세부과제 연차실적 보고서

연차실적 보고서

과제유형	1. 기초미래선도형 (O) 2. 공공인프라형 ( ) 3. 산업화형 ( )				
대과제명	초연결통신 기초·원천기술 개발				
세부과제명	암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천 기술 개발				
세부과제 책임자	소속 및 부서	정보보호연구본부 암호기술연구실	직위 (직급)	실장 (책임연구원)	
	성명	장구영			
총연구기간	2015년 01월 01일 부터 2017년 12월 31일 까지 (36개월)				
당해연도 연구기간	2016년 01월 01일 부터 2016년 12월 31일 까지 (12개월) (2차년도)				
총연구비	정부출연금	2,728,518 천원	당해년연구비	정부출연금	915,109 천원
	민간부담금	93,600 천원		민간부담금	31,200 천원
	계	2,822,118 천원		계	946,309 천원
참여인력(M/Y)	총 연 구 기 간	63명 (20.6M/Y)			
	당해연도 연구기간	27명 (8.4M/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.

2016년 12월 23일

세부과제책임자 : 장 구 영 (인)
직 할 부 서 장 : 황 승 구 (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
- 2013년 전세계 유출량은 5억 5,200만 건에 달하며, 이 중 20% 이상이 국내에서 발생한 것으로 추산됨(Symantec, 2014)

< 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

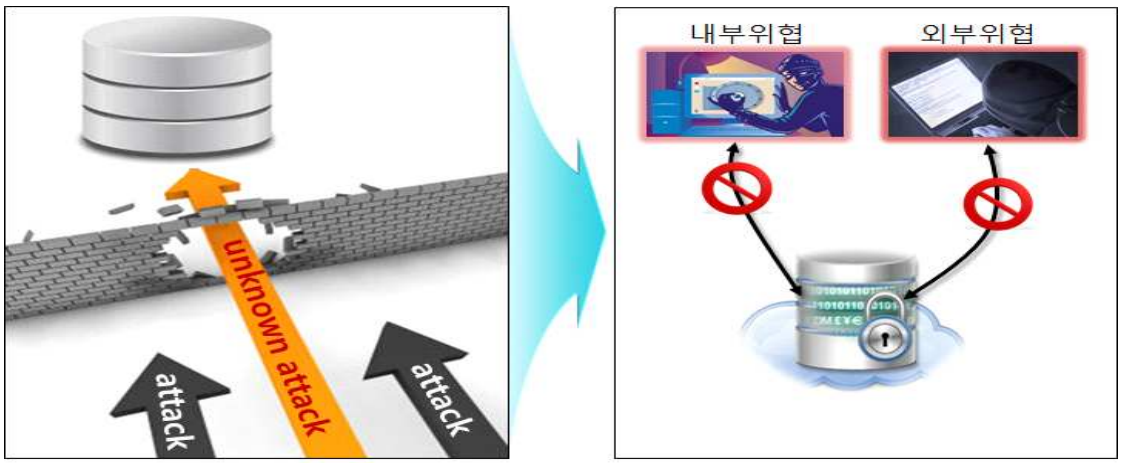
- 개인정보보호법(2014.8.7 시행)은 개인정보 수집 최소화 및 관리에 대한 법적 책임을 강화하고 있으며, 주민등록번호 등과 같은 고유 식별 정보에 대한 암호화를 명시하는 내용을 포함하는 등 민감 정보 암호화에 대한 기술적 필요성을 제기함

- 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

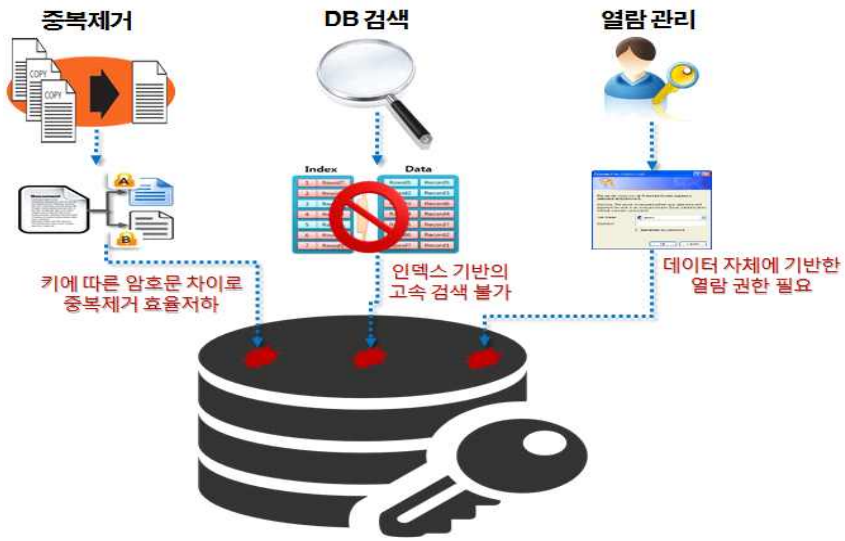
2. 연구개발과제의 중요성

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
- SW 방식의 DB 암호화는 평균 7배의 성능 저하가 발생하여, 3천여 개에 달하는 우리나라 금융회사 가운데 고객 정보를 암호화해 관리하는 곳은 47개사에 불과할 정도로 암호화 적용이 저조한 상황임(인텔코리아, 2014)



< 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

○ 급증하는 데이터의 저장 비용 절감을 위한 데이터 중복 처리 기술에 대한 연구가 진행되어 왔으나, 암호화에 의한 기밀성 유지 상태에서도 저장의 효율성을 제공하는 암호데이터 중복 처리 기술 개발은 최근 본격적으로 시작되고 있음
- 급증하는 데이터에 대응하기 위해 데이터베이스 스토리지 비용 절감이 중요해짐에 따라, 평문 데이터에 대한 중복 처리 기술은 Drop Box, Google Drive, Mozy 등과 같은 클라우드 기반 스토리지 서비스에 적용되고 있음
- 암호데이터 중복 처리 기술은 2002년 최초로 기술 개념이 도입된 이후 단편적인 연구 결과에 머무르다가, 2013년도에 최초로 암호학적 안전성 개념이 제안되고 이를 기반으로 증명 가능한 안전성이 제공되면서 본격적인 연구가 시작되고 있음
- 현재 데이터에 의해 암호키가 결정되는 message-locked encryption을 중심으로 연구가 수행 중에 있으나, 기본적인 안전성 요구 사항만 만족하는 기술로 향후 다양한 공격 위협에 대응할 수 있는 원천 기술의 연구가 필요한 상황임
- 낮은 엔트로피를 가지는 데이터의 경우, 현재 알려진 암호데이터 중복 처리 기술로는 안전성을 보장하기 어려워 안전성 강화를 위한 연구가 시도되고 있음
- 국내에서는 평문 및 암호데이터에 대한 중복 처리 기술에 대한 동향 분석 수준의 결과가 일부 발표되고 있음
- 향후 암호데이터 중복 처리 기술에 대한 연구는 암호학적 안전성에 개념 고도화, 효율성 개선, 다양한 목적 및 응용 환경 지원이 가능한 기능 부가형 원천 기술 개발 방향으로 진행될 것으로 전망됨

○ 암호데이터 소유권 검증 기술은 데이터 자체를 기반으로 데이터의 소유권 부여, 유지 및 검증을 제공하는 기술로 전 세계적으로 관련 연구가 전무한 상황임
- 기존 사용자 정보 기반 인증을 통한 권한 관리나 접근 제어와 같은 시스템적인 소유권 검증 기술은 권한 이상의 데이터 열람이 가능하여 데이터 프라이버시 침해 우려를 낳고 있음
- 평문데이터에 대한 소유권 검증 기술을 위한 안전성 모델 및 설계 개념을 암호데이터 소유권 검증 기술에 단순 적용하기에는 구조적 차이로 인한 어려움이 존재함
- 현재 암호데이터 중복 처리 과정에서 데이터의 실제 보유 여부 검증을 위한 제한적인 목적으로 일부 이론적인 연구가 수행
- 암호화에 의한 기밀성을 유지하면서 데이터 기반의 소유권 부여, 유지 및 검증이 가능한 새로운 암호데이터 소유권 관리 모델의 정립 및 이를 처리할 수 있는 원천 기술 개발이 필요함

○ 암호데이터 검색 기술은 높은 안전성 제공을 목적으로 한 이론적인 방향으로 연구가 진행되어 왔으나, 데이터베이스 보안에 대한 필요성 증가로 실제 서비스 적용 가능한 암호데이터 검색 기술에 대한 요구가 증가하여 성능 현실화를 위한 실용화 가능한 구조 설계 및 기존 기술의 성능 개선 방향의 연구가 수행되고 있음
- 검색 가능 암호 기술은 암호화된 데이터베이스에서 효율적인 검색을 목적으로 2000년에 처음으로 제안되었으며, 초기에는 높은 안전성을 추구하는 이론적인 연구가 주로 수행됨

- 2006년 최초로 검색 시간이 데이터베이스에 저장되어 있는 전체 데이터 수에 무관한 대칭키 기반 암호데이터 검색 기술인 SSE가 제안된 이후, 관련 기술 개선을 위한 연구가 진행되고 있음
- 대칭키 기반 암호데이터 검색 기술은 빠른 검색 성능을 제공하는 키워드 검색 위주 연구 결과가 제안되어 왔으나, 데이터 추가/삭제와 같은 동적 데이터 처리를 위한 기본 기능 및 범위 검색 등과 같은 부가 기능 제공의 어려움이 존재
- 2004년 데이터 저장 및 검색 주체가 상이한 환경에서도 암호데이터 검색이 가능한 공개키 기반의 기술이 제안된 이후, 다양한 부가 기능 제공 및 안전성 강화를 위한 연구가 진행되었으나 실제 응용 환경에 적용되기에는 제한된 성능을 제공함
- 공개키 기반 암호데이터 검색 기술은 높은 안전성 및 부가 기능 제공이 용이하지만, 데이터 검색 시간이 데이터베이스에 저장된 데이터 총량에 비례하는 비효율성으로 인해 현실적으로 실제 응용 환경에 적용하기에는 성능적 한계를 지님
- 국내의 암호데이터 검색 기술에 대한 연구는 대학 및 연구소를 중심으로 단편적인 연구가 수행되고 있음
  · 고려대, 포항공대 등 대학을 중심으로 암호데이터 검색 방법에 대한 이론적인 연구가 일부 수행되고 있으나, 단편적인 결과에 머무르고 있음
  · 대부분 기존 기법들의 단순 변형 위주의 단편적인 연구에 그쳐 활용 및 확장에 한계가 있으며, 효율성에 대한 근본적인 취약점이 존재함
  · ETRI는 암호데이터 conjunctive 키워드 검색 등 관련 기술에 대한 IPR을 일부 확보하고 있음
- 향후 암호데이터 검색 기술은 이론적인 안전성 위주의 연구에서 벗어나 현실 적용 가능한 기술 개발을 위해, 효율성을 강조한 대칭키 기반의 암호데이터 검색 기술을 바탕으로 데이터 추가/삭제와 같은 동적 데이터 처리 및 다양한 부가 기능을 제공하는 방향으로 연구가 진행될 것으로 전망됨

O 단순한 암호화 기반의 기밀성 제공에서 벗어난 다양한 암호데이터 처리 서비스의 실현을 위해 이론적으로 다루어졌던 암호데이터 중복 처리 기술, 암호데이터 검색 기술들에 대한 구현 연구가 시도되고 있음
- 신생 업체인 Bitcasa사는 클라우드 스토리지에서 초기 수준의 암호데이터 중복 처리 기술인 convergent encryption을 활용해 파일 단위의 암호데이터 중복 처리 기술을 일부 구현하였으나, 안전성 관점의 문제가 존재함
- Elastic Security사는 클라우드 스토리지 서비스에서의 블록 단위 중복 제거 및 데이터의 기밀성을 보장하기 위한 기본 보안 아키텍쳐를 제안함
- CipherCloud사는 클라우드 환경에서 데이터 암호화 및 인덱싱을 통한 검색 기술을 개발하였으나, 관련 기술의 주요 작업이 게이트웨이에 집중되어 있어 가용성 및 보안성이 취약함
- 미쓰비시사는 클라우드 환경에서 키워드 검색을 수행하는 검색 가능한 암호화 플랫폼을 개발하였으나, 공개키 방식의 검색 기술 활용으로 인해 데이터 처리 성능에 한계가 존재함
- Fujitsu사는 동형 암호를 이용한 암호데이터 검색 기술을 발표하였으나, 암호화된 상태로 검색을 수행한 후 전체를 복호화하는 구조에서 발생하는 성능 문제로 실제 응용 환경 적용이 어려운 상황임

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

O 미래 IoT 환경에서 예상되는 대규모 데이터에 대한 저장 시스템의 안전성과 저장 성능 향상을 위한 원

2. 산업적 기대효과

O 국내 DB 산업은 2011년 이미 10조 이상의 규모를 형성하고 있어, 데이터 보호가 의무화될 시 DB 보호를 위한 기술 필요성이 증대되어 DB 보안 솔루션 산업도 폭발적으로 성장할 것으로 예상됨 (출처 : 한국데이터베이스진흥원, 2011년도 국내 데이터베이스 산업 시장 분석 결과보고서, 2011.12)

- ‘2013년 10대 국가정보화 트렌드’에 따르면, 대량 데이터 활용에 따른 개인정보 유출 가능성을 우려하여 클라우드/빅데이터 활성화의 핵심 선결 과제로 보안 문제를 지적하고 있음 (출처 : 한국정보화진흥원, 2013년 10대 국가정보화 트렌드, 2013.2)
- 빅데이터 및 클라우드 환경에서도 신뢰할 수 있는 데이터 보호 기술의 개발은 결과적으로 해당 산업 시장의 확대 및 조기 정착을 견인할 수 있는 새로운 동력원이 될 것으로 판단됨

O 암호화된 데이터베이스 활용 기술의 고도화를 통해 정보의 기밀성과 활용성을 동시에 제공하여 그 동안 구축하기 힘들었던 공공데이터 활용 서비스 산업의 조속한 활성화 및 이에 따른 고용 촉진을 기대할 수 있음

- 국내에서는 재난 전조 감지, 구제역 예방, 맞춤형 복지 서비스 제공, 물가 관리, DNA, 개인맞춤

형 의료 시스템 구축의 분야까지 활용 범위를 넓혀간다는 구상을 수립하고 있음 (출처 : 국가정보화전략위원회, 빅데이터를 활용한 스마트 정부 구현(안), 2011.10)

3. 경제적 기대효과

O 클라우드/빅데이터 환경에서 데이터 활용을 기반으로 한 서비스 확대 및 새로운 보안 시장 창출을 견인할 수 있음

O 프라이버시 보호에 대한 신뢰성을 확보하여 공공데이터 활용 서비스 시장이 활성화 될 것으로 예상되며, 이에 따른 천문학적 부가효과가 발생될 것으로 예상됨

- 영국은 공공데이터 개방에 따라 약 150억 파운드의 경제적 효과와 2017년까지 58,000개의 신규 일자리가 창출될 것으로 예측 (출처 : 한국정보화진흥원, 창조경제 기반조성을 위한 공공데이터 개방과 활용 사례, 통권 제72호, 2014.3)

4. 사회문제해결 기대효과

O 국내외에서 발생하고 있는 개인정보 유출에 따른 사회적 피해 규모는 수치로 표현할 수 없을 정도로 심각하며, 신용 사회의 근간을 위협한다는 점에서 데이터 유출 방지를 위한 원천 기술 개발은 파급효과가 매우 높음

O 해킹이나 내부 공모자에 의한 데이터 유출의 근본적인 해결책을 제공함으로써, 관련 사건 발생에 따르는 사회적 피해 복구 비용 절감

- 산업연구원의 분석에 따르면, 국내에서 개인정보 유출이나 해킹에 의한 피해액은 2015년 13조 4,000억원에서 2030년 26조, 7,000억원으로 피해 규모가 대폭 증가할 것으로 예상 (출처 : 산업연구원, e-KEIT 산업경제정보, 제 586호, 2014.4)

O 지식정보보안 산업의 트렌드가 개인 및 사회 안전으로 빠르게 진화하면서 주요 사회 인프라 및 공공서비스의 프라이버시 정보 노출 위협에 대한 국민적 불안감 해소

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 및 검색 기술 설계	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 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. 2차년도(2016년) 연구 개발 내용 및 범위

연구 목표	내용
암호데이터 저장 및 검색 기술 설계	가) 연구 개발 목표 O 암호데이터 저장 및 검색 기술 설계 - 암호데이터 중복 처리 기술 • 파일 단위 암호데이터 중복 처리 알고리즘(SW, IPR) • 성능 : 1sec/1MB(1MB 파일 단위 암호데이터 중복 처리를 위한 평문데이터 중복 처리 대비 부가 시간) - 데이터 추가/삭제 기능 제공 동적 암호데이터 검색 알고리즘(IPR) • 검색 성능 : O(n) 미만(n : DB에 저장된 전체 암호데이터 수) 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

2. 연구 개발 추진 체계 및 방법

2-1. 연구 개발 추진 체계

○ 한국전자통신연구원 주도로 암호데이터 저장, 열람 및 검색을 위한 암호 원천 기술 개발
- 암호데이터 저장 분야에서는 암호데이터 중복 처리 기술 및 데이터 자체에 기반한 암호데이터 소유권 검증 기술을 개발
- 암호데이터 검색 분야에서는 이론적인 기술에서 벗어나 현실 적용 가능한 암호데이터 검색 기술을 개발

○ 원천 기술 및 IPR의 전략적 확보
- 국내외 기술 동향 및 환경 변화를 파악하여, 과제에 적극 반영
- 암호데이터 저장, 열람 및 검색 관련 암호 원천 기술 확보
- 개발된 원천 기술을 기반으로 국내외 특허 동향에 대한 면밀한 분석을 통해 우수 IPR의 전략적인 확보 추진

○ 산·학·연 협력을 통한 기술 고도화 추진
- 원천 기술은 한국전자통신연구원 정보보호연구본부를 중심으로 연구
- 국내 학계와의 공동연구를 통해 개발된 기술에 대한 안전성 검증 협력
- 암호데이터 저장 및 검색 기술에 대한 국내외 기술 동향 및 발전 방향 검토를 통한 연차별 목표 점검을 수행하여, 국내외 환경 변화에 능동적으로 대처할 수 있는 기술 개발 수행
- 기술 개발 초기 단계부터 국내 업체와의 긴밀한 협력을 통해 실 서비스 환경의 요구 사항 반영을 반영한 기술 개발 수행
- 암호 포럼 등을 통한 전문가의 의견 청취, 국내외 표준화 동향 파악 및 관련 기관과의 협력을 통한 표준화 참여

○ 민감 데이터 보호를 위한 개인정보보호 관련 정부 정책을 반영한 기술 개발 추진

< 총년도 연구 개발 추진 체계 >

2-2. 2차년도 연구 개발 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 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

2-3. 전년도(2015년) 평가 의견 수정・보완 사항

O 평가 의견 1 : 최종 목표를 위해 연구개발 진행 단계에서 정략적 수치를 고려하면서 진행 필요
- 반영 사항 : 암호데이터 중복 처리 분야의 최종 목표치인 460ms 이하/1MB (1MB 파일 단위 암호데이터 중복 처리를 위한 평문데이터 중복 처리 대비 부가 시간) 달성을 위한 2차년도 구체적인 성능 목표치 1sec 이하/1MB 반영

O 평가 의견 2 : 공동연구기관의 역할 및 연구 내용 구체화 필요
- 반영 사항 : 파일 단위 암호데이터 중복 처리 설계, 안전성 검증 및 성능 최적화 연구를 ETRI와 공동연구기관이 협력하여 개발

O 평가 의견 3 : 기술 개발 목표 설정 및 추진 체계에 수요자(수요기업) 연계 내용을 포함하는 것이 좋을 것으로 판단됨

- 반영 사항 : 수요자 연계 내용을 연구 개발 추진 체계에 반영(국내 업체와의 협력을 통해 실 서비스 요구 사항이 반영된 기술 개발)

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. 성과지표

O 기술 개발 성과 지표

성과지표 (주요성능 Spec)	세계최고 수준	연구최종 목표	'16년 기술 개발 목표치	검증 방법	목표설정 타당성
암호데이터 중복 처리 기술 (기능/성능)	데이터 손실 공격 가능 (460ms/ 1MB)[1]	데이터 손실 공격 방지 (460ms 이하/ 1MB)	파일 단위 암호데이터 중복 처리 알고리즘 (1sec/1MB)	목표 기술에 대한 설계서 및 특허 증빙 자료 제시	암호데이터 중복 처리 기술의 기반이 되는 파일 단위 암호데이터 중복 처리를 위한 핵심 원천 기술 및 IPR 확보를 목표로 설정
암호데이터 검색 기술 (기능/ 검색 성능)	검색 성능 O(n)[2]	검색 성능 O(m)[3]	동적 암호데이터 검색 알고리즘 (O(n) 미만)	목표 기술에 대한 설계서 및 특허 증빙 자료 제시	데이터 추가/삭제가 빈번히 발생하는 동적 환경에서, 사용자 프라이버시를 보호하면서 암호데이터에 대한 검색이 가능한 기술에 대한 원천 IPR 확보를 목표로 설정

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

○ 연구산출물 성과지표

<table>
<tr><th colspan="4">공통지표</th><th colspan="4">자율지표</th></tr>
<tr><th colspan="3">지표명</th><th>총사업연도</th><th>'16년도</th><th colspan="2">지표명</th><th>총사업연도</th><th>'16년도</th></tr>
<tr><td colspan="3">SCI(E) 논문(건)</td><td>9건 (게재 승인 이상)</td><td>3건</td><td>과학적 성과</td><td>표준화된 IF 상위 20% SCI 논문(건)</td><td>1건 (제출 이상)</td><td>-</td></tr>
<tr><td rowspan="5">특허 (건)</td><td rowspan="2">국내</td><td>출원</td><td>9건</td><td>3건 (출원 및 제출)</td><td rowspan="4">기술적 성과</td><td>특허활용률 (기술이전건수/ 특허등록보유건수)</td><td>-</td><td>-</td></tr>
<tr><td>등록</td><td>-</td><td>-</td><td>국제표준특허(건)</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">국제</td><td>출원</td><td>6건 (출원 및 제출)</td><td>2건 (출원 및 제출)</td><td>국제표준승인표준 기고서(건)</td><td>-</td><td>-</td></tr>
<tr><td>등록</td><td>-</td><td>-</td><td>3극 특허(건)</td><td>-</td><td>-</td></tr>
<tr><td colspan="3">기술이전(건)</td><td>-</td><td>-</td><td rowspan="2">경제적 성과</td><td rowspan="2">연구비 대비 기술료 수입(%)</td><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td colspan="3">기술료(억원)</td><td>-</td><td>-</td></tr>
</table>

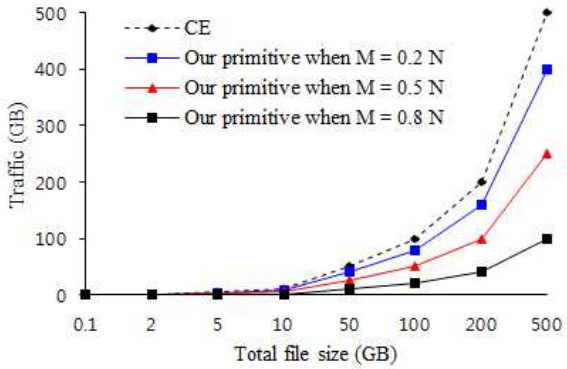
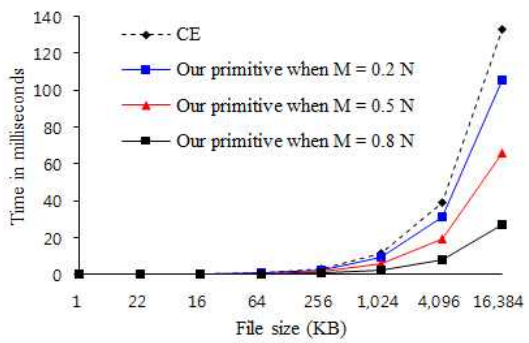
제 3 장 2차년도(2016년) 연구 개발 결과

제1절 2차년도 성과 목표 달성도

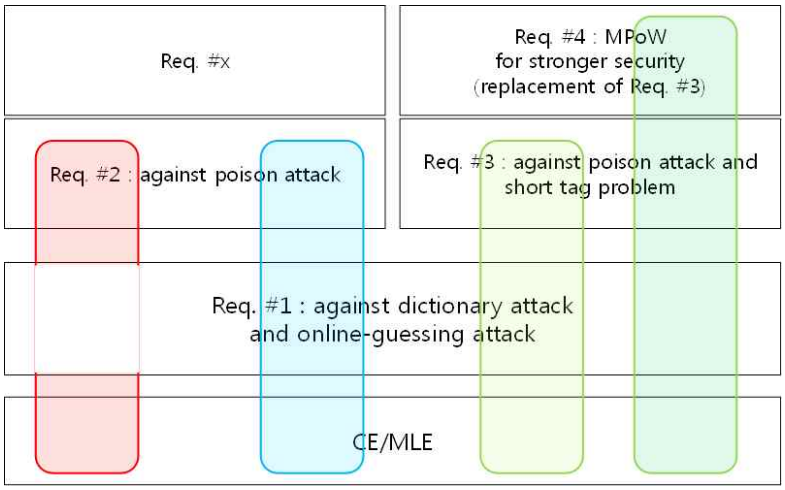
성과지표 (주요성능 Spec)	기술개발 목표치	성과	달성도(%)
암호데이터 중복 처리 기술	파일 단위 암호데이터 중복 처리 알고리즘 (1sec/1MB)	○ **파일 단위 암호데이터 중복 처리 알고리즘 설계** - 보안 요구 사항에 따라 다양한 중복 처리 알고리즘을 선택할 수 있는 구조 - 키 서버, PoW(Proofs of Ownership) 등의 기존의 우수한 중복 처리 기법을 수용하는 파일 단위 중복 처리 알고리즘 설계 - Poison attack, Dictionary attack 등의 역기능을 방지하는 안전성 제공 ○ **파일 단위 암호데이터 중복 처리 검증 SW 개발** - 클라이언트, 서버, 키 서버로 구성된 중복 처리 알고리즘 테스트 프로그램 구현 - 총 11종의 중복처리 알고리즘 구현 - 1MB 평문 파일 대비 암호 파일 업로드 시 부가 시간 : 56ms* * 실험실 內 동일 라우터 및 자체 설계 DB 환경에서 실험 (차년도 실제 네트워크 환경 및 Openstack Swift 적용) ○ **Time-Locked 기반 제어 가능 중복 처리 기술을 이용하여 파일 신원 확인 공격에 대한 안전성 제공** - 서버 주도형의 기존 파일 신원 확인 공격 대응 기술과 달리 사용자가 프라이버시 강도를 조절할 수 있는 구조로 되어 있어 사용자가 자신의 프라이버시 성향에 따라 안전성 강도 선택 가능 - 최초로 업로드 되는 파일을 제외하고 기반 기술과 동일한 성능 제공할 수 있어 매우 효율적으로 파일 신원 확인 공격을 방지할 수 있음	100%
암호데이터 검색 기술	동적 암호 데이터 검색 알고리즘 (O(n) 미만)	○ **동적 암호데이터 활용 환경을 위한 요구 사항 분석 및 안전성 모델 정립** - 암호데이터 검색 기술에 대한 안전성 모델 수정을 통한 서버의 자체적인 검색 인덱스 관리 모델을 제시하고 이에 기반한 동적 환경 및 다양한 부가 기능 제공을 위한 암호데이터 검색 프리미티브 기술 확보	100%

		- 동적 데이터 관리 환경을 위한 서로 다른 공개키로 암호화된 데이터에 대한 동일성 검사가 가능한 공개키 암호화 기술 안전성 모델 정립 및 기술 설계 **O Bloom Filter Tree 기반 동적 암호데이터 검색 기술 설계** - 가공이 용이한 Bloom Filter를 검색 인덱스로 활용하여 Bloom filter tree 구조의 검색 인덱스 설계 방식 제공 - 전체 데이터 수에 대한 sublinear 검색 성능 O(m log n) 제공 * n : 전체 데이터 수, m : 검색된 데이터 수 - Bloom Filter의 중첩 성질과 Counting Bloom Filter 기술 적용을 통해 효율적인 데이터 추가/삭제 기법 제시	
SCI(E) 논문(건)	3건(게재 승인 이상)	O SCI(E) 논문 6건 게재	200%
국내 특허 출원(건)	3건(출원 및 제출)	O 국내 특허 2건 출원 및 1건 제출	100%
국제 특허 출원(건)	2건(출원 및 제출)	O 국제 특허 3건 제출	150%
표준화된 IF 상위 20% SCI 논문(건)	-	O 1건 게재(Information Sciences)	-

제2절 연구 수행 내용 및 결과

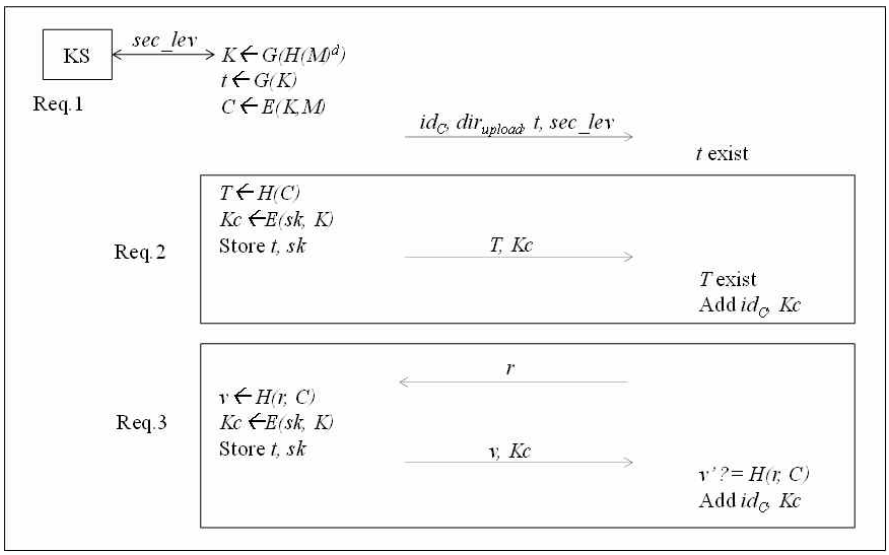
연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	○ 안전성과 효율성을 만족하는 Client-Side 암호데이터 중복 처리 프리미티브 설계 - 데이터 손실 공격(Poison attack)에 대한 안전성 제공 • 데이터 위조 공격에 대한 방지 기능 제공 . 정상 사용자는 공격자에 의해 다른 파일로 대체된 위조 파일을 다운로드 하지 않음 • 데이터 삭제 공격에 대한 방지 기능 제공 . 공격자에 의해 사용자의 원본 파일이 서버에서 삭제되지 않음 • 해쉬 함수의 충돌 저항성 특성에 기반한 안전성 보장 - 네트워크 전송량 및 서버 계산량 감소 • 중복된 데이터 양에 비례하여 네트워크 전송량 감소 . 저장할 전체 데이터(N) 중에서 중복되는 데이터(M) 만큼 비례하여 전송되는 네트워크 트래픽 감소  <데이터 중복 비율에 따른 전송되는 트래픽 양> • 업로드 단계에서 서버는 중복되지 않는 데이터만 태그 계산 . 서버에서의 해쉬 연산 감소로 전체 성능 향상  <데이터 중복 비율에 따른 서버의 해쉬 연산 시간>

연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	○ 파일 단위 암호데이터 중복 처리 알고리즘 설계 - Dictionary attack, Poison attack 등에 대한 역기능을 방지하기 위해 사용자의 보안 수준 선택에 따른 Lego 타입의 설계 방식 적용 • 보안 요구사항에 따라 레고 블록을 조립하는 구조 . Req. #1) Dictionary attack 방지 . Req. #2) Poison attack 방지 . Req. #3) Poison attack과 짧은 태그 사용 문제 방지 . Req. #4) Req. #3 이상의 강한 안전성 요구

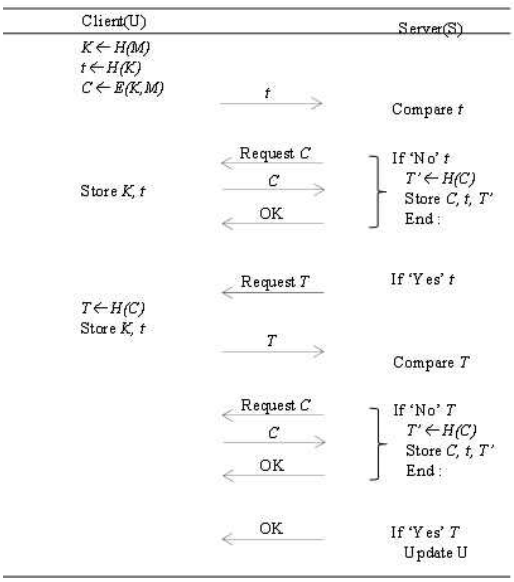
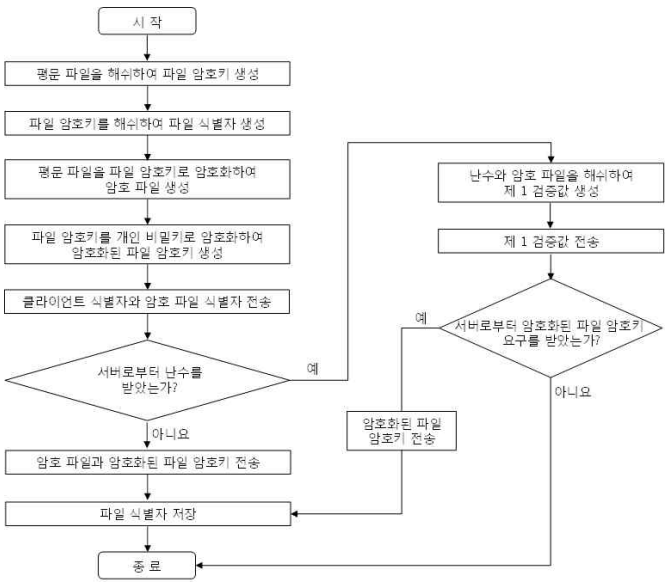


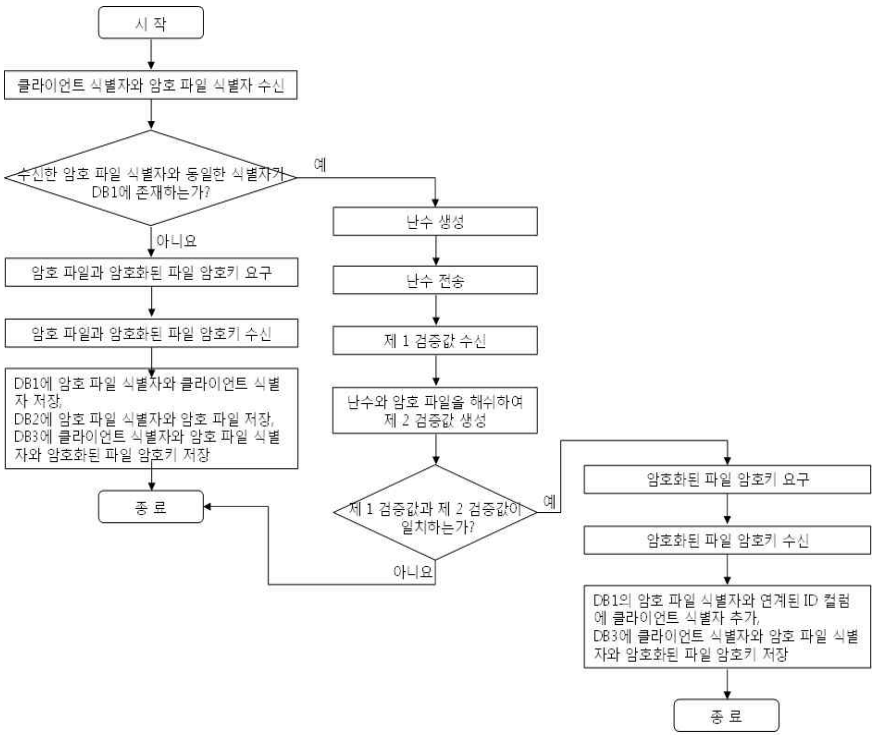
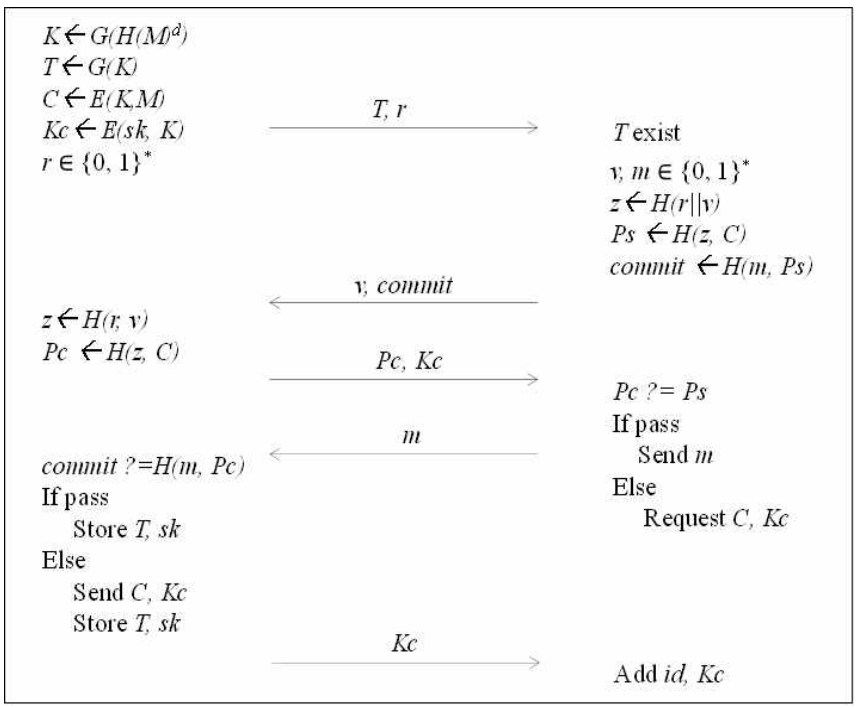
<보안 레벨 조정이 가능한 레고 타입의 설계 방식>

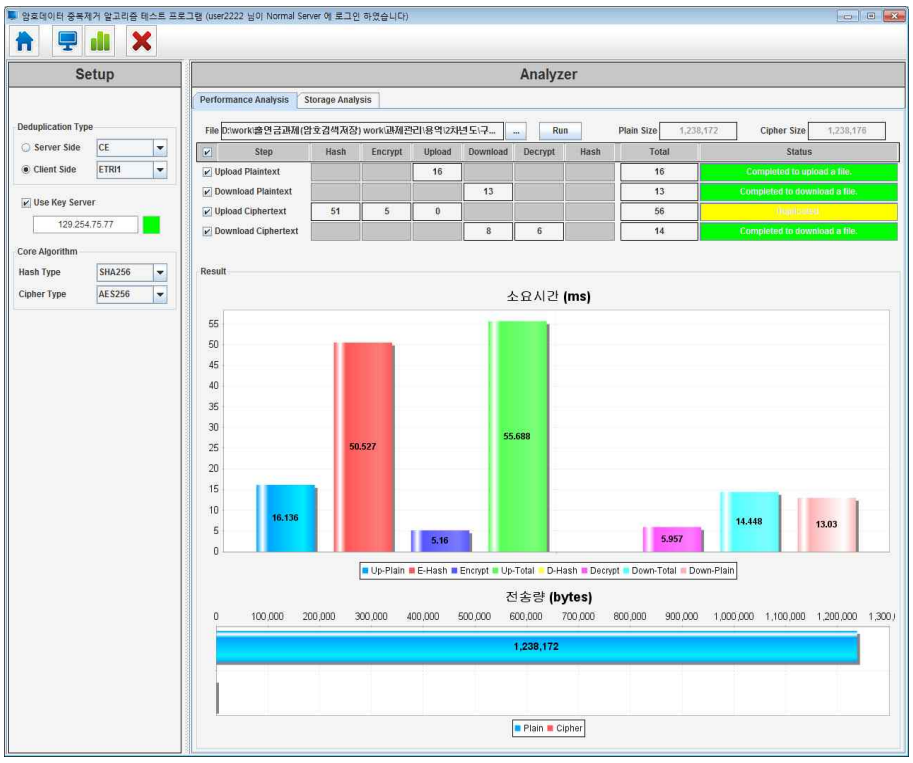
- Client-Side File-level 암호데이터 중복 처리 알고리즘 설계
  • 키 서버, PoW(Proofs of Ownership) 등의 중복 처리 기법과의 자유로운 결합을 통해 효율성 저하 없이 다양한 중복 처리 기법 수용

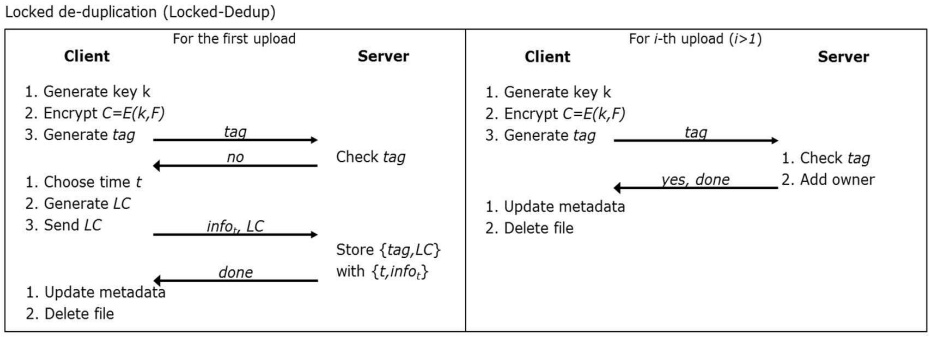


<다양한 보안 요구사항을 만족하는 파일 단위 중복처리 알고리즘>

연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	• 보안 요구사항에 대응하는 구체적인 해결 방법 . Sol. #1) 동일한 데이터는 동일한 키를 사용하는 결정적 암호 문제를 해결하기 위해 RSA-OPRF 프로토콜 적용한 Dupless의 키 서버 사용 Cloudedup 방식의 부가적인 암호화, IBM의 인덱스 서버, Privilege key 및 속성기반 암호 적용 가능성 연구 . Sol. #2) 두 가지 타입의 태그(짧은 키로부터 유도된 태그, 긴 메시지로부터 유도된 태그)를 사용하고, 두 가지 모두 일치하는 경우에만 중복제거 실행  <클라이언트에서의 파일 소유 검증 비교에 의한 암호파일 중복처리 알고리즘> . Sol. #3) Challenge-Response 형태의 클라이언트 파일 소유 유무 검증  <클라이언트에서의 파일 소유 검증 비교에 의한 암호파일 중복처리 알고리즘>

연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	 <서버에서의 파일 소유 검증 비교에 의한 암호파일 중복처리 알고리즘> Sol. #4) Commitment 형태의 양방향 상호 인증 방식  <상호 인증을 이용한 암호 파일 중복처리 알고리즘>

연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	○ 파일 단위 암호데이터 중복 처리 검증 SW 개발 - 목표 • Poison attack과 Dictionary attack을 방지하는 파일 단위 중복처리 SW 개발 • 성능 : 1MB 평문 파일 대비 암호 파일 업로드 시 부가 시간 < 460ms - 실험방법 • Java + Openssl crypto library를 이용한 클라이언트, 서버, 키 서버 구현 • 실험실 內 동일 라우터 사용 (차년도 실제 네트워크 환경에서 적용) • 자체 설계 DB 사용 (차년도 Openstack Swift 적용) - 결과 • 평문 및 암호문 업로드 시간 : 16ms . 실제 네트워크 환경에서 증가할 것으로 예상됨 • 암호 파일 중복처리를 위한 부가 연산 시간 : 56ms . 실제 네트워크 환경에서도 유사한 시간이 예상됨 • 파일 중복 시 암호 파일은 업로드 없음  <암호 파일 중복처리 검증 프로그램>

연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	○ 파일신원 공격에 안전한 Time-Locked 기반 제어 가능 중복처리 프로토콜 설계 - 본 연구 결과로 개발된 신원 확인 공격 대응 기술은 사용자가 본인의 프라이버시 강도를 조절할 수 있는 구조로 되어 있어 사용자가 자신의 프라이버시 성향에 따라 안전성 강도를 조정할 수 있음  <제어가능 중복처리 프로토콜> • 사용자가 본인이 저장하는 데이터에 대해 중복 처리 제한 시간을 선택할 수 있도록 구성된 기술로써 일종의 시간봉인(time-lock) 기능을 활용하여 설계됨 • 카운터 기반의 대응 기술에서는 서버가 관리하는 카운터를 통해 특정 파일이 중복 처리에 활용되는 시점을 확인하는 형태이기 때문에 중복 처리 제한에 대한 강제성이 없었으나, 본 연구 개발 기술의 경우 정해진 시간 간격으로 특정 정보를 생성하는 시간 서버(time server)에서 매 시간 공개하는 정보를 기반으로 중복 처리 활용이 가능하도록 기술적으로 강제하는 기술임 • 시간 서버가 공개하는 정보는 각 시간에 대응되는 일종의 타원곡선 기반의 서명 값에 해당하는 정보로 시간 서버의 비밀키를 알지 못하면 생성할 수 없는 값임. 안전성 관점으로, 시간에 대응되는 비밀 정보를 시간 서버의 도움 없이 생성하는 것은 서명 위조와 동일한 강도의 안전성 제공함 - 임의의 Client-Side 중복 처리 기법에 쉽게 적용할 수 있는 기술로, 파일 신원 확인 공격에 취약한 각 파일별 초기 업로드 시점을 제외하고 기반이 되는 중복 처리 기법의 성능을 유지하는 구조로 설계되어 성능 면에서는 일반적인 중복 처리 기법과 거의 유사한 성능 제공 • 파일별로 초기 업로드하는 사용자의 경우, 시간을 기준으로 중복 처리 제한을 설정하기 위한 부가 비용이 발생함 • 중복 처리 제한이 설정된 파일의 경우 중복 처리 가능한 데이터에 추후 설정 변경을 지원하기 위한 데이터가 추가되나, 이는 고정된 짧은 상수 길이의 데이터로 전체 저장량에 큰 영향을 미치지 않음

연 구 내 용	연 구 결 과

암호데이터 중복 처리 기술 설계

	Cost for the first upload				
	Computational Cost		Size of Message		# of Round
	Server	Client	Server	Client	
No-Dedup	-	C_E+C_{Tg}	-	$\ell_T+\ell_F$	2
SS-Dedup	C_{Tv}	$C_K+C_E+C_{Tg}$	-	$\ell_T+\ell_F$	2
CS-Dedup	C_S+C_{Tv}	$C_K+C_E+C_{Tg}$	-	$\ell_T+\ell_F$	4
CS-Dedup$^+$	C_S+C_{Tv}	$C_{KS}+C_E+C_{Tg}$	-	$\ell_k+\ell_T+\ell_F$	6
Locked-Dedup	C_S	$C_K+C_E+C_{Tg}+C_L$	-	$\ell_T+\ell_F+\ell_t$	4
Locked0Dedup$^+$	C_S	$C_{KS}+C_E+C_{Tg}+C_L$	-	$\ell_k+\ell_T+\ell_F+\ell_t$	6

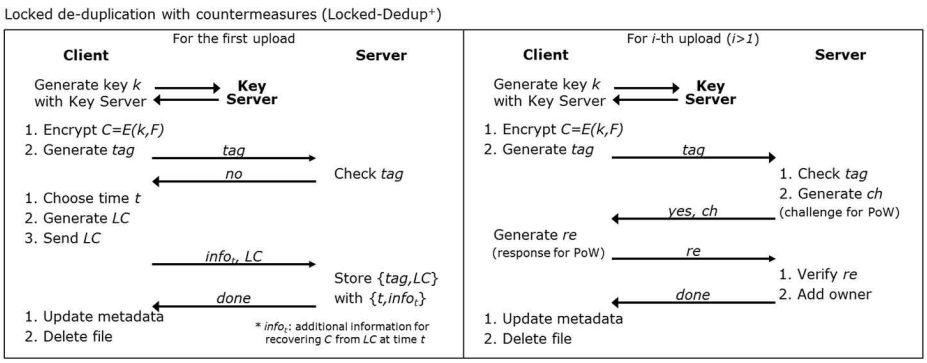
<Time-Locked 중복처리에서의 최초 사용자 처리 비용>

- 중복 처리 가능한 형태로 저장된 데이터에 대한 업로드 요청 시, 일반적인 데이터 업로드 과정과 동일하게 수행되어 연산량 및 전송 데이터의 길이 등의 비용이 일반적인 중복 처리 과정과 동일하게 소요됨

	Cost for the i-th upload $(i>1)$				
	Computational Cost		Size of Message		# of Round
	Server	Client	Server	Client	
No-Dedup	-	C_E+C_{Tg}	-	$\ell_T+\ell_F$	2
SS-Dedup	C_{Tv}	$C_K+C_E+C_{Tg}$	-	$\ell_T+\ell_F$	2
CS-Dedup	C_S	$C_K+C_E+C_{Tg}$	-	ℓ_T	2
CS-Dedup$^+$	$C_S+C_{PoW\text{-}S}$	$C_{KS}+C_E+C_{Tg}+C_{PoW\text{-}C}$	ℓ_c	$\ell_k+\ell_T+\ell_r$	6
Locked-Dedup	C_S	$C_K+C_E+C_{Tg}$	-	ℓ_T	2
Locked0Dedup$^+$	$C_S+C_{PoW\text{-}S}$	$C_{KS}+C_E+C_{Tg}+C_{PoW\text{-}C}$	ℓ_c	$\ell_k+\ell_T+\ell_r$	6

<Time-Locked 중복처리에서의 사용자 처리비용>

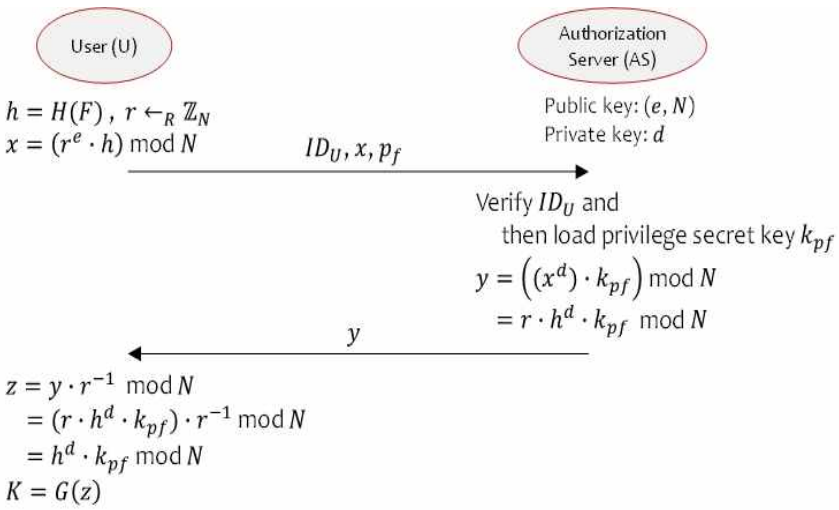
- 파일 신원 확인 공격 외의 위협에 대응하기 위해 기존에 알려진 대응 기술들을 동시에 적용할 수 있어 기존 보안성 강화 기술들과 함께 사용하여 다양한 공격에 대응하는 안전한 중복 처리 서비스 제공 가능

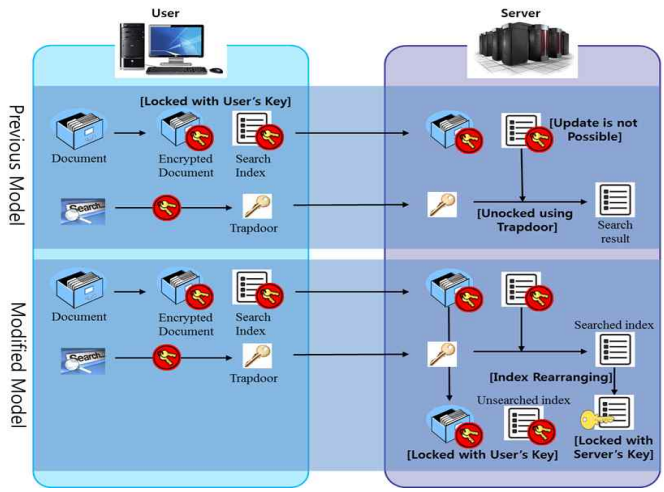


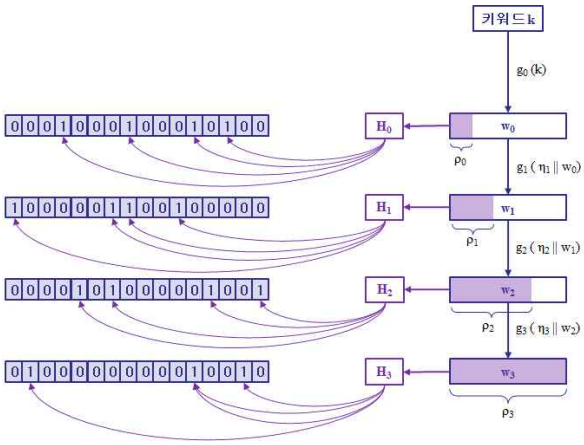
<알려진 공격에 안전한 제어가능 중복처리 프로토콜>

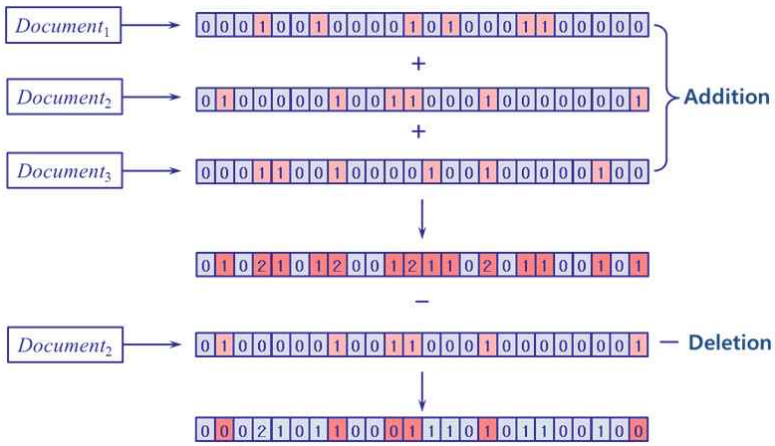
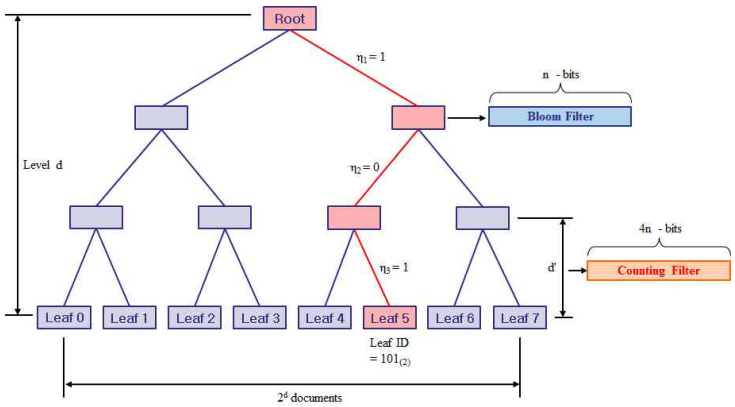
- 제안 기술은 기존에 동일 파일이 저장되어 있지 않은 경우에 한하여 동작하는 것이므로 중복 처리 기능에 영향을 미치지 않고, 동일 파일이 저장되어 있는 경우에는 일반적인 중복 처리 기법이 동일하게 동작하므로 기존의 중복 처리 기술의 안전성 향상 기술을 적용함에 있어 제약이 따르지 않음

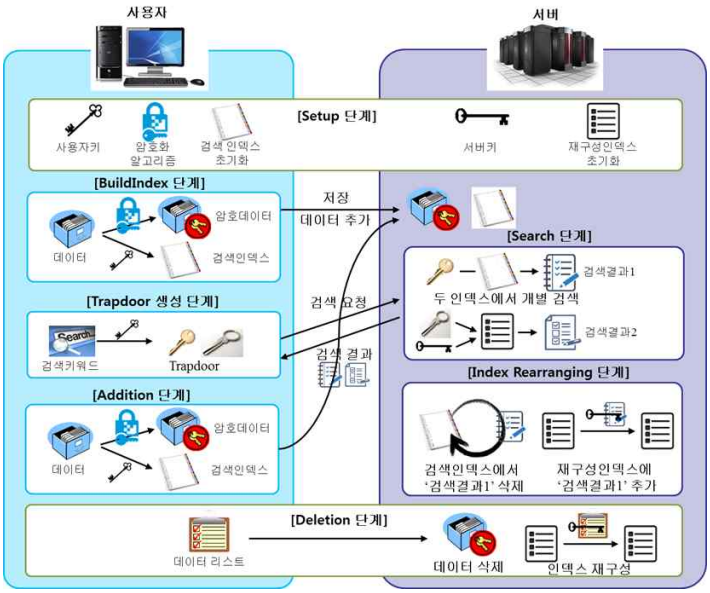
연 구 내 용	연 구 결 과
암호데이터 중복 처리 기술 설계	• 전수 조사 형태의 공격에 대응하기 위한 기술로, 파일에 대응되는 키 생성을 지원하는 보조 서버를 도입하여 데이터에 대한 키를 무작위로 추정하여 시도할 수 있는 다양한 형태의 공격을 약화시킬 수 있음 • 실제 데이터 소유하지 않은 사용자가 특정 데이터에 대한 소유권 획득하는 문제를 대응하기 위해 소유권 증명 기술을 도입하여 적법한 사용자에게만 소유권 부여하는 기능 제공 가능
암호데이터 소유권 검증 모델 연구	○ 암호데이터 소유권 검증 기술 분석 - 기존의 암호데이터 중복 처리 서비스 기술에서는 동일 파일을 가지고 있는 사용자의 경우 동일한 키를 생성할 수 있는 특성을 기반으로 설계됨 • 동일한 데이터도 다른 키를 사용하면 상이한 암호문으로 생성되기 때문에 이론적으로 중복되는 데이터가 발생할 수 없기 때문에 데이터에서 키가 생성되는 방식으로 설계되어 있음 - 중복 처리 서비스 제공을 위해 기본적으로 요구되는 특성이 해당 서비스의 취약점의 근본적인 원인이 됨 • 동일한 파일에 동일한 키가 할당되는 특성으로 인해, 낮은 엔트로피를 가지는 파일의 경우 파일을 추측하고 대응되는 키를 생성할 수 있음 • 무분별한 데이터 추측을 통한 키 생성으로 인한 공격에 대응하기 위한 기술로 키 생성 서버를 사용하기도 함 • 키 서버는 파일에 대응되는 키를 생성하는 방식을 함수 형태로 공개되어 누구나 계산 가능한 형태로 제공하지 않고, 키 서버에 의해서만 계산 가능한 값을 생성 - 데이터에 동일한 키가 대응되는 구조는 특정 스토리지 서버가 다수의 사용 그룹에 스토리지 서비스를 제공하는 서비스 그룹 간 보안 특성 차이에 의해 의도치 않은 취약점이 발생할 수 있음 • 상기 기술된 취약점이 동일 서비스 그룹 내의 문제에서 타 서비스 그룹을 포함한 대상에서의 문제로 위협이 파급됨 • 서비스 그룹별로 다른 수준의 보안 서비스를 제공할 수 있어서, 동일 스토리지를 사용하는 서비스 그룹 중에서 낮은 수준의 보안을 제공하는 서비스 그룹에서 제공하는 수준으로 해당 스토리지 사용하는 전체 서비스 그룹의 보안 강도가 낮아질 수 있음 • 능동적인 공격자의 경우, 악의적으로 공격 대상 서비스 제공 서버와 동일한 스토리지 서버에 접근해 데이터 중복 처리 기능에서 발생하는 특성 기반의 공격을 시도할 수 있음 • 기대하는 수준의 보안 수준과 실제 제공될 수 있는 보안 수준이 다른 것은 스토리지 서비스의 안전성 측면에서 매우 큰 문제점이 될 수 있음

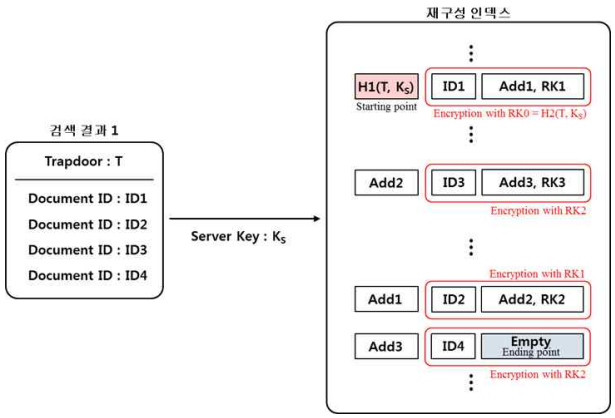
연 구 내 용	연 구 결 과
암호데이터 소유권 검증 모델 연구	○ 권한에 기반한 암호데이터 소유권 검증 및 중복 처리 프로토콜 설계 - 제안 기술은 동일 스토리지 서버 내에서도 서비스 그룹에 따라 별도의 권한을 부여함으로써, 다른 서비스 그룹에 존재하는 동일 파일에 의한 안전성 훼손을 방지하고 독립적인 보안 서비스 유지가 가능함 • 파일에 대응되는 키를 생성하는 방식으로는 DupLess에서 도입된 키 서버 기반의 방식을 사용함으로써 동일 파일에 동일 키 값이 생성되도록 구성 • 서비스 그룹별로 상이한 키를 생성함으로써 그룹 간에 동일한 키가 사용되는 것을 방지하여, 타 그룹에서 저장한 동일 데이터에 의한 보안 위협을 방지할 수 있음 (아래 그림은 권한별 키 생성 방법)  <암호데이터 중복처리를 위한 권한별 키 생성 프로토콜> - 각 파일이 저장되는 최대 개수는 서비스 그룹의 수와 동일하여 실제 중복 처리로 인한 저장 공간 관리 비용 개선 효과는 감소하나, 타 그룹과 동일 파일 저장함으로 인해 발생하는 안전성 문제가 해결됨 • 서버가 각 서비스 그룹별로 별도의 데이터 관리를 하는 정책적인 해결 방법도 존재하나, 해당 정책의 반영을 통해 비용 증가가 야기되어 기술적으로 강제할 수 있는 방법이 바람직함 • 제안 기술에서는 키 생성 서버와 스토리지 서버가 상이하게 구성되어 있어 스토리지 서버가 다른 권한으로 암호화된 파일은 동일 파일에 대해 타 권한으로 암호화된 파일과 다른 파일로 인식하게 되어 권한별 스토리지 분리가 기술적으로 제공됨

연 구 내 용	연 구 결 과
동적 환경을 위한 암호데이터 검색 기술 설계	○ 동적 암호데이터 검색 기술에 대한 안전성 모델 정립 - 기존 암호데이터 검색 기술의 안전성 모델은 동적으로 데이터가 변화하는 환경에 비효율적임 • 암호데이터 검색 기술은 데이터에 대한 암호화와 동시에 검색을 위한 '검색인덱스'를 추가로 생성 • 검색인덱스는 저장된 데이터의 핵심 키워드에 대한 정보를 포함하고 있기 때문에 데이터 기밀성 보장을 위해 별도의 암호화 과정이 요구됨 • 기존 암호데이터 검색 기술은 저장된 데이터에 대한 높은 기밀성 제공을 목적으로 설계되어 검색인덱스의 생성/확인/수정의 모든 과정이 사용자의 비밀키에 기반하여 처리 • 높은 검색 효율성 제공을 위해 데이터 사이의 연관성에 기반한 검색인덱스 설계 방식이 주로 사용하는데, 이 경우 데이터가 추가/삭제되는 경우 해당 데이터와 연관된 모든 검색인덱스에 대한 수정이 요구되기 때문에 검색인덱스의 수정 과정에 사용자가 참여하는 기존의 모델은 비효율적임 - 암호데이터 검색 기술에 대한 적용 환경 및 안전성 요구조건 분석을 통해 새로운 안전성 모델 제시 • 기존 암호데이터 검색 기술에서는 데이터 서버를 잠재적인 공격자로 설정하며, 높은 안전성 제공을 위해 데이터 서버에 제공되는 비밀 정보를 최소화하도록 설계됨 • 하지만, 데이터 검색이 서버에 의해서 이루어지기 때문에 한 번 검색된 데이터에 대한 일부 정보는 서버에 의해 수집 가능 • 사용자가 제공한 검색인덱스에서 한 번 검색이 수행된 부분의 인덱스를 분리하여 관리하는 안전성 모델 제시  <동적 암호데이터 검색 기술을 위한 안전성 모델>

연 구 내 용	연 구 결 과
동적 환경을 위한 암호데이터 검색 기술 설계	• 서버는 검색인덱스에서 검색에 활용된 부분 인덱스를 자체적으로 재구성하고 서버의 비밀키로 기밀성을 제공하여 동적인 데이터 활용 환경에서 검색인덱스 수정 과정을 서버 단독으로 수행 • 기존 암호데이터 검색 기술의 안전성을 훼손하지 않으면서 서버에 의한 검색인덱스 관리 기능 제공을 통해 높은 활용성 제공이 가능 ○ 데이터 추가/삭제가 자유로운 동적 환경을 위한 효율적인 암호데이터 검색 기술 설계 - Bloom Filter Tree 기반의 검색 인덱스를 활용한 동적 암호데이터 검색 기술 설계 • Bloom Filter는 집합에서 원소의 포함 관계를 효율적으로 확인 가능한 데이터 구조로 Tree의 각 노드가 Bloom Filter로 구성되는 Bloom Filter Tree 구조의 검색 인덱스 구성을 통해 O(m log n)의 암호데이터 검색이 가능  <Bloom filter 기반 암호데이터 검색 인덱스 생성 알고리즘> • Bloom Filter 기반의 검색 인덱스는 각각의 키워드에 대한 해쉬 연산을 통해 얻어진 Bloom Filter의 한 원소의 값을 1로 변환하는 방식으로 구성되기 때문에, 서로 다른 키워드를 포함하는 두 Bloom Filter에 대한 Bitwise-OR 연산을 통해 두 키워드를 포함하는 Bloom Filter가 생성 • Bitwise-OR 연산을 통한 Bloom Filter 중첩을 활용하여 자유로운 데이터 추가 기능을 제공 • 각각의 원소가 하나의 bit 정보로 표현되는 기본적인 Bloom Filter를 각각의 원소가 일정 범위의 정수로 표현되는 Counting Bloom Filter로 확장하고, 각 원소 단위의 덧셈/뺄셈을 활용하여 데이터에 대한 추가/삭제 기능을 제공하는 검색 인덱스 갱신 방법 제시

연 구 내 용	연 구 결 과
동적 환경을 위한 암호데이터 검색 기술 설계	 <Counting Bloom filter를 활용한 데이터 추가/삭제> • 검색 인덱스에 대한 저장 효율성을 위해 일반 Bloom Filter와 Counting Bloom Filter를 융합한 Bloom Filter Tree 구성  <Bloom filter tree 구조> • Bloom Filter Tree를 활용한 검색 인덱스 구성으로 O(m log n)의 검색 성능을 제공하면서 자유로운 데이터 추가/삭제가 가능한 암호데이터 검색 기술 설계 | | [Goh04] | [CGK06] | [KPR12] | Ours | |---|---|---|---|---| | Index Size | O(n) | O(n+k) | O(n+k) | O(n) | | Search Time | O(n) | O(m) | O(m) | O(m log n) | | Basic Structure | Bloom Filter | Linked Chain | Linked Chain | Bloom Filter Tree | | Dynamic Update | Static | Static | O(1) | O(1) | | | | | - O(n) size deletion table 필요 - linked chain의 update를 과정에서 일부 security 훼손 | - Counting bloom filter 사용을 통한 deletion | <Bloom filter tree를 활용한 동적 암호데이터 검색 기술 비교>

연 구 내 용	연 구 결 과
동적 환경을 위한 암호데이터 검색 기술 설계	- 개선된 안전성 모델을 바탕으로 검색 인덱스 재구성을 통한 효율적인 데이터 추가/삭제가 가능한 암호데이터 검색 기술 설계안 제시 • 기존 암호데이터 검색 기술에서 데이터에 대한 기밀성 보장을 위해 검색 인덱스는 사용자의 비밀키에 의해서 암호화되며, 서버 등의 다른 주체에 의한 수정이 용이하지 않음 • 암호데이터에 대한 검색 과정에서 검색에 활용된 검색인덱스에 대한 일부 정보는 서버에 공개되기 때문에 공개된 부분 인덱스에 대한 안전성 모델 수정을 통해 효율적으로 검색인덱스를 관리할 수 있는 기법 설계 • 검색에 활용된 부분 인덱스를 기존의 검색인덱스에서 분리하여 서버가 재구성하는 인덱스 재구성 기법 제시 • 사용자가 제공한 검색인덱스와 서버가 구성한 재구성인덱스를 동시에 활용하는 검색 기법 설계를 통해 동일한 키워드 검색에 대해 사용자가 제공한 검색인덱스 만을 사용한 검색 보다 빠른 검색 가능  <검색인덱스 재구성을 통한 암호데이터 검색 기술 개념도> • 한 번 검색된 데이터에 대한 인덱스 재구성 과정에서 기존의 검색인덱스에서 삭제되기 때문에 데이터 추가의 경우 사용자는 신규 데이터와 동일한 검색인덱스 생성 • 재구성된 인덱스는 서버의 비밀키를 통해 기밀성이 보장되어 재구성인덱스에 포함된 데이터 대한 삭제 과정은 서버에 의한 독자적인 인덱스 수정 과정으로 수행 • 검색 인덱스 재구성 방식 변화를 통해 다양한 추가 기능 제공을 위한 기술적 토대 제공

연 구 내 용	연 구 결 과
동적 환경을 위한 암호데이터 검색 기술 설계	 <Linked List를 이용한 검색인덱스 재구성 기법> ○ 동적 데이터 관리 환경을 위한 서버 간 암호데이터 비교 기술 개발 - 동일성 검사 기능을 제공하는 공개키 암호화 기술(PKEET - Public Key Encryption with Equality Test)에 대한 안전성 모델 정립 • Equality test 기능을 제공하는 공개키 암호화 기술(PKEET - Public Key Encryption with Equality Test)은 서로 다른 공개키로 암호화된 데이터 사이의 데이터 활용을 가능하게 하는 기술로 2010년 이후 연구가 활발히 이루어지고 있음 • 데이터를 하나의 서버에 집중하지 않고 복수의 데이터베이스에 분산 저장 및 활용하는 동적 데이터 관리 환경을 위한 프리미티브 보호 기술 • 서로 다른 기관이 보유하는 민감 정보를 데이터 프라이버시 침해 없이 활용 가능 • 기존의 PKEET 기술은 랜덤 오라클 모델을 사용한 안전성 증명에 기반하고 있어, 현실적 활용을 고려한 표준 모델에 기반한 PKEET 기술 설계 연구 수행 • Post-quantum 암호를 고려한 Lattice 기반 문제 등을 활용한 PKEET 기술 설계 연구 수행 • 기존 PKEET 기술에 대한 안전성 분석을 통해 취약점을 제시하고 이에 대한 계산 효율성과 저장 효율성을 유지하면서 안전성을 개선한 기법 설계 - 임의의 CDH 가정에 기반한 PKEET 기술 설계를 위한 일반적인 구성 방법 제시 • 임의의 CDH 가정에 기반한 공개키 암호데이터 검색 기술에 대해, 서버 간 암호데이터 비교 기능을 제공하는 일반적인 구성 방법 설계 • Trapdoor 제공 여부를 기반으로 Type-I, Type-II 공격자 모델 제시

연 구 내 용	연 구 결 과
동적 환경을 위한 암호데이터 검색 기술 설계	• 랜덤 오라클 모델에서 Type-1 공격자에 대한 OW-ID-CCA2 안전성과 Type-2 공격자에 대한 IND-ID-CCA2 안전성을 최초로 달성하는 PKEET 설계

		[19]	[18]	[12]†	Ours
Comp of	Enc	3Exp	5Exp	6Exp	6Exp + 2SE
	Dec	3Exp	2Exp	5Exp	3Exp + 2SE
	Test	2Pairing	4Exp	2Pairing + 2Exp	2Exp + 2SE
Size of	PK	$\|\mathbb{G}\|$	$2\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	$3\|\mathbb{G}\|$
	CT	$3\|\mathbb{G}\| + \|\mathbb{Z}_p\|$	$4\|\mathbb{G}\| + \|\mathbb{Z}_p\| + 2\lambda$	$5\|\mathbb{G}\| + \|\mathbb{Z}_p\|$	$2\|\mathbb{G}\| + 10\lambda$
	TD	–	$\|\mathbb{Z}_p\|$	$\|\mathbb{Z}_p\|$	$\|\mathbb{Z}_p\|$
Security	Type-I	OW-CCA2	OW-CCA2	OW-CCA2	OW-CCA2
	Type-II	–	IND-CCA2	IND-CCA2	IND-CCA2
Assumptions		CDH	CDH	CDH	CDH

<PKEET 기술 성능 및 안전성 비교>

• 동일성 검사 기능을 제공하는 ID 기반 암호화 기술(IBEET : ID-Based Encryption with Equality Test)로 확장 설계 방식 제시

		IBEKS ([1]+[14])	IBEET ([11])	Ours (with BF-IBE [4])
Comp of	Enc	7Exp	6Exp	6Exp
	Dec	-	2Pairing+2Exp	3Pairing+2Exp
	Test	4Pairing	4Pairing	2Pairing+2Exp
Size of	PK	$15\mathbb{G}$	$2\mathbb{G}$	$4\mathbb{G}$
	CT	$4\mathbb{G}+\mathbb{G}_T$	$4\mathbb{G}+\mathbb{Z}_p$	$2\mathbb{G}+5\|\mathcal{H}\|$
	TD	$12\mathbb{G}$	$\mathbb{G}$	$\mathbb{G}$
Fun	KS	Yes	Yes	Yes
	ET	No	Yes	Yes
Security		IND-ID-CPA	OW-ID-CCA2	IND-ID-CCA2
ROM		No	Yes	Yes
Assumption		ℓ-DBDHE & aug ℓ-DL	BDH	BDH

<IBEET 기술 성능 및 안전성 비교>

제3절 연구 성과

1. 연구 결과의 질적 우수성

O 암호데이터 중복 처리 기술 설계

- Lego 타입의 파일 단위 암호데이터 중복 처리 알고리즘 설계
  - 형상에 따라 여러 방식으로 레고 블록을 조립하는 것처럼, 보안 요구사항에 상응하는 중복 처리 알고리즘을 선택, 결합할 수 있는 구조
  - Dupless 방식의 키 서버, PoW(Proofs of Ownership) 등의 기존의 우수한 중복 처리 기법을 수용하는 파일 단위 중복 처리 알고리즘 설계
  - 사용자의 보안 레벨 선택에 따라 Dictionary attack, Poison attack 등에 대한 역기능을 방지하는 안전성 제공

- 암호데이터 중복 처리 알고리즘 구현 및 성능 평가 프로그램 개발
  - 파일 단위 중복처리 알고리즘 테스트 프로그램 개발
    * 클라이언트, 서버, 키 서버로 구성된 암호데이터 중복 처리 시뮬레이션
    * 7종의 Client-side 및 4종의 Server-side 중복처리 알고리즘 구현 (알고리즘 추가 가능)
    * 알고리즘별 업로드(파일 암호 및 태그 생성 포함), 다운로드(파일 복호 및 태그 검증 포함), 중복제거 기능 수행
  - 암호 데이터 중복 처리 알고리즘 성능 평가
    * 평문 파일과 대비하여 암호 파일 중복처리에 필요한 부가 시간 측정
      (평문 파일 업로드/다운로드, 암호 파일 업로드/다운로드/중복 처리 시간 측정)
    * 타입별/알고리즘별 업로드/중복처리時 데이터 전송량 및 스토리지 사용량 그래프 제공

- 최초로 사용자 중심의 파일 신원 공격 대응 제공하는 제어 가능 중복 처리 기술 개발하여 파일 신원 확인 공격에 대한 안전한 서비스 제공 가능
  - 파일 신원 확인 공격(identification attack)은 공격자가 서버 DB에 데이터의 존재여부를 확인함으로써 시도할 수 있는 공격으로 사용자의 프라이버시를 크게 훼손할 수 있음
  - 기존의 파일 신원 확인 공격에 대한 대응 방식은 서버 주도형 방식으로 안전성 결정하는 변수를 프라이버시 보호 대상인 사용자 측에서 관여할 수 없는 구조로 되어 있음
  - 본 기술은 기존 기술과 달리 사용자가 본인의 프라이버시 강도를 조절할 수 있는 구조로 되어 있어 사용자가 자신의 프라이버시 성향에 따라 안전성 강도를 조정할 수 있음
  - 최초로 업로드 되는 파일을 제외하고 기반 기술과 동일한 성능 제공할 수 있어 매우 효율적으로 파일 신원 확인 공격을 방지할 수 있음

O 동적 환경을 위한 암호데이터 검색 기법 개발

- 동적 암호데이터 활용 환경을 위한 요구 사항 분석 및 안전성 모델 정립
  - 기존 암호데이터 검색 기술 안전성 모델에 대한 수정을 통해 검색 인덱스에 대한 효율적인 관리가 가능한 신규 안전성 모델 제시
  - 동일성 검사가 가능한 공개키 암호화 기술에 대한 안전성 모델 분석을 통해 기존 기법의 안전성 문제 제시 및 개선안 설계

- Bloom Filter Tree 기반의 동적 암호데이터 검색 기법 설계
  • 가공이 용이한 Bloom filter를 검색 인덱스로 활용하여 검색 시간이 암호데이터 전체 수에 무관한 sublinear 검색 시간을 제공하는 Bloom Filter Tree 기반의 암호데이터 검색 프리미티브 기술 설계
  • Bloom Filter의 중첩 성질을 이용한 데이터 추가 및 Counting Bloom Filter를 이용한 효율적인 데이터 삭제 기능 제공
- 개선된 안전성 모델을 바탕으로 검색 인덱스 재구성을 통한 암호데이터 검색 기술 설계안 제시
  • 암호데이터에 대한 안전성 훼손 없이 검색 과정에 활용된 부분 인덱스의 정보를 활용하여 서버가 독자적인 검색 인덱스를 재구성하는 방안 제시
  • 사용자의 개입이 요구되는 검색 인덱스 수정 과정의 비효율성을 제거하여 동적 암호데이터 활용 환경을 위한 효율적인 암호데이터 검색 인덱스 관리 기술 제공
  • 인덱스 재구성 과정에서 다양한 부가 기능 추가가 용이한 프리미티브 기술 확보
- 동일성 검사 기능을 제공하는 공개키 암호화 기술(PKEET)의 일반적인 설계 방법 제시
  • 임의의 CDH 가정에 기반한 공개키 암호데이터 검색 기술에 대해, 서버간 암호데이터 비교 기능을 제공하는 semi-generic 구성 방법 설계
  • 기존 기법에 비해 유사한 성능에서 강화된 안전성을 제공하는 PKEET 설계 방식

O Information Sciences (IF 상위 20% SCI) 게재 등 SCI(E) 논문 6건 게재

2. 정량적 연구 성과

O 논문 실적

번호	구분	논문명	논문발표학회명 또는 게재지	년도, 권호	SCI(E) 등재 여부
1	게재	Semi-generic transformation of revocable hierarchical identity-based encryption and its DBDH instantiation	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	2016, E99-A(1)	SCI(E)
2	게재	Explicit formulae for Mastrovito matrix and its corresponding Toeplitz matrix for all irreducible pentanomials using shifted polynomial basis	Integration - the VLSI journal	2016, 53	SCI(E)
3	게재	Symmetric searchable encryption with efficient range query using multi-layered linked chains	Journal of Supercomputing	2016, 72(11)	SCI(E)
4	게재	Efficient multiplication based on Dickson bases over any finite fields	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	2016, E99-A(11)	SCI(E)
5	게재	CCA2 attack and modification of Huang et al's public key encryption with authorized equality test	Computer Journal	2016, 59(11)	SCI(E)
6	게재	Semi-generic construction of public key encryption and identity-based encryption with equality test	Information Sciences	2016, 372	SCI(E) (IF 상위 20% 저널)
7	발표	Authorized convergent encryption for client-side deduplication	MobiSec 2016	2016	비SCI(E)

O 국제 특허

번호	구분	특허명	출원번호	출원국	출원일
1	국외		PR20160549US (출원 중)	미국	2016. 9. 5 (제출일)
2	국외		PR20160562US (출원 중)	미국	2016. 9. 8 (제출일)
3	국외		PR20161030US (출원 중)	미국	2016.11.25. (제출일)

O 국내 특허

번호	구분	특허명	출원번호	출원국	출원일
1	국내		10-2016-143636	한국	2016. 10. 31
2	국내		10-2016-0149839	한국	2016. 11. 10
3	국내		PR20161030KR (출원 중)	한국	2016.11.25. (제출일)

O 기술문서

번호	구분	제목	주요 내용	등록 일시
1	TDP	암호화된 데이터베이스에서의 데이터 저장 및 검색을 위한 암호 원천 기술 개발 요구사항정의서 V2.0	암호데이터 저장 및 검색을 위한 암호 원천 기술 개발 사용자 및 시스템 요구 사항 정의	2016. 11. 24
2	TDP	암호데이터 중복 처리 기술 설계서 V2.0	파일 단위 암호데이터 중복처리 알고리즘에 대한 설계	2016. 11. 24
3	TDP	암호데이터 검색 기술 설계서 V2.0	동적 데이터 활용 환경을 위한 안전성 모델 및 암호데이터 검색 기술에 대한 설계	2016. 12. 1

제4절 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	307,300	0	307,300	0	100%	-	
- 내부인건비(정)	307,300	0	307,300	0	100%	-	
2. 직접비	523,000	0	407,358	0	77.9%	-	
2.1 외부인건비	66,000	0	50,967	0	77.2%	-	
2.2 연구시설・장비 및 재료비	63,270	0	62,648	0	99%	-	
2.3 연구활동비	66,934	0	45,786	0	68.4%	-	
2.4 연구과제추진비	23,383	0	11,504	0	49.2%	-	
2.5 연구수당	64,460	0	0	0	0%	-	
2.6 위탁연구개발비	80,000	0	80,000	0	100%	-	
2.7 연구지원비	3,733	0	3,733	0	100%	-	
2.8 성과활용지원비	53,624	0	51,124	0	95.3%	-	
2.9 평가・관리비	1,596	0	1,596	0	100%	-	
2.10 공동연구비	100,000	31,200	100,000	31,200	100%	100%	
3. 간접비	75,809	0	75,809	0	100%	-	
4. 장비구입비	8,500	0	8,500	0	100%	-	
합 계	914,609	31,200	798,967	31,200	87.4	100%	

※ 12월 21일 기준

제5절 국내외 관련 분야의 환경 변화

O 개인·기기·산업이 연결되는 초연결 사회로 변화함으로써 개인 정보 유출 경로가 다각화되고 피해 또한 대형화됨에 따라, 사용자 데이터의 프라이버시 침해에 대한 우려가 커지고 있어 데이터베이스 암호화를 정책적으로 추진 중에 있으나 기술적 제약에 의해 현실 서비스 적용이 지연되고 있음

- ICT가 실생활 사물과 주요 사회기반시설 인프라에 접목되면서 사이버 공간의 위험이 현실세계로 전이 확대되고 있으며, '네트워크상의 정보보호'에서 사이버 세상의 안전한 삶을 보장하는 '사이버 세상에서의 안전'으로 진화
- 사용자 데이터의 프라이버시 침해를 방지하기 위해서는 중요 데이터에 대한 암호화가 필수적이며, 개인 프라이버시 인식 제고에 따라 암호화 대상이 개인정보보호법에 명시된 고유 식별번호에서 점차 확대될 것으로 예상
- 개인정보보호법(2014.8.7 시행)은 개인정보 수집 최소화 및 관리에 대한 법적 책임을 강화하고 있으며, 주민등록번호 등과 같은 고유 식별 정보에 대한 암호화를 명시하고 있음
- 2015년 7월 28일 개인정보보호법 시행령 개정안에 의하면 주민등록 보관 규모가 100만명 미만일 경우 2016년 12월 31일까지, 100만명 이상인 경우 2017년 12월 31일까지 암호화 조치를 완료해야 함
- 2015년 11월 10월 미래창조과학부, 행정자치부 등과 정부 3.0 추진위원회는 국무회의에서 K-ICT 클라우드 컴퓨팅 활성화 계획 확정을 통해 현재 3% 수준인 클라우드 이용률을 10배 이상인 30% 이상으로 확대하여 3년간 최대 4.6조(공공부문 1.2조)의 클라우드 시장 창출 목표를 발표하였으나, 암호화를 통한 데이터 보안 조치가 선행되어야 함
- 하지만, 단순 데이터베이스 암호화 기술 적용에 따른 기능적/성능적 제약으로 현실 서비스 적용은 계속 지연되고 있어 암호화된 데이터에 대한 활용 기술의 중요성이 부각되고 있으며, 이에 대한 기술 수요가 급증할 것으로 예상됨

O 데이터베이스 및 클라우드/빅데이터 환경에서 보안 기능과 활용성을 동시에 만족하는 암호 기술에 대한 요구가 증가하고 있음

- 2016년에는 데이터 중복으로 인한 스토리지 비용이 약 500억 달러에 육박하고 중복 데이터 용량은 300 엑사 바이트를 초과할 것으로 예상됨에 따라, 평문 뿐 아니라 암호문의 중복 처리가 매우 중요한 이슈가 되고 있음
- 데이터베이스 처리 성능 저하 없이 암호문을 복호화하지 않은 상태에서 키워드 검색과 부가기능 검색이 가능한 검색 가능 암호에 대한 시장 수요가 증가하고 있음
- 사용자의 요구에 의해 클라우드 스토리지에 대한 데이터 암호화가 적용되기 시작하였으며 국내에서도 2015년 11월 네이버 클라우드가 파일 암호화 기능을 추가하였으나, 대부분의 경우 기존의 일반 암호 기술을 적용하여 암호데이터에 대한 중복 처리가 지원되지 않고 있음
- 평문 수준의 데이터 처리 기술을 제공함으로써 현행 제공되는 수준의 데이터 서비스를 암호데이터 대상으로 제공할 수 있는 효율적인 기반 기술 개발에 대한 연구가 꾸준히 이루어지고 있으며, 이에 현실 적용 가능성을 높이기 위한 기술 개발의 중요성이 높아지고 있음
- 양자 컴퓨터에 대한 기존 암호기술의 안전성 훼손 가능성에 따라 quantum-safe 암호 기술에 대한 관심이 고조되고 있으며, 암호데이터 활용 기술에서도 기존 기술을 quantum-safe 암호 기술을 이용한 기술로 대체하기 위한 연구가 시작됨

제6절 연구결과의 활용 가능성 및 파급 효과

O 안전하고 스마트한 초연결 사회로 진화하는 환경에서 성능 문제로 적용이 지연되고 있는 데이터 암호화 도입을 위한 원천 기술로 활용하여, 초연결 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
- 안전한 초연결 서비스 보안 인프라 구축 및 신규 지능형 사이버 보안 시장 창출에 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