클라우드 환경에서 블록 암호를 이용한 암·복호화 알고리즘 성능 분석 및 모듈 개발

이홍재*, 신재형**, 신용태***
*숭실대학교 융합소프트웨어학과
**채드윅국제학교
***숭실대학교 컴퓨터학과
Jace@ssu.ac.kr*, jsshin2018@chadwickschool.org**, shin@ssu.ac.kr***

Performance Analysis and Development Algorithm Module using Block-ciphers in Cloud Computing Environment

Hong-Jae Lee*, Jayhyung Shin**, Yong-Tae Shin***
*Dept of Software Convergence, Soongsil University
**Chadwick International School
***Dept of Computing, Soongsil University

요 약

클라우드 서비스가 점차 증가함에 따라 사용자가 클라우드에 데이터 및 파일을 저장하는 일이 빈번해졌다. 하지만 클라우드 환경에 특성상 사용자에 데이터는 통합되어 저장·관리되는데 이때 여러 가지의 정보 유출에 대비한 보안적인 측면의 연구가 필요하다. 본 논문에서는 데이터가 유출 되더라도 암호화를 통해서 유출 시에도 원본 데이터를 확인할 수 없도록 하는 암호화 모듈을 개발하였고 블록암호 알고리즘인 AES, ARIA, SEED, HIGHT, LEA를 통하여 각각의 알고리즘 안정성 및 성능을 분석 하여 클라우드 환경에서 가장 적합한 알고리즘을 확인하였다.

1. 서론

최근 소프트웨어 및 하드웨어 기술의 발전이 가속화됨에 따라 사회의 관심이 4차 산업으로 집중되고 있다. 그 중 하나인 클라우드 컴퓨팅 서비스는 모든 자원을 소프트웨어 기반으로 가상화 하여 제공하고, 하이퍼바이저를 사용해 사용자들에게 효율적으로 자원을 할당하는 형태를 갖는다. 그러므로 사용자별로 사용하거나 저장하는 데이터는 논리적으로 구분되어 자원이 할당되지만 물리적으로는 동일한 자원을 공유한다. 그로인해 사용자의 데이터가 클라우드 서비스 공급업체에 저장되어 내부자 혹은 악의적인 관리자로 인해 데이터가 유출 될 수 있고, 다수의 사용자들이 공용으로 자원을 사용하기 때문에 데이터가 유출될 가능성이 존재한다.[1]

따라서 본 논문에서는 클라우드 환경에서 사용자의 데이터 및 이미지가 유출되어도 암호화를 통해 원본 데이터를 보존할 수 있고 인가된 사용자에게는 복호화를 통해 원본 이미지를 확인할 수 있도록 데이터에 따른 암·복호화 모듈을 연구 및 개발하였고, 각 블록암호에 대해 성능 분석을 하였다. 2장에서는 관련연구로 대표적인 국내 블록암호(ARIA, SEED, HIGHT, LEA)와 미국표준기술연구소(NIST)에서 제정된 국제적으로 사용되는 블록암호(AES)를 조사하였고, 3장에서는 국내 블록암호 알고리즘의 성[1]능평가를 위해 암호화 속도, CPU 사용량을 지표로 사용하는 모듈 개발을 진행하였다. 암·복호화할 데이터는 가장 대중적으로 사용되고 있는 이미지 포맷인 JPEG 이미지를 이용하여 성능평가 분석을 진행하였다. 이후 성능평가를 바탕으로 4장 결론에서 알고리즘 성능 분석을 하겠다.

2. 관련연구

2.1 AES(Advanced Encryption Standard)

AES는 NIST가 표준 블록암호 알고리즘인 DES를 대체하기위한 공모를 개최해 채택된 미국 표준 블록알고리즘이다.[2, 3] AES는 대칭키 알고리즘으로 정보를 암호화 및 복호화 할 수 있다. 128bit의 블록크기를 가지며, 128/192/256 키길이를 선택하여 암호화 할 수 있고, 라운드 수는 키길이에 따라 10/12/14 라운드로 구성되어 있다.[2]

2.2 ARIA(Academy, Research Institute, Agency)

ARIA는 Academy(학계), Research Institute(연구소), Agency(정부기관)의 첫 글자들을 따서 이름 지은 것으로,

본 연구는 중소기업청에서 지원하는 2016년도 산학연협력 기술개발사업(기업부설연구소 신규설치)(No. C0268191)의 연구수행으로 인한 결과물임을 밝힙니다.

국내 전자정부 구현으로 인해 경량 환경 구현을 위해 최적화된 범용 블록 알고리즘이다. AES와 동일규격인 128bit의 블록 크기와 128/192/256bit 에 가변적인 키 길이를 지원한다. 라운드 수는 키 길이에 따라 12, 14, 16라운드이다.[3]

2.3 SEED

SEED는 국내 금융, 무선, 전자상거래 등에서 활용 가능한 블록암호알고리즘으로 개발되었고, 개인정보 등과 같은 중요한 정보를 보호하기 위해 개발된 알고리즘이다. 특정한 환경에 적용하기 보다는 다양한 환경에서도 구현될 수 있도록 개발된 대표적인 민간 표준 암호이다. 초기 SEED 알고리즘은 Block Size는 128bit, Key Length는 128bit로 구성되어있으며, 알고리즘의 보안성 강화를 위해 256bit 키를 추가적으로 연구·개발하여 지원하고 있다. 라운드 수는 각각 16/24로 구성되어있다.[4, 5]

2.4 HEIGHT (HIGh security and light weigHT)

HIGHT는 대칭키 암호로, 블록 단위로 데이터를 처리하는 블록암호이다. 스마트카드, 인터넷뱅킹, RFID 등과 같은 다양한 저전력·경량화 환경에서 데이터의 기밀성을 제공하기 위해 개발된 알고리즘이다. Block Size는 64bit이며 Key Length는 128bit로 구성되며, 라운드 수는 32로 고정되어 구성됐다.[6]

2.5 LEA (Lightweight Encryption Algorithm)

LEA는 최근 사물인터넷 시장의 크기가 기하급수적으로 커지고 있는데 소프트웨어 환경에서 AES에 성능을 뛰어넘는 목표를 위해 개발 되었다. Block Size는 128bit이며 key Length 128, 192, 256bit로 구성되어 있으며 라운드 수는 각각 24/28/32를 가진다.[7]

다음 표는 각각의 블록암호 알고리즘의 구성을 표로 나타낸 것이다.

<표 1> 블록암호 알고리즘의 구성

구분	KeyLength (bits)	BlockSize (bits)	Round 수
AES	128/192/256	128	10/12/14
ARIA	128/192/256	128	12/14/16
SEED	128/256	128	16/24
HIGH	128	64	32
LEA	128/192/256	128	24/28/32

3. 성능 평가

본 3장에서는 전체 시스템 암·복호화 성능 측정을 하기 위한 모듈 개발에는 블록암호 운영방식 중 CBC운영모드로 암호화 하는 방식을 사용하였다. CBC모드는 입력 값으로 IV(Initial Value)벡터값이 추가되어 기존 ECB모드에서와 같은 동일한 파일과 값에도 전혀 다른 결과를 도출하기 때문에[8] 안정성을 위해 CBC모드로 암호화 하였다.

3.1 개발환경

개발 환경으로 사용된 컴퓨터는 OS는 Windows 10 pro x64, CPU는 Intel i7 3.4GHz, RAM은 DDR3 16.0GB, Visual Studio 2015를 사용하여 언어는 C++로 구현했다. AES는 오픈소스 프로젝트인 OpenSSL에서 제공하는 오픈소스를 활용 하였으며, ARIA, SEED, HIGHT, LEA는 한국인터넷진흥원 공식 홈페이지에서 제공하는 오픈소스 코드를 사용하였다.

현재 대표적인 클라우드 서비스 업체인 아마존 클라우드 서비스(AWS)와 MS클라우드 서비스(Azure)에서 C++로 개발된 모듈들에 대해 SDK를 제공하고 있어 본 성능 분석모듈이 클라우드 환경에서도 알고리즘별 성능 분석에 대해 일정한 형태에 결과 값을 확인할 수 있다.

3.2 보안성 평가

각 암호 알고리즘별 보안성을 평가하기 위해선 시스템의 안전성 수준을 만족할 수 있어야 한다. 안정성 수준은 어느 정도의 보안강도를 만족해야하는지를 의미하며 보안강도란 암호 알고리즘이나 해쉬함수의 취약성을 찾아내는데 소요되는 작업량을 수치화한 것으로 키 길이에 따라 80/112/128/192/256bit로 정의되어 있다.[9]

128bit의 보안강도는 2^{128}의 계산을 해야 취약성을 알아낼 수 있다는 것이며 이는 키를 찾아내기 위해 Brute Force방식으로 공격한다면 초당 10^9 번의 공격시도를 했을 시 대략 10^{21}년 정도의 시간이 걸리게 된다. 현재 구현에 사용한 모든 암호 알고리즘의 키길이는 128bit로 고정하여 구현하였기 때문에 보안적으로 안전하다 할 수 있다.

3.3 성능 측정

이미지의 보편성과 일반성을 만족하기 위해 선택한 JPG이미지는 다음과 같다.

<표 2> 각 이미지별 실제 이미지 및 크기

이름	실제 이미지	크기 (가로 * 세로)
Lena		512 * 512
백마상		1152 * 2048

숲		1836 * 3264

성능 분석은 파일에 데이터가 아닌 이미지 표시에 필요한 실제 데이터만을 가지고 암·복호화 수행하였으며 암호화된 이미지도 그림파일로 인식이 가능해 열람해서 볼 수 있도록 구현하였다. 실제 이미지 저장방식과 동일하기 때문에 데이터가 유출되더라도 암호화되었기 공격자는 원본 파일을 알아 볼 수 없다. 다음 프로그램 구현을 통해 블록 암호 알고리즘의 암·복호화 속도 및 CPU사용량을 측정하였다.

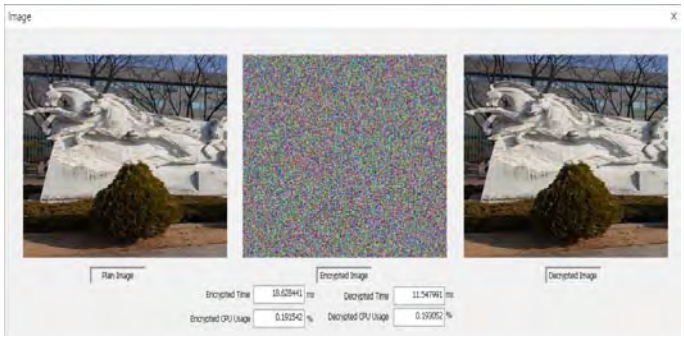

그림 1 암호 알고리즘 암·복호화 성능측정

본 성능분석모듈은 그림 2와 같이 이미지를 암호화를 통해 가독성이 없는 이미지로 암호화 하여 변환된 이미지를 복호화 하였고3가지의 이미지 암호화 수행시간은 다음과 같다.

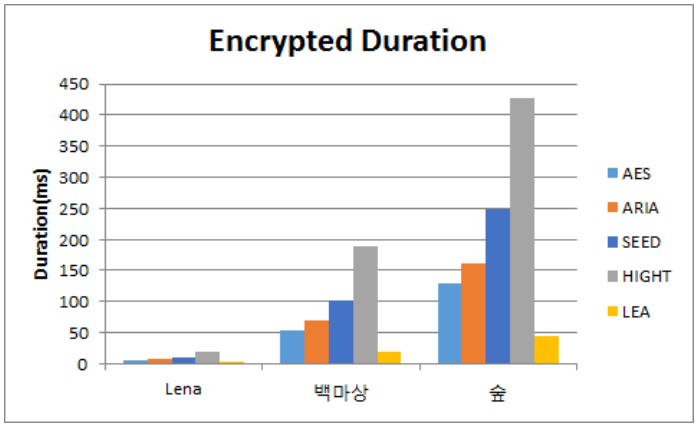

그림 2 이미지에 따른 암호화 수행시간

그림 2와 같이 Lena, 백마상, 숲 이미지의 암호 수행시간은 암호 알고리즘마다 동일한 비율에 분석시간을 갖는다. HIGHT암호가 시간이 가장 높게 측정되었으며, 그다음으로 SEED, ARIA, AES 와 LEA순으로 LEA의 성능이 가장 좋은 것으로 알 수 있다.

다음은 수행한 시간과 함께 측정한 이미지별 CPU사용량을 그래프로 표시하였다

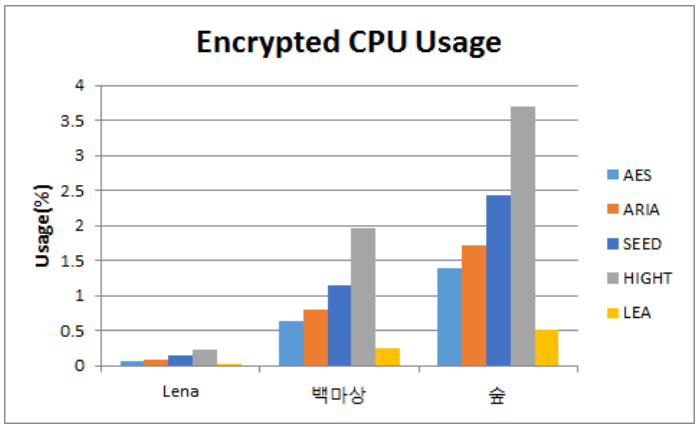

그림 3 이미지에 따른 암호화 CPU사용량

그림 3과 같이 암호화 CPU사용량 측정결과 또한 수행시간과 동일한 암호 알고리즘 순으로 측정되었다. 모든 이미지에서 동일한 LEA가 가장 적은 CPU사용량을 나타내었고, 그다음 순서로는 AES, ARIA, SEED, HIGHT순이었다.

그 다음으로 살펴볼 그래프는 암호화된 이미지를 복호화 수행 중에 성능을 측정하였다.

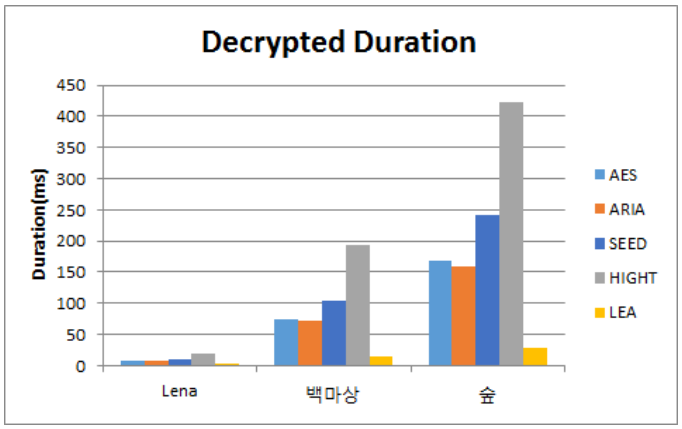

그림 4 이미지에 따른 복호화 수행시간

그림 4와 같이 복호화 수행시간을 살펴보면 Lena, 백마상, 숲 이미지에 따라 암호화 수행시간과 차이가 크게 나타나지는 않았다는 걸 알 수 있다. 각각의 수행시간 순서로는 HIGHT, SEED, AES, ARIA, LEA순으로 수행시간이 많은 것을 확인하였다.

마지막으로 살펴볼 그래프는 복호화에 CPU사용량이 얼마만큼 소요되는지에 대해 알아보겠다.

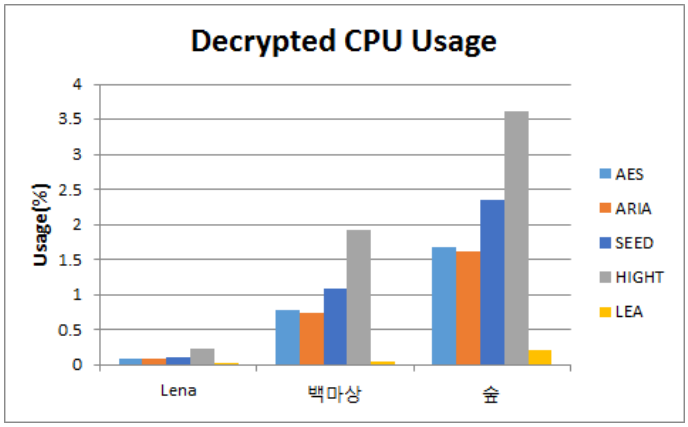

그림 5 이미지에 따른 복호화 CPU사용량

그림 5를 살펴보면 3개의 이미지 모두 동일한 비율의 CPU 사용량이 나타났다. 복호화 CPU 사용량은 복호화 수행시간과 동일한 순서로 나타났고, HIGHT, SEED, AES, ARIA 그리고 LEA순으로 나타난걸 알 수 있다.

4. 결론 및 향후연구

클라우드 환경에서 데이터 암호화하기 위해 선택된 미국표준블록암호와 국내표준블록암호 등 총 5개의 블록암호 알고리즘의 성능분석 후 표본화 하였고, 5개의 알고리즘의 보안기준을 키 길이 128bit로 통일화 하여 보안강도와 안정성이 검증된 결과 값을 얻을 수 있었다. 5개의 블록암호 알고리즘에 성능을 비교분석해본결과 LEA가 암·복호화시 수행시간 및 CPU소모량이 가장 낮아 비교분석한 암호 알고리즘 중에서 성능이 가장 우수하다는 결과값과 HIGHT가 가장 성능이 낮음을 알 수 있다. 이러한 연구 결과를 통해 향후 클라우드 환경에서의 적용되어 보안이 점차 증대되어 안정성이 높아진다면 클라우드 산업이 보다 더 활성화 될 것이다.

참고문헌

[1] 구원본 등 5명, “클라우드 서비스에서 보안 기술적 측면을 고려한 정보보호 요구사항에 관한 연구”, 보안공학연구논문지, 제10권 제 3호, 2013.06

[2] NIST, FIPS-197 Announcing the ADVANCED ENCRYPTION STANDARD(AES), nov 26, 2001

[3] 박기태, “OpenSSL상에서 경량 암호 알고리즘 구현 및 성능평가”, 동국대학교, 2015

[4] 한국인터넷진흥원, SEED 128 알고리즘 상세 명세서, 2009

[5] 한국인터넷진흥원, 256비트 블록 암호알고리즘(SEED) 분석 보고서, 2009

[6] 한국정보통신기술협회, 64비트 블록암호 HIGHT, 2008

[7] 한국정보통신기술협회, 128비트 경량 블록 암호 LEA, 2013

[8] Biham, Eli. "On modes of operation." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1993.

[9] 한국인터넷진흥원, 암호 알고리즘 및 키길이 이용 안내서, 2013