http://dx.doi.org/10.14400/JDPM.2013.11.12.311

스마트 그리드 환경에서 개인정보 보호를 위한 효율적인 비밀분산 데이터 관리 방안

이성용*, 여상수*
목원대학교 컴퓨터공학부*

Efficient Secret Sharing Data Management Scheme for Privacy Protection in Smart Grid Environment

Sung-Yong Lee*, Sang-Soo Yeo*
Division of Computer Engineering, Mokwon University*

요 약 스마트 그리드 환경에서 소비자의 개인 프라이버시를 보호하기 위해서, 민감한 개인정보 데이터에 대한 보안 정책과 기술 프레임워크를 마련하는 것은 매우 중요한 일이다. 본 논문은 스마트 그리드에서의 개인정보보호를 위해서 제안된 데이터 비밀분산 관련 기법들을 소개하고, 기존 기법들의 문제점을 설명한다. 본 논문에서 제안하는 기법은 분산、복원 알고리즘에서 라운드 횟수를 감소시키고, 데이터베이스의 개수 또한 조절할 수 있도록 함으로써 효율성과 안전성 측면에서 향상됨을 보여준다.

주제어 : 스마트 그리드, 개인정보보호, 비밀분산, 보안

Abstract It is very important to design security policy and technical framework on sensitive private data in order to protect user privacy in smart grid environment. This paper introduces secret data sharing schemes proposed for privacy protection in smart grid, and presents technical problems of them. The proposed scheme in this paper, reduces the number of rounds in sharing process and also in restoration process, and can select how many databases would be used, so eventually it shows enhancements in terms of efficiency and security.

Key Words : Smart Grid, Privacy Protection, Secret Sharing, Security

1. 서론

스마트 그리드는 전기 시스템의 융통성, 보안, 신뢰성, 효율성 그리고 안전성을 향상시키기 위하여 각종 센서를 사용하여 감시하고 관리하고 자동화하며, 각종 IT 기술을 접속시킨 지능형 전력망을 의미한다[1]. 기존 폐쇄적인 구조의 전기 시스템과 달리 스마트 그리드는 전기의 발전, 송배전, 소비 등에 관련된 다양한 요소들이 통합된 네트워크 구조를 이루고 있으며, 이를 통해서 양방향 통신을 지원하는 개방형 전력 시스템이 스마트 그리드의 주된 특징이다[2]. 개방형 양방향 통신은 스마트 그리드의 핵심으로서, 이 기술을 바탕으로 기존 전기 시스템에 비해 자기 복구, 수요반응, 전력 품질보장, 전력거래등과 같은 다양한 기능들을 제공하게 된다. 이처럼 양방향 통

* 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2011-0014394).
Received 10 September 2013, Revised 6 December 2013
Accepted 20 December 2013
Corresponding Author: Sang-Soo Yeo (Mokwon University)
Email: sangsooyeo@gmail.com

ISSN: 1738-1916

신 구조는 전반적인 전기 시스템 운영에 있어서 다양한 기능과 향상된 효율을 기대할 수 있지만 기존의 폐쇄형·단독망 구조의 전기 시스템 운영에서 문제가 되지 않던 다양한 보안 이슈를 발생시키는 원인이 된다. 스마트 그리드는 국가 기반시설임과 동시에 그 안에서 다루어지는 데이터 또한 개인 프라이버시와 관련된 민감한 정보이기 때문에 데이터에 대한 기밀성, 신뢰성, 무결성의 보장이 필요하다. 그러므로 발생 가능한 보안이슈와 그 해결책에 대한 연구는 반드시 진행해야 할 문제이다.

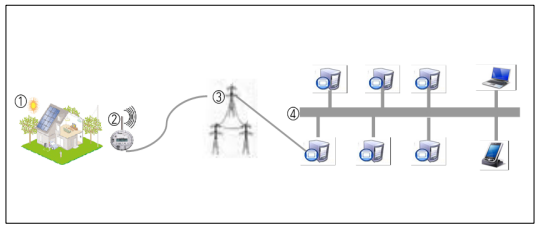
본 논문에서는 스마트 그리드 환경에서 발생 가능한 보안이슈를 데이터의 흐름과 연계하여 살펴본 후, 이를 통해 스마트 그리드 환경에서 데이터의 보안이 갖는 의미를 정의 할 것이다. 마지막으로 정의된 의미에서의 보안이슈에 대한 선행 연구를 살펴보고, 좀 더 향상된 효율성과 안전성을 제공하는 개선안을 제안 할 것이다.

본 논문의 구성은 다음과 같다. 제2장에서는 데이터 보안에 대한 정의와 관련 연구를 살펴본다. 제3장에서는 관련 연구에 대한 분석을 진행하고 제4장에서 분석한 내용을 바탕으로 개선안을 제안한다. 마지막으로 5장에서는 본 논문의 전체적인 결론을 내리고자 한다.

2. 데이터 보안과 관련 연구

2.1 데이터 보안

스마트 그리드에서 데이터의 보안은 다양한 의미를 갖는다. 그 의미를 스마트 그리드 환경에서 데이터의 흐름과 연계하여 살펴보면 다음과 같다. 먼저 [Fig. 1]은 스마트 그리드 환경에서 데이터의 흐름에 대한 것을 나타낸 것이고 표1은 각 흐름별 데이터의 동작과 그에 따른 보안이슈를 나타낸 것이다. ① ~ ④ 단계는 각각 스마트 홈, AMI, 스마트 그리드 기반 통신망, 서비스 제공 영역을 나타내며, 흐름별로 분석하여 분류 할 경우 ① ~ ② 단계, ③단계 그리고 ④단계를 각각 데이터수집, 데이터 전송, 데이터 가공 및 처리 단계로 분류할 수 있다[3]. 이후 얻을 수 있는 결론은 스마트 그리드는 전력정보의 수집과 전송 및 처리를 통해 전력의 효율적인 제공뿐만 아니라 처리된 데이터를 이용한 소비자에 대한 다양한 전력 서비스 제공에도 그 의미가 있다는 것이다. 그러므로 본 논문에서는 스마트 그리드의 본질을 데이터의 처리를 통해 소비자에 대한 서비스 제공을 목표로 하는 스마트한 전력 시스템으로 보고, 여기에서 데이터의 보안이 갖는 의미를 ④단계에서 발생 가능한 보안이슈에 대한 보호로 정의할 것이다. 따라서 앞으로 분석할 데이터 보안과 관련된 연구의 분석과 제안은 소비자의 개인 프라이버시 데이터에 대한 보호를 그 목적으로 한다.



[Fig. 1] Data Flow in Smart Grid

2.2 Shamir 및 Kurihara 비밀분산

데이터베이스에 데이터를 분산시켜 저장함으로써 기밀성을 보장하기 위한 논의는 지속적으로 이루어져 왔다. 그 중 대표적인 두 가지 방식으로 Shamir 비밀분산 방식과 Kurihara 비밀분산 방식이 있다. Shamir 방식은 1979년에 제안된 임계치 비밀분산 기법으로서, 다항식 보간법을 사용하여 데이터를 비밀조각 n개로 분산하여 저장하며, 분산된 데이터들이 일정 수치(임계치) 이상으로 모이지 않을 경우 원래의 데이터로 복원이 불가능하게 하여 기밀성을 보장 한다 그러나 다항식 보간법의 사용은 처리 과정에서 발생하는 지연시간 때문에 실제 데이터 모델에 적용하기에는 적합하지 않다.

Kurihara 방식은 Shamir 방식과 같이 임계치 비밀분산에 기반을 두고 기밀성을 보장 한다 Shamir 방식과 달리 임계치의 수치를 임의로 확장할 수 있어 좀 더 유연한 데이터 분산 처리가 가능하며, Shamir 방식의 지연시간 문제를 개선하기 위해 배타적논리합(XOR) 연산을 수행함으로써 다항식 보간법을 대체하여 지연시간 발생 문제를 일정 부분 해결하였다.

그러나 Shamir 방식과 Kurihara 방식은 데이터의 용량이 적고 그 종류가 일정할 경우에만 적용이 가능하기 때문에 다루어지는 데이터의 크기가 매우 크고, 종류 또한 양한 스마트 그리드 환경에서는 실제 적용 시 문제가 발생하게 된다[4].

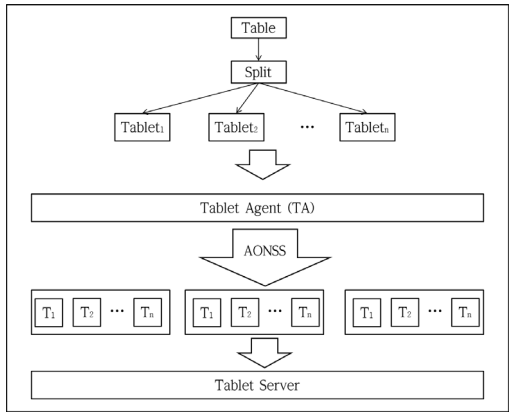
〈Table 1〉 Data Flow & Security Issue in Smart Grid

Step	Data Flow	Security Issue
①	• The data related to power consumption is primarily collected through the collection device in the duct and data concentration device. • The collected data are delivered to the smart meter to transfer them to utility by integrating them with each other.	• Certification and customers and smart products • Collect customers' data • Interoperability between smart products • Security vulnerability of wireless sensors • Control authority about electricity usage
②	• Read the smart meter by controlling it remotely. • Integrate real time metering information with each other.	• Security vulnerability of smart meters • Privacy in smart meters • Control of access to smart meters
③	• Exchange and transmit information through information-based networks	• Vulnerability in wire and wireless communications networks • Cell security vulnerability in power line-based communications
④	• Store, process, and use customers' data which were transmitted • Calculate account and provide profile and customized services • Retransmit the data which were transmitted to customers by processing them.	• Privacy in consumer data • Control about customers' electricity usage

2.3 AONT 암호화 기반 데이터 비밀분산

앞서 언급한 것과 같이 Shamir 및 Kurihara 비밀 분산과 같이 임계치를 기준으로 복원의 유·무를 결정하는 방식을 AONT(All Or Nothing) 방식이라 하는데, 기존의 AONT 방식은 대용량 데이터 처리의 비효율성 문제뿐만 아니라, 데이터를 분할해 다수의 데이터베이스에 분산·저장하고 이를 관리하는 데 있어서 분산된 각각의 데이터베이스에 대한 악의적 침입, 변조, 데이터마이닝, 관리자의 개입과 같은 공격 유형에 매우 취약하다는 문제가 있다. 따라서 분산을 통한 기밀성 보장뿐만 아니라, 각 데이터베이스에 대한 독립적인 안전성을 보장하기 위해 AONT 기법에 비밀분산(Secret Sharing) 기술을 도입한 AONSS(All Or Nothing Secret Sharing) 기법이 제안되었으며[5], 이때 스마트 그리드 환경에서 발생하는 대용량 데이터 처리를 위해 펩타바이트 규모의 대용량 데이터를 분산 관리하기 위한 시스템으로 데이터 모델, 오퍼레이션, 서버 구성 등 대용량 데이터를 정형화된 포맷으로 분산클러스터 환경에 저장하는 시스템인 Neptune을 추가하여 이용한다[6]. 앞으로 이것을 PS기법이라 명명한 뒤 논문을 진행할 것이다. 또한 제안 기법의 구조는 [Fig. 2]와 같으며, 동작 방식은 다음과 같다.

1) 하나의 테이블을 row key 범위로 Split 한다. 여기서, Split된 단위를 Tablet라고 한다.



[Fig. 2] PS Scheme

2) 분리된 Tablet은 TA에 의해 AONSS 방식을 사용하여 분산되고 Table로부터 작성된 Tablet를 관리한다.

3) 분산된 Share(T1, T2, ... , Tn)들은 Neptune Master에 의해 Table Server에 할당된다. 복원 시에는 할당된 Share들로부터 TA에 의해 Tablet이 복원된다.

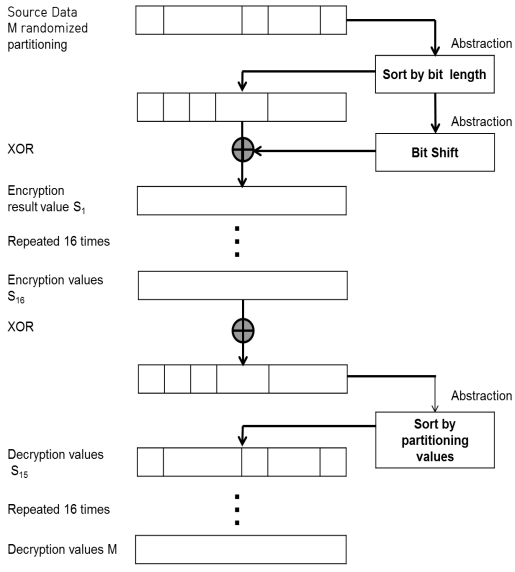
3. PS기법 분석

3.1 PS기법 개요

논문[5]에서 제안된 PS기법은 Neptune 시스템 안에서

AONT 암호화를 기반으로 하는 스마트 그리드 환경에서의 개인정보 비밀분산 기법이다. 이 기법은 분산과 복원 단계로 구성된다. 개인정보 분산 단계는 임의의 난수를 발생시켜 원본 데이터 ℓ을 분할한다. 분할된 데이터를 길이 순으로 정렬한 후, XOR 연산을 수행함으로써 암호화를 진행한다. 개인정보 복원 단계는 분산 저장된 데이터베이스에서 암호화된 분산 조각들을 통합한 뒤, 개인정보 분산 단계와 역순으로 복호화를 진행한다. 암호화와 복호화가 수행되는 과정의 한 단계는 암호학에서 라운드라 표현하며, PS기법은 각 단계에서 16회의 라운드 횟수를 갖는다. 이것은 PS 기법의 암호화 방식이 대칭키 기반 암호화의 대표적인 기법인 DES 암호화에서 그 개념을 가져왔기 때문으로 생각된다.

그림 3은 PS기법의 암호화 방식 개념도이며, 추상화와 XOR 연산 과정을 수행하는 방식, 그리고 16회의 라운드를 진행하는 것은 비슷하지만, 최초 원본 데이터를 분할할 때, 의사난수를 발생시켜 임의로 분할시키는 것과, 추상화 과정에서 인증키인 S-BOX를 사용하지 않는 점에서 차이를 보이며, 동작방식은 다음과 같다.



[Fig. 3] PS Encryption

1) 데이터를 의사난수 발생기를 사용하여 임의의 개수로 분할한다.
2) 분할한 데이터 조각을 길이 순으로 정렬해 추상화를 실시한다.
3) 길이 순으로 정렬된 데이터를 XOR 연산 시키는데, 이때 XOR 연산을 수행할 피연산자는 정렬된 데이터를 비트이동 시킴으로써 얻어낸다.
4) 이와 같은 과정을 16회 수행함으로써 암호화를 진행한다.
5) 복호화는 암호화와 반대의 순서로 진행하는데, 이때 필요한 정렬정보와 XOR 연산의 피연산자 정보는 암호화에서 사용된 정보를 바탕으로 한다.

PS기법을 사용함으로써 얻을 수 있는 가장 큰 장점은 인증키를 사용하지 않음으로써 인증키의 관리가 필요 없으며, 인증키의 분실로 입을 수 있는 보안침해 위협 또한 발생하지 않는다는 것이다. 그 외에도 다음과 같은 장점이 존재하기 때문에, 스마트 그리드 환경에 매우 적합한 기법이다.

1) Shamir 및 Kurihara의 임계치 기반 비밀분산 방식은 데이터베이스에 저장되는 비밀 조각의 크기가 원본 데이터 ℓ과 같게 되어 분산 저장할 데이터베이스가 n개 일 경우, 처리되는 데이터의 크기가 $\ell \times n$이 된다. 그러나 PS기법에서는 각 데이터베이스가 처리해야하는 비밀조각의 크기가 $\frac{\ell}{n}$이 된다. 따라서 분산 저장할 데이터베이스가 n개 일 경우 처리되는 총 데이터의 크기는 $\frac{\ell}{n} \times n$이 되어 원본 데이터의 크기가 ℓ로 일정하게 유지된다.
2) 다항식 보간법을 통한 연산이 아닌 XOR 연산과 의사난수를 기반으로 작동되므로, Shamir 기법에 비하여 고속 비밀분산 및 복원이 가능하다. 또한, 연산과정에서 블록단위의 제한을 받지 않고 기억장치로 연산이 가능한 전체 길이를 한 번에 처리할 수 있다.
3) Neptune 시스템을 기반으로 원본 데이터를 분할한 뒤, 다시 의사난수를 기반으로 비밀조각으로 나누기 때문에, 스마트 그리드의 개인정보 조각을 모두 생성한 이후에도 개인정보 조각의 개수를 자유롭게 조절할 수 있다.
4) 의사난수를 기반으로 비밀조각을 나누기 때문에, 개인정보 조각의 크기를 자유롭게 조절할 수 있다. 이러한

점은 개인정보 취급에 용이하다.

3.2 PS기법의 문제점

PS기법을 제안한 논문[5]에서는 의사난수 발생기에서 초기 발생하는 random seed에 대한 공격에 대해 보안 취약점이 발생할 수 있다고 설명하고 있다. 또한 PS기법은 AONT 구조에 기반을 두었기 때문에 원본 데이터의 크기 ℓ이 공개될 경우 각 비밀조각을 통해 원본 데이터의 유추가 가능한 문제가 존재한다 하였다.

본 논문에서는 PS기법의 분석결과 이와 같은 문제점 이외에도 다음과 같은 문제점들을 제시하고자 한다.

1) 분산하는 비밀조각 개수의 제한을 두지 않을 경우, 저장을 위해 필요한 데이터베이스의 개수 또한 함께 증가하게 된다. 이것은 데이터베이스 구성을 위한 비용적 측면에서 비효율성을 초래할 수 있다.
2) 앞서 제시한 데이터의 원본과 분산 데이터 크기의 총합이 같게 되어 발생하는 효율성에 대한 언급은 각 라운드에서 발생해 보안 데이터베이스에 추가적으로 저장되는 분할정보(Seed) 값과 XOR 피연산자 정보를 고려하지 않은 결과이기 때문에, 일정 크기 이하의 데이터 처리 시 오히려 Shamir 및 Kurihara 방식보다도 더 많은 양의 정보를 저장하게 된다.
3) 암호화 시 발생하는 추가 데이터가 공개될 경우 분산 저장된 데이터의 복호화가 가능하게 된다. 그러므로 기존의 키 관리의 번거로움이 없는 대신, PS기법에선 보안 데이터베이스를 따로 두어 관리하게 되는데, 논문[5]에서는 이러한 보안 데이터베이스 관리에 대한 언급이 없으며, 추가 데이터 관리에 필요한 노력과 비용에 관한 언급 또한 하고 있지 않다

따라서 본 논문에서는 이와 같은 문제점을 개선하기 위해 PS기법을 기반으로 한 개인정보 분산 기법에 대한 제안을 하려 한다.

4. 개인정보 분산기법 제안

4.1 제안기법

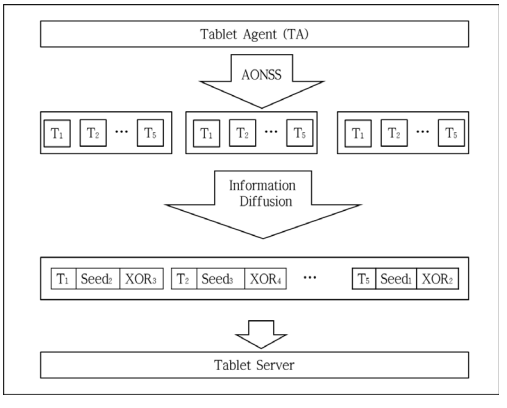
개인정보 비밀 분산을 통해 얻고자 하는 목표는 보안성의 향상과 대용량 데이터 처리에 있어 필요한 효율성 확보라고 전제할 때, 보안성과 효율성 사이에는 트레이드오프 관계가 성립한다. 앞서 밝힌 PS기법의 문제점을 개선하기 위해서는 이러한 보안성과 효율성의 관계를 이해하고 두 성질 사이에서 적절한 균형을 맞춰야 할 필요가 있다. 따라서 이를 위해 다음과 같은 제안을 하고자 한다.

1) PS기법과 마찬가지로 AONT 암호화를 기반으로 함과 동시에, 암호화 단계에서 비밀 조각의 크기 가변성은 유지하되 비밀조각의 개수를 16개미만으로 (본 논문에서는 임의로 5개)로 한정한다.
2) 암호화와 복호화를 수행할 때 PS기법에서 제안한 각 단계별 16회의 라운드 수행 횟수를 그 보다 작은 횟수로 감소시킨다. (본 논문에서는 임의로 5회로 예를 든다)
3) 암호화 과정에서 발생하는 추가 데이터를 보안 데이터베이스에 따로 저장하지 않고, Seed 값과 XOR 연산에 필요한 피연산자 정보를 적절히 분산시켜 각각 다른 데이터베이스에 독립적으로 분산저장 한다.

4.2 제안구조와 세부 진행 과정

4.2.1 제안구조

[Fig. 4]는 제안 구조를 나타낸 것으로 그림2의 구조와 유사하나, Seed값과 XOR 연산에서 발생하는 피연산 정보가 비밀조각에 랜덤으로 분산 저장되는 차이가 있다. 이 방식으로 암호화 과정에서 발생하는 추가 데이터에 대한 보안성을 유지한다.



[Fig. 4] Proposed Scheme

4.2.2 개인정보 데이터 분산 단계

표2는 제안기법의 세부 진행 과정에서 사용하는 용어의 정의이며, 개인정보 데이터 분산 단계는 라운드의 횟수에 따라 그 과정에 약간의 차이가 존재한다.

〈Table 2〉 Terminology

$\oplus$	: XOR
$\|\|$	: Bit Concatenate
M	: Message Text
S	: Result Text
r	: Random nonce
O	: Round number

각 라운드의 결과를 S라 할 때 라운드의 구분은 $S(O_i)(i=1,2,\ldots,5)$으로 한다. i가 홀수일 경우의 분할값을 얻기 위한 과정은 [Fig. 5]와 같으며, 다음과 같이 진행된다.

최초 크기가 ℓ인 원본 데이터 M에 대해 의사난수 발생기로 ℓ 미만의 균일한 r을 발생시킨다.

r에 기준하여 원본 데이터 M을 5개의 조각으로 분할한다.

$$M = m_1||m_2||\ldots||m_5$$

분할한 블록의 길이에 비례하여 오름차순으로 재구성한다. 분할된 블록의 길이가 같은 블록의 경우는 정렬 시 그 순서를 고려하지 않아도 된다.

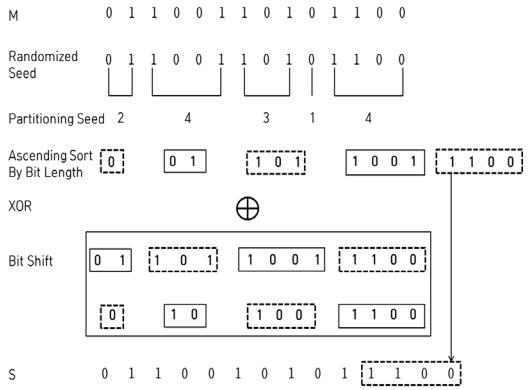
$$m_1||m_2||\ldots||m_5 \rightarrow m_5||\ldots||m_2||m_1$$

오름차순 정렬된 M을 XOR($\oplus$) 연산을 통해 결과값 S를 생성한다. XOR 연산은 제일 뒤의 분할값은 그대로 내리고 나머지 분할값을 한 칸씩 비트이동 시킨 뒤, 수행한다.

$$m_5||\ldots||m_2||m_1 \oplus m_4||\ldots||m_1 = S$$

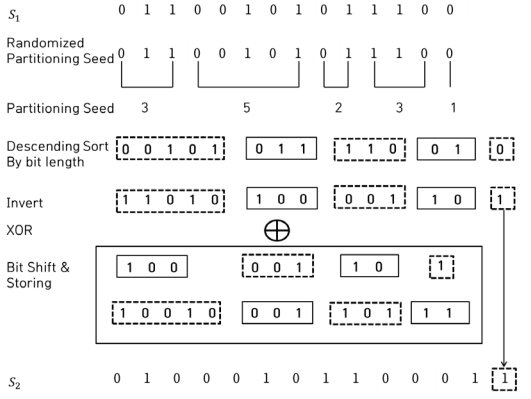
이때 앞의 분할값 크기와 뒤의 분할값 크기가 다른 경우, 뒤의 분할값의 크기를 앞의 분할값 크기에 맞춘다. 즉, 뒤의 분할값을 앞에서부터 크기를 맞춘 후 남게 되는 비트 부분은 삭제한다.

최초 분산단계에서 M을 통해 결과값 S를 얻어낸 후, 그 값을 $S(O_1)$로 정의한다. 그 후 각 라운드는 이전 단계에서 얻어진 $S(O_i)(i=1,2,\ldots,5)$를 이용 해 분산 데이터를 얻어 낸다.



[Fig. 5] Odd Round Diffusion

다음으로 i가 짝수가 되는 경우의 분할값을 얻기 위해 [Fig. 6]과 같은 과정을 수행한다.



[Fig. 6] Even Round Diffusion

즉, 홀수차 라운드에서 수행한 S를 가지고 의사난수 발생기로 발생시킨 r을 이용해 5개의 비밀조각으로 분할한다.

$$S = s_1||s_2||\ldots||s_5$$

분할한 r의 길이에 비례하여 내림차순으로 재구성

한다.

$$s_1||s_2||\dots||s_5 \rightarrow s_5||\dots||s_2||s_1$$

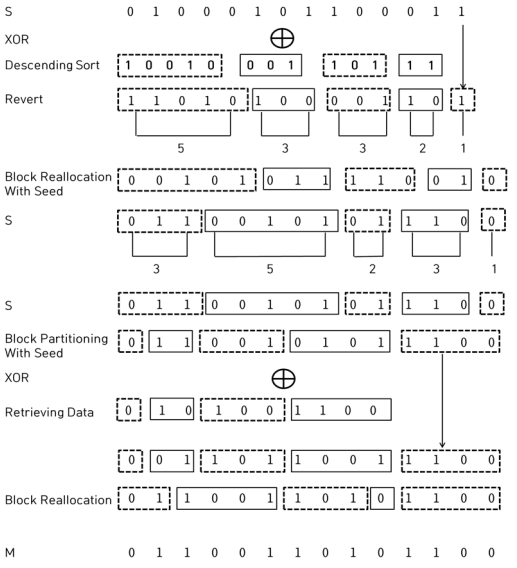
내림차순으로 재구성한 값에 대해 Invert를 취하고 홀수차 라운드에서와 마찬가지로 XOR 연산을 수행한다.

$$Invert[s_5||\dots||s_2||s_1] \oplus s_4||\dots||s_1 = S(O_2)$$

이때 XOR 연산을 위해 비트 이동을 할 경우 앞과 뒤의 분할값 크기가 맞지 않는 경우, 그 크기를 맞춰준다. 단, 뒤의 분할값의 길이가 앞의 분할값에 비해 그 길이가 길 경우엔, 비트의 삭제가 아니라 각 블록마다 {1,0} 비트를 추가해준다. 같은 과정을 반복 수행하여 $S(O_5)$의 값을 얻어내고, 이 값이 분할된 기준으로 개인정보를 구성해 5개의 데이터베이스에 저장함으로써 개인정보의 비밀분산이 완료된다. 각 라운드에서 발생하는 r에 대한 데이터 분할 정보(Seed)와 XOR 연산에 피연산자로 쓰이는 비트 이동된 분할값은 임시 버퍼에 저장 해 두었다가 분산단계의 마지막 라운드에서 각 비밀조각에 교차 저장하도록 한다.

4.2.3 개인정보 데이터 복원 단계

개인정보 데이터 복원 단계는 [Fig. 7]과 같이 분산 단계의 역순으로 수행하는 것을 기본으로 한다.



[Fig. 7] Data Recovery

먼저 5개의 데이터베이스에 분산 저장된 데이터를 가져와 데이터 통합을 수행한다. 데이터 통합 시 분산 단계에서 생성된 각 라운드 별 Seed 값과 XOR 피연산자의 정보 또한 얻어진다.

통합된 데이터 $S(O_5)$에 대해 XOR 연산을 수행한다. XOR 연산과정은 복원과정과 같으며, 이때 통합 단계에서 얻어진 라운드별 Seed값과 XOR 피연산자 정보가 연산에 이용된다. 만약 $S(O_5)$를 이용 해 $S(O_4)$를 복원하려 한다면, 분산 과정 중 4 라운드에서 발생한 Seed값과 XOR 피연산자 정보가 필요하다.

4.3 제안기법의 효율성 및 안전성

제안한 기법은 PS기법에 비해 다음과 같은 장점이 있다.

1) 비밀조각의 개수를 한정함으로써 각 라운드별 비밀조각의 분할정보(Seed)의 크기가 감소하게 된다. 이는 대용량 데이터의 처리를 요구하는 스마트 그리드 환경에서 매우 중요한 의미를 갖는다.
2) 라운드 횟수를 감소시킴으로써 각 라운드에서 발생하는 Seed 값과 XOR 연산에 필요한 피연산자 데이터의 총합이 줄어들게 된다. 이것은 앞에서와 마찬가지로 대용량 데이터의 처리를 요구하는 스마트 그리드 환경에서 보안효과 측면의 손실과 효율적 측면의 이익 효과를 비교했을 때, 미비한 보안 측면의 손실을 감수할 만큼의 효율성 증가를 기대할 수 있을 것으로 판단된다.
3) 보안 데이터베이스에서 따로 관리되던 기존의 Seed값과 XOR 연산에 필요한 추가정보를 랜덤으로 분산하여 저장함으로써, 단일 데이터베이스에 대한 공격 위험도를 분산시키는 효과가 있다. 즉, 보안 데이터베이스에 대한 침해 위협을 개선할 수 있고, 기존 AONT 기반의 특성인 임계치 이상의 정보가 모여야만 복호화가 가능한 장점을 가져올 수 있기 때문에 기밀성의 향상이 기대된다.

본 제안은 PS기법을 기반으로 하기 때문에 PS기법이 가지는 빠른 연산 속도와, 원본 데이터의 길이와 분산된 데이터 길이의 총 합이 같다는 특징을 그대로 가지며, 비밀값과 복원하는데 필요한 비밀 정보 또한 여러 곳으로

분산시키는 암호학적인 특성까지도 가지게 된다. 이로 인해 전국민을 대상으로 하는 거대한 용량의 스마트 그리드 환경에도 적용가능한 수준의 기법이라도 판단된다.

5. 결론

본 논문에서는 스마트 그리드 환경에서 발생하는 데이터에 대한 보안을 소비자의 개인 프라이버시 데이터에 대한 보호의 개념으로 정의하고, 이러한 데이터가 가공·처리될 때 발생 가능한 보안이슈에 대한 해결방안으로 제시된 기존 데이터 비밀분산 관리 기법(PS 기법)을 분석하였다. 이러한 분석을 통해서 효율성과 안전성을 최대한 유지하면서, PS 기법의 세부 진행 알고리즘을 수정함으로써 PS기법의 문제점을 개선하고자 하였다.

또한 기존 PS기법에서 단일 보안 데이터베이스에 저장하던 Seed값과 XOR 연산에 필요한 피연산자 정보를 다수의 데이터베이스 서버로 분산 저장함으로써 안전성을 더욱 높이도록 하였다.

분산 데이터베이스의 개수를 정하는 것은 매우 중요한 문제이다. 본 논문에서는 예로 들어 5개로 설정하였지만, 실제로 적용하기 위해서는 보안성의 보장과 효율성의 확보를 위한 적절한 개수의 분산 데이터베이스 서버를 확보해야 할 것이다. 이와 관련된 사회공학적 공격과 관련된 안전성 또한 고려되어야 할 것으로 판단된다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2011-0014394).

REFERENCES

[1] Hae-Chun Jung, Training of electricity IT experts is a key of Smart Grid success. Digital Power News Global Worldwide Trend, 2009.

[2] Whon-il Park, Duk-Chan Yoon, Smart Grid Projects and Privacy Issues : Propose of Smart Grid Governance. Research of Technique, Vol. 26, No. 2, 2010.

[3] Kyungbok Lee,JiEuin Dokko, Jiyeon Yoo, Sook-Yeon Lee, Jong-in Lim, Customers' participation in Smart Grid and security issue. Customers' participation in Smart Grid and security issue, Vol. 19, No. 4, 2009.

[4] A. Shamir, How to Share a Secret. Communication of the ACM, Vol. 22, No. 11. pp. 612-613, 1979.

[5] Namje Park, Youjin Song, Secure Distributed Data Management Architecture Using AONT Encryption in Smart Grid Environment. The Journal of The Korea Information and Communications Society, Vol. 35, No. 10, 2010.

[6] Hyung-joon Kim, Neptune : Bulk distributed data management system. NHN, 2008.

이 성 용(Lee, Sung-Yong)

- 1995년 2월 ~ 현재 : 목원대학교 컴퓨터공학부 4학년 재학
- 관심분야 : 정보보호
- E-Mail : lemuria0322@naver.com

여 상 수(Yeo, Sang-Soo)

- 1997년 2월 : 중앙대학교 컴퓨터공학과(공학사)
- 1999년 2월 : 중앙대학교 대학원 컴퓨터공학과(공학석사)
- 2005년 8월 : 중앙대학교 대학원 컴퓨터공학과(공학박사)
- 2009년 3월 ~ 현재 : 목원대학교 컴퓨터공학부 교수
- 관심분야 : 정보시스템, 멀티미디어, 정보보호
- E-Mail : sangsooyeo@gmail.com