Regular paper
Journal of the KIECS. pp. 199-204, vol. 15, no. 1, Feb. 29. 2020, t. 99, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2020.15.1.199

SHA-256 기반의 캡슐화된 전자의무기록 문서 저장 시스템

이효승* · 오재철**

SHA-256 based Encapsulated Electronic Medical Record Document Storage System

Hyo-Seung Lee* · Jae-Chul Oh**

요 약

IT기술의 발달로 현재 여러 분야에서 융·복합 시스템을 적용하고 운영 중에 있다. 그중 대표적인 분야가 의료분야로 나노기술 및 바이오 기술을 접목하여 다양한 형태로 발전해 나가고 있다. 하지만 실제 의료데이터를 운영하고 관리하는 측면에서는 기술적인 혁신이 부족한 것이 현실이다. 대표적인 예로 전자의무기록 또는 SAM 파일과 같이 데이터를 전송 또는 보관하는 업무의 운영에 있어 현재는 데이터와 문서의 양식을 별도로 저장하고 조합하는 형태를 취하고 있으며 그렇지 않은 경우에도 종이에 기록 후 보관하는 방식을 고수하고 있다. 본 연구에서는 데이터와 문서의 양식을 캡슐화 하고 업무 처리상 발생할 수 있는 문서 형태 그대로를 데이터화 하여 운영 및 보관할 수 있는 EMR 시스템을 설계 및 구현함으로써 업무적인 측면과 관리적인 측면에서 보다 효율적인 전자문서의 운영이 가능할 수 있기를 기대한다.

ABSTRACT

With the development of IT. convergence systems are applied and operated in many different fields. A representative field among them is medical service, which develops in diverse types in combination with nano-technology and bio technology. However, there is a lack of technical innovation in terms of medical data operation and management. For example, data and documents are saved and integrated separately depending on their forms when electronic health records or data like SAM files are transmitted or kept. In other cases, such records and data are still kept after being recorded in paper. This study tries to design and implement the EMR system that makes it possible to capsulize forms of data and documents and to digitalize documents in work process as they are in terms of operation and storage. The system is expected to support efficient operation of electronic documents in the aspects of work and management.

키워드

EDI, Hash Algorithm, EMR, Health Screening
전자 문서 교환, 해시 알고리즘, 전자 의무 기록, 건강 검진

Ⅰ. 서 론

IT산업의 발전과 4차 산업 혁명을 바탕으로 현재 다양한 분야에서 IT 기술이 활용되고 있으며 특히 의료분야에서는 나노기술, 바이오기술, 신소재기술 등 다양한 융합 기술들이 활용되어 지고 있다[1].

* 순천대학교 컴퓨터공학과(hodol0@naver.com)
** 교신저자 : 순천대학교 컴퓨터공학과
· 접 수 일 : 2020. 01. 28
· 수정완료일 : 2020. 02. 06
· 게재확정일 : 2020. 02. 15
· Received : Jan. 28, 2020, Revised : Feb. 06, 2020, Accepted : Feb. 15, 2020
· Corresponding Author : Jae-Chul Oh
Dept. Computer Engineering , Sunchon National University,
Email : ojc@sunchon.ac.kr

이렇게 다각도로 기술개발이 이루어지고 있는 상황에서 이러한 기술개발이 가져올 다량의 데이터를 효율적으로 운영하기 위해 현재 운영하고 있는 데이터 처리 시스템을 확인해볼 필요성이 있을 것이다.

현재 다수의 의료기관에서 의료 데이터를 효율적으로 관리하는 방안을 검토 중에 있으며 그 예로 모바일 애플리케이션을 이용하여 건강검진 데이터를 입력 및 관리하거나, NCS(National Competency Standard:국가직무능력표준) 기반의 의료정보 관리를 위한 퇴원분석 프로그램을 개발하는 등의 다양한 연구가 진행 중에 있다[2-3]. 하지만 이러한 연구는 대형의료기관 또는 일부 의료기관에 한하여 이루어지고 있으며 현재 대부분의 의료기관에서는 데이터를 효율적으로 운영하고 관리하고자 하는 측면에서 EMR 이라는 전자의무기록 형태의 전자문서를 도입하여 사용하고 있다.

전자의무기록은 종이서류로 된 진료기록부에 비해 기록 및 보관이 용이하여 의료계에 급속도록 보급되었으며, 기존의 종이 방식에 비해 시간적, 경제적 비용이 대폭 감소된다[4-5].

하지만 전자의무기록을 포함하여 현재 의료기관에서 사용 중인 전자문서는 대부분 데이터와 문서의 양식을 별도로 보관하고 필요 시 매칭 하는 방식으로 운영된다. 이러한 경우 해당 서식이 변경되었을 경우 그에 맞는 관리가 필요하게 된다. 그렇지 못할 경우 데이터와 양식이 맞지 않아 시스템의 불완전성을 가져오게 된다. 또한 타 기관으로 데이터를 전송할 경우 번거로움을 가중시키게 된다. 본 연구에서는 현재의 전자문서 방식을 개선하기 위해 데이터와 문서의 양식을 해시를 기반으로 캡슐화 하여 보관 관리할 수 있는 시스템을 설계하고 개발하기 위해 Ⅱ장에서 기존의 전자의무기록과 관련된 연구내용을 소개하고 Ⅲ장에서는 본 연구의 설계, Ⅳ장에서는 시스템의 개발, Ⅴ장에서는 테스트 및 운영에 대한 결과를 통해 결론을 맺고자 한다.

Ⅱ. 관련연구

2.1 해시

해시는 평문의 길이와 상관없이 모두 일정한 길이의 값을 도출하게 되며 변조되기 전의 데이터를 추측하기가 불가능 하다는 특징을 가지고 있기 때문에 데이터의 위조・변조 검사 및 데이터의 안전한 보관, 통신의 안전성 증명 등을 이유로 활용범위가 확대되고 있다[6].

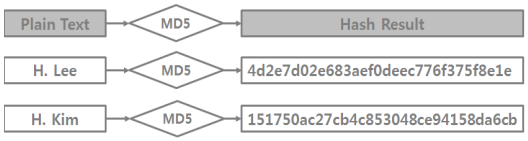

그림 1. MD5 해시 알고리즘 변환 결과
Fig. 1 MD5 Hash algorithm conversion result

현재 국내에서 사용 중인 인증서 관련 해시 알고리즘은 SHA-256으로 최대 2^{64}bit 미만의 길이를 갖는 메시지에 대하여 다이제스트를 출력하여 값을 생성한다[7].

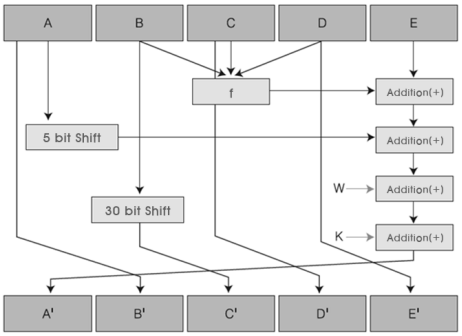

그림 2. SHA-256 해시 알고리즘 동작 과정[8]
Fig. 2 SHA-256 hash algorithm operation process[8]

또한 Piecewise 해싱기법을 이용해 해시 값의 정보 일부를 추출하여 파일의 유사도를 측정하는 등의 연구를 통해 파일 및 문서 관리와 데이터 운용에 적합한 방식이라는 점이 부각되고 있으며 블록체인의 기반이 되는 기술이기도 하다[9].

2.2 전자의무기록

전자의무기록은 진료 시 발생하게 되는 업무와 관련된 검사, 수술, 상해기록 등 환자의 건강과 관련 있는 모든 자료를 입력 및 보관하는 전산 시스템을 말한다[10].

전자의무기록 시스템은 현재 의료기관에서 처방전달 시스템보다 더 중요한 시스템으로 자리를 잡아가고 있으며 그 효율성을 인정받고 있다.

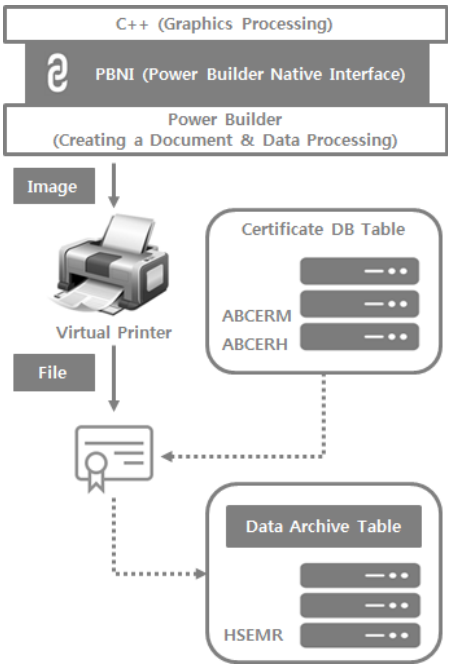

그림 3. 그래픽 요소를 포함하는 EMR 구조 설계
Fig. 3 Structural design of EMR including graphic elements

현재 대부분의 전자의무기록 시스템은 그래픽 형태와 텍스트 형태로 구분하고 있으며 그림3과 같이 그래픽 형태의 자료와 텍스트 형태의 자료를 한꺼번에 저장하기 위해 파일단위로 저장하여 인증하는 방식의 전자의무기록이 연구되기도 하였다[11].

이러한 방식은 종이 차트형태와 동일하여 사용에 어려움이 없어 그래픽 EMR의 장점을 그대로 수용할 수 있지만 저장하여야 하는 데이터의 양이 많고 그래픽과 서식지를 연동하는 단계에서 여러 단계를 수행함에 있어 많은 지연 시간이 발생되고 시스템에 부하를 가져오게 되는 단점이 발생하게 된다. 이러한 이유로 실무 단계에서의 사용이 적절하지 못하다고 판단하여 본 연구에서는 이러한 문제들을 보완하기 위해 관련 문서의 양식과 그 양식에 기술되어야 하는 관련 데이터를 뷰어 형태가 아닌 소스 형태로 저장하고 인증하는 방식의 EMR의 설계 및 개발을 통해 전자문서 형태를 한 단계 진화 시키고자 하였다.

III. 해시기반의 캡슐화된 EMR 시스템 설계

본 연구에서는 데이터와 문서양식을 별도로 저장하여 운영하는 EMR의 전자문서 형태를 보다 효율적으로 운영 관리하기 위해 캡슐화하고 이를 이중 해시처리하여 보안과 보관, 관리 측면에서 이점을 가질 수 있도록 설계하였다.

데이터와 문서양식을 캡슐화한 데이터윈도우의 소스코드를 파워빌더에서 제공하는 PBBLOB 형태로 1차 해시를 수행하고 이를 통해 생성된 메시지 다이제스트에 개인키를 이용하여 또 한 번 SHA-256 방식으로 2차 해시처리 한다.

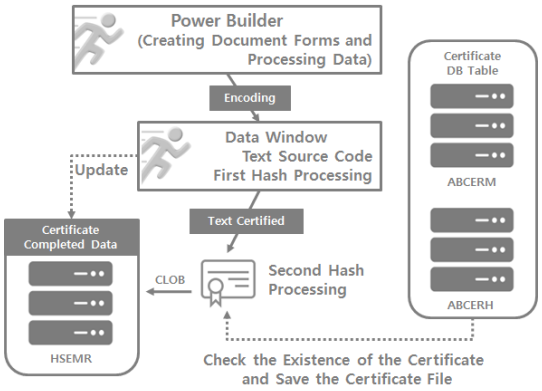

그림 4. 해시기반의 캡슐화된 EMR 시스템 설계
Fig. 4 Design of hash-base encapsulated EMR system

이렇게 생성된 2단계의 해시코드 결과 값은 HSEMR 이라는 테이블의 컬럼에 CLOB 형태로 데이터와 문서양식을 한꺼번에 저장하고 관리할 수 있도록 설계하였다.

본 연구의 설계 내용을 실제 사용하기 위해서는 이러한 방식을 통해 생성된 전자문서가 평문 상태로 정확히 복원 가능한지, 해당 문서의 양식이 올바르게 생성되는지, 각각의 데이터가 양식의 해당 위치에 정위치 하는지 등에 대한 검증이 필요할 것이다.

이에 해시 값 형태로 생성된 데이터를 문서형태로

복원하기 위해서는 그림 5와 같이 앞서 진행하였던 1, 2차 해시 작업을 역방향으로 진행하여 문서를 도출하는 방식을 통해 검증할 수 있을 것이다.

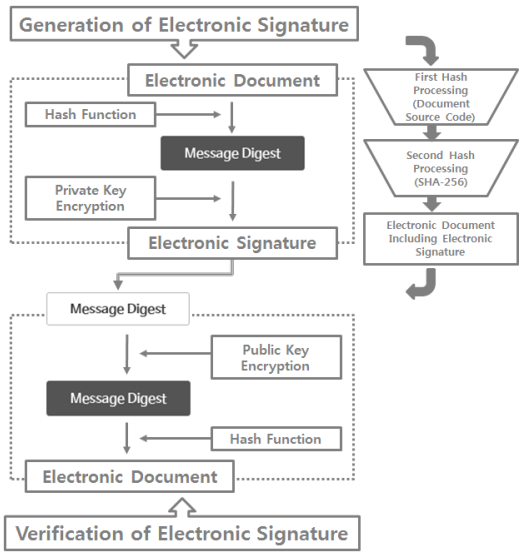

그림 5. 해시기반의 캡슐화된 EMR 인증 및 검증 관계
Fig. 5 Hash-based encapsulated EMR certification and validation relation

이러한 방식은 관리 포인트가 줄어들고 이와 동시에 서식지에 포함되어야 하는 의료진의 도장 및 서명과 같은 각종 이미지 및 문서의 양식을 문서 자체에 포함시킬 수 있기 때문에 관리적인 장점 외에 의미상으로도 종이 문서와 동일하게 적용할 수 있으며 텍스트(소스)를 통한 처리방식이기 때문에 기존의 파일에 대한 처리 또는 이미지 처리에 비해 처리 속도가 빠르다는 장점을 제공 할 수 있다.

Ⅳ. 해시기반의 캡슐화된 EMR 시스템 구현

해시기반의 캡슐화된 EMR 시스템을 구현하기 위해 먼저 DataWindow에 Freeform 형식으로 생성된 양식지에 조회 또는 입력을 통해 데이터를 기록하고 PBBLOB 형태로 변환하여야 한다.

String ls_capdata // PBBLOB로 캡슐화된 데이터
ll_rv = dw_docum.GetFullState(ls_capdata)
ll_rtn = gf_dwcap(코드, 번호, 일자, 년도, 성명, '문서명', ls_capdata)

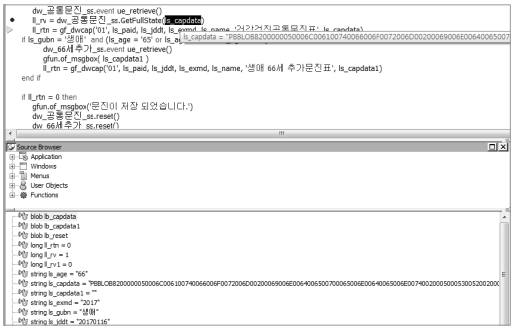

그림 6. PBBLOB 데이터 추출을 위한 디버그 화면
Fig. 6 Dubug screen for PBBLOB data extraction

위와 같이 캡슐화 1차 해시 변환과정을 거치면 "PBBLOB8200000050006C006100740066006F0072006D00200069006E00640065007000650006E00640065006E00740020005000530052002000460069006C006500200046006F0072006D00610074002C002000430006F0070007..." 등 과 같이 일반적인 방법으로 해독하기 어려운 형태로 변형되어 그 값의 유추가 쉽지 않게 된다.

이렇게 해시 처리 된 데이터는 이미지 및 데이터의 포함여부 및 그 내용 량에 상관없이 서식지당 총 300,000Byte의 크기를 가지며 킬로바이트로 환산할 경우 약 293KByte 정도로 데이터의 양을 최소화 할 수 있다.

본 연구에서는 보안 및 전자의무기록의 법적 효력을 제공하기 위해 앞서 생성된 캡슐화 된 1차 해시 데이터에 대하여 그림 7과 같이 현재 국내 공인인증 방식인 SHA-256을 적용하여 2차 해시를 수행하게 된다.

그림 7. SHA-256 해시 작업을 위한 인증서 로그인
Fig. 7 Certificate login for SHA-256 hash operation

인증을 위한 SHA-256 해시 작업의 경우 각각의 문서를 별도로 처리하거나 당일 생성된 문서 데이터 중 SHA-256 해시 처리되지 않은 데이터에 대하여 일괄적으로 작업할 수 있도록 구현하였으며, 인증 처리된 문서의 경우 문서 내부에 SHA-256 해시 처리에 대한 작업자 및 작업일시 등을 기록하여 추후 해당 문서의 위조, 변조 여부를 확인할 수 있다.

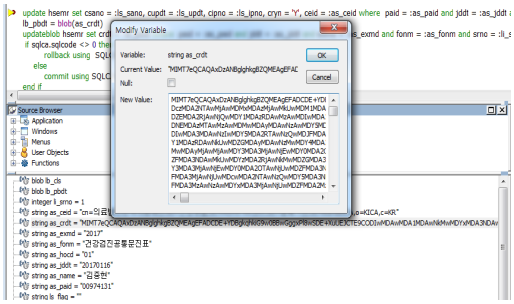

그림 8. SHA-256 해시 데이터 추출을 위한 디버그 화면
Fig. 8 Debug screen for extracting SHA-256 hash data

그림 8은 1차 해시를 진행한 후 생성된 PBBLOB 형식의 데이터에 2차적으로 SHA-256 해시 과정을 진행하여 생성된 데이터를 확인하기 위한 디버그 화면으로 2차 해시 코드 값이 저장된 변수의 값은 "MIMT7eQCAQAxDzANBglghkgBZQEAgEFADCDE+YDBgkqhkiG9w0BB..."과 같이 1차 해시를 통해 생성된 PBBLOB 데이터와는 전혀 다른 데이터로 생성되었다. 또한 이를 2중 복호화 하였을 경우 원본과 동일 한 문서로 변경됨을 확인 할 수 있었다.

이로 인해 전자문서에 대한 보안성이 강화되고 기존 그래픽파일 인증방식에 비해 1/3 이하의 처리 속도로 향상 시킬 수 있으며, 2차 해시 알고리즘을 통해 도출된 해시 데이터 역시 1차 해시를 통해 생성된 PBBLOB 형식의 데이터와 동일하게 293KB 으로 데이터 보관과 관련하여 다양한 장점을 가질 수 있다.

Ⅴ. 결 론

1차 해시 알고리즘을 통해 도출된 PBBLOB 데이터와 2차 해시 알고리즘인 SHA-256 형식을 통한 데이터 및 해당 전자문서에 대한 개인정보 및 기초 데이터를 한 ROW에 저장한다고 가정 할 경우 한 ROW에 저장된 데이터의 크기는 825KB 정도이다. 이는 1TB 용량에 저장 할 경우 약 1,260,260 ROW 만큼의 데이터를 저장 할 수 있으며, 이는 하루 200명의 환자에 대하여 1명당 평균 3개의 서식지가 발생하는 의료기관으로 가정하였을 경우 5년에서 6년 정도의 데이터를 보관할 수 있을 것으로 계산된다. 단, 이 수치는 압축 전의 계산으로 압축 알고리즘을 추가할 경우 이보다 더 높은 효율을 가질 수 있을 것으로 예상된다. 이렇게 서식지에 데이터를 포함하는 형태의 전자문서는 기존에 서식지와 데이터를 분리하여 데이터만을 인증하던 시스템과 달리 문서 자체에 전자서명을 적용하면서도 작은 용량과 빠른 처리가 가능하기 때문에 이를 이용한 진보된 형태의 EMR로 발전하거나 각종 EDI 관련 업무에 대한 적용이 가능할 것으로 기대된다.

본 논문은 학위논문의 일부를 발취하여 재구성하였음.

References

[1] S. Lim, K. Kang, J. Seo, and G. Kim, "The Development of Vital Sign Web Viewer Systems using HL7 Protocol," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 3, no. 2, 2008, pp. 112-117.

[2] H. Lee and J. Oh, "Design and Development of Health Screening Data Input Mobile Application Using App-Inventor," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 1, 2018, pp. 193-198.

[3] J. Choi, "The Development of Discharge Analysis Educational Program on NCS-Based for Medical Information Management," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 5, 2017, pp. 957-964.

[4] U. Park, "Inveted Article : Study for Improvement of the Doctor;s Satisfaction and Completeness of the Medical Record in the EMR System," *Korean J. of Hospital Management*, vol. 16, no. 2, 2011, pp. 19-30.

[5] Y. Noh, I. Choi, S. Jeong, and S. Kim, "The Study on Difference in Volume of the Data between Elecronic Medical Record and Paper-based Medical Record: Comparison of Chief Complaint and Present Illness on Medical Record," *J. of the Korea Socity of Health Informatics and Statistics*, vol. 32, no. 2, 2007, pp. 27-37.

[6] G. Kim, "A Study on Hash Function in Criminal Procedure," *Korean Criminological review*, vol. 29, no. 2, 2018, pp. 199-225.

[7] Y. Choi, K. Hong, and H. Lee, "Digital Signature Act(DSN) & PKI based on DSA," *Communications of the Korean Institute of Information Scientists and Engineer*, vol. 18, no. 1, 2000, pp. 13-20.

[8] D. Yang, *Information Security Introductory*. Seoul: Hanbit Academy, 2013.

[9] S. Oh, S. Kim, J. Kim, and Y. Ko, "File Similarity Evaluation Scheme Using Hash String," *J. of Korean Institute of Information Technology*, vol. 12, no. 5, 2014, pp. 65-72.

[10] H. Jin and E. Choi, "A Study on Factors Affecting the Reception Attitude toward Electronic Medical Record," *J. of Digital Convergence*, vol. 10, no. 4, 2012, pp. 279-268.

[11] H. Lee and J. Oh, "A Study on the Health Screening Solution by Using Electronic Medical Record," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 7, 2015, pp. 825-830.

저자 소개

이효승(Hyo-Seung Lee)

2005년 동국대학교 정보통신공학과 (공학사)
2008년 순천대학교 정보통신공학과 (공학석사)
2018년 순천대학교 컴퓨터공학과 (공학박사)
2013년 ~현재 청암대학교 컴퓨터정보보안과 강사
2016년 ~현재 순천대학교 컴퓨터공학과 강사
※ 관심분야 : 의료정보시스템, u-헬스케어, IoT

오재철(Jae-Chul Oh)

1978년 전북대학교 전기공학과 (공학사)
1982년 전북대학교 컴퓨터공학과 (공학석사)
1988년 전북대학교 컴퓨터공학과 (공학박사)
1984년~1986년 기전대학교 전자계산학과전임강사
1986년~현재 순천대학교 컴퓨터공학과 교수
※ 관심분야 : 임베디드시스템, USN, 네트워크 설계 및 분석