원이 집중되었고 전기(1.3%), 정밀기기(0.4%), 전자(0.4%), 자동차(0.4%) 순으로 특허출원된 것으로 집계
- 블록체인의 기술적 특성을 이용하여 데이터 거래를 포함하여 사물인터넷(IoT), 인증 정보 관리, 콘텐츠 서비스, 저작권 관리, 물품 거래 추적, 전자투표 등 산업 전반에서 적용이 가능하므로 이와 관련된 특허출원은 계속 증가할 것으로 전망

❍ TTP에 의존하지 않는 데이터 시큐리티 기술 분야는 연구 초기 단계로 미국과 중국을 중심으로 기계학습 기반 키 교환 및 암호화 기술에 대한 특허가 일부 출원되고 있음

❍ 애플, 구글, 아마존, 페이스북, 마이크로소프트, IBM 등 세계 최고 수준의 ICT 기업들은 프라이버시 관련 특허 다수 확보

- 최근에는 기계학습을 이용한 프라이버시, 블록체인에서의 프라이버시 보호, IoT 환경에서의 프라이버시 보호, 자율 자동차에서의 프라이버시 보호에 관한 특허가 집중적으로 출원되고 있음
- 기존의 기술 들은 데이터가 집중되는 기업 위주로, 수집된 데이터를 독점적으로 활용하기 위한 기술이 대부분이며, 사용자 중심의 프라이버시 보호 기술에 대한 특허는 미미함

나. 핵심요소 및 접근방법

❍ 데이터 시큐리티 보장 기술

- TTP-free 환경에서 사전 공유 정보 없이 시큐리티를 보장하기 위한 요구사항 및 안전성 모델 정립

- 신경망 학습을 통한 동기화 기반의 비밀 키 교환 및 인증된 키교환 기술
- 키/알고리즘 독립형 데이터 암복호화 기술

❍ 데이터 프라이버시 보호 기술

- TTP-free 환경의 데이터 소유권/주권 요구사항 및 프라이버시 요구사항 도출
- 트러스트 데이터 생산자 확인 및 소유권 증명 기술
- 프라이버시 강화 트러스트 데이터에 대한 부인방지 및 접근 권한 세분화 관리 기술

❍ TTP-free 실시간 데이터 트러스트 보장 네트워킹 기술

- 트러스트 데이터 비즈니스 요구 사항 분석 및 기술 요소 도출
- TTP-free 데이터 전달을 위한 네트워킹 기술

❍ 트러스트 데이터 거래 기술

- TTP-free 시큐리티 보장 기술과 네트워킹에 의한 신뢰 환경에서의 두 객체간의 차세대 분산 데이터 거래 기술

다. 혁신성과 독창성

❍ 신속한 거래가 필수인 데이터 비즈니스 분야에 적용될 수 있는 실시간 데이터 안전 거래 지원 기술

- 분산 환경에서의 데이터 거래 플랫폼으로서 일부 시도되고 있는 블록체인 기술은 새로운 데이터 추가 시마다 발생하는 참여자 사이의 블록 합의 절차 등에 의해 신속한 거래가 필수인 비즈니스 분야에 적용되기에는 효율적이지 못함
- 초연결 주체간 데이터 거래가 일반화 되는 상황에 대비한 인터넷 스케일 데이터 거래 네트워킹 지원

❍ 데이터 거래를 위한 효율적이며 실용적인 차세대 데이터 거래 기술

- 현 블록체인 기술은 신뢰되지 않는 환경에서 노드간의 합의를 통한 신뢰 형성을 이루기 위해 참여 노드의 경제적 인센티브를 기반으로 설계되어있어 확장성에 근본적인 한계를 가지고 있으며, 공개된 스마트 컨트랙트의 DDoS공격 및 악의적인 사용을 방지하기 위한 실행 코드 단위의 수수료 부과를 함으로써 실제 도입시 경제적인 부담으로 작용
- TTP-free 데이터 생성의 완벽한 보안과 안전한 네트워킹 환경에 기반한 확장성 및 효율성을 제공하는 차세대 데이터 거래 기술
- 인스트럭션 한계를 갖지 않는 가상 실행 환경 제공

❍ TTP에 의존하지 않고 통신 주체들의 독자적인 키 교환 및 시큐리티 보장 기술

- 현재의 암호시스템은 고정된 수학적 난제에 기반한 안전성을 제공하는 설계방식을 활용하기 때문에 컴퓨팅 환경의 변화에 따라 수학적 난제의 안전성이 훼손되는 경우에 암호시스템 자체의 안전성을 보장하기 어려움
- 또한, 특정 수학적 난제 중심 암호시스템 설계 방식의 경우 처음 난제를 생성한 주체에 대해 안전성을 의존하기 때문에 TTP 중심 시스템의 한계 극복이 어려움
- 학습 기반 암호화 기술은 기존 고정된 난제에 안전성을 의존하지 않기 때문에 공개키 암호시스템으로 대변되는 현대 암호 시대의 패러다임을 극복하기 위한 TTP-free 중심의 새로운 안전성 제공을 위한 혁신적이며 도전적인 목표임

2 과제목표 및 수행과정

1. 과제목표

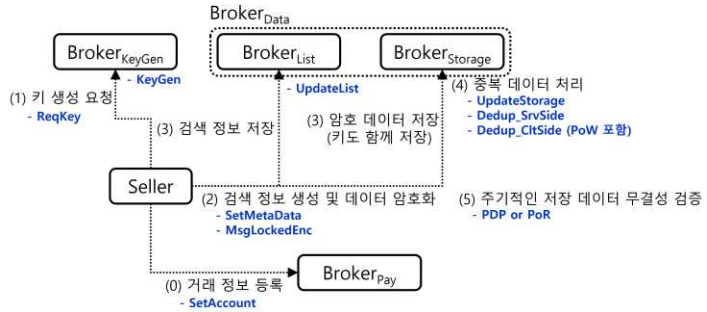
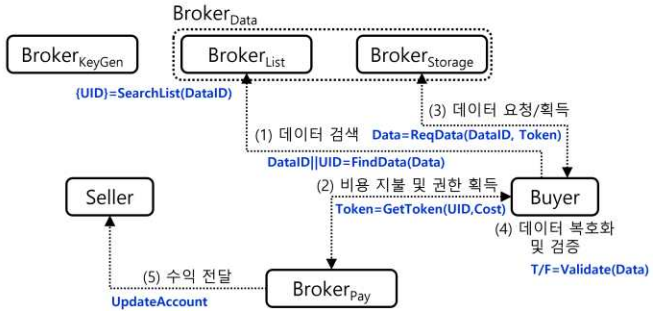
<table>
<tr><th colspan="3">구분</th><th>주요 내용</th></tr>
<tr><td rowspan="6">연구개발 목표 및 내용</td><td colspan="2">최종 목표</td><td>○ 기존 TTP 기반 환경에 의존하지 않고 데이터 주권과 안전한 교환을 보장하는 트러스트 데이터 커넥톰 원천기술 개발
※트러스트 데이터 커넥톰 (TDC) : 초연결 지능사회에서 사람, 사물(공간, 생물, 정보, 비즈니스)등이 유기적 상호작용으로 생성한 데이터에 대해 데이터 주권 및 안전한 교환을 제공하는 TTP-free 데이터 거래/활용 신뢰인프라
○ 정교화·자동화 해킹을 원천차단하는 사이버보안 핵심 기술 개발</td></tr>
<tr><td rowspan="2">1단계</td><td>목표</td><td>• TTP-free 키교환 및 분산 자율거래 신뢰 플랫폼
• 주요 ICT 인프라 해킹대응 솔루션 (보안과제)</td></tr>
<tr><td>내용</td><td>- 트러스트 데이터 커넥톰 구조 설계
- 신경망 학습 기반 인증된 키교환 기술 설계
- TTP-free 데이터 프라이버시 보호 기술 연구
- TTP-free 트러스트 데이터 거래 프로토콜 연구</td></tr>
<tr><td rowspan="2">2단계</td><td>목표</td><td>• 트러스트 데이터 거래 실증 서비스
• 분산 개인 주권/안전성 보장 데이터 거래 실증
• 국방 ICT 인프라 해킹 대응 서비스 (보안과제)</td></tr>
<tr><td>내용</td><td>- 트러스트 데이터 거래 실증 서비스 PoC
- TTP-free 부인방지/접근 권한 세분화 기술 연구
- 트러스트 데이터 거래 책임성 추적 기술 개발
- TDC 통합 시스템 구축 및 PoC</td></tr>
<tr><td rowspan="2">당해 연도</td><td>목표</td><td>• 트러스트 데이터 커넥톰 서비스 개발
• 트러스트 데이터 커넥톰 서비스 PoC 시스템 구축
• TTP-free 데이터 시큐리티 강화 기술 연구
• TTP-free 트러스트 데이터 거래 확장 기술 연구</td></tr>
<tr><td>내용</td><td>○ 트러스트 데이터 커넥톰 구조 및 서비스 연구
• 트러스트 데이터 커넥톰 서비스 개발 및 시스템 구축
- 트러스트 데이터 커넥톰 서비스 개발
- 트러스트 데이터 커넥톰 서비스 PoC 시스템 구축

○ TTP-free 트러스트 데이터 생성 기술 연구
• 데이터 시큐리티 강화 기술 설계
- 학습 기반 인증된 키교환 기술에 대한 수학적 안전성 모델 정립
- 키/알고리즘 정보 비공유 환경에서 데이터 시큐리티 강화 기술 안전성 모델 정립
- 키/알고리즘 정보 비공유 환경에서 데이터 암복호화 기술 설계
- 데이터 프라이버시 보호 확장 설계
- 제어가능 프라이버시 제공 기술 설계
- 데이터 접근 권한 세분화 관리 기술 설계

○ TTP-free 트러스트 데이터 커넥팅 기술 연구
• 트러스트 데이터 블록체인 네트워킹 기술 개발
- 블록체인 네트워킹(트랜잭션캐스팅&블록캐스팅) 라이브러리 개발
- 블록체인 네트워킹 테스트넷 구축 및 시험
• 트러스트 데이터 거래 확장 기술 개발
- 트러스트 데이터 거래 책임성 추적 기술 개발
- 트러스트 데이터 거래 플랫폼 구축</td></tr>
</table>

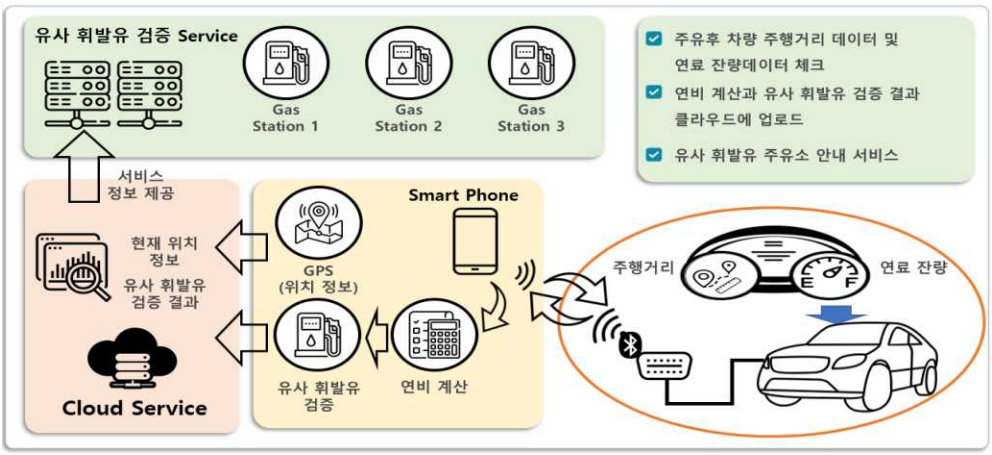
2. 과제 연차별 수행과정 및 내용

○ (2단계) 1차년도(2022년도) 개발 내용 및 범위

수행 기관	개발 목표	개발내용 및 범위
ETRI (주관)	트러스트 데이터 커넥톰 구조 및 서비스 연구	• 트러스트 데이터 커넥톰 서비스 환경 고도화를 위한 데이터 수집/생성 모듈 연구 - 기존 데이터 수집/생성 모듈의 기능 분석 및 트러스트 데이터 커넥톰 환경에서 안전한 데이터 거래 지원을 위한 서비스 흐름 구성 연구 · 세 종류 참여자인 판매자, 구매자, 그리고 다수의 중재자를 중심으로 트러스트 데이터 커넥텀 구성 및 서비스 흐름 구성 - 각 참여자 역할 및 참여자 사이의 정보 교환 정의 · 서비스의 핵심 절차인 데이터 등록과 구매를 기준으로 데이터 거래 서비스 흐름 분석 · 각 절차에서 신뢰기관 역할 최소화를 위한 참여자의 역할 정의 및 절차 설계 기능 목록 - 데이터 등록  <데이터 등록 절차> 기능 목록 - 데이터 구매  <데이터 구매 절차> • 데이터 관리 기술에 대한 추가 요구사항 도출 및 데이터 관리 모듈 고도화 - 보안 요구사항 추가 도출 및 대응 방식 분석 · 암호화 상태 데이터 유통의 경우, 구매자는 거래 완료 이전에 데이터 확인 불가 · 거래 공정성을 보장을 위한 보호 수단으로 공정 서명 교환 방식 활용 · 기존 공정 서명 방식에서 중재자에 대한 의존도가 높음, 중재자에 대한 의존도를 낮추기 위한 새로운 기술의 개발 필요 - 서비스 흐름도 설계 과정 및 도출된 요구사항을 반영한 데이터 관리 모듈 고도화 구현 • 트러스트 데이터 생성 기술 검증을 위한 응용서비스 모델 고도화 - 차량데이터 기반 응용 서비스 고도화(신규서비스 모델 개발 1종, 서비스 모델 고도화 1종) - (신규서비스) “자율주행시스템 오동작 정보 및 위치정보 기반 안전지도 서비스” 모델 개발 · 자율주행차량에 탑재된 자율주행시스템의 오동작 및 인위적 차량제어권 전환 로그와 해당 시점 위치정보(GPS)를 활용한 자율주행자동차 전용 안전지도 서비스

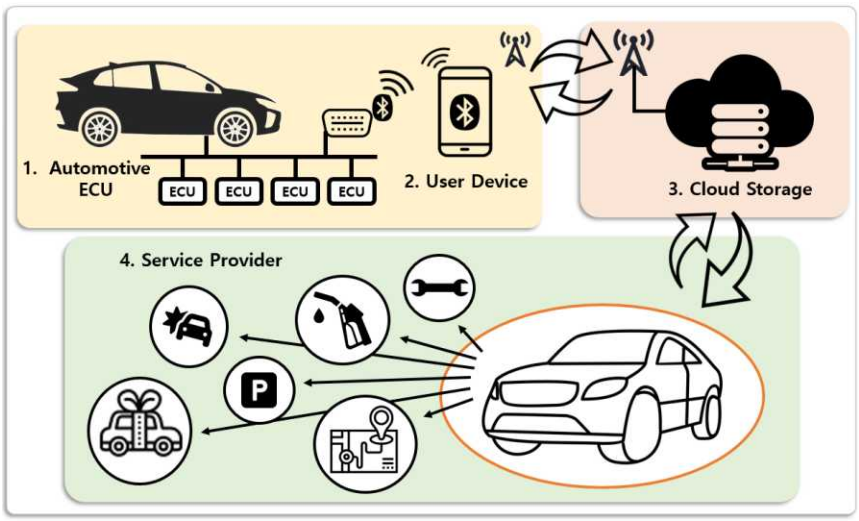
<자율주행시스템 오작동 정보 및 위치정보 기반 안전 지도 서비스 개요>

- (서비스 모델 고도화) 유사 휘발유 주입 검사 서비스
  · 차량의 주유 직후와 소비된 연료의 잔량 차이 비교를 활용한 유사 휘발유 검증 서비스
  · 전 세계 모든 차량이 공통 지원하는 OBD2 PID 범용데이터 이용 주유 전/후의 연료 잔량 획득 가능(범용서비스 개발 가능)



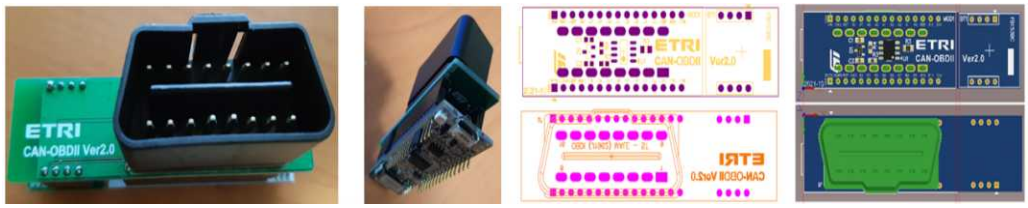
<유사 휘발유 주입 검사 서비스 고도화 개요>

• 트러스트 데이터 생성 기술을 이용한 응용 서비스 검증 테스트 환경 고도화
- 차량데이터 기반 서비스 개발을 위한 범용 아키텍처 정의 및 서비스 흐름 구성
  · 1. 데이터 생성 주체(자율주행자동차)
  · 2. 데이터 수집 주체(운전자 모바일 단말)
  · 3. 데이터 저장 주체(클라우드 저장소)
  · 4. 데이터 사용 주체(서비스 제공자)



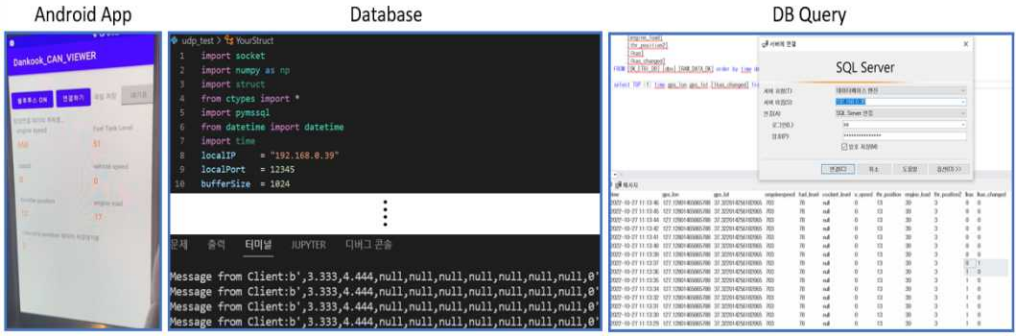
<차량생성 데이터 기반 서비스 환경 구성 고도화 개요>

• 트러스트 데이터 기반 응용 서비스 검증을 위한 테스트 환경 H/W & S/W 고도화
- 차량데이터 수집을 위한 OBD2-to-Bluetooth 디바이스 H/W & S/W 개발(범용 & 제조사 특화 데이터 동시 수신 가능)
· 차량 내 설치 디바이스 설계 및 구현



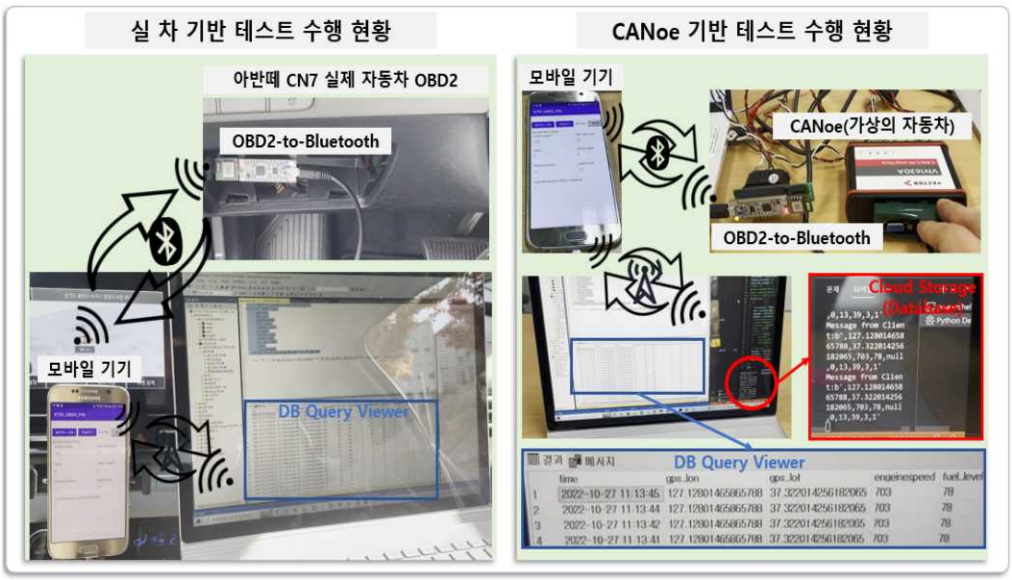
<차량생성 데이터 수집을 위한 차량 설치 디바이스 설계 및 구현체>

· 차량데이터 수신 및 클라우드 전송을 위한 스마트폰 애플리케이션 개발(Android App)
· 차량데이터 수집 및 분석을 위한 클라우드 스토리지 개발(데이터베이스 구축)
· 수집 데이터 기반 서비스 개발을 위한 데이터 조회 프로그램 제공(DB query 프로그램)

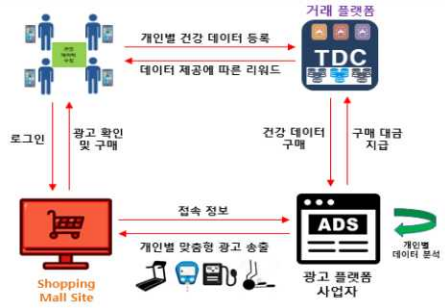
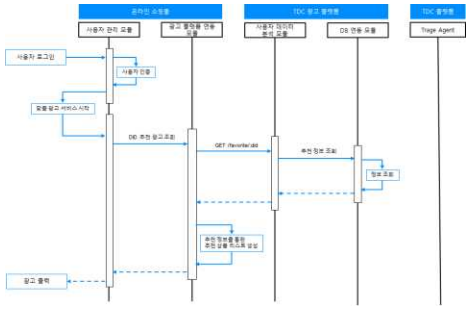


<스마트폰 애플리케이션, 클라우드 스토리지, 데이터 조회 프로그램 구축 현황>

• 응용 서비스 검증을 위한 실 차량 & 시뮬레이터 기반 테스트
- 상기 구축된 테스트 환경 검증을 위한 실 차량 & Automotive Network Simulator 기반 테스트 수행
· 아반떼 CN7 차량과 Vector CANoe Simulator 기반 테스트 수행
· 아반떼 CN7 기반 (신규서비스) "자율주행시스템 오동작 정보 및 위치정보 기반 안전지도 서비스" 모델 가능성 검증
· 아반떼 CN7 기반 (고도화서비스) 유사 휘발유 주입 검사 서비스 모델 가능성 검증 완료
· Vector CANoe 기반 (고도화서비스) 유사 휘발유 주입 검사 서비스 모델 가능성 검증 완료



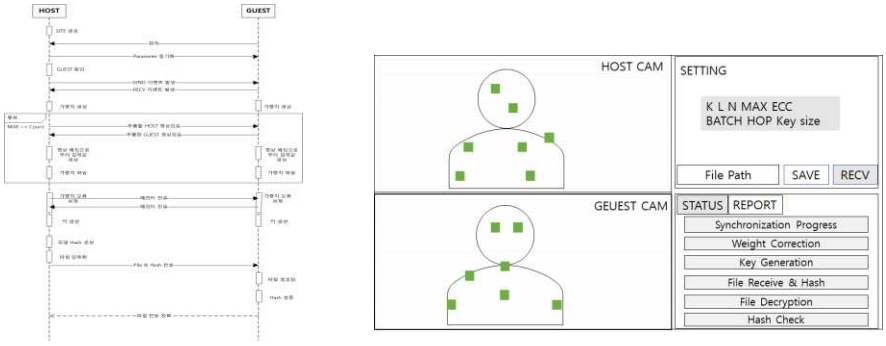
<트러스트 데이터 기반 응용 서비스 검증 테스트 수행 개요>

		• Healthcare Assistant 서비스 PoC 구현 - 데이터 생성자가 데이터 제공에 대한 직접적인 보상을 받을 수 있는 서비스 · 사용자가 스마트 단말을 통해 건강 데이터(혈압/심박수/심전도/체성분/운동량 등)를 수집하여 거래플랫폼으로 업로드 · 온라인 맞춤형 광고 사업자는 통계적 데이터로 활용하기 위해 거래플랫폼을 통해 건강 데이터 구매 및 분석 · 해당 사용자가 쇼핑몰 접속 시, 광고 사업자를 통해 개인 맞춤형 광고를 송출 · 거래플랫폼은 제공된 건강 데이터 생성/제공자에게 온라인 맞춤형 광고 사업자로부터 받은 리워드를 직접 지급  <Healthcare Assistant 서비스 개념도>  <Healthcare Assistant 서비스 플로우> ※ 주요결과물 - 차량데이터 기반 트러스트 데이터 커넥톰 서비스 모델 2종 - Healthcare Assistant 서비스 PoC 시스템 1종 - 차량데이터 수집/관리를 위한 HW/SW 모듈
	TTP-free 트러스트 데이터 생성 기술 연구	• 신경망 학습 기반 키교환 기술에 대한 안전성 모델 설계 및 검증 - 신경망 학습 기반 키교환 기술에 적용 가능한 안전성 모델 제시 · 신경망 학습 기반 암호 기술은 기존 암호 기반 기술과 달리 특정 수학적 난제에 안전성을 의존하지 않기 때문에 증명가능 안전성 모델을 통한 안전성 증명이 불가능 · 증명가능 안전성 모델을 대체하는 계산기반 안전성 모델 설계 · 키생성과 동일 수준 학습을 수행하는 공격자를 가정, 키생성 과정의 모든 공개 정보에 접근 가능한 다수의 공격자가 존재하는 환경에서 공격 성공 가능성을 계산적으로 제시 - 계산기반 안전성 모델을 통한 키교환 기술 안전성 증명 제시 · 공격 성공확률이 가장 높은 majority 공격 기법을 사용하는 공격자 가정 · 다수의 파라미터에 대해서 키교환 시뮬레이터를 통해 공격자의 성공 확률을 분석 $L = 30$ / $L = 35$ / $L = 40$ $hop = 1$(legacy algorithm): 0.0001 / 0.0001 / 0.0001 $hop = 2$: 0.0001 / 0.0004 / 0.0001 $hop = 3$: 0.0027 / 0.0009 / 0.0001 $hop = 4$: 0.0286 / 0.0103 / 0.0038 $L = 25$ / $L = 50$ 1-3 random walk: 0.0159 / 0.0001 $SCRN(1bit)$: 0.41 / 0.0000(0/10000) 1 bit / 2 bit / 3 bit / 4 bit P_E: 0.0000 / 0.0003 / 0.0007 / 0.0208 <안전성 강화 기술 적용에 따른 안전성 분석 결과> · "Improvement of the Efficiency of Neural Cryptography based Secret Key Exchange Algorithm" 국제 우수 학회 IEEE S&P 제출 (2022.12.2) • 신경망 학습 기반 데이터 암복호화 기술 설계 - 수학적 난제를 활용하지 않는 데이터 암복호화 설계 방식 제시 · 기존 데이터 암복호화 기술은 특정 수학적 난제에 안전성을 의존하기 때문에, 난제에 대한 안전성이 훼손되는 경우 안전성이 보장되지 못하며, 설계 방식 변경이 어려움 · 특정 난제 및 고정된 알고리즘에 의존하지 않는 데이터 암복호화 사용을 통해 예측하기

어려운 미래 위협에 사전 대비 가능

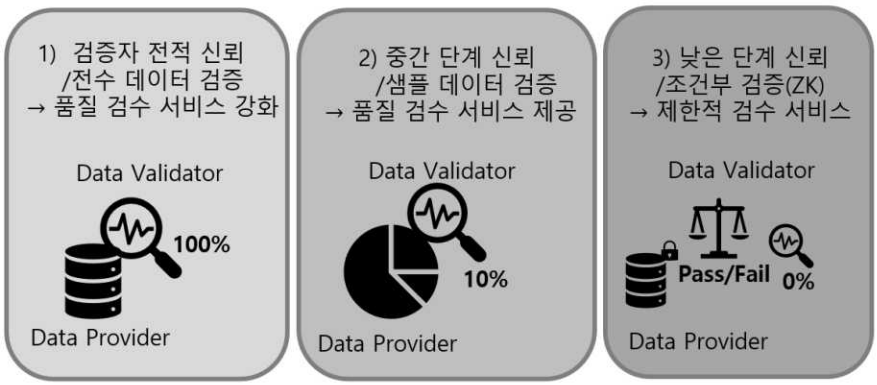
- 학습을 통한 신경망 동기화 방식을 통한 데이터 암복호화 기술 설계
  · 전송된 암호데이터를 학습데이터로 활용하는 신경망 동기화 진행
  · 학습데이터 비공개에 따라 기존 키교환 기술에 비해 높은 안전성 제공 가능
  · 학습데이터 재사용을 통한 높은 동기화 효율성 제공

• 신경망 학습 모델 기반 키 교환 실용성 검증을 위한 응용서비스 설계
- 상호 영상영역 기반으로 seed 추출 기술 설계
- 추출된 seed를 기반으로 신경망 학습 모델 기반 키 생성



<신경망 학습에 기반한 키생성 테스트 모듈>

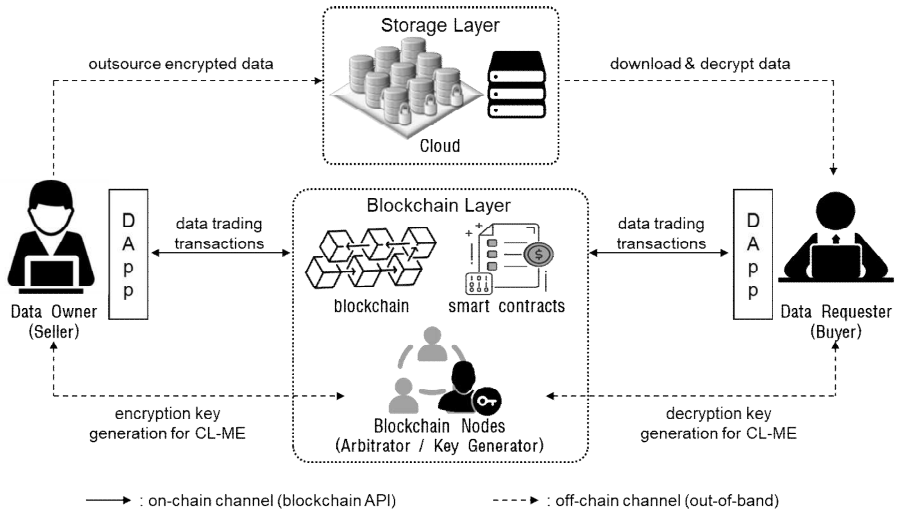
• 탈중앙화된 데이터 거래 환경에서 데이터 유효성 검증 모델 개발
- 데이터 주권 및 프라이버시 보호를 위한 탈중앙화 데이터 거래 환경에서 데이터 유효성 검증 프레임워크 제시
  · 거래 편의성을 위한 영지식증명 기반 데이터 유효성 검증 프로토콜 제안
  · 거래 데이터 위/변조 필터 제공 및 스마트 컨트랙트 기반 거래 자동화 가능
- 데이터 프라이버시 수준 및 특성에 따른 단계별 검증 방법 제시
  · 참여 검증자에 대한 데이터 노출 수준, 검증 수준을 선택적 이용
  · 다양한 데이터의 특성에 맞는 다양한 데이터 유효성 검증 방법 제공



<데이터 프라이버시 중요도 및 특성에 따라 검증 레벨 선택>

• 탈중앙 환경에서 사용자 중심 데이터 접근권한 세분화 관리 기술 연구
- 암호학적 접근 제어 기법 분석
  · ABE (Attribute-Based Encryption) 기법: 단일 실패 지점의 문제 및 사용자가 항상 온라인 상태이어야 한다는 한계점 가짐, 데이터 소스 식별을 위한 전송자액세스 제어 불가
  · ACE (Access Control Encryption) 기법 : 신뢰가능한 sanitizer 필요, 계층적 규제 환경(예: 군대, 정부) 기반 시스템 적합
  · ME (Matchmaking Encryption) 기법 : 데이터 기밀성, 액세스 프라이버시, 소스 식별 등의 속성을 지원하는 새로운 암호학적 프리미티브, 사용자 중심 데이터 거래에서 접근 권한 관리에 적합한 암호학적 프리미티브

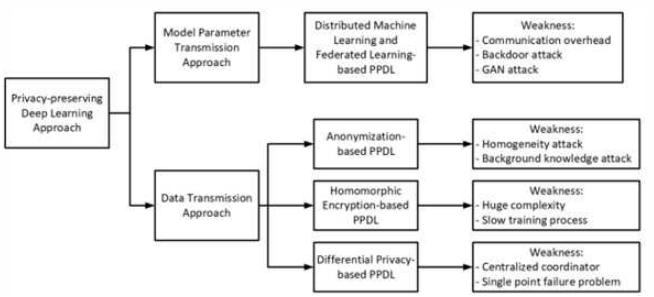
- 중앙신뢰기관 비의존적 사용자 중심 접근권한 관리 기술 연구
  · ME 기법 기반 탈중앙화된 데이터 거래/공유 기법 설계
  · ME 기법에 기반하여 데이터 소유자와 데이터 요청자의 양방향 접근 권한 적용
  · 기존 CL-ME 기법을 수정한 mCL-ME 기법을 적용하여, 고정된 중재자 노드(TTP)가 없는 블록체인 기반의 탈중앙화된 데이터 거래 모델 설계



<탈중앙 접근권한 관리 시스템 모델>

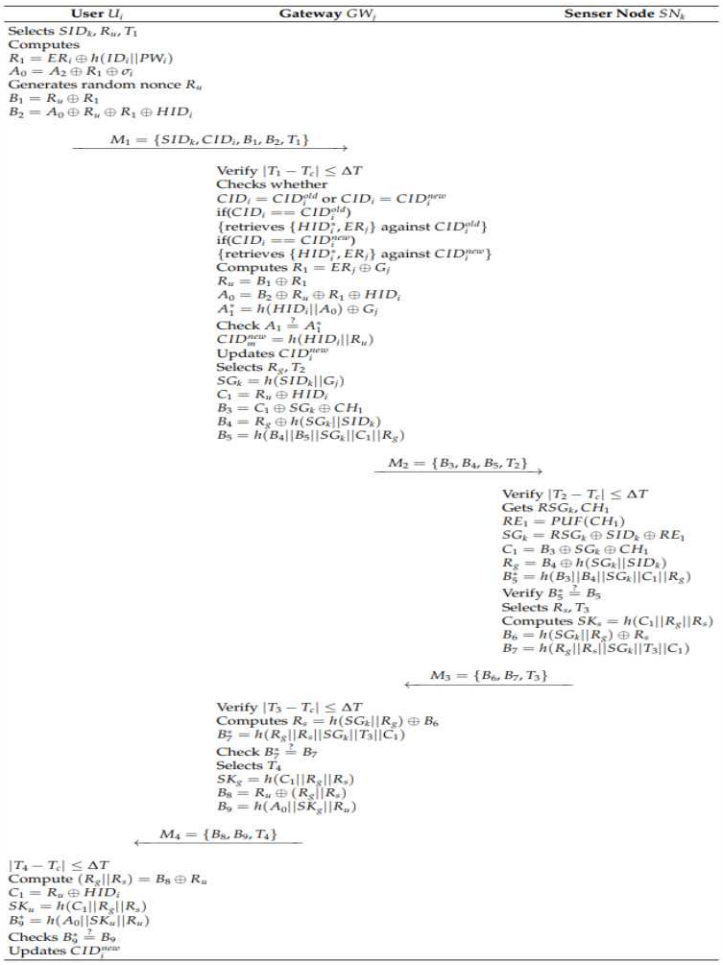
- 양방향 접근 권한 관리, 부인 및 부정 방지, 공정성, 적시성의 요구 사항 만족
- 블록체인의 저장 공간과 성능 문제를 최소화하기 위해 온체인(on-chain)과 오프체인(off-chain)을 결합한 하이브리드(hybrid) 방식으로 구성

• 데이터 프라이버시 보호를 위한 심층학습 모델 구성 요소 연구
- 고전적인 프라이버시 보호 기술 분석
  · 그룹 기반의 익명화 기술 : k-익명화, l-다양성, t-근접성, m-불변성 등
  · 암호학적 기법: 동형 및 함수 암호, 안전한 다자간 암호 연산
  · 차등 파라이버시 기술
  · 보안 Enclave : Intel SGX, RYoan Sandbox
- 심층 학습 기반 프라이버시 보호 기술 분석
  · 심층학습 계층 구성 방법
  · 합성곱 신경망(CNN), 적대적 내트워크(GNN), SVM
  · k-clustering, 순환 신경망(RNN)
- 각 프라이버시 보호 방식별 장단점 분석을 통한 개인데이터 유통 안전성 요구사항 도출



<프라이버시 보호 방식 분석>

• 개인데이터 활용 서비스 환경에서 프라이버시 강화를 위한 인증 및 키분배 프로토콜 연구
- 개인데이터 활용 서비스 환경의 데이터 프라이버시 보호 기술 최신 동향 분석
  · IoT 기반 무선 의료 센서 네트워크 환경에서 개인데이터 보안을 위한 사용자 인증 및 기법 연구
  · 멀티 서버 환경을 위한 키 동의 생체 측정 및 PUF 기반 인증 기법 연구
  · 스마트홈 환경에서의 개인정보보호를 위한 사용자 인증 기법 연구
- 무선 의료 네트워크를 위한 PUF 기반 안전하고 경량화된 상호 인증 프로토콜 방식 설계
  · PUF(Physical Unclonable Function)을 활용하여 물리적 보안 위협을 방지
  · Fuzzy extractor를 활용한 생체 정보 기반 Three-Factor 인증 모델 정립

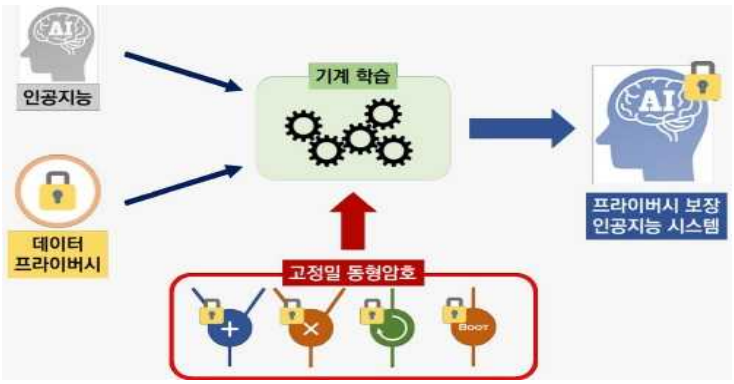


<무선 의료 네트워크 환경을 위한 PUF 기반 인증 프로토콜>

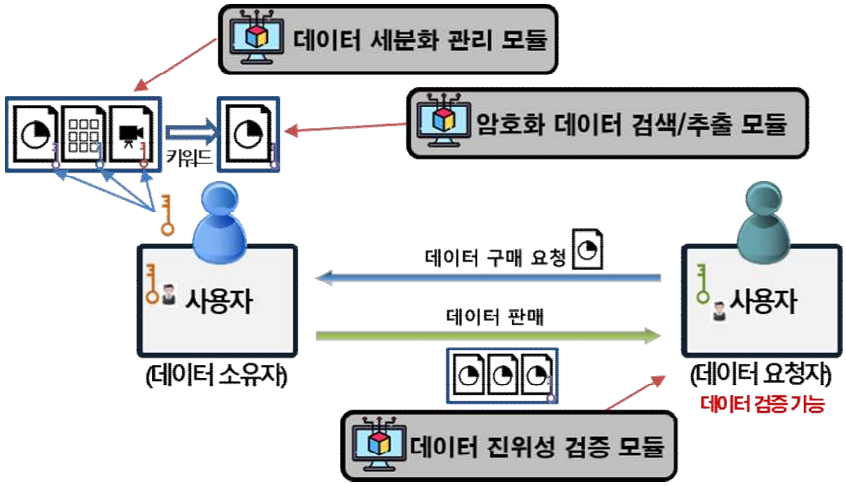
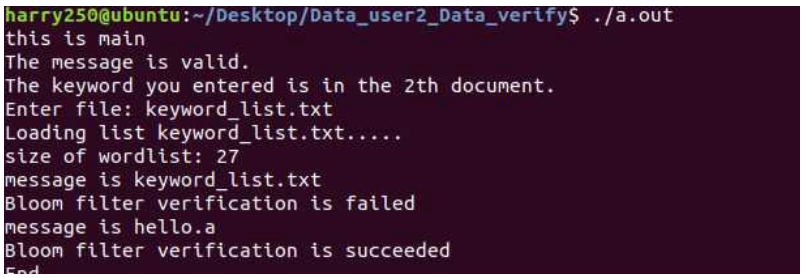
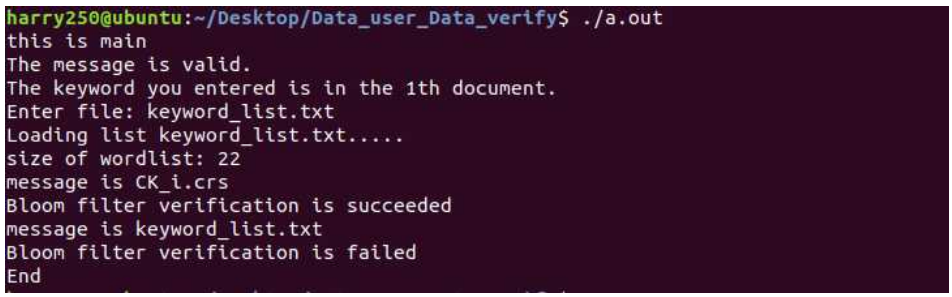
· Provably Secure PUF-based Lightweight Mutual Authentication Scheme for Wireless Body Area Networks, (Electronics, SCIE 논문 게재 예정)

• 개인데이터 공유 활용 환경에서 사용자 공개 데이터에 대한 프라이버시 보호 기술 연구

- 공개 영상 데이터에 대한 프라이버시 보호 기술 분석
  · 비식별화 기술은 사람이 식별할 수 없도록 모든 영상·이미지를 깨뜨리고, 인공지능 학습만 가능하도록 처리
  · 데이터에서 개인 식별정보를 삭제하는 동시에 인공지능 개발에 필요한 정보를 보존하여 문자·표정 인식 등 다양한 응용 분야에서 원본 데이터와 동일한 수준으로 데이터를 활용
  · 동형암호 알고리즘은 실수 연산을 지원하여 기술을 통해 암호화된 데이터가 상용의 인공지능 시스템에 적용되어 데이터의 프라이버시가 보장
- 트러스트 데이터 커넥톰을 통한 개인데이터 유통 과정의 데이터 프라이버시 보호를 위한 적용 가능 기술 분석

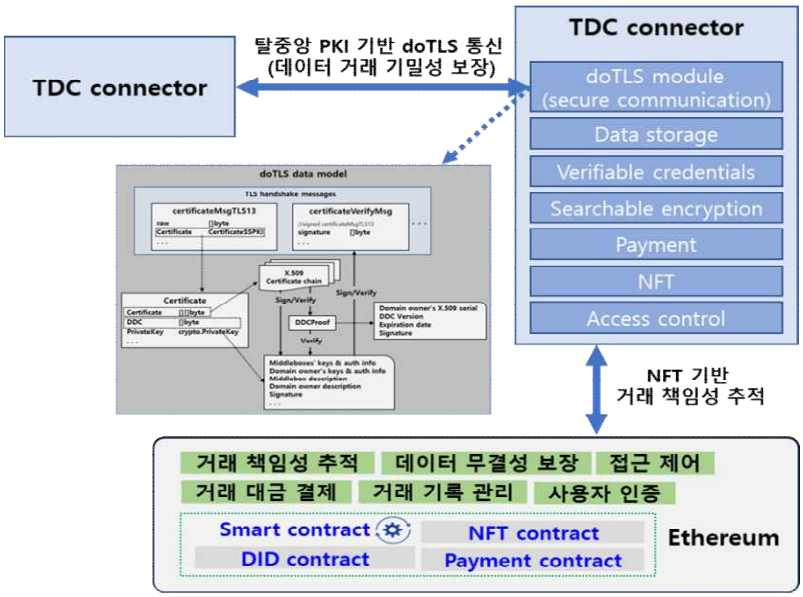


<인공지능에서 데이터 프라이버시 보장을 위한 고정밀 암호화>

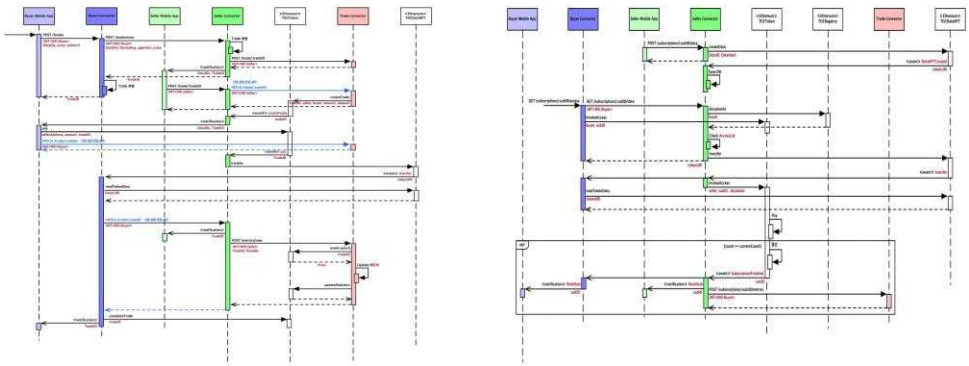
		※ 주요결과물 - 신경망 학습 기반 데이터 암복호화 기술 설계서 및 키교환 응용 S/W - 탈중앙화 데이터 거래를 위한 영지식 증명 기반 노출없는 데이터 유효성 검증 기술 (IPR) - 분산환경의 사용자 중심 접근권한 관리 기술 설계서
	TTP-free 트러스트 데이터 커넥팅 기술 연구	• 집계 키 암호 기반 다중 위임 개인 데이터 접근제어 및 책임성 추적 기술 개발 - 개인 데이터 중심 키 및 데이터 접근 관리 알고리즘 개발 · 데이터 세분화 관리를 위한 Key aggregate 기반 키/데이터 접근 관리 모듈 개발 · 고정된 키 사이즈로 다중 데이터 암호화 및 복호화 가능 · 암호화된 상태의 데이터 중 원하는 데이터에 대한 독립적인 키 업데이트 가능  <집계 키 암호 기반 다중 위임 개인 데이터 접근제어 알고리즘> - 데이터 활용도 향상을 위한 검색 가능한 암호화 및 권한 위임 기술 개발 · Searchable Encryption 기반 암호화 데이터 검색 기술 개발 · 암호화 상태의 데이터 검색 가능 기술로 데이터 활용도 향상 가능 · 데이터 가용성 보장을 위한 데이터 소유자 중심 데이터 접근 권한 위임 기술 개발  <검색 가능한 집계 키 암호화> - 데이터 책임성 보장을 위한 데이터 검증 기술 개발 · 거래 데이터 신뢰성 향상을 위한 Bloom Filter 기반의 데이터 키워드 검증 기술개발 · 데이터에 포함된 키워드를 기반으로 데이터 신뢰성 보장 가능  <Bloom Filter 기반 데이터 키워드 검증> - SCIE 국제 논문지 2편 게재

· A Secure Data Sharing Based on Key Aggregate Searchable Encryption in Fog-enabled IoT Environment, IEEE TNSE (상위20% SCIE 저널) 게재
· A Secure Personal Health Record Sharing System with Key Aggregate Dynamic Searchable Encryption, Electronics, 게재

- 트러스트 데이터 거래 플랫폼 개발
· NFT 기반 데이터 거래 책임성 추적 기능 설계 및 스마트 컨트랙트 개발
· NFT 기반 거래 책임성 추적 가능한 데이터 일괄거래 및 구독거래 프로토콜 개발

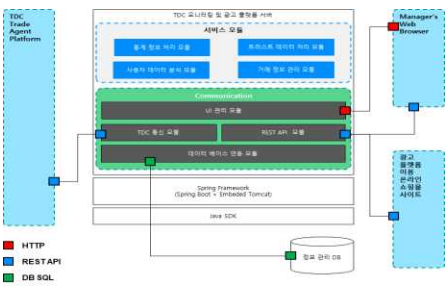


<트러스트 데이터 거래 플랫폼 확장 기술 구조>


<책임성 추적 가능한 데이터 일괄거래 및 구독거래 Sequential Flow>

- 트러스트 데이터 거래 검증 도구 제작
· 트러스트 데이터 전체 거래 과정을 검증하고 가시화하는 도구
· 플랫폼/단말 간, 구매자/판매자 단말 간 거래 과정의 성공/실패/진행 과정 가시화
· 거래 실패 시 발생지점/원인/조치방안 등을 팝업 형태로 출력
· 기개발된 단말 App. 및 모니터링 툴 연계

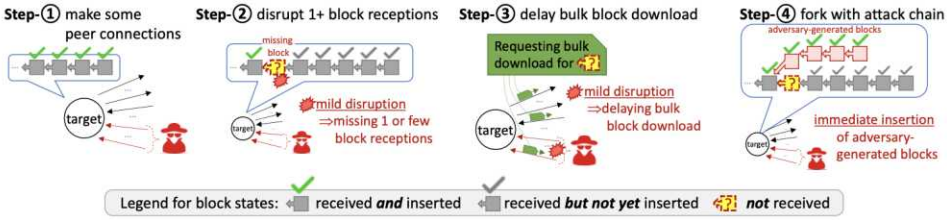
<트러스트 데이터 거래 검증 도구 개념도>



<트러스트 데이터 거래 검증 도구 구조>

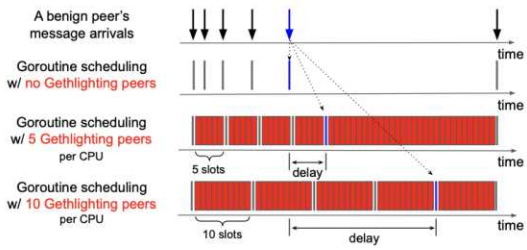
- 사용자 프라이버시 보호를 위한 doTLS 기반 데이터 거래 기밀성 보장 통신 기능 개발
  · doTLS 라이브러리를 데이터 거래 플랫폼에 적용하여 프라이버시 보호 가능한 기밀성 보장 통신 기능 구현

• 블록체인 네트워크 파티셔닝 연구 및 공격 저항성 기술 개발
- 블록체인 네트워크에서 Eclipsing이 필요없는 파티셔닝 공격 가능성 발견
  · 스테이트 기반 블록체인의 특징에 따른 새로운 공격 방법 확인



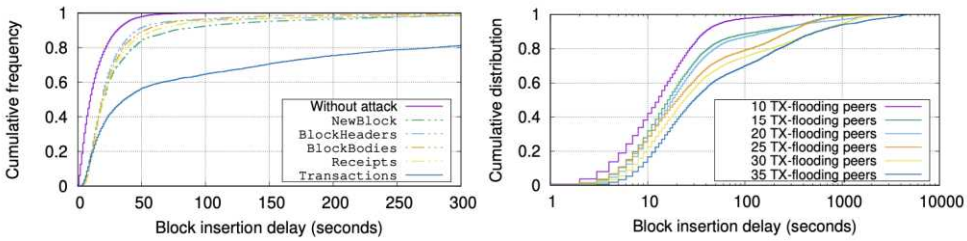
<Eclipsing이 필요없는 블록체인 파티셔닝 공격의 절차>

  · 블록체인 노드의 Per-peer isolation 문제점을 이용하는 공격 벡터 확인



<Per-peer isolation 문제점으로 인한 지연 문제점 개념도>

  · 블록체인 메시지 종류 및 공격 피어 수에 따른 공격 영향력 분석



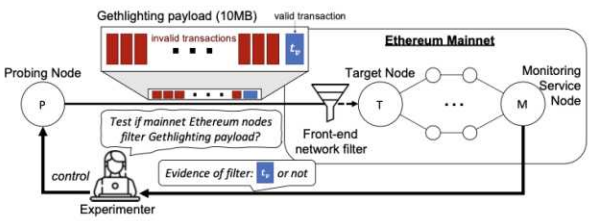
<메시지 종류와 피어 수에 따른 지연 블록 처리 지연 측정 결과>

- 실제 이더리움 블록체인 네트워크를 대상으로한 공격 가능성 및 영향력 검증
  · 이더리움 테스트넷 실험을 통해 실제 운영중인 노드의 취약점 확인

Client-*codename* (or registered name)	Kind	# of nodes (tested)	# of conns	Max block insertion delay
Geth-*omnibus*	RPC	39 (3)	28–34	9,092–9,560 sec
Geth-*d*****	RPC	1	32	2,529 sec
Infura signer	Miner	1	14	280 sec
Infura bootnode	Bootnode	1	40	4,153 sec
Akasha bootnode	Bootnode	1	40	2,891 sec
Geth-*P*********	Unknown	1	40	4,292 sec
Geth-*l****	Unknown	1	28	3,686 sec
Geth-*S***	Unknown	1	40	1,269 sec

<테스트넷 실험을 통한 취약점 확인>

  · 이더리움 메인넷 실험을 통해 공격에 사용된 벡터가 실제 이더리움 망에서 유효함 확인



Client-*codename*	Kind	# of nodes	Valid txid prefix
Geth-*EthereumPPLNS*	Miner	18	0xe64630
Geth-*EthereumSOLO*	Miner	3	0x336fae
Geth-*E*********	Miner	2	0x9ab8c0
Geth-*e*********	Miner	1	0x43ea7b
Geth-*c*********	Miner	1	0xfb90a5
Geth-*omnibus*	RPC	63	0xd21bf1
Geth-*A*********	RPC	18	0x4d8d64
Geth-*M*********	RPC	6	0x6f9017
Geth-*a*********	RPC	3	0xe4ecd0
Geth-*I*****	Misc	1	0x96ece0
Geth-*k****	Misc	1	0xd0ffe8
Geth-*m*********	Misc	1	0xe92dd9
Geth-*W*********	Misc	1	0x15b684
Geth-*p******	Unknown	4	0x0b884d

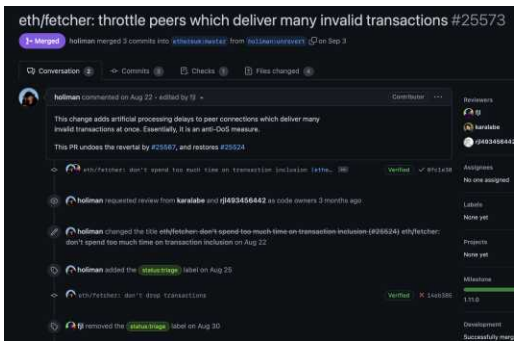
<메인넷 실험 개념도 및 실험 결과>

- 제안된 파티셔닝 공격 취약점 해결 방안 제시 및 이더리움 코드 구현

Countermeasures	Corresponding Ethereum's Characteristics	Related Attack Steps	Disadvantages or Side Effect
Taming TX-flooding	**[EC1]**	Step-② & Step-③	Significant changes to P2P
Bounded transaction handling	**[EC1]**	Step-② & Step-③	A few worst-case delays, slow TX handling
Making clients block synchronized first	**[EC1]**	Step-② & Step-③	Weak transaction propagation
Gethlighting-resistant block propagation	**[EC2], [EC5]**	Step-②	Msg complexity, risk of DoS
Banning Gethlighting peers	**[EC3]**	Step-② & Step-③	False positives, risk of new attacks
Overprovisioning clients	**[EC5]**	Step-② & Step-③	Expensive

<6가지 파티셔닝 공격 취약점 해결 방안>

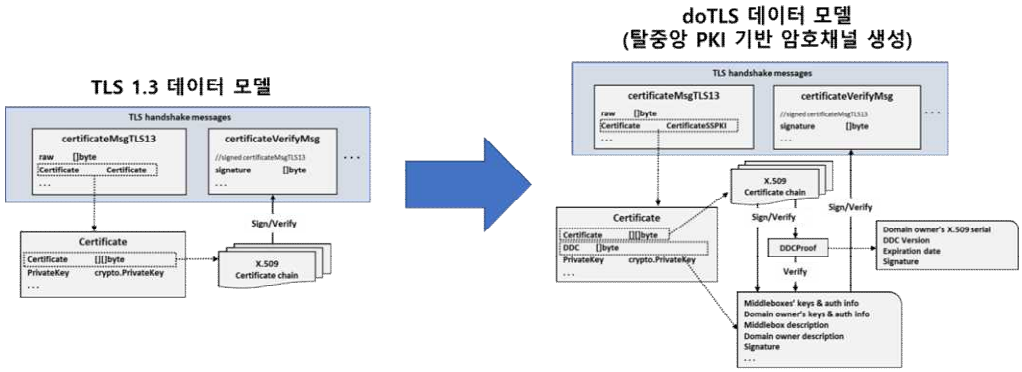
- 이더리움 재단 취약점 보고 및 논문 제출
  · 이더리움 재단 버그 바운티 프로그램을 통해 취약점 및 해결방안 제출 (2022/7)
  · 취약점 및 해결방안 채택 (2022/9)
  · 이더리움 취약점 패치 1.11.0 버전 적용 (2022/11)



<Geth 1.11.0 버전에 적용된 취약점 패치>

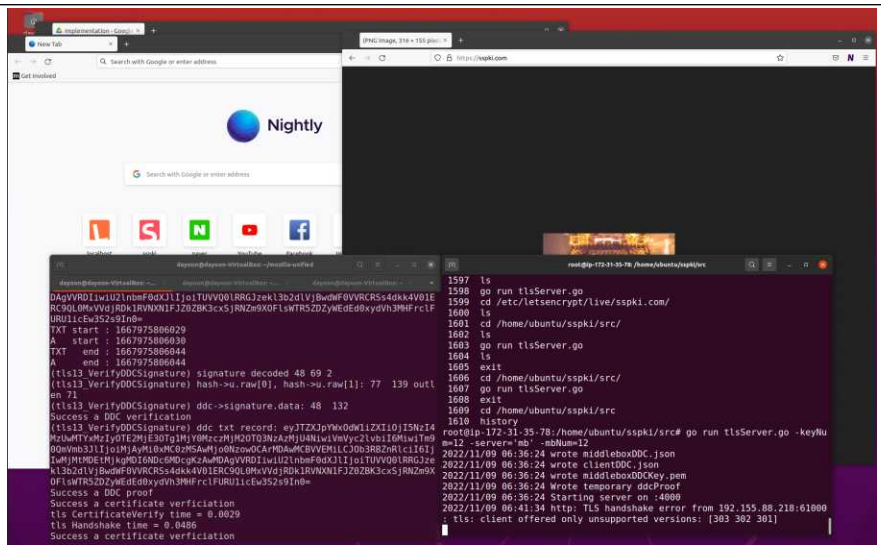
  · NDSS 2023 "Partitioning Ethereum without Eclipsing It" 1저자 Major Revision 진행 중 (2022/11)

• 거래 참여자 프라이버시 보호를 위한 탈중앙 Web PKI (doTLS) 프로토콜 개발
  - 중앙 기관 (CA) 독립적으로 사용자 인증 정보 관리 가능한 TLS 데이터 모델 설계
    · 사용자 인증키 위임/폐기 가능한 Domain-Defined Credential (DDC) 데이터 구조 설계
    · DDC 기반 사용자 인증 및 DDC 유효성 검증 프로토콜 및 알고리즘 개발
    · 기존 Web PKI 및 TLS 프로토콜과 호환 가능한 doTLS 데이터 모델 설계



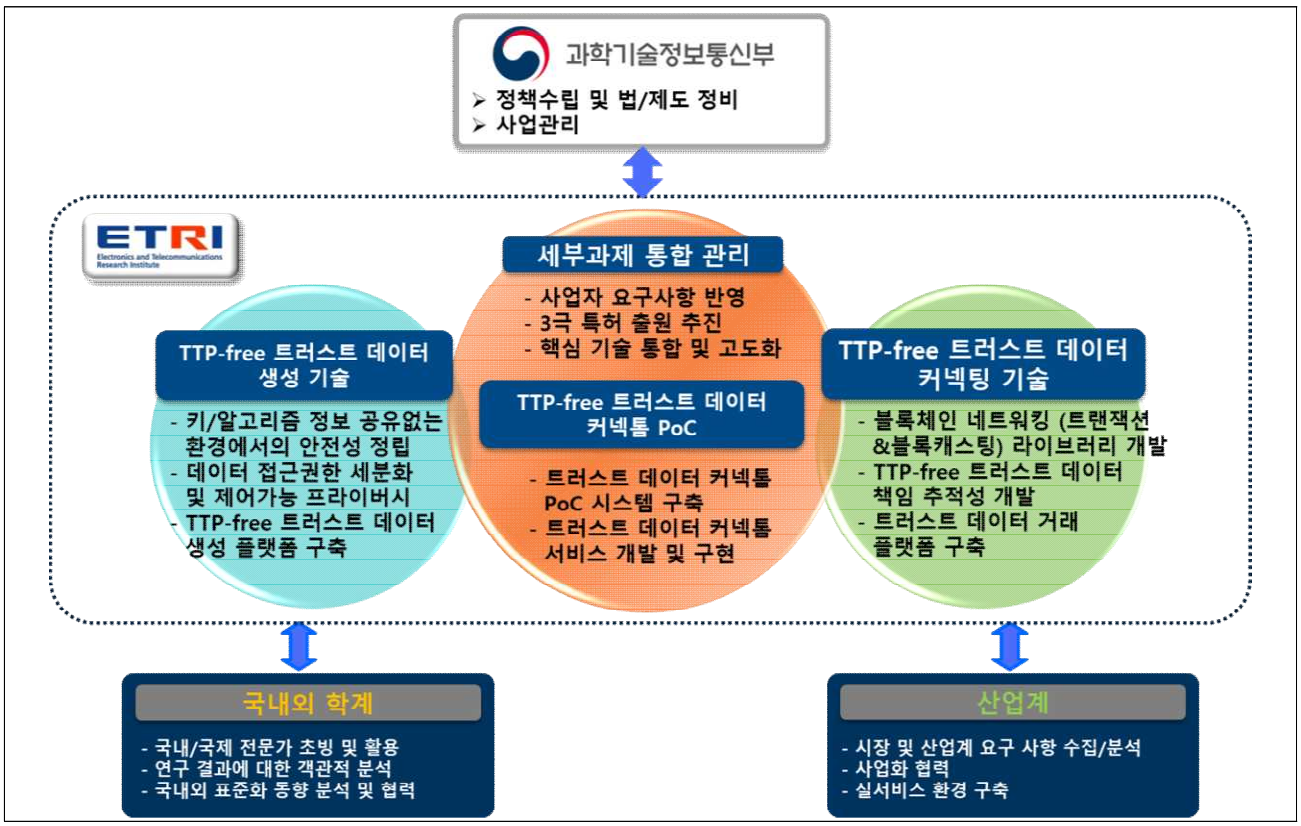
<doTLS 데이터 모델>

  - 기존 웹 인프라와 호환 가능한 doTLS Go언어 라이브러리 및 Firefox 브라우저 개발
    · Go 언어 TLS package에 doTLS 서버 및 클라이언트 기능 개발
    · Firefox Nightly의 NSS 라이브러리에 doTLS 클라이언트 기능 개발
  - 웹 환경에서 doTLS 기능 및 성능 실험을 통해 데이터 거래 프로토콜 적용 가능성 확인
    · 실제 인터넷 망에서 사용되는 웹 인프라 (Let's Encrypt CA 인증서, Google Cloud, Firefox browser, Cloudflare DNS) 실험 환경 구축
    · 실험을 통해 doTLS 기반 사용자 인증 기능 및 암호 채널 통신 성능 확인

		 <웹 환경에서의 doTLS 실험 결과> - 국제 특허 1건 출원 (예정) · SYSTEM AND METHOD FOR INDEPENDENTLY MANAGING AUTHENTICATION INFORMATION USING DID - 국내 특허 1건 출원 · 인증 기관과 독립적으로 인증서 내의 인증 정보를 관리하기 위한 방법 - 국내 학술대회 1건 개재 · 사용자 주권을 보장하는 블록체인 기반 개인데이터 거래 플랫폼 구조 연구, 한국통신학회 2022년도 추계종합학술발표회 ※ 주요결과물 - 집계 키 암호 기반 분산데이터 접근 제어 알고리즘 S/W - TTP-free 사용자 인증 doTLS 프로토콜 라이브러리 S/W - 트러스트 데이터 플랫폼 S/W - 트러스트 데이터 거래 검증 도구 SW
부경 대학교 (위탁1)	탈중앙 환경에서 사용자 중심 데이터 접근권한 세분화 관리 기술 연구	• 탈중앙 환경에서 사용자 중심 데이터 접근권한 세분화 관리 기술 연구 - 사용자 중심 데이터 접근권한 관리 기술 동향 분석 - 탈중앙 암호 데이터 거래 환경을 위한 데이터 접근권한 세분화 요구사항 분석 - 중앙신뢰기관에 비의존적인 사용자 중심의 접근권한 관리 기술 연구
계명 대학교 (위탁2)	개인데이터 활용 서비스 환경에서 데이터 프라이버시 강화를 위한 인증 및 키분배 프로토콜 연구	• 개인데이터 활용 서비스 환경에서 데이터 프라이버시 강화를 위한 인증 및 키분배 프로토콜 연구 - 개인데이터 활용 서비스 환경에서 발생가능한 사이버 보안 위협 및 최신 동향 분석 - 개인데이터 활용 서비스 환경의 보안기술 요구사항 및 데이터 프라이버시 최신 보안기술 동향 분석 - 개인데이터 활용 서비스 환경에서 사용자 중심의 데이터 프라이버시 강화를 위한 인증 및 키분배 프로토콜 분석 및 설계
상명 대학교 (위탁3)	신경망 학습을 이용한 사용자 공개 데이터의 정보보호 기술 연구	• 신경망 학습을 이용한 사용자 공개 데이터의 정보보호 기술 연구 - 사용자 공개 데이터에서의 프라이버시 보호 기술 최신 동향 분석 - 사용자 공개 데이터에서의 프라이버시 요구사항 분석 - 신경망 학습을 이용한 사용자 공개 데이터에서의 프라이버시 보호 기술 고도화 연구
국제 사이버 보안 연구원 (위탁4)	데이터 프라이버시 보호를 위한 심층학습모델 구성요소 연구	• 트러스트 데이터 커넥톰 서비스에서 데이터 프라이버시 보호를 위한 심층학습모델 연구 - 개인데이터 거래 활용에 따른 심층 학습용 개인정보 보호 방안 연구 - 심층학습에 적용되는 암호학적 요소 기술 및 프로토콜 연구 - 프라이버시 보호 심층학습의 구성요소 장단점 분석
KAIST (위탁5)	블록체인 네트워크의 전체적 안전성을 위한 기반 기술 개발	• 블록체인 네트워크의 전체적 안전성을 위한 기반 기술 개발 - 블록체인 네트워크 안전성에 대한 최신 연구 동향 분석 - 퍼블릭 블록체인 네트워크의 전체적 안전성에 대한 측정 기반 분석 - 블록체인 네트워크의 전체적 안전성을 제공하기 위한 핵심 기술 연구 개발
경북 대학교 (위탁6)	TTP-free 기반 사용자 중심 데이터 책임성 보장 알고리즘 개발	• TTP-free 기반 사용자 중심 데이터 책임성 보장 알고리즘 개발 - 개인 생성 데이터 책임성 보장 기술 개발 - 개인 데이터 관리 기술 최신 연구 동향 분석 - 개인 데이터 관리를 위한 키 및 데이터 관리 기술 개발

3. 과제수행기간 추진체계 및 방법

가. 과제수행 추진체계



❍ 한국전자통신연구원 주도로 기존 TTP 기반 환경에 의존하지 않고 데이터 주권과 안전한 교환을 보장하는 트러스트 데이터 커넥톰 원천기술로서 'TTP-free 트러스트 데이터 생성 기반 기술' 및 'TTP-free 데이터 커넥팅 기술' 연구 추진

- 오픈소스 프로젝트 활용 및 공개 정책을 통해 개발 부담 최소화 및 핵심 원천 기술 확보 집중
- 위탁연구기관을 통해 학습 기반 데이터 시큐리티 보호 기술에 대한 안전성 모델 검증 및 고도화 진행
- 블록체인 네트워크의 전체적 안전성을 위한 기반 기술 연구 및 개인 데이터 중심의 데이터 책임성 보장 기술 개발을 학계와 위탁 연구 예정
- 최종 트러스트 데이터 커넥톰 PoC를 위해, 핵심 개발 결과인 'TTP-free 트러스트 데이터 생성 기반 기술' 및 'TTP-free 데이터 커넥팅 기술'에 대한 통합 시스템 구축 진행

❍ 국내외 관련 산업 분야의 동향 및 컴퓨팅 환경 변화에 대한 적극적인 정보 수집 추진

❍ 국내 산업계 및 관련 기관 전문가와의 연계를 통해 개인데이터 유통 활용 서비스 분야의 요구사항 반영을 통한 연구 개발 결과에 활용성 강화 진행

❍ 국내 기업과의 협력을 통해 과제 연구 결과에 대한 기술이전 및 상용화 논의 진행

나. 과제수행 방법

❍ 개인데이터 유통 환경 분석을 통해 정의된 서비스 시나리오에 대한 다양한 검토 의견 수렴을 통한 PoC 최적화 서비스 선정, TTP-free 트러스트 데이터 생성 기술 및 TTP-free 트러스트 데이터 커넥팅 기술에 기반한 트러스트 데이터 커넥톰 통합 시스템 구축 추진

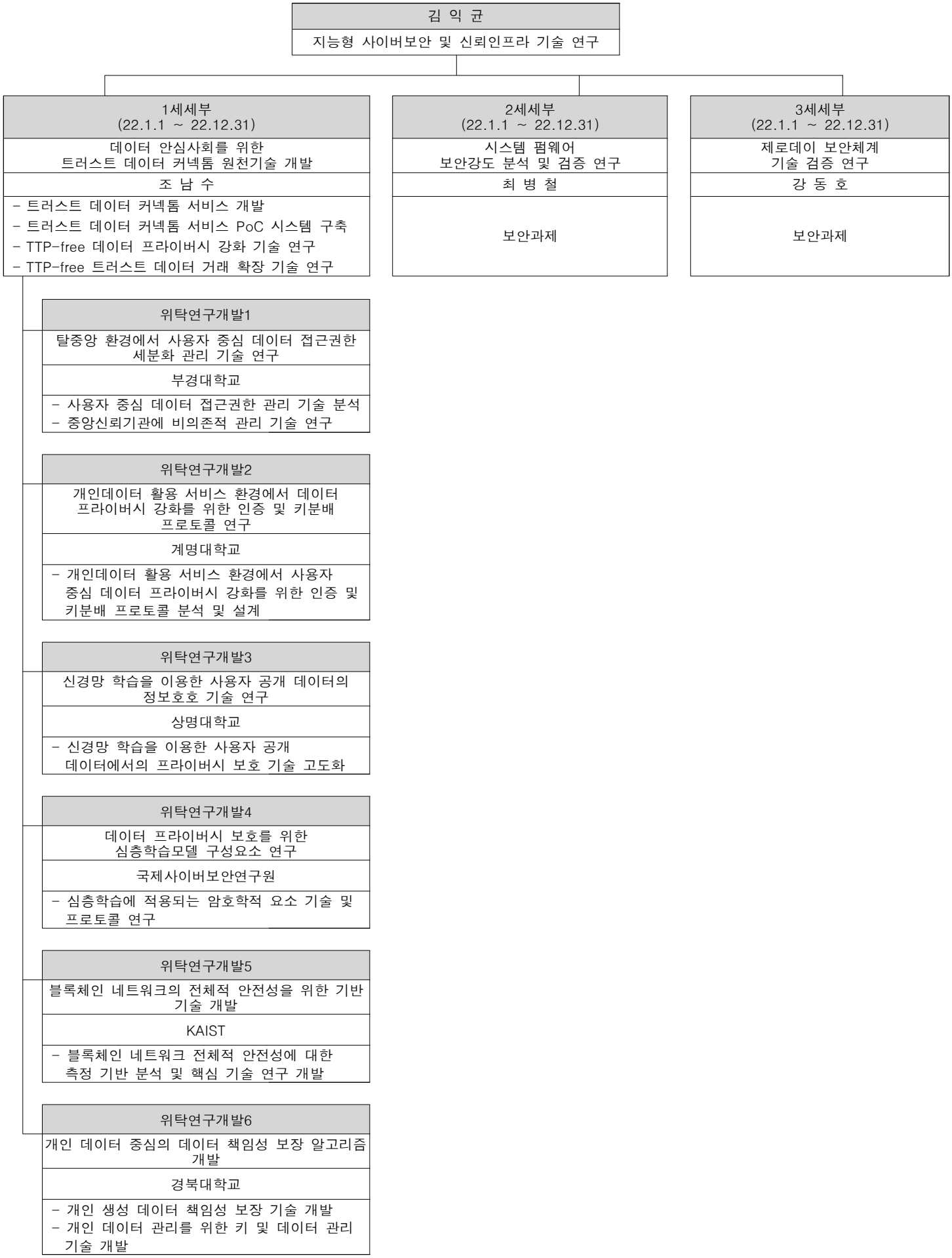
❍ 트러스트 데이터 생성 기술

- 1단계에서 확보된 TTP-free 키교환 기술을 토대로 TTP-free 트러스트 데이터 커넥톰 환경에서의 시큐리티 보장을 위한 안전성 모델 정립과 안전성 강화 기술 연구로 확장 추진
- 1단계에서 확보된 신경망 학습 기반 암호 설계 기술을 기반으로, 신경망 학습에 기반한 키/알고리즘 공유 정보 없는 환경에 적용 가능한 데이터 암복호화 알고리즘 설계 추진
- TTP-free 환경의 데이터 프라이버시 강화를 위한 제어가능 프라이버시 기술 및 데이터 접근권한 세분화 기술 개발
- 확보된 핵심 기술을 트러스트 데이터 커넥톰 환경에 적용하기 위한 트러스트 데이터 생성 플랫폼 구축 및 핵심 기술 고도화 추진

❍ 트러스트 데이터 커넥팅 기술

- 블록체인 네트워크 안전성에 대한 최신 연구 동향 분석, 퍼블릭 블록체인 네트워크 안전성 측정을 통해 블록체인 네트워크의 전체적 안전성을 위한 기반 기술 도출
- 개인이 생성하는 데이터를 개인이 직접 안전하고 효율적으로 관리하고 데이터에 대한 책임성을 보장하는 연구를 통해 TTP-free 환경의 사용자 중심 데이터 책임성 보장 기반 기술 도출
- 블록체인 원장 모델과 블록, 트랜잭션 정보 전달을 위한 全네트워크적 구조 분석을 통해 블록체인 네트워크 안정성과 효율성을 위한 원장 및 전달 기술 제시
- 블록체인 SW 및 데이터 거래 소프트웨어 분석을 통해 거래 책임성 보장 가능한 트러스트 데이터 거래 플랫폼 구축
- 트러스트 데이터 거래 과정에서 플랫폼과 단말 간, 구매자/판매자 단말 간의 전체 거래 과정을 검증하고 가시화하는 도구 제시

다. 과제수행 편성도(세부기술 수행체계)



3 과제 수행결과 및 목표달성도

1. 과제 수행결과

<table>
<tr><th>구분</th><th>2021년도 (성과)</th><th>2022년도 (성과)</th></tr>
<tr><td>정량</td><td>
<table>
<tr><th colspan="2">논문</th><th colspan="4">특허</th><th colspan="2">기술이전</th></tr>
<tr><th rowspan="2">SCI(건)</th><th rowspan="2">비SCI(건)</th><th colspan="2">해외(건)</th><th colspan="2">국내(건)</th><th rowspan="2">건수</th><th rowspan="2">금액(백만원)</th></tr>
<tr><th>출원</th><th>등록</th><th>출원</th><th>등록</th></tr>
<tr><td>8건</td><td>3건</td><td>3건</td><td>-</td><td>4건</td><td>-</td><td>-</td><td>-</td></tr>
</table>
※논문 목표(2건) 대비 400% 달성

※국내/국제 특허 목표(2건/2건) 대비 각 200%, 150% 달성

•(사업화) 해당사항없음
•(표준화) 해당사항없음
•(기타) 해당사항없음</td><td>
<table>
<tr><th colspan="2">논문</th><th colspan="4">특허</th><th colspan="2">기술이전</th></tr>
<tr><th rowspan="2">SCI(건)</th><th rowspan="2">비SCI(건)</th><th colspan="2">해외(건)</th><th colspan="2">국내(건)</th><th rowspan="2">건수</th><th rowspan="2">금액(백만원)</th></tr>
<tr><th>출원</th><th>등록</th><th>출원</th><th>등록</th></tr>
<tr><td>10건</td><td>3건</td><td>3건</td><td>1건</td><td>3건</td><td>2건</td><td>-</td><td>-</td></tr>
</table>
※논문 목표(3건) 대비 333% 달성

※국내/국제 특허 목표(2건/1건) 대비 각 150%, 300% 달성

•(사업화) 해당사항없음
•(표준화) 해당사항없음
•(기타) 해당사항없음</td></tr>
<tr><td>정성</td><td>• 특정 TTP에 의존하지 않은 multi-domain 환경에서 프라이버시 보장 기술 제공
- multi-domain 환경에서 다중 TTP 기반 유연한 데이터 권한 관리 모델 제시
- 기밀성, 인증 및 데이터 권한 부여를 제공하는 토큰 기반 multi-domain 인증 모델 설계</td><td>• 기존 특정 수학적 난제에 의존하는 증명가능 안전성 모델 적용이 불가능한 신경망 학습 기반 암호 기술에 대한 계산 기반 안전성 모델 제시 및 이를 적용한 안전성 검증 수행
- 우수 국제 학회 IEEE S&P 논문 제출</td></tr>
</table>

가. 세부 정량적 성과

[과학적 성과]

□ 논문(국내외 전문 학술지) 게재

번호	논문명	학술지명	주저자명	호	발행기관	SCIE 여부	게재일	등록번호 (ISSN)	기여율 (%)
1	BPPS: Blockchain-Enabled Privacy-Preserving Scheme for Demand-Response Management in Smart Grid Environments	IEEE Tr. On Dependable and Secure Computing	박기성	-	IEEE	**SCIE (상위 20%)**	2022.03.29	1545 -5971	100
2	A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions	IEEE Internet of Things Journal	유성진	Vol.9	IEEE	**SCIE (상위 20%)**	2022.10.15	2327 -4662	70
3	A Secure Data Sharing Based on Key Aggregate Searchable Encryption in Fog-enabled IoT Environment	IEEE Tr. On Network Science and Engineering	이준영	vol.9 Issue. 6	IEEE	**SCIE (상위 20%)**	2022.11.1	2327 -4697	100
4	Rcryptect: Real-time detection of cryptographic function in the user-space filesystem	Elsevier Computers & Security	이승광	-	Elsevier	SCIE	2022.1.1	0167 -4048	30
5	On the Security of a Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks	Applied Sciences	박기성	-	MDPI	SCIE	2022.04.23	2076 -3417	100
6	SALS-TMIS: Secure, Anonymous, and Lightweight Privacy-Preserving Scheme for IoMT-Enabled TMIS Environments	IEEE Access	유성진	Vol.10	IEEE	SCIE	2022.06.08	2169 -3536	100
7	On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain	IEEE Access	손승환	Vol.10	IEEE	SCIE	2022.07.15	2169 -3536	100
8	PUFTAP-IoT: PUF-based three factor authentication protocol in IoT environment focused on sensing devices	Sensors	이준영	Vol.22, No.18	MDPI	SCIE	2022.09.19	1424 -8220	70
9	A Secure Personal Health Record Sharing System with Key Aggregate Dynamic Searchable Encryption	Electronics	오지현	vol.11 Issue.19	MDPI	SCIE	2022.10.06	2079 -9292	100
10	Practical Order-Revealing Encryption with Short Ciphertext	IEICE Trans. on Information and Systems	윤택영	Vol. E105-D, No.11	IEICE	SCIE	2022.11.1	1745 -1361	50

□ 국내 및 국제 학술회의 발표

번호	발표명	학회명	발표자	발표일시	장소
1	분산환경에서 사용자 데이터 공유를 위한 접근제어 방식에 관한 연구	통신학회	박기성	2022.11.17	경주
2	사용자 주권을 보장하는 블록체인 기반 개인데이터 거래 플랫폼 구조 연구	통신학회	윤대근	2022.11.17	경주
3	데이터 자율 거래를 위한 모니터링 툴 개발에 관한 연구	통신학회	문승진	2022.11.17	경주

□ 기술 요약 정보

※ 해당사항없음

□ 보고서 원문

※ 해당사항없음

□ 생명자원(생물자원, 생명정보)/화합물

※ 해당사항없음

[기술적 성과]

□ 지식재산권(특허, 실용신안, 의장, 디자인, 상표, 규격, 신품종, 프로그램)

번호	지식재산권 등 명칭 (건별 각각 기재)	국명	출원			등록			기여율	활용 여부
			출원인	출원일	출원 번호	등록인	등록일	등록번호		
1		미국	-	-	-	조남수	2022.08.02	11403284	100	-
2		미국	-	-	-	이창현	2022.11.08	11494403	100	-
3		미국	허환조	2022.05.02	17/734273	-	-	-	100	-
4		미국	박기성	2022.06.06	17/832766	-	-	-	100	-
5		미국	허환조	2022.09.27	17/953515	-	-	-	100	-
6		한국	-	-	-	허환조	2022.03.15	2376254	100	-
7		한국	-	-	-	이창현	2022.10.04	2452250	100	-
8		한국	윤대근	2022.03.10	2022-0030198	-	-	-	100	-
9		한국	허환조	2022.06.28	2022-0079132	-	-	-	100	-
10		한국	김주영	2022.2.23	2022-0023538	-	-	-	100	-

o 지식재산권 활용 유형

※ 해당사항없음

□ 저작권(소프트웨어, 서적 등)

※ 해당사항없음

□ 신기술 지정

※ 해당사항없음

□ 기술 및 제품 인증

※ 해당사항없음

□ 표준화

ㅇ 국내표준

※ 해당사항없음

ㅇ 국제표준

※ 해당사항없음

[경제적 성과]

□ 시제품 제작

※ 해당사항없음

□ 기술 실시(이전)

※ 해당사항없음

□ 사업화 투자실적

※ 해당사항없음

□ 사업화 현황

※ 해당사항없음

□ 매출실적(누적)

※ 해당사항없음

□ 사업화 계획 및 무역 수지 개선 효과

※ 해당사항없음

□ 고용 창출

※ 해당사항없음

□ 고용 효과

※ 해당사항없음

□ 비용 절감(누적)

※ 해당사항없음

□ 경제적 파급 효과

※ 해당사항없음

□ 산업 지원(기술지도)

※ 해당사항없음

□ 기술 무역

※ 해당사항없음

[사회적 성과]

□ 법령 반영

※ 해당사항없음

□ 정책활용 내용

※ 해당사항없음

□ 설계 기준/설명서(시방서)/지침/안내서에 반영

※ 해당사항없음

□ **전문 연구 인력 양성**

※ 해당사항없음

□ **산업 기술 인력 양성**

※ 해당사항없음

□ **다른 국가연구개발사업에의 활용**

※ 해당사항없음

□ **국제화 협력성과**

※ 해당사항없음

□ **홍보 실적**

※ 해당사항없음

□ **포상 및 수상 실적**

※ 해당사항없음

[인프라 성과]

□ **연구시설・장비**

※ 해당사항없음

[그 밖의 성과]

※ 해당사항없음

나. 계획하지 않은 성과 및 관련 분야 기여사항

ㅇ이더리움 블록체인 소프트웨어 취약점 1건 공식 보고 및 패치 적용 완료

- 본 과제 연구를 통해 발견한 블록체인 네트워크 파티셔닝 문제점을 실제 이더리움 블록체인 네트워크를 대상으로 실험, 공격 가능성 확인
- 이더리움 재단(Ethereum Foundation)에 문제점 공식 보고를 통해 채택 되었으며, 제공한 해결방안이 Go Ethereum v1.11.0 버전에 적용됨

2. 목표달성도

가. 과제 수행 목표달성도 (기술개발 성과지표)

<table>
<tr><td colspan="5">전략목표5 국가지능화 융합 기술 개발로 혁신성장 동인 마련</td></tr>
<tr><td>계획 및
목표달성도</td><td>계획 (2단계 2022-2024)</td><td colspan="2">목표달성도 (2단계 2022-2024)</td><td></td></tr>
<tr><td>전략목표
로드맵</td><td>공공·국민생활 문제해결형 국가지능화 융합 핵심기술 개발</td><td colspan="2">공공·국민생활 문제해결형 국가지능화 융합 핵심기술 개발</td><td></td></tr>
<tr><td>성과목표
5-5</td><td>지능형 사이버보안 및 신뢰인프라 융합 기술</td><td colspan="2">지능형 사이버보안 및 신뢰인프라 융합 기술</td><td></td></tr>
<tr><td>달성목표</td><td>o 트러스트 데이터 거래 실증 서비스 PoC
o TTP-free 부인방지/접근권한 세분화 기술 연구
o 트러스트 데이터 거래 책임성 추적 기술 개발
o 트러스트 데이터 커넥톰 통합 시스템 구축 및 PoC</td><td colspan="2">o 트러스트 데이터 거래 실증 서비스 PoC 발굴
o TTP-free 부인방지/접근권한 세분화 기술 연구
o 트러스트 데이터 거래 책임성 추적 기술 개발
o 트러스트 데이터 커넥톰 통합 시스템 개발을 위한 핵심 모듈 개발</td><td>달성도
60%
('23년 달성예정)</td></tr>
<tr><td rowspan="3">위 목표의
달성 지표 및
평가 기준</td><td>연구개발 달성목표</td><td>연구개발 달성실적</td><td>달성도</td><td></td></tr>
<tr><td>① 키교환 기술에 대한 수학적 안전성 모델 제시</td><td>• 키교환 기술에 대한 안전성 모델 제시 및 이를 통한 안전성 검증 결과 제출
*'21년 SCIE 논문 게재를 통한 검증 완료, '22.12 개선안 논문 제출 (IEEE S&P)</td><td>100%</td><td></td></tr>
<tr><td>② TTP-free 트러스트 데이터 커넥톰 응용 서비스 제공</td><td>•트러스트 데이터 커넥톰 응용 서비스 발굴</td><td>30%
('23년 달성예정)</td><td></td></tr>
</table>

나. 공통지표

구분	기본지표				심화지표			
	지표명	총사업연도	'21년도	'22년도 (달성도)	지표명	총사업연도	'21년도	'22년도 (달성도)
과학적 성과	SCI(E) 논문	10	2	3 / (10)	표준화된 IF 상위 20% SCI 논문(건)	2	-	- / (3)
기술적 성과	국내특허(출원)	8	2	2 / (3)	특허활용률 (기술이전건수/ 특허등록보유건수)	-	-	-
	국내특허(등록)	3	-	- / (2)				
	국제특허(출원)	6	2	1 / (3)	국제표준승인표준 기고서(건)	-	-	-
	국제특허(등록)	2	-	- / (2)	3극 특허(건)	1	-	-
경제적 성과	기술이전(건)	-	-	-	연구비 대비 기술료 수입(%)	-	-	-
	기술료(억원)	-	-	-				

나. 자율지표

※ 해당사항없음

3. 목표 미달 시 원인분석

※ 해당사항없음

4 관련 분야에 대한 기여

가. 과학적·기술적·경제적·사회적 파급효과

(1) 과학적 성과

- 신경망 학습 기반 키교환 기술에 대한 안전성 모델 정립 및 설계된 키교환 기술에 대한 안전성 검증 수행 (국제 우수 학회 IEEE Security and Privacy 논문 1건 제출중)
- 분산환경에서 안전한 데이터 수집 및 거래를 위한 키 관리 기술 연구
  (IEEE IoT 저널, IF10.2 포함 SCIE 논문 3건 게재)
- 새로운 블록체인 파티셔닝 공격 및 해결 방안 제시
  (이더리움 소프트웨어 취약점 1건 공식 보고 완료, 최고 수준 학회 NDSS '23 논문 최종 revision)
- Searchable Encryption 기반 암호화 데이터 검색 기술로 분산 데이터 활용도 향상
  (IEEE TNSE 저널 게재, IF5.33)
- 총 SCIE 논문 10편 게재(SCIE 상위 20% 3편 포함), 국내/국제학술대회 3편 발표

(2) 기술적 성과

- 차량데이터 서비스 모델 설계 및 데이터 수집/관리 모듈 개발
- 신경망 학습기반 키교환 기술 활용을 위한 키교환 시뮬레이터 구현
- 탈중앙화 데이터 거래 환경에서 노출을 최소화한 데이터 유효성 검증 방법 설계
  (3극 특허 출원을 통한 IPR 확보 진행)
- TTP-free한 환경에서 안전하게 사용자주도 데이터 거래가 가능한 플랫폼 구현
- 국제/국내 특허 3건/3건 출원 및 국제/국내 특허 1건/2건 등록을 통한 핵심 IPR확보

(3) 경제적 성과

- 혁신적인 패러다임의 데이터 교환 플랫폼으로 기존 대규모 플랫폼 사업자에 집중화된 데이터 비즈니스 및 데이터를 이용한 신규 비즈니스 시장 형성 기여
- 트러스트 데이터 커넥톰 환경의 다양한 개인데이터 활용 서비스 발굴 및 PoC 구현을 통해 확보한 기술을 바탕으로 다양한 개인데이터 기반 산업에 활용 가능

(4) 사회적 성과

- 개인 데이터 주권 및 프라이버시 보장을 통해 기존 중앙 집중적인 데이터 수집/가공/활용 기반의 데이터 산업으로 제공하기 어려웠던 개인 데이터 관련 新서비스 분야 창출에 기여
- 공공 데이터 인프라, 산업 인터넷, 스마트 시티 등 데이터 인프라의 신뢰 제고를 위한 기반 신뢰 인프라 플랫폼으로 활용

나. 후속 과제에 도움을 줄 수 있는 연구 결과

- 본 과제를 통해 확보된 신경망 학습 기반 암호화 기술 설계 노하우 및 신경망 학습 고도화 기술을 바탕으로, 향후 양자 컴퓨터 등 새로운 위협에 대응 가능한 新암호기술 설계에 활용 가능

- 본 연구과제를 통해 확보된 TTP-free 환경의 자율적이고 안전한 데이터 거래 플랫폼 핵심 원천기술을 향후 분산환경에서의 데이터 거래 생태계 구축 실증과제의 기반기술로 활용, 또한 향후 국가 정책으로 추진되는 개인데이터의 안전한 활용을 위한 마이데이터 기반 기술 및 융합 프라이버시 보호 분야 R&D에 활용 가능 (※개인정보보호위원회 R&D 로드맵 '21.11.)

5 성과관리 및 활용계획

가. 성과관리 현황

<table>
<tr><th>구분</th><th colspan="4">주요내용</th></tr>
<tr><td rowspan="3">데이터
생산 및 관리</td><td colspan="4">o 데이터 간략 설명
전 세계 8개 지점에 분포된 퍼블릭 블록체인 풀노드(비트코인, 이더리움, 이오스)에 수신되는 블록 및 트랜잭션의 로그 기록</td></tr>
<tr><td>데이터 유형</td><td>텍스트</td><td>연구데이터
파일 포맷</td><td>Text (TXT)</td></tr>
<tr><td colspan="4">o 데이터 수집/생산 방법
블록 및 트랜잭션 로그 수집을 위해 수정된 비트코인 코어 클라이언트, 이더리움 클라이언트, 이오스 클라이언트로부터 출력된 로그 파일을 일별로 클라우드 노드의 VM에 저장. 클라우드 VM의 하드디스크에 저장된 일별 로그 파일을 주기적으로 연구소 내의 저장 공간으로 이동</td></tr>
<tr><td>데이터
저장 및 보존</td><td colspan="4">o 데이터 보존 및 백업 방안
연구데이터는 연구소 내에 설치된 NAS(Network Assisted Storage)에 저장되며, NAS는 8개의 4TB HDD가 RAID 6로 구성되어 총 21.8TB의 용량이며, 최대 2개의 HDD가 동시에 고장나는 경우에도 Fault tolerance를 제공할 수 있도록 설정되어 있어 별도의 백업은 필요하지 않음</td></tr>
<tr><td rowspan="3">데이터
공동활용</td><td colspan="4">o 공동활용 가능한 연구데이터 종류
①SW ②소스코드 ③수치 ❹텍스트 ⑤이미지 ⑥음향 ⑦동영상 ⑧기타( )</td></tr>
<tr><td colspan="4">o 공개 범위
①원외공개 ②원내공개 ③제목만 공개(원내, 원외) ❹비공개(2)
* 비공개 사유 (비공개의 경우 사유 선택)
1. 법령, 국가 또는 정부로부터 연구데이터의 비공개를 요청 받은 경우
2. 연구목적상 장기간의 데이터 획득이 요구되는 연구과제
3. 기관 원장으로부터 일정기간동안 데이터의 비공개를 승인받은 경우
4. 연구책임자의 데이터 비공개 요청

o 공개의 경우, 공유 시점
해당사항없음

o 공개의 경우, 공개·공유 방법
해당사항없음</td></tr>
<tr><td colspan="4">o 연구데이터의 공개·공유 제한 사항
해당사항없음</td></tr>
</table>

나. 성과활용 계획

(1) 기술적

- 과제를 통해 확보한 핵심 기술은 21세기의 오일로 불리우는 데이터를 기반으로 하는 미래 초연결 지능사회 플랫폼인 오픈 디지털 커넥톰을 실현하고, 초연결 지능사회의 다양한 서비스 분야에 활용하여 관련 파생 기술 및 서비스 창출에 기여할 수 있음

- TTP에 모든 시스템의 안전성을 의존하는 현재의 시큐리티 기반 기술의 한계를 극복하여 미래의 예측하기 어려운 보안위협으로부터 데이터 시큐리티를 보장하는 TTP-free 시큐리티 보장을 위한 기반 기술로 활용

(2) 사회문제해결

- 개인 데이터 주권 및 프라이버시 보장을 통해 기존 중앙 집중적인 데이터 수집/가공/활용 기반의 데이터 산업으로 제공하기 어려웠던 개인 프라이버시 데이터 관련 서비스 분야로 확산

(3) 확보된 기술의 사업화 전략

- 과제 결과로 도출된 응용 서비스에 대한 실증 서비스 검증을 통한 상용화 가능성을 확인하여, 국가 공공 서비스에 先적용 후 민간 서비스로 확장하여 신 서비스 산업 창출 기반 조성

6 향후 과제 수행계획

가. 과제 목표 및 내용

□ 연구개발목표

- TTP-free 트러스트 데이터 커넥톰 통합 검증 및 고도화

□ 연구개발내용

❍ 트러스트 데이터 커넥톰 구조 및 서비스 연구

- 트러스트 데이터 커넥톰 서비스 개발 및 시스템 구축

❍ 통합 PoC

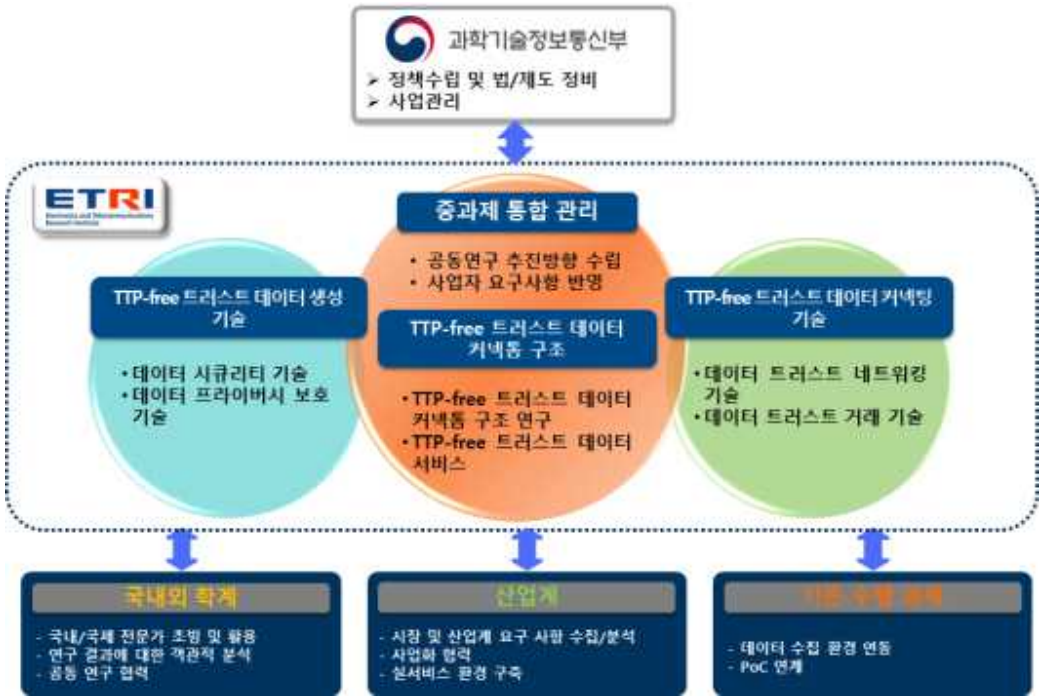
- 트러스트 데이터 커넥톰 통합 검증
  - 트러스트 데이터 커넥톰 통합 시스템 구축
  - 서비스 실증 및 기능 개선
- TTP-free 트러스트 데이터 생성 기술 고도화
  - TTP-free 환경의 인증된 키교환 및 데이터 암복호화 모듈 개발
  - 프라이버시 보장 트러스트 데이터 생성 모듈 개발
- 트러스트 데이터 블록체인 네트워킹 고도화 기술 개발
  - 블록체인 네트워킹을 위한 집약가능(aggregatable) 초경량 트랜잭션/블록 구조 설계
  - 블록체인 네트워킹을 위한 집약가능(aggregatable) 초경량 트랜잭션/블록 구조 개발
- TTP-free 트러스트 네트워킹 기술 고도화

나. 국내외 관련 분야 환경변화

❍ 개인정보보호에 대한 관심이 높아지면서 개인정보 수집/관리/활용 등에 대한 국가적 가이드라인 마련이 활발해지고 있음

- 개인데이터 활용에 대한 법적/제도적 장치가 마련되는 시점으로 새롭게 변화하는 데이터 활용 환경에 맞는 서비스 개발이 요구됨
- 개인데이터 주권에 대한 사회적 관심도가 높아지면서 확보된 기술에 대한 적극적인 활용 방안 확보가 필요

다. 과제수행 추진전략



❍ 한국전자통신연구원 주도로 기존 TTP 기반 환경에 의존하지 않고 데이터 주권과 안전한 교환을 보장하는 트러스트 데이터 커넥톰 원천기술로서 'TTP-free 트러스트 데이터 생성 기반 기술' 및 'TTP-free 데이터 커넥팅 기술' 연구 추진

- 오픈소스 프로젝트 활용 및 공개 정책을 통해 개발 부담 최소화 및 핵심 원천 기술 확보 집중
- 위탁연구기관을 통해 학습 기반 데이터 시큐리티 보호 기술에 대한 안전성 모델 검증 및 고도화 진행
- TTP-free 분산환경에서의 데이터 접근제어 기술에 대한 모델 연구를 국내 위탁연구기관과 협업을 통해 진행

❍ 국내외 관련 산업 분야의 동향 및 컴퓨팅 환경 변화에 대한 적극적인 정보 수집 추진

❍ 국내 학계와의 공동연구를 통해 최신 연구 동향 교환 및 연구 개발 방향에 대한 의견 수렴

❍ 국내 표준화 전문가와의 연계를 통해 최신 표준화 동향 분석 및 연구 개발 결과에 대한 표준화 논의 진행

라. 과제수행 일정 및 기대 성과

□ 추진일정

<table>
<tr><th>연도
연구내용</th><th colspan="2">1차년도(2020)</th><th colspan="2">2차년도(2021)</th><th colspan="2">3차년도(2022)</th><th colspan="2">4차년도(2023)</th></tr>
<tr><th></th><th>상반기</th><th>하반기</th><th>상반기</th><th>하반기</th><th>상반기</th><th>하반기</th><th>상반기</th><th>하반기</th></tr>
<tr><td rowspan="4">TTP-free
트러스트 데이터
커넥톰 구조 및
서비스 연구</td><td colspan="2">데이터 커넥톰
요구사항 보완</td><td colspan="2">데이터 커넥톰 서비스
요구사항 및 기능
규격 정의</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">데이터 커넥톰 구조
설계 보완</td><td></td><td>데이터
커넥톰
서비스
설계</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">데이터 커넥톰 서비스 개발 및
PoC 시스템 구축</td><td colspan="2"></td><td colspan="2">데이터 커넥톰 서비스
성능 개선</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">TTP-free 트러스트
데이터 커넥톰 통합
PoC 검증 및
데이터 커넥톰 서비스
실증</td></tr>
<tr><td>TTP-free
트러스트 데이터
생성 기술 연구</td><td>신경망
학습을
통한
인증된
키교환
기술 설계</td><td>키교환
기술 검증
시스템
구축</td><td colspan="2">학습 기반 데이터
시큐리티 안전성 모델
정립 및 암복호화
기술 연구</td><td colspan="2">키/알고리즘 정보
공유 없는 환경에서의
안전성 모델 정립 및
데이터 암복호화 기술
설계</td><td colspan="2" rowspan="3">통합 PoC 및
기능/성능 고도화</td></tr>
<tr><td colspan="2">프라이버시 보장
트러스트 데이터 생성
기술 설계</td><td colspan="2">프라이버시 강화
트러스트 데이터
부인방지 기술 설계</td><td>제어가능
프라이버시
제공 및
접근권한
세분화
관리 기술
설계</td><td>프라이버시
보장
트러스트
데이터
생성 모듈
개발</td></tr>
<tr><td>TTP-free
트러스트 데이터
커넥팅 기술 연구</td><td colspan="2">트러스트 데이터
블록체인 네트워킹
구조 연구</td><td colspan="2">블록체인
트랜잭션/블록 캐스팅
모델 설계</td><td colspan="2">블록체인
네트워킹(트랜잭션캐
스팅&블록캐스팅)
라이브러리 개발</td></tr>
<tr><td colspan="2">트러스트 데이터 거래
프로토콜 개발</td><td colspan="2">거래 안전성 보장
데이터 접근 제어
기술</td><td colspan="2">트러스트 데이터 책임
추적성 기술 개발</td></tr>
</table>

□ 기대성과

❍ 과제를 통해 확보한 핵심 기술은 21세기의 오일로 불리우는 데이터를 기반으로 하는 미래 초연결 지능사회 플랫폼인 오픈 디지털 커넥톰을 실현하고, 초연결 지능사회의 다양한 서비스 분야에 활용하여 관련 파생 기술 및 서비스 창출에 기여할 수 있음

❍ 과제 결과로 도출된 응용 서비스에 대한 실증 서비스 검증을 통한 상용화 가능성을 확인하여, 국가 공공 서비스에 先적용 후 민간 서비스로 확장하여 신 서비스 산업 창출 기반 조성

❍ TTP에 모든 시스템의 안전성을 의존하는 현재의 시큐리티 기반 기술의 한계를 극복하여 미래의 예측하기 어려운 보안위협으로부터 데이터 시큐리티를 보장하는

TTP-free 시큐리티 보장 기반 기술로 활용

❍ 개인 데이터 주권 및 프라이버시 보장을 통해 기존 중앙 집중적인 데이터 수집/가공/활용 기반의 데이터 산업으로 제공하기 어려웠던 개인 프라이버시 데이터 관련 서비스 분야로 확산

마. 다음 단계 연구개발비 사용계획

(단위 : 천원)

구 분	1차년도 (2020년)	2차년도 (2021년)	3차년도 (2022년)	4차년도 (2023년)	합계
	금액	금액	금액	금액	
1. 인건비(Ⅰ, 인건비 배부액)	**1,585,000**	**1,599,000**	**1,634,000**	**1,634,000**	**6,452,000**
o 내부인건비(정규직)	1,579,000	1,596,000	1,634,000	1,634,000	6,443,000
o 연구지원인력인건비(정규직)	6,000	3,000	0	0	9,000
2. 주요사업비(직접비)	**2,849,000**	**2,964,000**	**2,883,000**	**2,883,000**	**11,579,000**
o 직접비(ETRI사용분)	2,849,000	2,964,000	2,883,000	2,883,000	11,579,000
o 국제공동연구개발비 (출연금 배부액)	0	0	0	0	0
o 연구개발부담비 (국내공동연구비_출연금배부액)	0	0	0	0	0
3. 간접비	**430,000**	**429,000**	**390,000**	**390,000**	**1,639,000**
4. 민간부담금	**0**	**0**	**0**	**0**	**0**
o 민간부담현금	0	0	0	0	0
o 민간부담현물	0	0	0	0	0
합 계	**4,864,000**	**4,992,000**	**4,907,000**	**4,907,000**	**19,670,000**

바. 사업화 추진 계획

※ 해당사항없음

사. 연구개발 성과의 활용방안 및 기대효과

□ 연구성과 활용 및 확산체계

❍ 정보의 생성·전달·유통 전 영역의 고신뢰화에 따른 패러다임 변화에 대응하기 위한 디지털 데이터 커넥톰 기술 선제 개발을 통한 미래형 데이터 산업 선도 가능

❍ 멀티 도메인간 데이터 유통이 필수적인 초연결 통신 환경에 대한 핵심원천기술 기술 경쟁력 확보

❍ 완전 분산화를 통한 초신뢰 데이터 검증 패러다임 창출 및 공공 데이터 인프라, 산업 인터넷, 스마트 시티 등 데이터 인프라의 신뢰 제고를 위한 기반 신뢰 인프라 플랫폼으로 활용

❍ 데이터의 생성 주체인 개인에게 소유권을 되돌리는 데이터 프라이버시 및 주권 보장 기술은 초연결 데이터 중심 사회에서 데이터를 활용하는 모든 산업에 활용

❍ TTP-free 데이터 시큐리티 기술은 TTP 비의존적인 정보보호 기술로 미래 데이터 중심 산업의 뿌리 기술로 활용

□ 세부실행 계획

❍ 데이터 거래/교환 미래 환경 분석을 통해 정의된 서비스 시나리오에 대한 산업계 검토 의견 수렴을 통한 고도화, 트러스트 데이터 커넥톰 요구사항 및 구조에 대한 최신 기술 발전 동향에 대한 추가 연구를 통한 트러스트 데이터 커넥톰 구조 개선 추진

❍ 도출된 트러스트 데이터 커넥톰의 구조를 기반으로 TTP-free 데이터 생성 기술 및 트러스트 데이터 커넥팅 기술의 세부 요구사항 및 요소 기술을 도출

❍ 트러스트 데이터 생성 기술 분야는 이전 연구에서 확보된 데이터 생성 기반 기술 고도화를 통한 실증 서비스에 적용

❍ 트러스트 데이터 커넥팅 기술 분야는 이전 연구에서 확보된 트러스트 데이터 커넥톰 구조 및 자율 데이터 거래가 가능한 트러스트 데이터 네트워킹 및 거래 제공을 위한 핵심 원천 기술을 바탕으로 서비스 개발 및 실증을 통한 기술 검증 및 고도화 개발

❍ 본 세부과제 수행을 통해 확보된 TDC 원천기술을 '국가지능화 융합기술 개발로 혁신성장 동인 마련' 대과제 내의 지역 산업기반 ICT 융합기술 고도화 지원사업에 포함된 스마트 의료·시티·이동체·농업·에너지·광융합 등의 다양한 데이터 서비스 구축에 활용

□ 성과활용 및 기대효과

❍ 과제를 통해 확보한 핵심 기술은 21세기의 오일로 불리우는 데이터를 기반으로 하는 미래 초연결 지능사회 플랫폼인 오픈 디지털 커넥톰을 실현하고, 초연결 지능사회의 다양한 서비스 분야에 활용하여 관련 파생 기술 및 서비스 창출에 기여할 수 있음

❍ 과제 결과로 도출된 응용 서비스에 대한 실증 서비스 검증을 통한 상용화 가능성을 확인하여, 국가 공공 서비스에 先적용 후 민간 서비스로 확장하여 신 서비스 산업 창출 기반 조성

❍ TTP에 모든 시스템의 안전성을 의존하는 현재의 시큐리티 기반 기술의 한계를 극복하여 미래의 예측하기 어려운 보안위협으로부터 데이터 시큐리티를 보장하는 TTP-free 시큐리티 보장 기반 기술로 활용

❍ 개인 데이터 주권 및 프라이버시 보장을 통해 기존 중앙 집중적인 데이터 수집/가공/활용 기반의 데이터 산업으로 제공하기 어려웠던 개인 프라이버시 데이터 관련 서비스 분야로 확산

7 연구개발비 사용실적

연구개발비 사용실적 현황

과제책임자	성명	김 익 균	직위	본부장
과제수행기간	전체	2020. 1. 1 - 2023. 12. 31(4년 0개월)		
	해당 단계	2022. 1. 1 - 2023. 12. 31(2년 0개월)		
	당해 연도	2022. 1. 1 - 2022. 12. 31(1년 0개월)		

연구개발기관의 연구개발비 (단위: 천원)		정부지원 연구개발비	기관부담 연구개발비		그 외 기관 등의 지원금				합계		
					지방자치단체		기타( )				
		현금	현금	현물	현금	현물	현금	현물	현금	현물	합계
총계		9,814,000	0	0	0	0	0	0	9,814,000	0	9,814,000
2단계	1년차	4,907,000	0	0	0	0	0	0	4,907,000	0	4,907,000
	2년차	4,907,000	0	0	0	0	0	0	4,907,000	0	4,907,000
당해연도		4,907,000	0	0	0	0	0	0	4,907,000	0	4,907,000

8 중요 연구변경 사항

※ 해당사항없음

[뒷면지]

본 문서에서 음영 처리된 부분은 ( ) 정보공개법 제9조의 비공개대상정보와 저작권법 및 그 밖의 다른 법령에서 보호하고 있는 제3자의 권리가 포함된 저작물로 공개대상에서 제외되었습니다.

주 의

1. 이 보고서는 한국전자통신연구원의 기본사업으로 수행한 개발과제 연차보고서이다.

2. 이 연구개발내용을 대외적으로 발표할 때에는 반드시 한국전자통신연구원에서 시행한 기본사업 결과임을 밝혀야 한다.