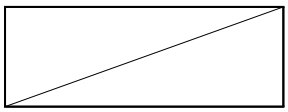
2015년 12월

15ZS1500



암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천기술 개발

Development of Storage and Search Technologies over Encrypted Database

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

세부과제 연차실적 보고서

연차실적 보고서

과제유형	1. 기초미래선도형 (O) 2. 공공인프라형 ( ) 3. 산업화형 ( )				
대과제명	SW·콘텐츠 기초·미래선도 기술 개발				
세부과제명	암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천 기술 개발				
세부과제 책임자	소속 및 부서	사이버보안기반연구부 암호기술연구실	직위 (직급)	책임연구원	
	성명	장구영			
총연구기간	2015년 01월 01일 부터 2017년 12월 31일 까지 (36개월)				
당해연도 연구기간	2015년 01월 01일 부터 2015년 12월 31일 까지 (12개월) (1차년도)				
총연구비	정부출연금	2,700,000 천원	당해년연구비	정부출연금	900,000 천원
	민간부담금	93,600 천원		민간부담금	0 천원
	계	2,793,600 천원		계	931,200 천원
참여인력(M/Y)	총 연 구 기 간	50명 (19.9M/Y)			
	당해연도 연구기간	18명 (6.1M/Y)			

참여기관	기관명	연구책임자	기관명	연구책임자
참여연구기관	공주대학교	홍도원		
위탁연구기관	부경대학교	이경현		
	명지대학교	서재홍		

키워드 (6~10개)	개인 정보 유출, 암호데이터 저장, 암호데이터 열람, 암호데이터 검색, 암호데이터 중복 처리, 암호데이터 소유권 검증

정부출연금사업 연차평가 보고서를 제출합니다.

2015년 12월 02일

세부과제책임자 : 장 구 영 (인)
직 할 부 서 장 : 한 동 원 (인)

한국전자통신연구원장 귀하

목 차

제 1 장 서 론

제1절 필요성 및 중요성

1. 연구개발과제의 필요성

○ 국내외적으로 빈번히 발생하고 있는 개인정보 유출 사례의 증가 및 피해 확산으로 인해 사용자 주요 데이터의 프라이버시 침해에 대한 우려가 커지고 있음

- 국내외 개인정보 유출 규모가 점차 대형화하는 추세에 있으며, 이에 따른 피해 확산이 가속화 되고 있음
- 2014년 1월 카드사에서 유출된 개인정보는 KB카드 5,300만 건, 롯데카드 2,600만 건, NH카드 2,500만 건으로 총 1억 4백만 건이며, 유출정보는 성명, 주민번호, 주소, 카드번호, 유효기간, 결재정보, 신용한도 등 거의 모든 개인정보를 포함하고 있음
-

< 국내 주요 정보 유출 사건 >

○ 개인정보 유출 방지를 위해 암호화 대상이 점차 증가하고 있으며 궁극적으로는 주요 데이터베이스에 대한 전체 암호화가 진행될 것으로 예상되나, 이에 대한 대비는 미흡한 실정임

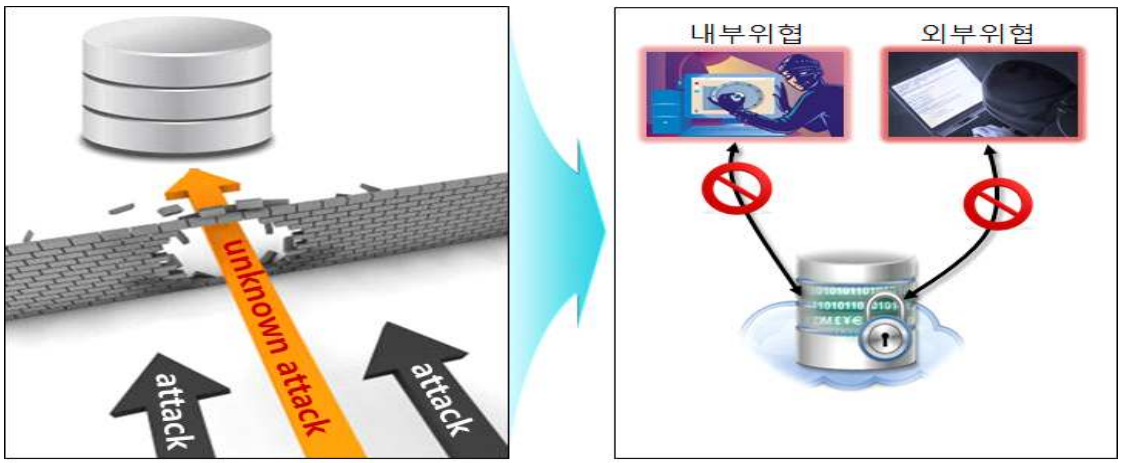
- 개인정보보호법(2014.8.7 시행)은 개인정보 수집 최소화 및 관리에 대한 법적 책임을 강화하고 있으며, 주민등록번호 등과 같은 고유 식별 정보에 대한 암호화를 명시하는 내용을 포함하는 등 민감 정보 암호화에 대한 기술적 필요성을 제기함

- 카드사 정보 유출 사건 이후 암호화 대상이 고유 식별 번호 중심에서 성명, 계좌정보, 신용카드번호, 주소, e-mail, 전화번호 등을 포함한 13종으로 확대되고 있음
- 국내외 데이터베이스 암호화 제품은 단순 암복호화 기술 위주로 적용된 상태로 데이터베이스 암호화에 따른 기능적/성능적 제약이 암호화 사용에 걸림돌로 작용하고 있음

O 이러한 상황을 극복하기 위해 데이터 기밀성을 유지하면서, 암호화된 데이터에 대한 활용을 극대화할 수 있는 암호 원천 기술 개발이 시급한 실정임
- 이에 암호화된 데이터베이스에서의 데이터 저장, 열람 및 검색과 같은 평문 데이터베이스의 필수 요구 조건을 제공할 수 있는 암호 원천 기술 개발이 시급함
- 또한 Standford, MIT, IBM, Google 등에서 암호데이터 활용 관련 연구가 진행 중에 있어, 국내외 시장 선점을 위해 암호화된 데이터베이스 환경에 적용할 수 있는 암호 원천 기술 연구와 관련 핵심 IPR 확보가 필요함

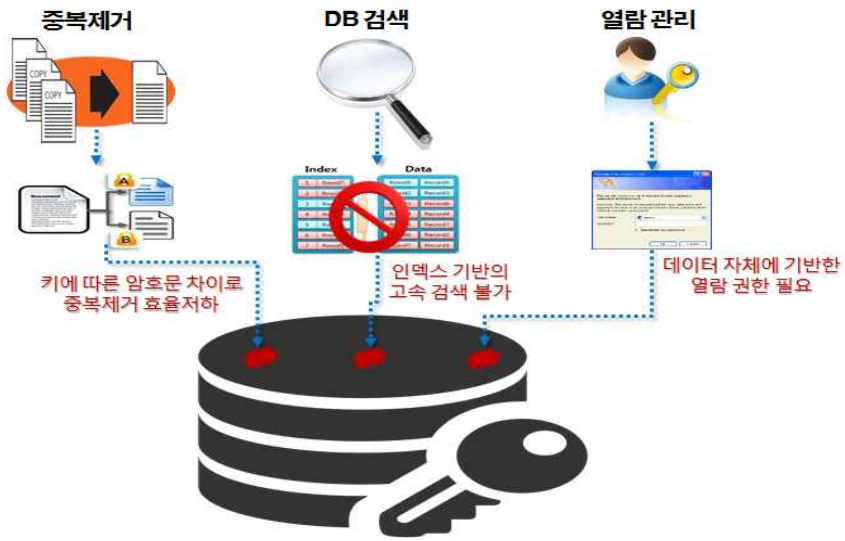
2. 연구개발과제의 중요성

O 기존의 방어 체계를 우회하는 지능적인 공격의 발달로 공격의 목표가 되는 데이터를 원천적으로 보호하기 위한 암호 기술에 대한 중요성이 증가하고 있음
- 개인정보의 저장·유통이 대량화, 광역화, 네트워크화 되면서 저장·유통되는 개인정보가 더욱 많은 위협에 쉽게 노출되고 있음
- 알려진 공격 유형에 단기적으로 대응하는 현존 방어 체계로는 새로운 공격 기술에 근원적으로 취약함
- 데이터 자체를 근본적으로 보호할 수 있는 데이터 중심적 보안으로 패러다임이 변화하고 있으며, 이를 해결할 수 있는 암호 원천 기술 개발이 중요해지고 있음
- 클라우드 컴퓨팅 보안으로 가장 잘 알려져 있는 조직인 CSA(Cloud Security Alliance)가 암호데이터 검색, 암호화 기반 접근 제어, 암호데이터 연산, 스토리지에 저장된 데이터에 대한 무결성 검증 등 빅데이터 환경에 필요한 암호 기술에 대한 10대 챌린지를 발표하는 등, 암호데이터 활용을 위한 원천 기술이 많은 주목을 받고 있음



○ 하지만, 데이터베이스 암호화에 따른 기능적/성능적 제약이 암호화 사용에 걸림돌로 작용하고 있음

- 현재의 단순 데이터베이스 암호화 기술은 암호데이터 활용을 위해 데이터 전체에 대한 복호화가 요구되어, 성능 저하 및 서버 관리자에 의한 데이터 프라이버시 침해 방지 어려움 등의 문제가 존재
-



< DB 암호화에 따른 주요 문제점 >

○ 데이터 유출의 원천적인 방지를 위한 데이터베이스 암호화를 통한 기밀성 보장을 기반으로 암호화된 데이터 활용을 위한 암호 원천 기술 개발이 중요함

- 암호데이터 활용을 위한 암호 원천 기술은 데이터 유출 사고 방지를 위한 데이터베이스 보호 기술 뿐 만 아니라, 클라우드/빅데이터 서비스 등과 같은 다양한 신규 서비스에서 사용자 데이터 프라이버시 보호를 위한 핵심 기술로 확대 적용이 가능해 중요성이 더욱 커지고 있음
- 따라서, 데이터 유출의 원천적인 방지를 위해 암호화된 데이터베이스에서 데이터 저장, 열람 및 검색과 같은 평문 데이터베이스의 기능적/성능적 요구 사항을 만족할 수 있는 암호 원천 기술 개발이 중요함

제2절 국내 · 외 기술 현황 및 접근방법

1. 국내 · 외 기술 현황

2. 접근방법

O 데이터 유출의 원천적인 방지를 위한 암호화된 데이터베이스 환경에서 데이터를 자유롭게 활용하기 위한 핵심 요소인 저장, 열람 및 검색의 3가지 기술 분야로 나누어 접근함

O 3가지 핵심 분야에 대한 핵심 기술 및 접근 방법은 다음과 같음

핵심 요소		접근 방법
암호데이터 저장/열람 기술	다양한 데이터 활용 환경에 대한 암호데이터 중복 처리 기술 개발	- Message-locked encryption 최신 기술 및 요구 사항 분석을 통한 암호데이터 중복 처리 기술 안전성 모델 연구 - 메시지 기반 암호화 핵심 설계 논리 개발 - 개발된 핵심 설계 논리를 바탕으로 파일 단위 암호데이터 중복 처리 기술 설계 - 다양한 데이터 활용 환경의 목적 달성을 위한 블록 단위/다중 사용자 처리 등의 기술 고도화를 통한 최적화 및 세분화 - 암호데이터 중복 처리 기술 성능 분석 및 개선 방안 연구
	데이터 기반의 소유권 검증 모델 연구 및 기술 개발	- 기존 데이터 소유권 관리 기술 및 응용 환경의 요구사항 분석을 통한 새로운 데이터 기반 소유권 검증 모델 설계 - 이를 바탕으로 데이터 기반의 암호데이터 소유권 검증 기술 설계 및 안전성 증명 - 프라이버시 강화를 위한 데이터 소유권 검증 기술 고도화
암호데이터 검색 기술	동적 환경에서의 암호데이터 검색 기술 개발 및 부가기능 제공	- 기존 암호데이터 검색 기술 및 현실 데이터베이스 구조 분석을 통해 현실 적용 가능한 기술 개발의 토대 마련 - 수용 가능 안전성 모델 연구를 통한 암호데이터 검색 기술에의 적용 방안 모색 - 암호데이터 키워드 검색 알고리즘 설계 및 이를 바탕으로 동적 환경의 요구 사항을 반영한 동적 암호데이터 검색 기술 개발 - 부가 기능 제공을 위한 암호데이터 검색 기술 개발 및 수용 가능 안전성 적용을 통한 기술 최적화

O 데이터 위탁 서비스의 활성화와 더불어 데이터 중복 처리 기술의 필요성이 급증하고 있지만, 데이터 암호화에 따른 기술적 어려움으로 인해 암호데이터에 대한 중복 처리 기술은 최근에야 알고리즘 설계 및 안전성 개념이 정립되고 있는 분야로 향후 기술적 발전 방향을 결정지을 수 있는 원천 기술 선점이 중요한 기술 분야임. 또한 현재 데이터 단순 저장 환경에만 적용되고 있는 중복 처리 기술을 클라우드 서비스를 포함한 다양한 응용 환경에서의 데이터 활용 목적에 따라 세분화된 암호데이터 중복 처리 기술로 확대

O 암호데이터 소유권 검증 기술은 데이터 자체의 열람 권한을 할당하여 현존 데이터 소유권 관리 기술에서 해결하지 못하는 내부자에 의한 데이터 유출 방지 등의 다양한 문제 해결을 위한 새로운 기술 분야의 제시가 목표임. 또한, 현재 관련 연구가 진행되고 있지 않아 원천 IPR 및 기술 선점을 통해 기술 선도 가능

O 암호데이터 검색 기술은 데이터 활용을 위해 필수적으로 요구되는 기술로 비교적 많은 연구가 이루어졌으나, 이론적인 위협까지 모두 반영한 과도한 암호학적 안전성 위주의 기술 개발이 주를 이루고 있

음. 이에 과도한 암호학적 안전성에 대한 재분석과 함께 현실적인 안전성과 효율성 제공을 목표로 하는 수용 가능 안전성 모델을 적용하여 현실 데이터베이스에 적용 가능한 실용적인 검색 가능 암호화 기술 개발 기대

O 이러한 암호데이터 저장, 열람 및 검색 기술을 통해 데이터의 기밀성 보장을 위한 암호화를 기반으로 암호화된 데이터를 평문데이터처럼 자유롭게 활용할 수 있는 새로운 데이터 보안 패러다임인 CipherData 트렌드를 선도할 수 있는 혁신적인 개발 목표임

제3절 연구개발과제 수행결과 기대효과

1. 기술적 기대효과

O 기존 보안 기술이 지니는 한계를 극복한 새로운 데이터 중심 보안으로의 변화를 선도하기 위한 핵심 원천 기술로 활용

- 정부, 금융 기관 등 대량의 개인정보를 관리하는 기관의 데이터베이스에 대한 근본적인 데이터 유출 방지 시스템 구축을 위한 핵심 기술로 활용
- 데이터베이스 단순 암복호화 기능에서 벗어난 암호데이터 저장, 열람 및 검색과 같은 암호데이터 활용 기술에 대한 원천 IPR 확보를 통한 핵심 기술 선점 및 선도 가능

O 클라우드/빅데이터 서비스 확산에 요구되는 프라이버시 보호 관련 기술의 고도화 견인

- 암호데이터 저장, 열람 및 검색 기술은 클라우드/빅데이터 서비스 등과 같은 다양한 신규 서비스로의 확대 적용이 가능해 기술적 파급 효과가 매우 높음
- 개인 데이터의 안전성을 보장하면서, 이를 활용하여 새로운 부가가치를 창출할 수 있는 데이터 공유 및 거래 프레임워크 설정을 위한 핵심 기술로 활용 가능

2. 산업적 기대효과

3. 경제적 기대효과

4. 사회문제해결 기대효과

제 2 장 연구 개발 목표 및 내용

제1절 최종 목표 및 연차 목표

1. 최종목표

구 분	내 용
최종목표	o 데이터 유출의 원천적인 방지를 위해 데이터베이스가 암호화된 상태로 데이터의 저장, 열람 및 검색이 가능한 암호 원천 기술 개발 - 암호데이터 중복 처리 기술 개발 - 암호데이터 소유권 검증 기술 개발 - 암호데이터 검색 기술 개발 
세부목표	o 암호데이터 중복 처리 기술 개발 - 메시지 기반 암호화 핵심 프리미티브 설계 - 파일 단위 암호데이터 중복 처리 기술 개발 - 블록 단위/다중 사용자 기반 암호데이터 중복 처리 기술 개발 - 데이터 손실 공격 방지를 위한 암호데이터 중복 처리 기술 안전성 모델 정립 및 검증 - 암호데이터 중복 처리 성능 : 460ms 이하/1MB (1MB 파일 단위 암호데이터 중복 처리를 위한 평문데이터 중복 처리 대비 부가 시간) o 암호데이터 소유권 검증 기술 개발 - 데이터 기반의 소유권 부여, 유지 및 검증을 위한 관리 모델 설계 - 데이터 기반의 암호데이터 소유권 검증 기술 개발 o 암호데이터 검색 기술 개발 - 암호데이터 키워드 검색 기술 설계 - 데이터 추가·삭제 기능을 제공하는 동적 암호데이터 검색 기술 설계 - 부가 기능을 제공하는 암호데이터 검색 기술 개발 - 수용 가능 안전성 모델 정립 및 이를 이용한 암호데이터 검색 기술 최적화 - 검색 성능 : O(m), m : 검색 키워드를 포함하는 데이터 수

2. 연차별 연구개발 목표

구 분	목 표	내 용
1차년도 (2015)	암호데이터 저장 및 검색을 위한 핵심 프리미티브 설계	o 암호데이터 중복 처리를 위한 핵심 설계 논리 개발 - Message-locked encryption 최신 기술 및 요구 사항 분석 - 중복 처리에 따른 데이터 손실 공격 분석 및 암호데이터 중복 처리 기술 안전성 모델 연구 - 메시지 기반 암호화 핵심 설계 논리 개발 o 암호데이터 검색을 위한 핵심 알고리즘 설계 - 암호데이터 검색 최신 기술 및 요구 사항 분석 - 수용 가능 안전성 모델 연구 - 암호데이터 키워드 검색 알고리즘 설계
2차년도 (2016)	암호데이터 저장, 열람 및 검색 기술 설계 및 안전성 검증	o 암호데이터 중복 처리 기술 설계 - 파일 단위 암호데이터 중복 처리 기술 설계 - 암호데이터 중복 처리 안전성 검증 - 암호데이터 중복 처리 성능 최적화 o 암호데이터 소유권 검증 모델 연구 - 적용 환경 분석을 통한 요구 사항 정의 - 데이터 기반의 소유권 부여, 유지 및 검증을 위한 관리 모델 설계 o 동적 환경을 위한 암호데이터 검색 기술 개발 - 동적 암호데이터 검색 기술 요구 사항 분석 및 안전성 모델 정립 - 데이터 추가·삭제 기능을 제공하는 암호데이터 검색 기술 개발 및 안전성 검증
3차년도 (2017)	암호데이터 저장, 열람 및 검색 기술 개발	o 암호데이터 중복 처리 기술 개발 - 블록 단위 암호데이터 중복 처리 기술 개발 - 다중 사용자 기반 암호데이터 중복 처리 기술 개발 - 암호데이터 중복 처리 기술 성능 분석 및 개선 연구 o 암호데이터 소유권 검증 기술 개발 - 데이터 기반의 암호데이터 소유권 검증 기술 설계 - 암호데이터 소유권 검증 기술 안전성 검증 o 암호데이터 검색 실용화 기술 개발 - 부가 기능 제공 암호데이터 검색 기술 개발 - 실용화를 위한 수용 가능 안전성 적용 방안 연구 - 수용 가능 안전성 기반의 암호데이터 검색 기술 최적화

제2절 연구 범위 및 연구 수행 방법

1. 1차년도(2015년) 연구 개발 내용 및 범위

연구 목표	내용
암호데이터 저장 및 검색을 위한 핵심 프리미티브 설계	가) 연구 개발 목표 O 암호데이터 저장 및 검색을 위한 핵심 프리미티브 설계 - 암호데이터 중복 처리를 위한 핵심 설계 논리 개발 • 메시지 기반 암호화 프리미티브(IPR) - 암호데이터 키워드 검색 알고리즘(IPR) 나) 연구 개발 내용 O 암호데이터 중복 처리를 위한 핵심 설계 논리 개발 - 암호데이터 중복 처리 최신 기술 분석 - 메시지 기반 암호화 기본 프리미티브 및 설계 논리 분석 - 메시지 기반 암호화 요구 사항 분석 및 정의 - 중복 처리에 따른 데이터 손실 공격 모델 분석 - 암호데이터 중복 처리 안전성 모델 정립 - 메시지 기반 암호화 기술 핵심 설계 논리 개발 O 암호데이터 검색을 위한 핵심 알고리즘 설계 - 암호데이터 검색 최신 기술 동향 분석 - 공개키/대칭키 기반 암호데이터 검색 기술 핵심 프리미티브 분석 - 암호데이터 검색 기술에 대한 요구 사항 분석 및 정의 - 암호데이터 검색 실용화를 위한 수용 가능 안전성 모델 연구 - 암호데이터 키워드 검색 알고리즘 설계

2. 연구 수행 방법

O 한국전자통신연구원 주도로 암호데이터 저장, 검색을 위한 암호 기술 연구에 대한 방향 설정 및 원천 기술 개발

- 한국전자통신연구원은 메시지 기반 암호화 핵심 설계 논리 및 암호데이터 키워드 검색 알고리즘을 개발
- 공동연구기관(공주대학교)은 암호데이터 중복 처리 기반 기술 연구를 통해 한국전자통신연구원과 메시지 기반 암호화 핵심 설계 논리 개발을 위해 협력
- 암호데이터 중복 처리 및 검색에 대한 핵심 원천 기술 개발 및 우수 IPR의 전략적인 확보

O 연차별 기술 개발이 최종 연구 결과물에 유기적으로 결합될 수 있는 연구 개발 수행
- 암호데이터 중복 처리 기술
  • 데이터베이스나 클라우드 서비스 등에서 암호데이터 중복 처리 시에 발생하는 데이터 손실 공격 시나리오 분석 및 안전성 모델 정립
  • 안전성 모델을 기반으로 메시지 기반 암호화 핵심 설계 논리 개발
- 암호데이터 검색 기술
  • 이론적인 안전성 증명 기법과 수용 가능 안전성 비교 분석 및 검토
  • 안전성 증명 가능한 키워드 기반의 암호데이터 검색 핵심 프리미티브 설계

O 미국, 유럽, 일본 등 선진국의 연구 프로젝트, 각종 국제 학회 및 저널 논문, 국내외 특허 등을 면밀히 검토하여 차별화된 연구 개발 수행

O 위탁연구기관 및 전문가 초청 등을 적극 활용하여 학계의 우수한 기술 확보

O SCI(E) 저널이나 국제 유수 학회 논문 기고를 통해 결과물의 국제적 검증 수행

O 1실 1사 기업과의 긴밀한 협력을 통한 상용 데이터베이스 환경 요구 사항 반영

제3절 성과 목표

1. 성과목표의 개요

O 개요
- 데이터 유출의 원천적인 방지를 위해 데이터베이스 암호화를 통한 기밀성을 기반으로 데이터의 저장, 열람 및 검색이 가능한 암호 원천 기술 개발

O 설정 근거
- 개인 정보 유출의 증가 및 피해 확산으로 사용자 데이터를 원천적으로 보호할 수 있는 암호 기술에 대한 요구가 증가하고 있으나, 데이터베이스 암호화에 따른 기능적/성능적 제약이 암호화 사용에 걸림돌이 되고 있음
- 이러한 상황을 극복하기 위해 암호화된 데이터베이스에서 데이터 저장, 열람 및 검색과 같은 평문 데이터베이스의 필수 요구 사항을 만족할 수 있는 암호 원천 기술 개발 및 핵심 IPR 확보를 위해 성과목표를 설정하였음

2. 성과목표의 개요

O 기술 개발 성과 지표 (총 사업 연도/ '15년도)

성과지표 (주요성능 Spec)	단위	세계최고 수준	기술개발 목표치	목표치 산출근거	검증방법	비고 (달성년도)
① 암호데이터 중복 처리 기술	기능/ 성능	데이터 손실 공격 가능 (460ms/ 1MB)[1]	메시지 기반 암호화 핵심 설계 논리	암호데이터 중복 처리 기술 개발을 위한 핵심 프리미티브 설계	목표 기술에 대한 설계서 및 특허 증빙 자료 제시	2015
			데이터 손실 공격 방지 (460ms이하/ 1MB)	암호데이터 중복 처리 과정에서 발생하는 데이터 손실 공격을 방지하면서, 기존 기술 대비 성능이 향상된 기술 개발을 위한 목표 설정	목표 성능에 대한 검증 자료 제시(시험결과서, 논문, 특허 증빙 자료 제시)	2017
② 암호데이터 검색 기술	기능/ 검색 성능	검색 성능 O(n)[2]	암호데이터 키워드 검색	암호데이터 검색 기술 개발을 위한 핵심 프리미티브 설계	목표 기술에 대한 설계서 및 특허 증빙 자료 제시	2015
			검색 성능 O(m)[3]	전체 데이터 수가 아닌 검색 키워드를 포함하는 데이터 수에 비례하는 검색 성능 제공을 통한 암호데이터 검색 성능 최적화를 목표로 설정	목표 성능에 대한 검증 자료 제시(시험결과서, 논문, 특허 증빙 자료 제시)	2017

1) 성능 비교치 : 1MB 파일 단위 암호데이터 중복 처리를 위한 평문데이터 중복 처리 대비 부가 시간

2) n : 전체 데이터 수

3) m : 검색 키워드를 포함하는 데이터 수

O 연구산출물 성과지표 (총 사업 연도/ '15년도)

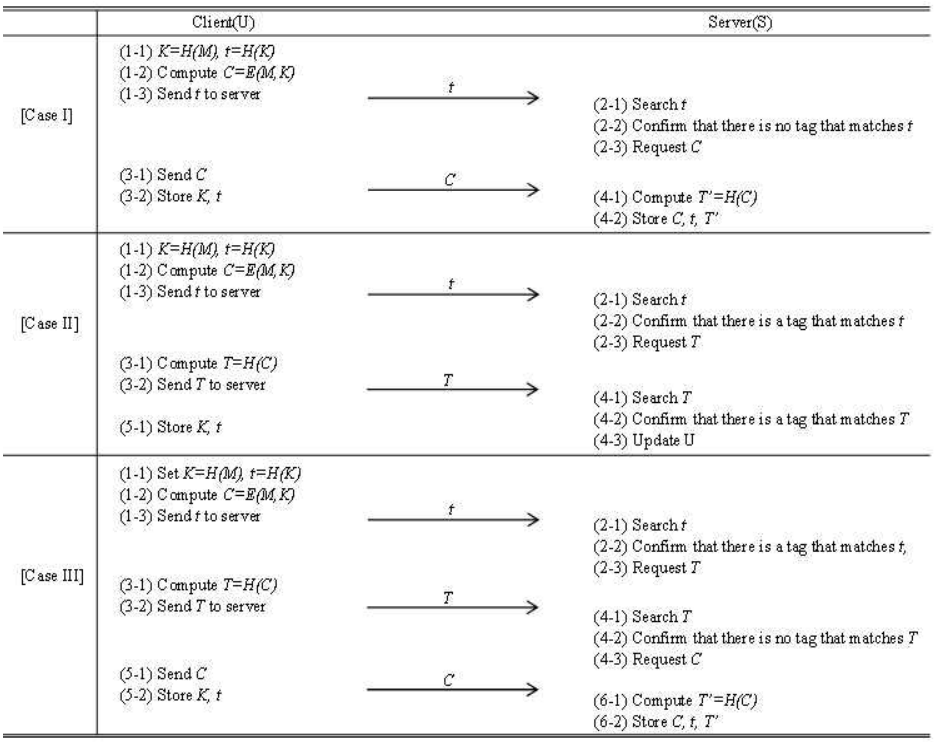
공통지표(필수제시)					특성지표(자율제시)		
지표명			총사업연도	'15년도	지표명	총사업연도	'15년도
SCI(E) 논문(건)			9건 (게재 승인 이상)	2건 (게재 승인 이상)	국제표준기고서(건)	-	-
특허 (건)	국내	출원	9건	3건 (출원 및 제출)	연구시제품(건)	-	-
		등록	-	-	소프트웨어(건)	2건	0건
	국제	출원	6건 (출원 및 제출)	2건 (제출)	기술문서(건)	15건	5건
		등록	-	-	부품설계(건)	-	-
기술이전(건)			-	-			
기술료(억원)			-	-			

제 3 장 1차년도(2015년) 연구 개발 결과

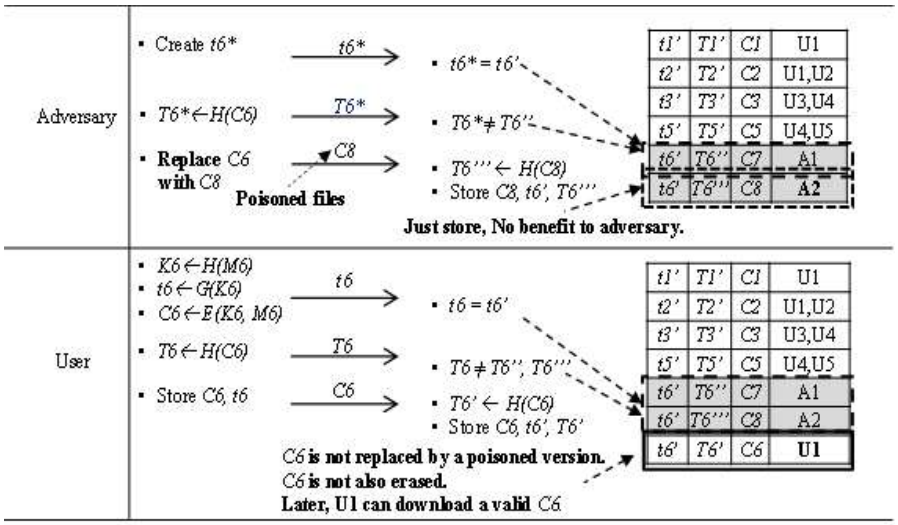
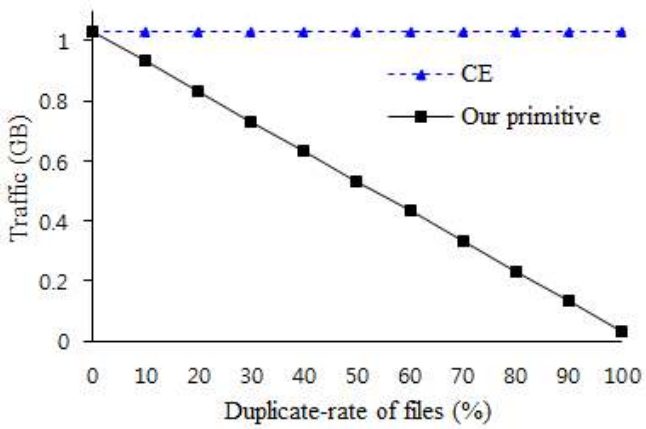
제1절 1차년도 성과 목표 달성도

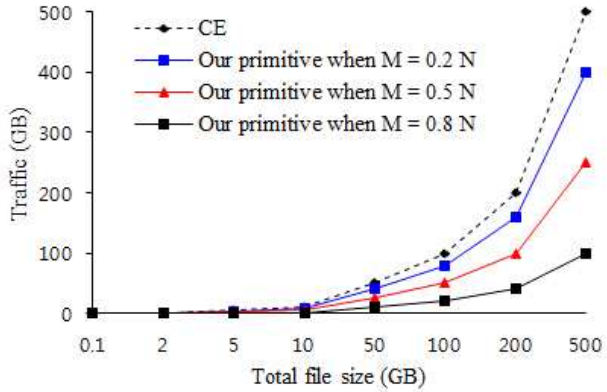
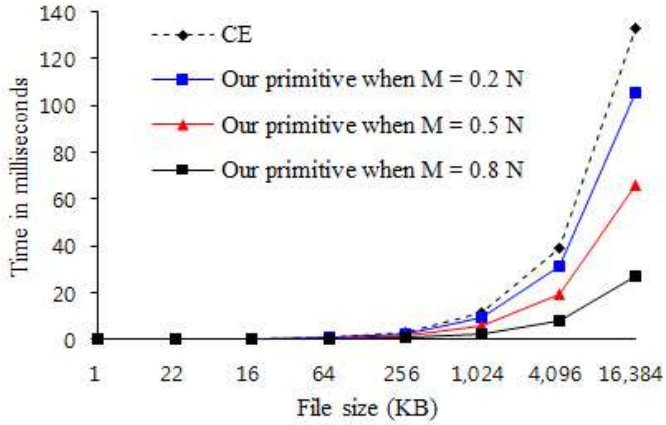
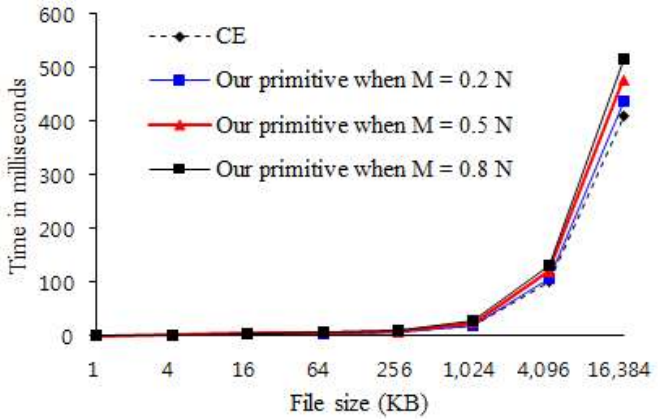
성과지표 (주요성능 Spec)	기술개발 목표치	성과	달성도(%)
암호데이터 중복 처리 기술	메시지 기반 암호화 핵심 설계 논리	O 메시지 기반 암호화 알고리즘 2종 설계 O Clinet-side 메시지 기반 암호화 프리미티브 설계 - 네트워크 전송량 및 서버 계산량 감소, 데이터 위조 공격 및 데이터 삭제 공격 방지 기능 제공 O 암호데이터 중복 처리를 위한 데이터 소유권 상호 검증 기술 설계 - 서버와 클라이언트의 데이터 소유 여부를 동시에 증명하는 최초의 소유권 검증 기법	100%
암호데이터 검색 기술	암호데이터 키워드 검색	O 암호데이터 키워드 검색 알고리즘 3종 설계 - 링크드 체인 구조 기반 확장 검색 가능 암호데이터 검색 프리미티브 알고리즘 설계 - 효율적인 검색을 위한 Bloom Filter Tree 검색 인덱스 구성 방법 설계 - 안전성-효율성 조정 가능 암호데이터 검색 기술 설계 O 검색 시간이 암호데이터 전체 수와 무관한 sublinear 검색 시간을 제공	100%
SCI(E) 논문(건)	2건(게재 승인 이상)	O SCI(E) 논문 2건 게재 O SCI 논문 1건 게재 승인	150%
국내 특허 출원 (건)	3건(출원 및 제출)	O 국내 특허 4건 제출	133%
국제 특허 출원 (건)	2건(제출)	O 국제 특허 3건 제출	150%
기술문서(건)	5건	O 요구사항정의서, 설계서 등 9건	180%

제2절 연구 수행 내용 및 결과

<table>
<tr><th>연 구 내 용</th><th>연 구 결 과</th></tr>
<tr><td>암호데이터 중복 처리를 위한 핵심 설계 논리 개발</td><td>
○ Client-side 메시지 기반 암호화 프리미티브 설계
- 기존의 MLE(Message Locked Encryption) 알고리즘의 문제점을 해결하는 새로운 방식의 프리미티브 설계
• 안전성과 효율성을 위해 두 가지 타입의 태그 사용
. 태그 1 : 짧은 키로부터 유도된 태그
. 태그 2 : 긴 메시지로부터 유도된 태그
. 태그 1과 태그 2가 모두 일치하는 경우에만 중복제거 발생
• Client-side 중복 처리 기능 제공
. 클라이언트는 중복된 파일을 서버로 전송하지 않음
. 서버는 중복되지 않는 파일에 대해서 태그 생성 및 검증을 통한 안전성 강화


<메시지 기반 암호데이터 중복처리 프로토콜>
- 데이터 손실 공격(Poison attack)에 대한 안전성 제공
• 데이터 위조 공격에 대한 방지 기능 제공
. 클라이언트는 공격자에 의해 다른 파일로 대체된 위조된 파일을 다운로드 하지 않음
</td></tr>
</table>

연 구 내 용	연 구 결 과
암호데이터 중복 처리를 위한 핵심 설계 논리 개발	• 데이터 삭제 공격에 대한 방지 기능 제공 . 공격자에 의해 사용자의 원본 파일이 서버에서 삭제되지 않음 • 기존의 Client-side MLE 알고리즘은 데이터 위조 공격과 데이터 삭제 공격에 취약하지만, 본 연구 결과는 두 가지 공격 모두에 안전 • Poison 공격 시도 및 공격 방지 시나리오 . 공격자는 $t6^*$ 와 $T6^*$을 추측한 후 정상적인 $C6$ 대신 위조된 $C8$을 보내지만, 정상 사용자는 올바른 $C6$ 다운로드 가능 . 해쉬 함수의 Collision-Resistance 성질에 의해 안전성 보장  <Poison 공격 시도와 방지 시나리오> - 네트워크 리소스(전송되는 트래픽) 감소 • 기존의 가장 대표적인 CE 기법과 비교 • 중복되는 전체 데이터(N) 중에서 중복되는 데이터(M) 만큼 비례하여 전송되는 트래픽 감소  < 업로드 시 데이터가 1GB 일 때, 전송되는 트래픽 양>

연 구 내 용	연 구 결 과
암호데이터 중복 처리를 위한 핵심 설계 논리 개발	 <저장할 데이터가 증가할 때, 중복 제거율에 따라 전송되는 트래픽 양> - 성능 분석 • 업로드 단계에서 서버의 암호 연산(해쉬(H)) 감소  <업로드할 때 서버에서의 해쉬 연산 시간> • 다운로드 단계에서 클라이언트는 해쉬(H) 연산 불필요 • 업로드 단계에서 클라이언트의 암호 연산(해쉬(H), 블록암호(E)) 비교  <업로드할 때 클라이언트에서의 해쉬 + 블록암호 연산 시간>

연 구 내 용	연 구 결 과
암호데이터 중복 처리를 위한 핵심 설계 논리 개발	- 안전성과 효율성을 동시에 만족하는 최초의 시도 . Poison 공격에 안전 & 네트워크 자원 절약하는 최초의 프리미티브 . 기존의 MLE 알고리즘(CE, HCE1, HCE2, RCE)은 트래픽 비효율 또는 Poison 공격에 취약 . 안전성/효율성/성능 비교

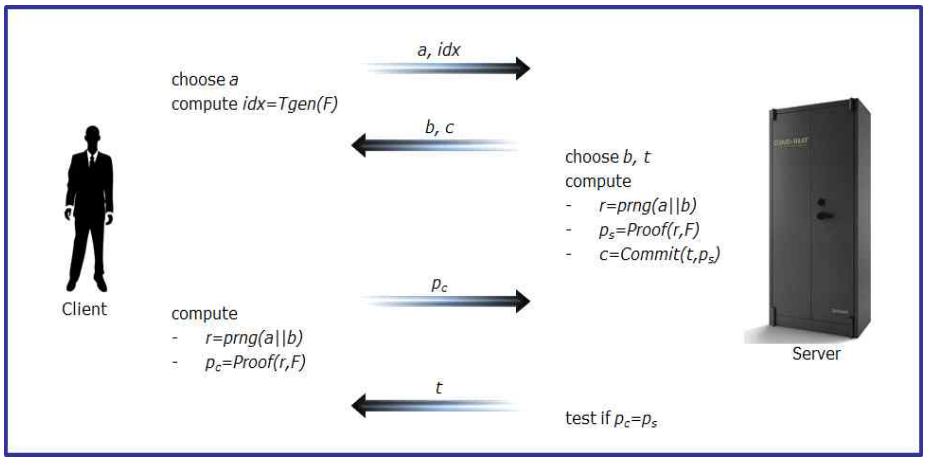
	Items to be compared			CE	HCE1	HCE2	RCE	Our primitive
Security	Against duplicate-faking attack (TC secure)			Yes	No	Yes	Yes	Yes
	Against erasure attack (STC secure)			Yes	No	No	No	Yes
Network	Comm. traffic required to upload	server-side		$N+n\cdot\|T\|$	$N+n\cdot\|t\|$	$N+n\cdot\|t\|$	$N+n\cdot(\|t\|+\|K\|)$	$N-M+$ $n\cdot\|t\|+m\cdot\|T\|$
		client-side			$N-M$ $+n\cdot\|t\|$	$N-M$ $+n\cdot\|t\|$	$N-M+n\cdot\|t\|$ $+(n-m)\cdot\|K\|$	
Perf.	Cryptographic operations	upload	at server	$n\times H$	-	-	-	$(n-m)\times H$
			at client	$n\times E$	$n\times G$, $(n-m)\times E$	$n\times G$, $(n-m)\times E$	$n\times G$, $(n-m)\times E$	$n\times G$, $m\times H$, $n\times E$
		download	at client	$n\times D$	$n\times D$	$n\times D$, $n\times H$	$n\times D$, $n\times H$	$n\times D$

n : 저장할 파일 개수, m : 중복된 파일 개수, N : n개의 파일 전체 크기
M : m개의 중복된 파일 전체 크기, t : 첫 번째 태그, T : 두 번째 태그
$|t|$: 첫 번째 태그의 크기, $|T|$: 두 번째 태그의 크기, $|K|$: 메시지 기반 암호키의 크기
H, G : 해쉬 함수, E, D : 암복호용 블록 암호

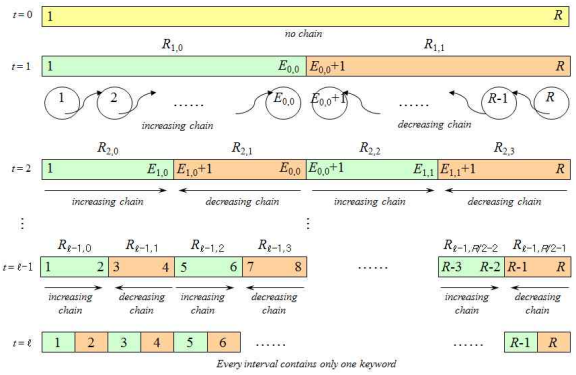
<안전성, 네트워크 트래픽, 암호 연산 횟수 비교>

○ 암호데이터 중복 처리를 위한 데이터 소유권 상호 검증 기술 설계

- 안전한 client-side 암호데이터 중복 처리를 위한 원천 기술로써, 서버와 클라이언트의 데이터 소유권을 동시에 증명하는 최초의 기법 설계
  - 서버는 클라이언트에게 특정 데이터를 실제로 전송받지 않고 소유권을 부여하기 위해 클라이언트가 실제로 보유하고 있는지 검증
  - 클라이언트는 실제로 데이터를 서버에게 전송하지 않고 본인의 파일을 삭제하므로, 데이터 삭제 전에 서버에 저장된 데이터가 업로드 하려는 데이터와 동일한지 검증
- 기존의 client-side 암호데이터 중복 처리를 위한 소유권 증명 기술보다 확장된 소유권 증명 기능을 제공하여 데이터 서비스의 신뢰성 향상
  - 기존에 설계된 안전한 client-side 암호데이터 중복 처리를 위한 소유권 증명 기술의 경우 클라이언트의 소유 여부를 증명하는 것으로 한정됨
  - 데이터 업로드 이후 서버의 데이터 보유 여부 확인 할 수 있는 기술은 존재했으나, 가장 중요한 업로드 시점에 서버와 클라이언트 두 주체의 데이터 소유 여부를 동시에 증명할 수 있는 기술은 본 개발이 최초임

연 구 내 용	연 구 결 과
암호데이터 중복 처리를 위한 핵심 설계 논리 개발	- 암호데이터 중복 처리를 위한 데이터 소유권 상호 검증 기술의 일반적인 설계 방법 제시 • 알려져 있는 태그 생성 함수, 의사 난수 생성 함수, (단방향) 소유권 증명 기법, 위임 기법을 사용하여 소유권 상호 검증이 가능한 지식 증명 기술의 일반적인 설계 방법을 제시함  <데이터 소유권 상호 검증 기술 일반적인 설계 기법> - 일반적인 설계 기술을 해쉬 함수만 사용하여 구현한 효율적 기법의 경우, 매우 적은 연산으로 서버와 클라이언트의 데이터 소유권을 동시에 검증할 수 있음 • 소유권 증명 제공하지 않는 단순한 client-side 암호데이터 중복 처리의 경우에도 태그를 생성하기 위해 최소 해쉬 1번의 연산을 수행해야 함 • 클라이언트의 데이터 소유권만 검증하는 경우에도 증명 정보 생성하기 위해 최소 해쉬 1번 이상의 연산이 수행됨 • 본 연구를 통해 개발된 기술의 경우 서버와 클라이언트가 해쉬 1번의 연산만 계산하여 자신의 소유권 증명 생성 및 상대방의 소유권 검증을 동시에 수행할 수 있음 ※ 고정된 짧은 길이를 가지는 입력에 대한 해쉬 계산은 파일 길이에 준하여 증가하는 해쉬 계산에 비해 매우 작아서 파일 길이에 비례하여 증가하는 해쉬 계산만 비용으로 언급하였음 ○ SCI 논문 2건(IEEE Communications Letters, ETRI Journal) 심사 중, 국제 특허 2건 및 국내 특허 2건 출원 중

연 구 내 용	연 구 결 과
암호데이터 검색을 위한 핵심 알고리즘 설계	○ 확장 검색 기능 추가가 용이한 암호데이터 검색 프리미티브 알고리즘 설계 - 링크드 체인 구조의 검색 인덱스 기법에 대한 확장 검색 기능 연구를 통한 신규 프리미티브 알고리즘 설계 • 동일한 검색 키워드를 포함한 암호데이터를 체인 형태로 구성하는 링크드 체인 검색 인덱스를 사용하여 효율적인 키워드 검색이 가능 • 링크드 체인 구조의 검색 인덱스는 검색 시간이 전체 데이터 수에 무관한, sublinear 검색 시간 제공 • 기존의 링크드 체인 구조의 검색 인덱스는 각각의 링크드 체인이 독립적으로 구성되어 검색 방식이 제한적임 • 다중 링크드 체인 구조를 설계하고, 하나의 암호데이터가 다수의 링크드 체인에 저장되어 다양한 방식의 검색 방식 제공 가능 - 다중 링크드 체인 구조를 이용한 암호데이터에 대한 효율적인 범위 검색 기법 연구 • 기존 암호데이터에 대한 확장 검색은 공개키 방식의 기법이 주류를 이루고 있으며, linear 검색 시간으로 현실 데이터 활용 환경에 부적합 • 대칭키 암호 프리미티브를 이용한 다중 링크드 체인 구조를 설계하여 암호데이터에 대한 범위 검색 기법 연구 • 전체 검색 시간이 전체 암호데이터 수에 무관한 sublinear 검색 시간을 제공하는 범위 검색 기법 제공

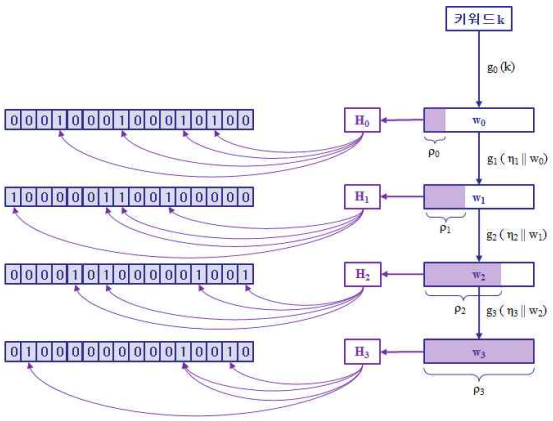
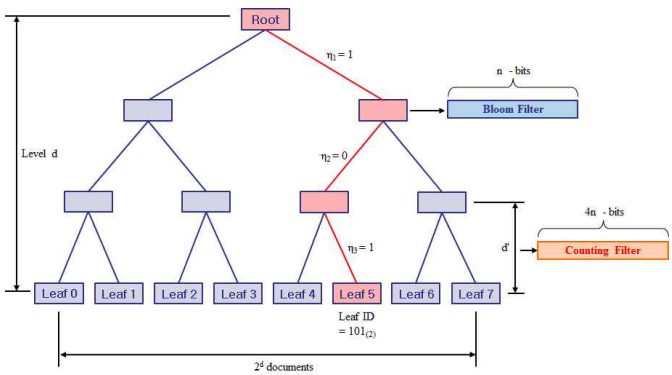


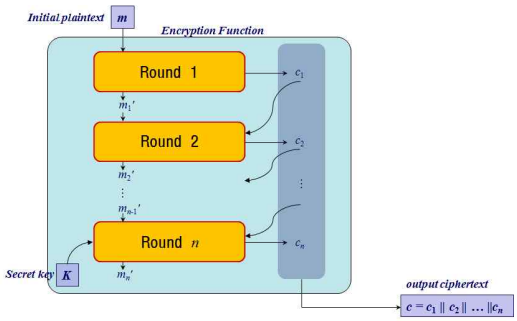
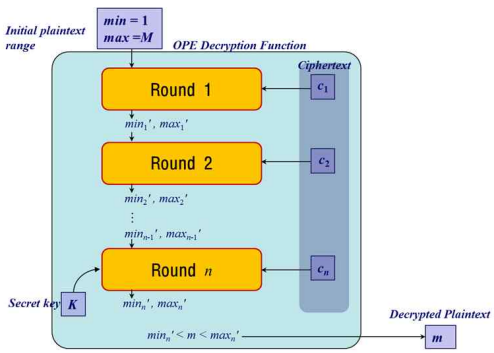
<범위 검색을 위한 다중 링크드 체인 구조>

	Enc. Type	Range Query	Efficiency		
			Index Size	Trapdoor Size	Search Time
Curtmola, et al.	Symmetric	N	O(N)	1 Link (address, s.key)	m symmetric decryptions
Boneh, Waters	Public	Y	O(NR)	3 points over EC	(2R+1)N Pairings
Shi, et al.	Public	Y	O(N log R)	5 log R points over EC	5N log R Pairings
Ours	Symmetric	Y	O((N+R) log R)	2 Links (address, s.key)	m+R symmetric decryptions

N : number of all documents
m : number of searched documents
R : total range
EC : elliptic curves

<관련 암호데이터 검색 기법 비교>

연 구 내 용	연 구 결 과
암호데이터 검색을 위한 핵심 알고리즘 설계	○ Bloom filter 기반의 암호데이터 검색 프리미티브 설계 - 암호화된 데이터에 대한 효율적인 키워드 검색이 가능한 기반 기술 발굴 및 이를 이용한 검색 인덱스 생성 방안 연구 • 집합 포함 관계에 대한 효율적인 검증이 가능한 bloom filter를 기반 기술로 활용한 암호데이터 키워드 검색 기법 연구 • 기존 bloom filter를 이용한 암호데이터 검색 기법 설계 시도가 있었으나, 각각의 데이터에 bloom filter를 단순 적용하는 방식으로 전체 암호데이터에 linear한 검색 시간을 제공하는 비효율적인 기법임 • 각각의 내부 노드가 bloom filter로 구성된 bloom filter tree를 검색 인덱스로 활용하는 암호데이터 키워드 검색 알고리즘 설계 • Tree 구조와 bloom filter의 장점을 결합하여 전체 데이터에 대한 sublinear 검색 시간 제공  <Bloom filter 기반 암호데이터 검색 인덱스 생성 알고리즘> - Bloom filter tree를 이용한 암호데이터 검색 알고리즘 최적화 연구 • 수용가능 안전성 개념 적용을 통해 요구 안전성 수준 및 저장 데이터 규모에 따른 bloom filter tree 구성 최적화 연구 • Bloom filter 기반 암호데이터 검색 기술에 대한 체계적인 안전성 분석  <Bloom filter tree 구조>

연 구 내 용	연 구 결 과
암호데이터 검색을 위한 핵심 알고리즘 설계	○ 실용적인 암호데이터 검색을 위한 안전성-효율성 조정 가능 암호데이터 검색 기술 설계 - 수용가능 안전성 적용을 통한 암호데이터 검색 기술에 대한 안전성-효율성 조정 방안 연구 • 제한적인 안전성을 바탕으로 평문의 순서 정보를 보존하는 순서 보존 암호화 기술 설계 • 복호화를 포함한 추가적인 연산 없이 암호데이터에 대한 대소 비교 및 범위 검색 기능 제공 • 수용가능 안전성 적용을 통해 요구 안전성 수준에 따른 암호문/평문 비율 조정 가능 • 순서 보존 암호화 기술에 대한 증명 가능 안전성 개념 적용을 통한 안전성 증명  <유사난수생성기를 활용한 데이터 암호화 알고리즘 구조>  <유사난수생성기를 활용한 데이터 복호화 알고리즘 구조> - 구현 효율성 강화를 통한 효율적인 설계 방식 제공 • 임의의 유사 난수 생성기(해쉬 함수, 블록암호 등을 유사 난수 생성기로 사용 가능)가 구현된 환경에서 추가적인 알고리즘 구현 없이 데이터 암/복호화 가능 • 암호문 길이 자유 선택 가능 : 암호화 함수에서의 추가적인 변수 선택을 통해 원하는 수준의 암호문/평문 비율 선택 가능 ○ SCI 논문(IEICE Transactions on Communications) 1건 게재, SCI 논문(Journal of Supercomputing) 1건 게재 승인, 국제 특허 1건 및 국내 특허 2건 출원 중

제3절 연구 성과

1. 정성적 연구 성과

O 암호데이터 중복 처리를 위한 핵심 설계 논리 개발
- 메시지 기반 암호화 알고리즘 2종 설계
- Client-side 메시지 기반 암호화 프리미티브 설계
  • 안전성과 효율성을 동시에 만족하는 client-side 메시지 기반 암호화 프리미티브 설계
  • 기존 CE 알고리즘 대비 네트워크 전송량 및 서버 계산량 감소
  • 데이터 위조 공격 및 데이터 삭제 공격 방지 기능 제공
- 암호데이터 중복 처리를 위한 데이터 소유권 상호 검증 기술 설계
  • 서버와 클라이언트의 데이터 소유 여부를 동시에 증명하는 최초의 소유권 상호 검증 기법 설계
  • 소유권 검증을 제공하지 않는 기초적인 client-side 중복 처리 기술과 유사한 성능을 제공하는 해쉬 기반의 효율적인 기법 제공

O 암호데이터 검색을 위한 핵심 알고리즘 설계
- 키워드 기반의 암호데이터 검색을 위한 핵심 프리미티브 설계
  • 확장 검색 기능 추가가 용이한 링크드 체인 검색 인덱스를 사용한 키워드 검색 프리미티브 기술 설계 및 다양한 방식의 체인 구성 방안 연구
  • Bloom filter tree를 이용한 검색 인덱스 구성 방식 연구를 통해 실용적인 암호데이터 검색 기술 설계를 위한 기반 기술 확보
- 실용적인 암호데이터 검색을 위한 안전성-효율성 조정 가능 암호데이터 검색 기술 설계
  • 수용 가능 안전성 적용을 통해 요구 안전성 수준에 따른 암호문/평문 비율 조정이 가능한 순서 보존 암호화 기술 설계
  • 임의의 유사 난수 생성기가 구현된 환경에서 추가적인 알고리즘 구현 없이 암/복호화 가능
- 검색 시간이 암호데이터 전체 수에 무관한 sublinear 검색 시간을 제공하는 암호데이터 키워드 검색 알고리즘 설계

2. 정량적 연구 성과

O 논문 실적

번호	구분	논문명	논문발표학회명 또는 게재지	년도, 권호	SCI(E) 등재 여부
1	게재	Efficient construction of order-preserving encryption using pseudo random function	IEICE Transactions on Communications	2015, E98-B(7)	SCI
2	게재	Low complexity multiplier based on Dickson basis using efficient Toeplitz matrix-vector product	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	2015, E98-A(11)	SCIE

3	게재 승인	Symmetric searchable encryption with efficient range query using multi-layered linked chains	Journal of Supercomputing	미정	SCI
4	게재	클라우드 스토리지 상에서의 프라이버시 보존형 소스 기반 중복데이터 제거기술	한국정보보호학회 논문지	2015, 25(1)	-
5	발표	Privacy preserving client-side deduplication scheme in cloud storage	APIC-IST 2015	2015. 7	-
6	발표	Encoding of Korean characters with less radix in format-preserving encryption	ICTC 2015	2015. 10	-
7	발표	Hybrid-type secure deduplication	ICONI 2015	2015. 12 발표 예정	-
8	발표	Necessity of incentive system for the first uploader in client-side deduplication	CUTE 2015	2015. 12 발표 예정	-
9	발표	Performance analysis of format-preserving encryption based on unbalanced-feistel structure	CUTE 2015	2015. 12 발표 예정	-
10	제출	Client-side deduplication for reducing network traffic and enhancing security	IEEE Communications Letters	미정	SCI
11	제출	Secure and practical client-side deduplication supporting mutual proof of ownership	ETRI Jouranl	미정	SCI

○ 국제 특허

번호	구분	특허명	출원번호	출원국	출원일
1	국외	Method for secure deduplication of encrypted data using tags	PR20150379US (출원 중)	미국	2015. 6. 9 (제출일)
2	국외	Method and system for mutual proof of ownership	PR20150398US (출원 중)	미국	2015. 6. 16 (제출일)
3	국외	Encrypted data search using Bloom Filter Tree	PR20150725US (출원 중)	미국	2015. 9. 9 (제출일)

○ 국내 특허

번호	구분	특허명	출원번호	출원국	출원일
1	국내	태그를 이용한 암호 데이터의 안전한 중복 처리 방법	PR20150379KR (출원 중)	한국	2015. 6. 9 (제출일)
2	국내	데이터 소유권 상호 검증 기술 설계 방법 및 시스템	PR20150398KR (출원 중)	한국	2015. 6. 16 (제출일)
3	국내	Bloom 필터 트리를 활용한 암호데이터 검색 기법	PR20150725KR (출원 중)	한국	2015. 9. 9 (제출일)
4	국내	안전성 강화형 순서 보존 암호화 기술	PR20150925KR (출원 중)	한국	2015. 10. 14 (제출일)

○ 기술문서

번호	구분	제목	주요 내용	등록 일시
1	TDP	암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천 기술 개발 요구사항정의서 V1.0	암호데이터 저장 및 검색을 위한 암호 원천 기술 개발 사용자 및 시스템 요구 사항 정의	2015. 9. 23
2	TDP	암호데이터 중복 처리 기술 설계서 V1.0	암호데이터 중복 처리를 위한 메시지 기반 암호화 프리미티브에 대한 설계	2015. 11. 23
3	TDP	암호데이터 검색 기술 설계서 V1.0	키워드 기반의 암호데이터 검색 기술에 대한 설계	2015. 11. 24
4	TM	암호데이터 중복 처리 기술 동향 분석	암호데이터 중복 처리 기술에 대한 최신 연구 동향 분석	2015. 8. 20
5	TM	검색가능암호 기술 분석	검색가능암호 기술에 대한 최신 연구 동향 분석	2015. 9. 24
6	TM	DupLESS 분석 및 구현	DupLESS 프로토콜에 대한 분석 및 구현 결과 제시	2015. 11. 23
7	TM	Revocable storage에서의 키워드 검색 기법 분석	Revocable storage에서 키워드 검색 기법에 대한 최신 연구 동향 분석	2015. 11. 23
8	TM	MLE Schemes 분석	MLE의 CE, HCE1, HCE2, RCE 기법 분석	2015. 12. 01
9	TM	Popularity/Unpopularity에 기반한 암호데이터 중복 처리 기술 분석	파일의 인기/비인기 정도에 따른 중복 처리 기술 분석	2015. 12. 01

제4절 국내외 관련 분야의 환경 변화

제5절 사업비 사용 현황

(단위:천원)

구 분 / 비 목	계 획		사용금액		집행률(%)		비고
	현 금	현 물	현 금	현 물	현 금	현 물	
1. 인건비	309,000	0	309,000	0	100%	-	
- 내부인건비(정)	309,000	0	309,000	0	100%	-	
2. 직접비	591,000	0	411,897	0	69.7%	-	
2.1 외부인건비	40,000	0	0	0	0%	-	
2.2 연구시설・장비 및 재료비	82,990	0	78,714	0	94.9%	-	
2.3 연구활동비	110,841	0	62,628	0	56.5%	-	
2.4 연구과제추진비	31,687	0	14,533	0	45.9%	-	
2.5 연구수당	69,460	0	0	0	0%	-	
2.6 위탁연구개발비	80,000	0	80,000	0	100%	-	
2.7 연구지원비	3,473	0	3,473	0	100%	-	
2.8 성과활용지원비	70,185	0	70,185	0	100%	-	
2.9 평가・관리비	2,364	0	2,364	0	100%	-	
2.10 공동연구비	100,000	31,200	100,000	31,200	100%	100%	
합 계	900,000	31,200	720,897	31,200	80.1%	100%	

※ 12월 1일 기준

제 4 장 2차년도(2016년) 연구 계획

제1절 2차년도 연구목표 및 내용

연구 목표	내용
암호데이터 저장, 열람, 검색 기술 설계 및 안전성 검증	가) 연구 개발 목표 O 암호데이터 저장, 열람, 검색 기술 설계 및 안전성 분석 - 암호데이터 중복 처리 기술 • 파일 단위 암호데이터 중복 처리 알고리즘(SW, IPR) - 데이터 추가/삭제 기능 제공 동적 암호데이터 검색 알고리즘 (IPR) 나) 연구 개발 내용 O 암호데이터 중복 처리 기술 설계 - 파일 단위 암호 데이터 중복 처리 기술 분석 및 안전성 모델 정립 - 파일 단위 암호 데이터 중복 처리 알고리즘 설계 - 암호데이터 중복 처리 기술 안전성 검증 - 파일 단위 암호데이터 중복 처리 검증 프로그램 개발 - 암호데이터 중복 처리 성능 최적화 연구 O 암호데이터 소유권 검증 모델 연구 - 적용 환경 분석을 통한 요구 사항 정의 - 암호데이터 소유권 검증 기술을 위한 암호 프리미티브 분석 - 암호데이터 소유권 검증 시나리오 분석 및 구성 - 데이터 기반의 소유권 부여, 유지 및 검증을 위한 관리 모델 설계 O 동적 환경을 위한 암호데이터 검색 기술 설계 - 데이터 추가/삭제를 위한 최신 기술 및 장단점 분석 - 동적 암호데이터 검색 기술에 대한 요구 사항 분석 및 정의 - 동적 암호데이터 검색 기술 안전성 모델 정립 - 데이터 추가/삭제 기능을 제공하는 암호데이터 검색 알고리즘 설계 및 안전성 증명

제2절 2차년도(2016년) 성과 목표 및 연구수행전략

1. 성과목표

○ 기술개발 성과지표(‘16년도)

성과지표 (주요성능 Spec)	단위	세계최고 수준	기술개발 목표치(‘16)	목표치 산출근거	검증방법
① 암호데이터 중복 처리 기술	기능/ 성능	데이터 손실 공격 가능 (460ms/ 1MB)[1]	파일 단위 암호데이터 중복 처리 알고리즘 (데이터 손실 공격 방지)	암호데이터 중복 처리 과정에서 발생하는 데이터 손실 공격에 대한 방지 기능을 제공하는 암호데이터 중복 처리 기술에 대한 원천 IPR 확보를 목표로 설정	목표 기술에 대한 설계서 및 특허 증빙 자료 제시
② 암호데이터 검색 기술	기능/ 검색 성능	검색 성능 O(n)[2]	동적 암호데이터 검색 알고리즘 (O(n) 미만)	데이터 추가/삭제가 빈번히 발생하는 동적 환경에서, 사용자 프라이버시를 보호하면서 암호데이터에 대한 검색이 가능한 기술에 대한 원천 IPR 확보를 목표로 설정	목표 기술에 대한 설계서 및 특허 증빙 자료 제시

1) 성능 비교치 : 1MB 파일 단위 암호데이터 중복 처리를 위한 평문데이터 중복 처리 대비 부가 시간
2) n : DB에 저장된 전체 암호데이터 수

○ 연구산출물 성과지표(총사업연도/ ‘16년도)

공통지표(필수제시)					특성지표(자율제시)		
지표명			총사업연도	‘16년도	지표명	총사업연도	‘16년도
SCI(E) 논문(건)			9건 (게재 승인 이상)	3건 (게재 승인 이상)	국제표준기고서(건)	-	-
특허 (건)	국내	출원	9건	3건 (출원 및 제출)	연구시제품(건)	-	-
		등록	-	-	소프트웨어(건)	2건	1건
	국제	출원	6건 (출원 및 제출)	2건 (출원 및 제출)	기술문서(건)	15건	5건
		등록	-	-	부품설계(건)	-	-
기술이전(건)			-	-			
기술료(억원)			-	-			

2. 연구 수행 방법

O 한국전자통신연구원 주도로 암호데이터 저장, 검색을 위한 암호 기술 연구에 대한 방향 설정 및 원천 기술 개발
- 한국전자통신연구원은 파일 단위 암호데이터 중복 처리 및 동적 암호데이터 검색 알고리즘을 개발하며, 암호데이터 소유권 관리 모델 연구를 수행
- 공동연구기관(공주대학교)은 암호데이터 중복 처리 기반 기술 연구를 통해 한국전자통신연구원과 파일 단위 암호데이터 중복 처리 기술 개발을 위해 협력
- 암호데이터 중복 처리 및 검색에 대한 핵심 원천 기술 개발 및 우수 IPR의 전략적인 확보

O 연차별 기술 개발이 최종 연구 결과물에 유기적으로 결합될 수 있는 연구 개발 수행
- 암호데이터 중복 처리 기술 및 소유권 검증 기술
  - 암호데이터 중복 처리 과정에서 발생하는 데이터 손실 공격 분석 및 안전성 모델링
  - 안전성 모델 및 1차년도에 개발한 메시지 기반 암호화 핵심 설계 논리를 기반으로 한 파일 단위 암호데이터 중복 처리 알고리즘 설계
  - 암호데이터 열람 과정에서 발생할 수 있는 데이터 프라이버시 침해 가능성에 대한 면밀한 분석을 통한 데이터 기반의 소유권 관리 모델 연구
- 암호데이터 검색 기술
  - 실시간 데이터 추가 및 삭제가 수행되는 동적 환경에서의 암호데이터 검색 기술에 대한 최신 기술 분석 및 안전성 모델 정립
  - 동적 환경에 적용 가능한 안전성을 기반으로 데이터 추가/삭제가 가능한 암호데이터 검색 알고리즘 설계

O 미국, 유럽, 일본 등 선진국의 연구 프로젝트, 각종 국제 학회 및 저널 논문, 국내외 특허 등을 면밀히 검토하여 차별화된 연구 개발 수행

O 위탁연구기관 및 전문가 초청 등을 적극 활용하여 학계의 우수한 기술 확보

O SCI(E) 저널이나 국제 유수 학회 논문 기고를 통해 결과물의 국제적 검증 수행

O 1실 1사 기업과의 긴밀한 협력을 통한 상용 데이터베이스 환경 요구 사항 반영

3. 2차년도 사업비 집행 계획

(단위:천원)

비 목 별	1세부			1세부 합계		
	ETRI	공동		ETRI	공동	합계
	현금	현금	현물			
1. 인건비	309,000	0	31,200	309,000	31,200	340,200
○ 내부인건비(정)	309,000	0	31,200	309,000	31,200	340,200
2. 직 접 비	491,000	85,000	0	491,000	85,000	576,000
가. 외부인건비	70,600	48,240	0	70,600	48,240	118,840
1) 내부인건비(계)	45,000	0	0	45,000	0	45,000
2) 외부인건비	25,600	48,240	0	25,600	48,240	73,840
나. 연구장비·재료비	110,228	1,871	0	110,228	1,871	112,099
1) 연구장비 및 시설비	98,300	0	0	98,300	0	98,300
2) 재료비 및 전산처리비	11,928	1,871	0	11,928	1,871	13,799
3) 시작품 제작비	0	0	0	0	0	0
다. 연구활동비	54,857	13,056	0	54,857	13,056	67,913
1) 국외여비	25,541	8,583	0	25,541	8,583	34,124
2) 수용비 및 수수료	6,297	1,350	0	6,297	1,350	7,647
3) 기술정보 활동비	23,019	3,123	0	23,019	3,123	26,142
라. 연구과제추진비	38,050	5,945	0	38,050	5,945	43,995
1) 국내여비	23,050	2,525	0	23,050	2,525	25,575
2) 회의-야근식대 다과비	13,800	3,000	0	13,800	3,000	16,800
3) 사무용품비	1,200	420	0	1,200	420	1,620
마. 연구수당	75,920	15,888	0	75,920	15,888	91,808
바. 위 탁 연 구 개 발 비	80,000	0	0	80,000	0	80,000
사. 연구지원비	3,796	0	0	3,796	0	3,796
아. 성과활용지원비	55,185	0	0	55,185	0	55,185
자. 평가·관리비	2,364	0	0	2,364	0	2,364
3. 간 접 비	0	15,000	0	0	15,000	15,000
합 계	800,000	100,000	31,200	800,000	100,000	931,200

제3절 연구결과의 활용 가능성 및 파급 효과

O 현재 성능 문제로 인해서 적용이 지연되고 있는 클라우드/빅데이터 서비스 환경의 데이터 암호화 도입을 위한 기반 기술로 활용하여, 암호데이터 기반 서비스 신뢰성 향상 및 사회적 현안 해결

- 암호데이터에 대한 저장 및 검색 기능을 평문과 유사한 수준으로 제공함으로써 현재 기술적 한계로 인해 평문 데이터 대상으로만 제공되는 현재의 데이터 서비스의 영역을 암호데이터로 확장, 나아가서 데이터 서비스 전체의 신뢰성을 향상시키기 위한 원천 기술로 활용
- 암호데이터 중복 처리를 위한 핵심 설계 기술은 암호데이터 저장 단계에서 스토리지 및 네트워크 비용 절감을 위한 원천 기술로 활용
- 기술이전 및 상용화를 통해 급속히 성장하는 암호데이터 관련 시장에서의 국내 업체의 기술 선도 지원 및 국가 경쟁력 제고

O 전 세계적으로 추진되고 있는 데이터 위탁 서비스 환경을 대비하여 향후 암호화된 데이터를 중심으로 한 신 데이터 보안 패러다임인 CipherData 트렌드 선도

- 정책적으로 금융, 의료, 교육을 비롯한 공공부문 데이터에 대한 위탁 환경을 통한 서비스가 추진되고 있으며, 민간 부문의 데이터 또한 이러한 변화를 따를 것으로 전망
- 데이터 프라이버시에 대한 관심이 커지면서 민감 데이터에 대한 암호화 적용은 사회적인 요구사항으로 발전하고 있으나, 기술적인 성능 문제로 인해 현실 서비스에 적용이 지연될 것으로 예상
- 이러한 상황을 해결하기 위해 관련 기관 및 기업의 효율적인 암호화된 데이터 활용 기술에 대한 요구가 커지고 있어, 본 과제의 암호데이터 저장/검색 핵심 프리미티브 기술이 다양한 방면의 암호데이터 활용 환경에 적용될 수 있을 것으로 기대함
- 또한, 이러한 프리미티브 기술을 바탕으로 암호데이터를 평문 데이터처럼 자유롭게 활용하는 신 데이터 보안 패러다임인 CipherData 트렌드를 창출 및 선도할 것으로 기대