PCI DSS Compliance를 위한 개인정보 암호화 설계

우만균*, 박지수**, 손진곤*+
*한국방송통신대학교 대학원 정보과학과
**SW중심대학사업단, 충남대학교
e-mail : woody138@knou.ac.kr

Design of Personal Information Encryption for PCI DSS Compliance

Man Gyun Woo*, JiSu Park**, Jin Gon Shon*
*Dept. of Computer Science, Graduate School
Korea National Open University
**National Center of Excellence in Software, Chungnam National University

요 약

최근 들어 개인정보 보호의 중요성에 대한 인식이 높아지고 있다. 개인정보 위협 요소 증가 및 유출 사고 증가 등으로 개인정보 보호 필요성이 높아지고 있으며, 개인정보보호법 발효 및 시행에 따른 기술적 보호 마련을 위하여 외국계 카드 발행사에서 지속적으로 PCI DSS(Payment Card Industry Data Security Standard)의 준수를 요청하고 있다. 카드 소유자의 데이터를 전송, 처리, 저장하는 환경에 대한 인증으로 적격업체 선정의 자격을 주기도 한다. 이러한 보안성 심의 기준이 강화되고 있으나 DB 암호화 제품인 TDE(Transparent Data Encryption) 방식의 암호화 방법은 암호화 기능 이외에 접근제어, 키 기밀성 보장을 위한 옵션의 추가 도입 검토가 필요하며, 서비스를 위해서 DB 전용 메모리 영역(SGA)의 Buffer Cache에 평문(Plain Text)으로 복호화한 후 로드하여 사용하므로 예상치 못한 또 다른 심각한 데이터 유출의 위험이 있다. 본 논문에서는 개인정보 암호화 방법을 연구하고 구현과정에서 발생한 문제에 대한 해결 과정을 설명하였다.

1. 서론

최근 네트워크와 인터넷의 발달로 사회가 급속하게 정보화됨에 따라 개인 정보의 가치 또한 빠르게 상승하고 있다. IT 서비스가 점차 다양화되고 개인 맞춤형 서비스로 발전됨에 따라 수집된 개인 정보의 불법적인 접근 및 유출, 해킹 등의 문제가 발생함에 따라 정보보호에 대한 관심이 증대되고 있다.

국내는 2014년 대량 카드 정보 유출 사고 이후 금융관련 보안 대책이 수립되었고, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률(정보통신망법)과 개인정보보호법에 의거하여 ISMS(Information Security Management System) 인증 제도를 통하여 정보보호 관리체계를 구축/운영하는 조직에 대해 인증기관이 객관적이고 독립적으로 평가하여 적합성 여부를 판단하고 있다.

최근 전자상거래와 핀테크가 발전되고 있으며, 결제산업이 핀테크 분야의 핵심 인프라가 예상되어 지불카드 정보보호의 중요성은 더욱 커지고 있다.

개인정보 유출 사고의 발생 원인을 살펴보면 금전적 이익을 얻기 위해 해킹 등 외부 침입으로 개인 정보가 유출되거나 내부자의 도용으로 누출되는 것으로 파악된다.

국내에서 발생한 주요 개인정보 유출 및 도용 관련 사건의 경우 대부분 금전적인 이익을 목적으로 하고 있다[1].

일반 기업에서 PCI DSS Compliance를 위한 개인정보 암호화 방법에 대한 안내를 받기 위해서는 특정 업체의 솔루션을 도입해야 하므로 실제로 구현을 위해서는 시간과 비용이 발생하며, 기존 방식의 개인정보 암호화 방법에서는 암호화에서 핵심 보안 요소인 키의 저장방식(키 기밀성)의 문제와 비밀번호와 같은 복호화를 할 수 없도록 규정한 항목에 대해서 복호화가 가능한 문제를 가지고 있다. 본 논문을 통하여 PCI DSS Compliance를 위한 개인정보 암호화 방법을 암호화 컬럼 사이즈 변환 방식으로 연구하고 연구 과정에서 발생한 문제에 대한 해결 과정을 설명하고자 한다.

2. 관련연구

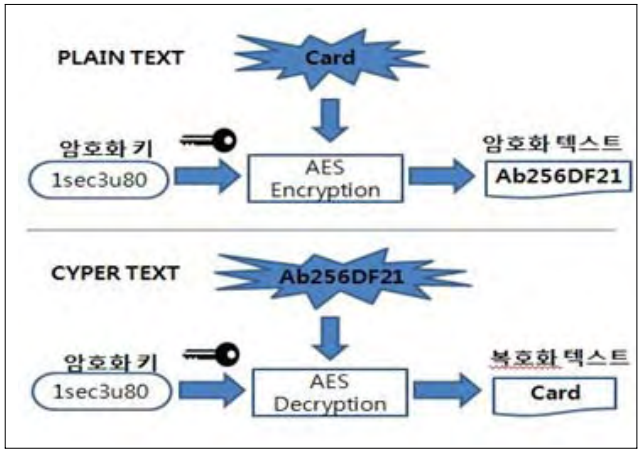
2.1 암호화 알고리즘

개인정보 암호화에 이용할 수 있는 암호 알고리즘으로 키의 특성에 따라 대칭키 혹은 비밀키 알고리즘, 공개키 알고리즘, 해시 알고리즘으로 분류할 수 있다. 개인정보 암호화의 경우 이름이나 주민등록번호와 같이 질의 처리마다 암/복호화가 지속적으로 발생하는 경우 속도가 빠른 대칭형 알고리즘이 적당하고, 고객의 패스워드와 같이 굳이 복호화가 필요 없는 항목인 경우에는 해시 알고리즘을 사용하는 것이 적당하다[2].

+교신저자

2.2 AES 알고리즘

AES(Advanced Encryption Standard) 알고리즘을 이용한 데이터베이스 암호화는 1990년대 들어 DES(Data Encryption Standard) 암호의 해독 가능성이 높아지고 1998년을 기점으로 DES는 표준 기한이 만료됨에 따라 미국 NIST(National Institute Of Standards and Technology)에서 1997년 9월 암호 키의 길이가 128 비트 이상인 새로운 블록 암호인 AES를 공모하였다. 총 21개가 응모하여 그중 1998년 8월 15개의 1차 후보가 올라, 1999년 4월 5개의 후보로 압축하여 최종적으로 2000년 10월 2일에 벨기에에서 제안해 만든 Rijndael(Rijmen & Daemen)이 AES로 채택되었다. Rijndael은 다른 AES 후보 기술보다 보안성, 성능, 효율성, 구현 용이성, 유연성 등의 항목에서 가장 우수한 기술로 평가받았고, 또한 이 기술은 서로 다른 다양한 컴퓨팅 환경에서도 우수한 성능을 보여주고 메모리를 적게 차지해 스마트카드 등 메모리 용량이 적은 장치에서 손쉽게 사용될 수 있다는 점이 특징이다. AES를 이용한 암호화 과정은 <그림1>과 같다[3].



<그림 1> AES를 이용한 암호화 과정

Rijndael알고리즘은 암호화와 복호화에 필요한 키를 동일하게 갖는 대칭형 블록암호로서, 128, 192, 256비트의 블록 크기와 키 길이를 지원한다. 암호화의 키 길이와 암호화의 기본 단위인 블록의 크기를 128, 192, 256비트 등으로 선택할 수 있다. 따라서 이 알고리즘에서는 키와 블록의 크기를 조합한 9가지의 다양한 선택이 가능하지만, 표준에서는 데이터 블록의 크기는 128비트로 제한하고 키의 크기는 128, 192, 256비트 중 선택할 수 있도록 하였다[4].

이 알고리즘의 장점으로는 다양한 키 길이를 갖고 있으며, 현재까지 발표된 취약점을 갖고 있지 않고, 소프트웨어나 하드웨어 상에서도 효율적으로 작동하고, 스마트카드 상에서도 동작하는 등의 장점이 있다[4].

본 논문에서는 개인정보 암호화 알고리즘으로 빠른 암·복호화 속도를 요구하며 암호키의 안정성을 위하여 AES 알고리즘을 사용하게 되었다.

2.3 PCI DSS 인증의 정의와 준수 목적 및 범위

PCI DSS는 결제 카드 브랜드 5개(VISA, Master, JCB, AMEX, Discover)사가 전개하고 있는 보안 프로그램의 근거가 되는 국제 데이터 보안 표준을 말하며 카드 소지자의 데이터를 저장, 처리, 전송하는 모든 사업자가 준수해야한 규칙을 정의한 표준이다. 그 검증 방법과 정도는 카드 브랜드 회사마다 정하고 있는 PCI DSS 운영 단체인 PCI SSC(PCI Security Standards Council)는 지불 카드 산업과 그들을 둘러싼 환경의 정보보안을 위해 국제 카드 브랜드 회사 5개에 의해 설립된 보안 협의 단체이며 주요 역할은 지불 카드 업계에 있어서 국제 표준 보안 PCI DSS의 유지관리, 인증감사기관(QSAC)의 인증관리 등을 관리하고 있다.

PCI DSS 준수 목적은 PAN(Primary Account Number)과 그에 따른 카드 소유자 데이터를 보호하는 것이 가장 큰 목적이며 준수 범위는 카드 소유자 데이터를 전송, 처리, 저장하는 환경, CDE(Common Desktop Environment)에 영향을 미치는 시스템 환경으로 범위를 정하고 있다. 2015년 1월 1일부터 PCI DSS의 최신 버전인 규격 3.0으로 전환되었으며 구체적인 내용은 6그룹에 12개의 요건, 요건별 보안 평가 절차는 399개 항목으로 나누어진 요구사항이라고 할 수 있다. PCI DSS 준수의 대응이 요구되는 기업으로 신용카드회사, 결제 대행 사업자, 가맹점이며 업종별로는 금융업(신용카드회사, 보험회사), 유통업(슈퍼, 편의점, 양판점, 백화점), 통신 판매업, 외식업, 운수업(철도, 항공, 택시 회사), 통신업(통신회사, ISP, CATV), 인터넷 비즈니스 산업(E커머스, 온라인 게임, 콘텐츠 공급자), 기타(병원, 교육, 주유소) 등이 있다. 이러한 이유로 결제 대행 사업자에 PCI DSS 인증 준수의 요구가 꾸준하게 요구되고 있으며 가맹점영업 및 자사 홍보의 수단으로 신용카드와 카드소유자의 데이터를 안전하게 보호한다고 활용하기도 한다.

3. 제안하는 개인정보 암호화 설계

3.1 개인정보 암호화 설계의 이슈사항

개인정보 암호화 시 고려해야 할 사항으로 실시간으로 데이터 암호화를 지원해야 하는 점이다. 신용카드 결제 시스템은 대표적인 24시간*365일 항시적인 서비스를 제공해야 하는 서비스로 중단이 발생하지 않아야 한다. 또한, 승인 시스템의 거래에 대해서 부하 분산을 위하여 DB 서버를 2개의 장비에 나눠서 동일한 구조의 데이터베이스에 거래내역을 동일하게 저장해야 하며 동일한 건수의 처리내역이 저장되어야 하는 이슈 사항이 있다.

신용카드 승인 요청 후에 카드사에 승인 처리를 한 이후 응답을 전송하기까지 3초 이내에 처리가 되어야 정상적인 처리가 된다. 취소 거래 시 원승인 거래의 조회 시에 3초 이상의 시간 소요가 되지 않도록 인덱스 처리가 되어야 한다.

신용카드 카드번호 암호화 처리 작업 후 지정된 인덱스를 스캔함에 있어 암호화된 데이터베이스의 원거래 검색에 대한 쿼리는 PLAIN TEXT(clear 한 카드번호)와 CYPER TEXT(암호화된 카드번호)를 조건으로 원거래 검색 시 정상적인 거래 건을 조회할 수 있어야 한다.

3.2 DB암호화 대상항목 및 정책

암호화 항목은 개인정보보호법 및 정보통신망법에 의거하여 정보 유출시 문제가 되는 DB(테이블/컬럼) 항목을 암호화하기로 정하고 대상 항목을 분류한다.

고유식별번호 : 주민등록번호(외국인등록번호), 여권번호
단방향암호화 : 비밀번호
금융관련정보 : 계좌번호, 신용카드번호
기타 : 성명, 전화번호, 휴대폰번호, 이메일 주소, 주소

암호화 항목 중 기타 항목을 제외한 타 항목은 전체를 암호화하는 것으로 원칙을 정하고 업무 필요성에 부분 암호화를 해야 할 경우 필요 정보를 컬럼을 분리하여 저장하고 원 컬럼은 전체 암호화를 한다. 하나의 필드에 다수의 속성값이 혼용되어 저장되는 경우에는 암호화 항목에서 제외한다.

암호화 정책은 전체암호화를 하는 경우에는 AES 256비트로 전체암호화를 진행하고 복호화가 불가능한 단방향 암호화는 SHA 256비트로 전체암호화를 진행한다.

3.3 DB 마이그레이션

암호화 정책 결정 후 DB 암호화 대상 컬럼을 조사하여 암호화 대상 컬럼에 대하여 데이터베이스 마이그레이션 계획을 세우게 된다. 데이터베이스 암호화시 Block Cipher 알고리즘을 사용하므로 16Byte 단위로 암호화 출력 사이즈가 변동되며 원본 데이터의 무결성을 검증하기 위한 HMAC값 16Byte가 추가된다. 암호화된 데이터는 Base64로 인코딩된 텍스트 형태로 저장되며 초기 암호화 시 기존 컬럼의 사이즈를 <표 1>를 참조하여 변경 작업이 선행되어야 한다.

<표 1> 암호화 컬럼 사이즈 변환표

구 분	컬럼 사이즈 변환 값					
원 본 데 이 터 (Byte)	1~15	16~31	32~47	48~63	64~79	80~95
Base64(Byte)	24	44	64	88	108	128
구 분	컬럼 사이즈 변환 값					
원 본 데 이 터 (Byte)	96~111	112~127	128~143	144~159	160~175	176~191
Base64(Byte)	152	172	192	216	236	256
구 분	컬럼 사이즈 변환 값					
원 본 데 이 터 (Byte)	192~207	208~223	224~239	240~255	256~271	272~287
Base64(Byte)	280	300	320	344	364	384
구 분	컬럼 사이즈 변환 값					
원 본 데 이 터 (Byte)	288~303	304~319	320~335	336~351	352~367	368~383
Base64(Byte)	408	428	448	472	492	512
구 분	컬럼 사이즈 변환 값					
원 본 데 이 터 (Byte)	384~399	400~415	416~431	432~447	448~463	
Base64(Byte)	536	556	576	600	620	
※ 계산법 : ((평문길이) + (16) - ((평문길이)%(16)) +2)/3*4						

각 시스템 간의 데이터 연계 시 단계별 암호화 적용에 따라 각 연계 단위로 암호화 또는 복호화를 수행하거나 기존 데이터 연계 방식을 그대로 유지하도록 하며 전체 연계 내역은 평문 데이터를 암호화된 DB 영역에 전달하는 경우 암호화 적용하고 암호화된 데이터를 평문 데이터 영역에 전달하는 경우 복호화를 적용하며 암호화된 데이터를 암호화된 DB 영역에 전달하는 경우 기존 연계방식 유지하며 평문 데이터를 평문 데이터 영역에 전달하는 경우 기존 연계 방식을 유지하도록 관리한다.

3.4 DB 이관

암호화 DB 구성과 관련하여 기존 운영 중인 신용카드, 현금영수증, 직불, 현금IC, 포인트 거래의 원장 정보에 대하여 승인에 필요한 최소 기간(3개월, 약 90일)의 거래내역에 대한 데이터 마이그레이션 작업이 병행되었으며 마이그레이션 된 타겟 데이터베이스에 대한 검증 시 암호화 컬럼에 대한 항목이 정확하게 암호화 처리 여부를 SQLAPI(쿼리)를 통하여 데이터 검증을 진행하였다. 추가로 프로그램 구현은 승인 처리 플로우 상에서 데이터베이스에서 조회하는 행위가 발생 시에는 DB 복호화 작업을 수행하는 프로그램을 개발하고 데이터베이스에 저장하는 행위가 발생 시에는 DB 암호화를 통하여 데이터베이스에 저장하도록 프로그램을 구현하였으며 데이터 마이그레이션 진행 시 암호화 컬럼사이즈 변환표에 의거하여 소스데이터베이스 컬럼의 사이즈가 증가된 컬럼의 크기로 대상 테이블을 신규로 생성하였고 마이그레이션이 끝난 이후에 인덱스 추가 및 통계정보 생성을 추가하였다.

4. 성능평가

4.1 실험 데이터 및 성능평가

제안하는 방법으로 암호화 설계 이후 데이터베이스 암호화 프로그램 개발 및 마이그레이션이 완료된 상태에서 데이터베이스 암/복호화 거래에 대한 테스트를 진행하였다. <표 2>에서는 암호화 정책 서버 로그인 시 시간 지연이 없이 로그인 처리됨을 알 수 있었다.

<표 2> 암호화 정책 서버 로그인 테스트

순번	시작시간	종료시간	수행시간
1	13:46:50	13:48:46	0:01:56
2	13:46:50	13:48:47	0:01:57
3	13:46:50	13:48:50	0:02:00
4	13:46:50	13:48:50	0:02:00
5	13:46:50	13:48:46	0:01:56
6	13:46:50	13:48:47	0:01:57
7	13:46:50	13:48:46	0:01:56
8	13:46:50	13:48:46	0:01:56
9	13:46:50	13:48:46	0:01:56
10	13:46:50	13:48:46	0:01:56
동시프로세스 : 10ea 테스트횟수 : 1ea 프로세스당 100만번 login 수행 검증요건 : login 시간이 0.5초 이상 지연 발생 검증 테스트결과 : 동시 프로세스 10ea에서 지연 발생 없음 확인			

현재 개발된 시스템이 OLTP 환경의 승인 처리 시스템이므로 성능 테스트의 우선 과제는 암호화 처리 시간의 검증이 중요하다. 승인 건별 DB 암/복호화 시간 테스트의 결과는 <표 3>, <표 4>와 같다.

<표 3> 승인 건별 DB 암호화 시간 테스트

클라이언트 프로세스개수	전송건수	전체 수행시간	0.01초 이상 소요건	max 암호화 소요시간
1개	1000건	2.748664초	9건	0.0419초
1개	1만건	22.63185초	50건	0.0525초
1개	10만건	229.7603초	591건	0.215729초
10개	1만건* 프로세스 10개	50.61357초	2956건	0.36128초
평균 암호화 시간 : 0.002685초(0.01초 이상 소요건 제외) 테스트회수 : 1ea 클라이언트로 1000번, 1만번, 10만번 수행 검증요건 : 최대암호화 소요 시간 검증 테스트결과 : 암호화 서버 MAX 처리 프로세스 도달 전까지 0.01초 이내 암호화 처리됨을 확인				

<표 4> 승인 건별 DB 복호화 시간 테스트

클라이언트 프로세스개수	전송건수	전체 수행시간	0.01초 이상 소요건	max 복호화 소요시간
1개	1000건	2.3399초	6건	0.023987
1개	1만건	22.87916초	49건	0.049432
1개	10만건	236.813초	550건	0.112581
10개	1만건* 프로세스 10개	51.9943초	2863건	1.81121
평균 복호화 시간 : 0.002281초(0.01초 이상 소요건 제외) 테스트회수 : 1ea 클라이언트로 1000번, 1만번, 10만번 수행 검증요건 : 최대복호화 소요 시간 검증 테스트결과 : 복호화 서버 MAX 처리 프로세스 도달 전까지 0.01초 이내 암호화 처리됨을 확인				

5. 결론

지금까지 PCI DSS Compliance를 만족하는 개인정보 암호화를 위한 정책 및 적용 기준을 알아보고 암호화 설계 과정에 대하여 설명하였다. PCI DSS 준수를 원하는 기업이 PCI DSS 준수를 위한 환경의 범위를 잘못 이해하여 PCI 프로젝트를 다시 시작하거나 요구 사항이 누락되어 프로젝트를 광범위하게 변경하지 않기 위해서 PCI DSS 준수 요구사항의 정확한 이해가 중요하다[5][6].

PCI DSS 평가 항목 중 일반 기업에서 구축을 위하여 가장 많은 시간과 비용이 소요되는 항목이 카드 소유자 데이터 보호 항목이다[7][8]. PCI DSS는 카드 정보 보호를 위하여 카드 정보가 처리되는 모든 시스템의 보안통제를 위한 기술적, 관리적 기준이라고 할 수 있다. 결론적으로 데이터베이스의 민감한 데이터의 보호를 위한 PCI DSS Compliance를 만족한다는 것은 저장된 데이터베이스를 암호화하는 것 이상을 의미한다. 정보보호 시스템 관리 및 암호화 관리 및 물리적 관리와 정보보호 활동에 대한 전반적인 관심과 보안을 책임지는 담당자는 물론 전사의 직원이 기업의 중요 정보자산 및 고객 정보를 보호하기 위해서 권고되는 수준으로 관리대책을 실시하여 정보보안사고의 발생 가능성을 줄이고, 정보보호 관리에 대한 인식 제고를 통해 사고가 발생하더라도 신속한 대응으로 기업의 가치 향상과 비즈니스 연속성을 보증하기 위한 기본적인 자세라고 할 수 있다.

참고문헌

[1] 이병엽, 박준호, 김미경, 유재수, “데이터베이스 규제 준수, 암호화, 접근제어 유형 분류에 따른 체크리스트 구현”, 한국콘텐츠학회논문지, Vol 11, No 2, 2011.

[2] 김보선, 홍의경, “교무업무시스템을 위한 데이터베이스 암호화 구현 및 성능 평가”, 멀티미디어학회논문지, Vol 11, No 1, 2008.

[3] 김천식, 김형중, 홍유식, “암호화 데이터베이스에서 영역 질의를 위한 기술”, 전자공학회 논문지, 제45권 CI편 제3호, 2008.5

[4] 전상덕, “AES 알고리즘을 이용한 데이터베이스 보호에 관한 연구”, 연세대학교 공학대학원, 2003.8

[5] James Rees, “The Challenges of PCI DSS compliance”, Computer Fraud & Security, December 2010.

[6] Georges Ataya, “PCI DSS audit and compliance”, Information Security Technical Report, 2010.

[7] 김동국, 장성용, “결제카드산업 데이터보안표준(PCI DSS) 적용방안에 대한 고찰”, 정보보호학회지, Vol 18, No 4, 2008.8

[8] 최용, “신용카드 정보보안 표준(PCI DSS)준수 방안에 관한 연구”, 한양대학교 공학대학원, 2009.2