SEED 블록암호알고리즘을 적용한 통합 사례관리 시스템(ICMP) 개발에 관한 연구

오동식* ·김영혁** ·임일권** ·이계귀** ·이재광**
*누리뜰 희망IT ·**한남대학교 컴퓨터공학과

A study on SEED block cipher algorithm for ICMP development

Dong-Sic Oh* ·Young-Hyuk Kim* ·Il-Kwon Lim* ·LiQiGui* ·Jae-Kwang Lee*
NuRiTteul Hope IT ·**Dept. of Computer Engineering, Hannam University
E-mail : *ods716@hanmail.net, **{yhkim, iklim, gkli, jklee}@netwk.hannam.ac.kr

요 약

본 논문에서는 보안성과 신뢰성에 우수한 특성을 갖는 국제 표준 SEED 블록 암호 알고리즘을 적용한 통합 사례관리 시스템(ICMP)을 제안하였다. 기존 통합 사례관리 시스템의 취약부분인 보안성과 신뢰성, 사용자 편의성 부분을 개선하여 최적화된 시스템에 탑재 되도록 Spring 기반 JAVA Framework 기술에 SEED 블록 암호 알고리즘을 적용하여 성능을 개선하였다. 그 결과로 사용자 인터페이스 부분의 성능을 개선하였으며 실제 응용분야에 적용 가능하다.

ABSTRACT

In this paper, propose for the international standards of security and reliability SEED block cipher algorithm is applied to the ICMP. This paper is improve security, reliability and user comfort of weakness existing integrated case management system on spring based java framework technology. As a result, part of the user interface to improve performance and can be applied to real world applications.

키워드
SEED, ICMP, Spring, Java Framework

Ⅰ. 서 론

사례관리의 개념이 도입된 이래로 10여년이 지난 지금 그 관심이 학문적, 실천적 차원을 넘어 정책적 차원으로까지 확대되고 있다. 이는 미국, 영국, 독일과 일본까지 사례관리가 서비스 전달체계의 핵심으로 발전되어 왔다.[1]

사례관리의 목적은 첫째 질병, 빈곤 등 복합적 문제를 갖고 있는 대상자들에게 건강관련 정보를 제공하고, 관리 능력을 배양하게 하는데 있으며[2], 크게 2가지 의미로 구분할 수 있다.[3]

첫째는 사례관리 실천에 관심을 갖는 개념으로, 사례관리를 사회복지실천의 한 방법으로 간주하는 것이다.

둘째, 사례관리체계에 관심을 갖는 개념으로 지역사회조직과 같은 옹호자로서의 기술을 강조하는 좀 더 거시적인 개념이다.

통합 사례관리는 사회복지, 의료, 재활, 정신건강 등 다양한 분야에서 사용되는 방법이며, 노인, 장애인, 노숙인 등 다양한 대상층에 적용되

는 특성을 가지고 있다. 이러한 적용영역의 광범위성과 다양성은 '사례관리'라는 용어의 정의가 매우 다양하며, 널리 수용되는 정의는 없다는 사실을 뒷받침한다. 장애인복지영역에서 사례관리를 정의함에 있어서도 이러한 다양성으로 인한 어려움이 존재하는데, 이는 사례관리가 사회문화적, 정치적 환경변화에 조응하면서 진화하는 개방적 개념[4]이라는 점에 기인한다.

이러한 관심과 함께 점차 사례관리 시스템의 필요성이 대두 되었고 통합 사례관리 시스템이 복지 기관 및 요양원에서 사용 되어왔다. 그러나 사례관리 시스템의 Server & Client 구조로 인한 동시 다발적으로 발생하는 Client들의 불규칙한 접속 환경 하에서 보안 신뢰성과, 사용자 편의성을 개선해야 할 필요성이 대두되어왔다. 이에 본 논문에서는 기존 통합 사례관리 시스템의 취약부분인 보안성과 신뢰성, 사용자 편의성 부분을 개선하여 최적화된 시스템에 탑재 되도록 Spring 기반 JAVA Framework 기술에 SEED 블록 암호 알고리즘을 적용하여 성능을 개선하고자 한다.

II. 관련연구

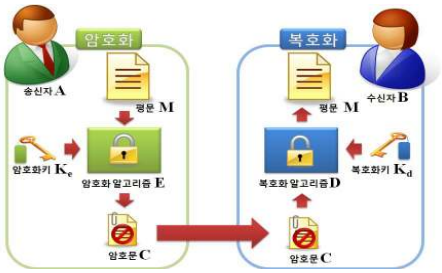
통합사례관리 시스템에 적용할 암호화 알고리즘은 국내 암호화 기술을 적용하는 취지에 입각하여 SEED, ARIA, HIGHT를 후보군에 올리게 되었다.

1. SEED 블록 암호 알고리즘

블록암호알고리즘 SEED는 128비트의 비밀키를 이용하여 128비트의 평문을 암호문으로 변환하는 암호 알고리즘을 말한다. SEED는 1999년 9월 TTA 표준으로 제정(TTAS.KO-12.0004)된 이후 금융권, 전자상거래, 정보보호제품(VPN) 등의 다양한 분야에서 데이터의 기밀성(Confidentiality)과 무결성(Integrity) 기능을 제공하기 위해 사용되고 있으며, nCipher, RSA Security, Chrysalis-ITS 등의 국외 주요 정보보호업체를 포함한 670개 이상의 국내외 산 학 연에서 SEED를 사용하고 있다.[5] 2010년 기준 전 세계적으로 한국을 비롯한 4개국만이 자국의 국산 블록 암호 알고리즘을 국제 표준으로 갖고 있으며, SEED의 경우 2010년 인터넷전화 사용자간 통화내용의 도청 등을 방지하기 위한 암호알고리즘(RFC5669)과 보안통신을 위해 암호키를 전달하는 기술(RFC5748) 등 2가지가 국제표준으로 등록되었을 만큼 국제표준과 신뢰성이라는 배경을 가지고 있다.

블록암호알고리즘의 경우, 암호알고리즘이 적용되는 블록크기가 정해져있기 때문에 정해진 길이보다 긴 데이터를 암호화하거나 데이터 무결성 검증을 하기 위해서는 블록암호알고리즘의 운영모드를 반드시 사용하게 된다. 부가적으로, 입력 데이터의 길이가 기본 블록크기의 배수가 되지 않으면 처리가 불가능하므로 입력 메시지의 길이가 블록 길이의 배수가 되도록 하기 위해 덧붙이기 방법을 사용해야 한다. 이에, 한국정보보호진흥원에서는 안전성 측면과 효율성 측면을 고려하여 SEED의 사용을 촉진하기 위해 SEED의 운영모드를 TTA 표준(안)으로 제안하여, 2003년 12월 TTA표준(TTAS.KO-12.0025)으로 제정하였다[6].

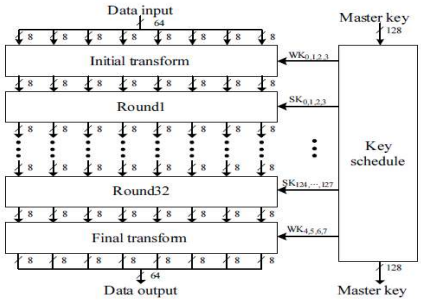
SEED는 대칭키 암호 알고리즘으로써, 블록단위로 메시지를 처리하는 국내표준 블록 암호 알고리즘이다. n비트 블록 암호 알고리즘이란 고정된 n비트 평문을 같은 길이의 n비트 암호문으로 바꾸는 함수를 말한다(n비트: 블록크기). 이러한 변형 과정에 암호키가 작용하여 암호화와 복호화를 수행한다.[7]



[그림 1] 암□복호화 과정

2. HIGHT 블록 암호 알고리즘

HIGHT는 RFID, USN 등과 같이 저전력 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 2005년 KISA, 구)국가보안연구소 및 고려대가 공동으로 개발한 64비트 블록암호 알고리즘으로 128비트 마스터키, 64비트 평문으로부터 64비트 암호문을 출력하고, SEED, AES 등 기타 알고리즘보다 간단한 구조로 설계되었다.[8] 그러므로 본 논문에서 목표로 하는 통합사례관리 시스템은 HIGHT가 목적으로 하는 규모의 컴퓨팅 환경이 아니므로 암호 알고리즘을 적용하는데 있어 부합하지 않는다.

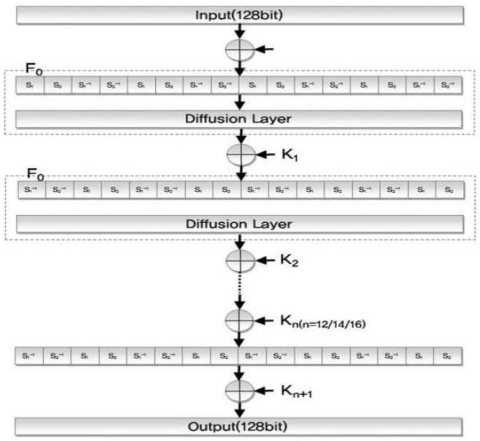


[그림 2] HIGHT block diagram

3. ARIA 블록 암호 알고리즘

ARIA는 경량 환경 및 하드웨어 구현을 위해

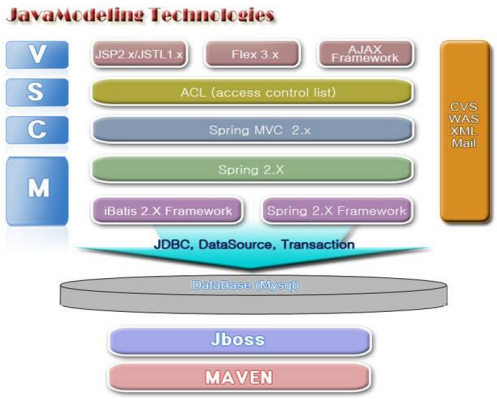
개발된 블록 암호알고리즘으로써 SEED와 함께 국내의 대표적인 표준 블록 알고리즘이다. Involutinal SPN 구조로 되어 있으며, 128비트 블록크기와 가변키(128, 192, 256비트) 크기에 따라 라운드 수(12, 14, 16)가 결정되는 구조이다. ARIA는 하드웨어 구현 및 8비트 환경에서 뛰어난 효율성을 가지고 있어 스마트카드 등 저전력 · 저성능의 플랫폼 및 ASIC에 적합하다. 물론 32비트 프로세서 등 고성능 플랫폼에도 적용은 가능하나 알고리즘의 성격상 경량 환경에 적합하므로 대규모 데이터베이스를 운용하는 거대 시스템에는 SEED가 더 적합한 면을 가지고 있다.[9]



[그림 3] ARIA architecture

III. SEED 블록 암호 알고리즘을 적용한 simulation

본 연구를 하기 위한 기본적인 시스템 구성은 다음과 같다.



[그림 4] Spring기반 통합 사례관리시스템 기본 구성모듈

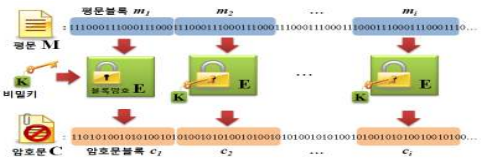
통합 사례관리 시스템은 Spring기반의 Java Framework로 구현을 하였으며, ICMP에 접속하는 방법은 웹페이지의 URL에 직접 IP주소를 입력하여 Server에 접근하는 방식을 사용하고 있다.

[그림 5] Client-Server 접속 과정

문제는 이러한 과정에서 Server의 IP주소와 위치가 외부로 노출되어 DDoS, Redirection, SQL injection 등과 같은 악의적인 공격을 받을 위험이 높다는 점이다. 특히 통합 사례관리의 특성상 많은 사용자들의 신상정보부터 공개를 꺼리는 비밀정보가 포함되어 있으므로 암 복호화를 통한 안전 접속은 중요한 문제이다.

IV. Simulation 결과

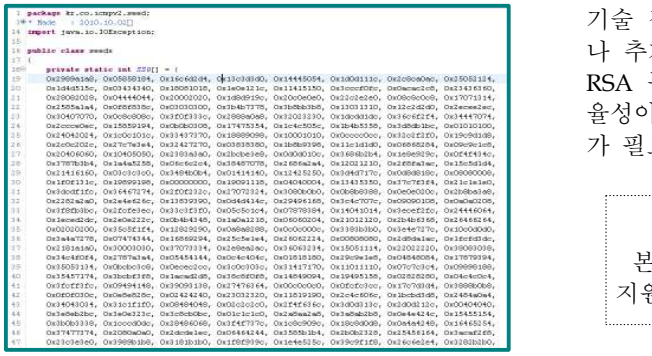
본 논문에서는 SEED의 운영 모드인 ECB, CBC, CFB, OFB, CRT 중 ECB모드로 구현을 하였다.



[그림 6] ECB 모드

시뮬레이션 결과는 외부 인터페이스의 이동 간에 발생하는 암□복호화 과정이다. 따라서 결과 확인을 위해 별도의 CUI 환경에서 확인하였다.

첫 번째 시뮬레이션 작업은 IP 주소를 암호화하여 네트워크상의 클라이언트들이 서버에 접속할 수 있게 보안 접근성을 개선한 부분이며, 두 번째 서버 접속 후 ID 와 Password를 접근함에 있어서 2차 보안 알고리즘을 적용하였다.

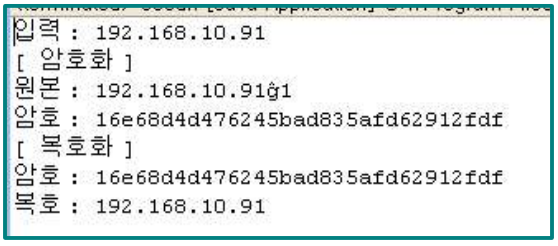


[그림 7] SEED algorithm code

```
byte pbUserKey[]  = {(byte)0x00, (byte)0x00, (byte)0x00, (byte)0x
                     (byte)0x00, (byte)0x00, (byte)0x00, (byte)0x

String str = "password";

char b = '\u011D';
String str1 = str + b;

System.out.print("입력 : ");
System.out.print(str);
System.out.print("\n");

byte[] passwordBytes = str1.getBytes("UTF-8");
int len = passwordBytes.length;
byte[] keyBytes = new byte[16];
if (len >= 16) {
    System.arraycopy(passwordBytes, 0, keyBytes, 0, 16);
 } else {
    System.arraycopy(passwordBytes, 0, keyBytes, 0, len);
     for (int i = 0; i < (16 - len); i++) {
        keyBytes[len + i] = passwordBytes[i % len];
     }
 }
```

[그림 8] password를 입력 받아서 구분기호와 패딩 작업 부분

최종적으로 구현된 결과물은 암호화가 이루어지면 DB에 저장되고, 이는 ICMP에서 접속 이벤트가 발생 시 복호화되어 화면상에 노출되지 않고 접속이 가능하게 된다.



[그림 9] SEED를 통한 ICMP 암 복호화

V. 결 론

사례관리는 전 세계적으로 복지서비스를 위해 대두되고 서비스이다. 본 논문에서 통합 사례관리 시스템을 구현하였고, Client-Server간의 접속 방식의 보안상 문제점을 해결하기 위하여 SEED, HIGHT, ARIA를 분석하였다. 각 암호화 알고리즘 특성상 적합하다 판단되는 SEED 알고리즘을 적용한 실험으로 기존에 노출되었던 보안상의 문제를 해결하였다. 이번 연구에서는 국내 표준 기술 접목을 위해 SEED 알고리즘을 사용하였으나 추가 연구 과제로서 ARIA, HIGHT 및 AES, RSA 등의 암호화 알고리즘을 적용하여 가장 효율성이 높은 암호화 알고리즘을 검증하는 연구가 필요하다.

감사의 글

본 연구는 중소기업청 2010 산학공동개발 지원사업의 지원을 받아 연구되었음

참고문헌

[1] 김영숙, 정국인, 박소라, “재가노인 사례관리의 욕구사정 정확도 향상을 위한 욕구추출 알고리즘 개발”, 한국사회복지학, Vol. 60, No. 1, 2008.

[2] 신영석, 신현웅, 황도경, “의료급여 사례관리 및 효과분석 Ⅱ”, 한국보건사회연구원 연구보고서, 2008.

[3] 정순둘, "재가노인을 위한 사례관리 네트워크 분석", 한국사회복지학 35권, 1998.

[4] 우국희, 김영숙, 임효연 , "지역사회복지관에서의 사례관리에 대한 사회복지사들의 주관적 경험과 인식", 사회복지정책 , 2007.9.

[5] 임선간, 강성우, “블록암호알고리즘 SEED의 운영모드 표준”, TTA journal, No.92, 2004.

[6] KISA, "블록암호알고리즘 SEED의 운영모드“, TTAS.KO-12.0025, 2003.

[7] 채철주, 이성현, 이재광, “자바 카드 API를 이용한 SEED 알고리즘 구현”, 한국콘텐츠학회 춘계종합학술대회 논문집, 2004 May 01.

[8] 한국인터넷진흥원, “HIGHT 블록암호 알고리즘 사양 및 세부 명세서”, 2009.

[9] 김용민, 김동규, 이문규, “전력분석공격 방지 기법을 적용한 ARIA 하드웨어 모듈 구현”, 대한전자공학회 하계학술대회 Vol. 33, No. 1, 2010.