클라우드 환경에서 안전한 PACS 데이터 전송을 위한 AES 암호화 알고리즘

조영복* · 우성희** · 이상호*

*충북대학교

*한국교통대학교

AES Encryption Algorithm for safe PACS data Transmission in the Cloud Environment

Young-bok Cho* · Sung-hee Woo**· Sang-ho Lee*

*Chungbuk National University, Korea National University of Transportation

E-mail : bogicho@cbnu.ac.kr

요 약

제안기법은 도래하는 클라우드 환경에서 원격의료 시스템을 위한 PACS에서 전송되는 의료정보의 정형데이터와 비정형 데이터의 안전한 전달을 위해 제안한다. 정형데이터는 의료영상과 같은 민감한 데이터로 AES암호화해 전달하고 비정형데이터는 의료이미지의 일부에서 비식별화를위해 암호화된 모자이크 비식별화기법을 이용해 전달한다. 암호화키의 안전성 평가를 위해 사이즈를 증가해가며 실험한 결과 128비트의 크기가 196, 256의크기로 암호화해도 128키와 큰 차이를 보이지 않음을 증명하였다..

ABSTRACT

The proposed scheme is proposed secure transmission of fixed data and unstructured data among medical information transmitted in PACS. Unstructured data uses the AES encryption algorithm as sensitive data And transmitted using encrypted mosaic encryption techniques for the non-identification of medical images, which are regular data. In addition, we have experimented with increasing the key size for encryption. As a result, we did not notice any significant difference between 128 - bit size and 128 - key size even when encrypting the size of 196,256

키워드

PACS, Medical image, AES Encryption, De-Identification, Cloud

Ⅰ. 서 론

이미 미국은 원격진료를 1997년 도입, 일본은 2015년 8월 원격진료에 관한 고시를 개정해 의사-환자간 원격의료를 전면 허용했다. 심지어 중국도 지난 2013년 시작해 B2B 원격진료는 정착단계에 진입했고 최근 B2C 원격 의료서비스를 본격적으로 도입한 지금 우리나나라도 언제가 열리게될 의료 시장을 준비하며 다양한 연구개발이 이루어지고 있다. 의료진단정보시스템은 아날로그 형태의 진단의료영상 데이터를 디지털 형태의 데이터로 획득하여 이를 네트워크를 통해 대용량 기억장치에 전송하여 저장함으로써 판독 및 검색 기능을 통합적으로 수행하는 시스템을 말한다[1]. 이처럼 정보화시대의 도래와 함께 환자에 대한 의료혜택의 기회를 확대하고, 최상의 의료서비스를 제공하려는 의료 기관들에게 병원 전산시스템은 빼놓을 수 없는 의료 기관 내주요 기반시설로서 등장하게 되었다[2]. 또한 클라우드 기반의 병원간 협진을 위한 원격진료 환경에서 안전한 의

료정보전달은 매우 중요하다. 또한 연동 된 의료 데이터의 검색이나 기타 제 3의 기관에 제공시 의료이미지의 경우 별다른 보호 조치 없이 일반적인 이미지 파일로 제공되고 프라이버시 보호에 문제가 될 수 있다[3]. 현재 병원에서 사용되고 있는 의료영상저장전송시스템(Picture Arching and Communication Systme :PACS)방식은 의료영상의 디지털화를 이루었고 이를 통해 병원내 모든 의료 영상장비들을 하나로 연동이 가능하게 되었다. 일반적으로 PACS 시스템의 의료영상 데이터는 의료이미지 데이터로 PACS 형식의 정형데이터와 비정형데이터로 영상에 대한 진단기록지가 메타데이터로 분류할 수 있다[4,5]. 그러나 이들 의료영상 장비가 의료영상저장시스템과 연동하기 위해서는 먼저 영상의 디지털화가 필요하다. 이를 구현하기 위해서는 영상표시 및 처리, 정보통신 및 네트워킹, 데이터베이스, 정보관리, 사용자 인터페이스와 정보저장관리등의 기술이 필요하고 이에 대표적인 것이 DICOM(Digital Imaging and Communi cation in Medicine)이다. DICOM은 서로 다른 영상 장비들간 하나의 표준 포맷을 선택해 의료영상을 송수신하기 위해 개발되었다[2]. 제안논문은 PACS 시스템에서 만들어진 의료영상이미지의 정형데이터와 비정형데이터의 안전한 전송을 위한 의료정보의 암호화와 의료 이미지의 비식별화 기법을 제공 한다.

II. 관련연구

2.1 의료진단정보시스템

지난 30년 동안 의료분야에서 디지털 장비 사용은 급격히 증가하였고, 첨단 방사선장비를 이용한 분야나 임상적인 분야까지 다양한 디지털 의료 장비를 갖추게 되었다. 특히 전산화단층촬영, 자기공명영상(MRI)을 이용한 분야에서 주도적으로 발전되고 있다. 또한 부서간 정보교류의 필요성이 증대되고 방대한 자료 관리에 수반하는 부대비용의 증가 등으로 의료진단정보시스템의 필요성이 부각되고 있어, 병원 종합 전산망 구축과 의료진단정보시스템의 도입은 병원의 필수요소가 되었다[2,3,5].

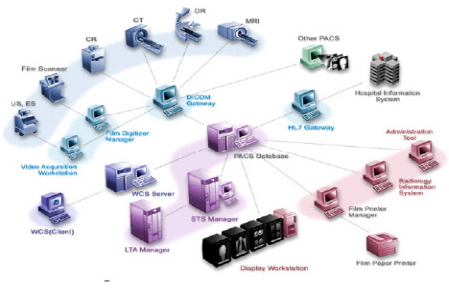


Fig 1. Configuration of medical diagnostic system

그림 1은 현재 병원에서 구현되는 의료진단정보시스템의 기본 구성도를 나타내고 있다. 의료영상정보시스템의 궁극적인 목표는 필름이 필요 없는 병원 시스템을 구축하는 것이며, 이를 위해서는 영상 표시 및 처리, 정보 통신 및 네트워킹, 데이터베이스, 정보 관리, 사용자 인터페이스와 정보저장 관리 등의 기술들을 통합하여야 한다. 의료진단정보시스템은 의료영상들을 디지털 형태로 획득한 후, 고속의 통신망을 통하여 전송하고, 과거의 X-ray 필름 보관 대신에 디지털 정보 형태로 의료영상을 저장하며, 방사선과 의사들과 임상 의사들이 기존의 필름 뷰 박스 대신에 영상조회 장치를 통하여 표시되는 영상을 이용하여 환자를 진료하는 포괄적인 디지털 영상 관리 및 전송시스템을 말한다[5,6,7].

2.2 데이터 전송에서 의료데이터 평가기준

방사선 영상 데이터 규격(DICOM)은 '식약청 PACS DICOM 데이터 호환성 향상 및 보안적용 가이드라인'에 따라 방사선 영상 데이터를 DICOM으로 인코딩해야 한다. 그리고 방사선 영상을 전송할 때는 방사선 영상 전송 표준 규격인 DIR CDA를 준수하도록 한다[4]. DIR CDA는 방사선 영상 보고서 필수 항목을 포함한다. 방사선 영상 보고서 필수 항목은 환자 정보, 방사선 영상 보고서를 작성한 의사정보, 진료 기관 정보, 판독 정보이다. 의무기록데이터 평가기준은 환자와 의사 측에서 죄하는 필수 정보는 의사가 조회하는 환자의 인적사항에 대한 정보 필수 항목(환자 ID, 환자 이름, 환자 주소, 환자 연락처, 성별, 생년월일)을 제공해야 한다. 그리고 환자가 조회하는 의료제공자 정보 필수 항목(의사 이름, 등록번호, 의료기관 이름, 의료기관 주소, 의사 전화번호, 진료과)을 제공해야 한다. 진료정보를 전송할 경우에는 진료정보 전송 표준 규격(진료기록 보고서 CDA)를 준수하여 진료정보를 전송한다. 환자의 개인정보 보호는 의료기관과 의료공급자(병원, 의사)는 환자의 개인정보를 보호해야 한다[3,8].

III. 클라우드 환경에서 안전한 PACS 데이터 전송을 위한 AES 암호화 알고리즘

제안 알고리즘은 AES 암호화 기술을 이용해 보안이 취약한 클라우드 환경의 의료데이터를 서로 안전하게 주고 받을수 있도록 데이터를 암호화 함으로 보안문제를 해결한다. PACS 시스템에서 만들어진 의료영상이미지는 크게 의료영상이 담긴 정형데이터와 영상위에 개인식별정보나 기타 의료기기에 의해 나타난 비정형데이터로 분리된다[5]. 제안논문에서는 의료영상데이터의 정형데이터와 비정형데이터의 안전한 전송을 위한 의료정보의 암호화와 의료 이미지의 비식별화 기법을 제공 한다.

Fig 2. Data separation in medical imaging

의료정보 암호화를 위해서서는 AES 암호 알고리즘을 이용해 서버 연결구간 정보를 암호화 한다. AES는 암호 및 복호과정에서 생성되는 중간 결과값 스테이트(State)를 바이트 단위로 4 * 4의 2차원 행렬로 간단히 표현할 수 있고, 4 * 4의 2차원 행렬은 기존의 행 우선이 아닌 열 우선으로 행렬의 순서를 표시한다. AES의 라운드 함수 내에 크게 4가지의 독립적인 함수가 있으며, 각각의 라운드 함수는 다음과 같다.

- SubBytes(SB): 8비트 Sbox를 이용한 비선형 바이트 치환 함수.
- ShiftRows(SR): 행 단위 왼쪽 회전 함수로 첫 번째 행은 변환하지 않으며, 두번째 행은 1바이트 회전 세번째 행은 2바이트 회전 네번째 행은 3바이트 회전을 적용하는 함수.
- MixColumns(MC): 열 단위로 혼합을 수행하는 32비트 선형 변환 함수.
- AddRoundKey(ARK): 라운드 키와 덧셈을 수행하는 함수.

AES 암호 알고리즘은 의료정보에 대한 암/복호화를 수행하며 암/복호화 전체 구성도는 [그림 3]과 같다.

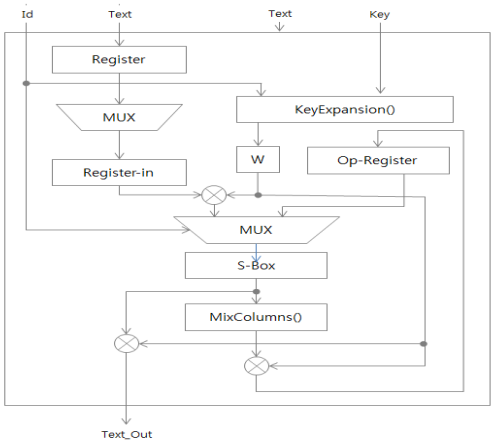


Fig 3. Proposed AES encryption module

KeyExpansion()부는 AES 암호 키를 입력받아 128 비트 라운드 키 W를 생성하는 역할을 하며 S-box는 개선된 S-box는 개선된 s-box를 사용하여 치환 연산을 수행한다. MixColumns()부는 xtime()함수를 사용하여 연산을 수행한다. 복호화 모듈에서는 InvShiftRows(), InvSubBytes(), AddRoundKey(), InvMixColumns() 순으로 복호화 데이터를 연산한다.

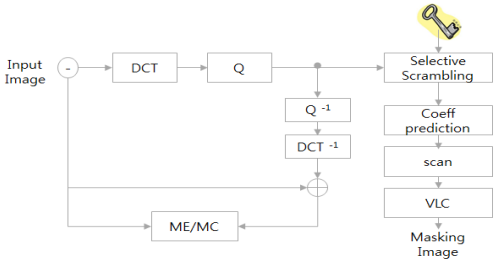


Fig 4. Mosic masking in encryption for de-identification

또한 의료영상 데이터의 비식별화를 위해 그림 4와 같이 암호화된 마스킹 기법을 적용함으로 전송 데이터를 보호하면서 의료이미지의 재식별을 효율적인 처리를 지원한다. 일반적으로 의료영상은 4방위의 꼭지점을 기준으로 정보가 들어가 있고 의료영상기기에 따라 조금씩 차이를 가지고 있기 때문에 제안 방식에서는 영상을 5×5 크기 블록을 랜덤 방식으로 발생시켜 이미지에 마스킹 처리를 함으로 비식별화를 위한 제안기법은 영상처리 기반으로 의료영상 비식별화를 제공 한다.

Ⅳ. 실험결과

이 논문에서 성능 실험을 위해 2개의 클러스터를 사용하였다. 클러스터 사양은 다음 표1 과 같다.

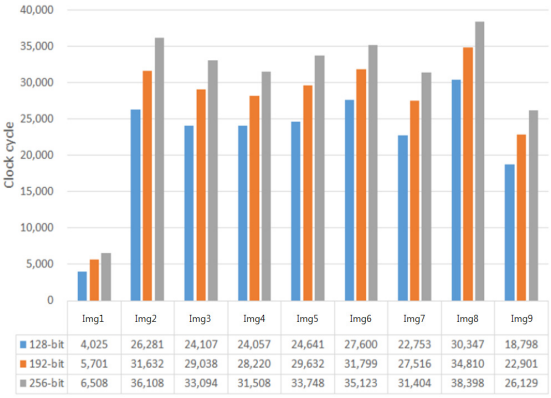
Table 1. Experimental Environment

3-nodes cluster	
cpu	i7-8200 (3.4GHz, 8cores)
Memory	4GB
HDD	1TB
Network	1Gbps

5-nodes cluster	
cpu	i5-2600 (2.9GHz, 8cores)
Memory	4GB
HDD	1TB*2(RAID-0)
Network	1Gbps

실험을 위해 암호화 알고리즘은 Visual studio C++로 AES 암/복호화, 마스킹 알고리즘을 구현하고 128비트의 키 사이즈를 기본으로 키사이즈를 192, 256으로 이미지를 암호화 하며 이미지의 중요 개인식별정보를 마스킹하여 전송시 전송률을 비교하였다. 제안 논문에서는 속도 최적화를

위해 라운드 키를 포함한 주요 함수는 loop unrolling 기법과 매크로 함수로 구현하였다. 또한 메모리 참조 연산을 최소화하기 위해 빈번하게 사용되는 메모리 값은 특정 변수에 저장하여 레지스터로 연산될 수 있도록 고려하였다. 구현 결과는 그림 5와 같고 프로세서의 clock cycle를 기준으로 난수생성 시간을 구현한 결과이다.



	Img1	Img2	Img3	Img4	Img5	Img6	Img7	Img8	Img9
128-bit	4,025	26,281	24,107	24,057	24,641	27,600	22,753	30,347	18,798
192-bit	5,701	31,632	29,038	28,220	29,632	31,799	27,516	34,810	22,901
256-bit	6,508	36,108	33,094	31,508	33,748	35,123	31,404	38,398	26,129

Fig 5. 128/192/256-bit Masked AES

제안하는 AES 마스킹 암호화 알고리은 라운드 키 생성과 사전 연산을 제외한 암호화 구간의 속도를 측정한 결과 미 적용 대비 4.67배로 빠른 것을 실험을 통해 확인할수 있었다. 제안 알고리즘은 마스킹 암/복호화시 발생하는 함수 호출을 생략할 수 있어 마스킹 변환이 필요한 대응기법보다 상대적으로 효율적인 것으로 나타났다. 또한 민감한 데이터의 안전성을 고려해 키 크기에 대한 속도 비율도 측정해본 결과 192, 256비트 역시 128비트와 속도 비율이 비슷했으며, 모든 기법의 속도 비율이 128비트에 비해 조금 더 개선되는 것을 알 수 있었다. 64비트 플랫폼에서 전체 라운드가 128비트의 AES암호화로 구현되었을 약 4.67배의 속도 저하만이 발생하고 마스킹을 적용시 약 1.2배의 속도 저하를 보였다. 실험에 사용된 영상은 수골 X-lay 영상을 대상으로 실험하였으며 디지털화된 의료영상의 크기나 영상획득의 기기 종류에 따라 실험 결과는 조금씩 달라 질 수 있을 것이다.

V. 결 론

제안 논문은 클라우드 환경에서 안전한 PACS 시스템에서 전송되는 데이터의 안전한 전송을 위한 AES암호화 알고리즘을 제안하였다. 의료영상 데이터의 특성을 고려해 정형데이터와 비정형데이터의 안전성 레벨을 맞춰 정형 데이터는 AES 암호화 알고리즘을 이용해 안전하게 전송될수 있도록 제공하고하고 비정형데이터의 경우 개인프라이버시 보호를 위해 암호화된 비식별화 알고리즘을 제공한다. 따라서 통계적 처리나 검색에서 의료데이터의 활용이 가능하면서도 안전성을 제공한다. 통신상에 전송되는 민감한 의료데이터로 안전성 강도를 높이기 위해 암호화 키의 강도를 실험함으로 128키와 큰 차이가 없음을 증명하였다.

ACKNOWLEDGMENTS

This research was supported by the CHUNGBUK TECHNOPARK, Korea, under the (Development of Prediction and Diagnosis System for Pediatric Adolescents Using Iris-based Image Mining) support program (201707021901)

참고문헌

[1] 조정호, and 김광현. "모바일 환경에서 의료 진단 정보 시스템의구현 및 의료 영상의 적합성 평가." 한국전자통신학회 논문지 vol.10.no.6 pp. 713-720, 2015.

[2] 조영복, 우성희, 이상호, “의료영상 보안을 위한 워터마크 인증 암호화 기법”, 한국정보통신학회논문지 vol, 21, no4, pp 107-114, 2017

[3] 배성철, 김일곤, 박샛별, 송준현, 이병기, 차지훈,오현주, “원격의료시스템의 성능 평가 기준”, FDC 법제연구논문지, vol.7, no.2, pp.53-57, 2012.

[4] Greenspan, A.T. Pinhas, Medical Image Categorization and Retrieval for PACS Using the GMM-KL Framework, IEEE Transactions on Information Technology in Biomedicine, Vol. 11, No. 2, pp. 190-202, 2007.

[5] 조영복, 우성희, 이상호, “의료영상 보안을 위한 워터마크 인증 암호화 기법”, 한국정보통신학회논문지 vol, 21, no4, pp 107-114, 2017

[6] Q. Jiang, J. Ma, Z. Ma and G. Li, “A privacy enhanced authentication scheme for telecare medical information systems”, Journal of Medical Systems, vol. 36, no. 3, pp. 1529-1535, 2012.

[7] K. J. Kim and S. P. Hong, “Privacy Information Protection Model in e-Healthcare Environment”, Journal of The Korean Society for Internet Informatin, vol. 10, no. 2, pp. 29-40, 2008.

[8] Y. B. Cho, and S. H Lee, “An IDE based Hierarchical Node Authentication Protocol for Secure Data Transmission in Environment”, Journal of The Korean Institute of Communications and Information Sciences, vol. 37B, no.3, pp. 149-157, 2013.