DOI : 10.5392/JKCA.2010.10.9.057

스마트 그리드의 소비자 보호를 위한 안전한 분산 데이터 관리 구조

Secure Distributed Data Management Architecture for Consumer Protection of Smart Grid

박남제*, 송유진**, 박광용***
제주대학교 교육대학 컴퓨터교육과*, 동국대학교 정보경영학과**, 동국대학교 전자상거래협동과정***

Namje Park(namjepark@jejunu.ac.kr)*, Youjin Song(song@dongguk.ac.kr)**,
Kwangyong Park(freemickey@dongguk.ac.kr)***

요약

스마트 그리드 기술은 소비자의 에너지 사용을 실시간으로 감시하고 비사용 기간 동안 차단 요구에 응답할 가정용 기기와 통신함으로써, 에너지 효율을 가정으로까지 확대해 준다. 그러나, 스마트 그리드에서 수집된 정보는 개인 정보의 라이브러리 형태가 될 것이므로 이것을 잘못 다루게 되면 소비자의 개인정보를 크게 해칠 수 있다. 소비자 중심의 투명성과 통제의 원칙이 처음부터 끝까지 필수 설계 원칙으로 취급되지 않는다면 중대한 우려가 있을 것이다. 본 논문에서는 All-Or-Nothing Transform(AONT) 암호화 모드의 특성을 이용하여 스마트 그리드 환경에서의 안전한 소비자 정보보호를 제공하기 위한 효율적인 데이터 분산 보안 관리방안을 제안한다. 본 논문에서 제안된 알고리즘은 처리속도 측면에서 데이터의 고속 분산 및 복원이 가능하며, 각 비밀조각 사이즈의 총합이 평문과 동일하여 스마트 그리드 시스템의 개인 데이터 처리에 적합하다.

■ 중심어 : | 지능형 전력망 | 스마트 그리드 보안 | 프라이버시 보호 | 개인정보보호 | 비밀분산 | 취약성 |

Abstract

Smart grid technology can expand energy efficiency into the home by monitoring consumer energy usage in real time and communicating with household devices that respond to demands to shut off during periods of non-use, allowing individual consumers to control their electricity usage more effectively. But, the information collected on a smart grid will form a library of personal information, the mishandling of which could be highly invasive of consumer privacy. There will be major concerns if consumer-focused principles of transparency and control are not treated as essential design principles from beginning to end. In this paper, using All-Or-Nothing Transform encryption mode for providing smart grid security, we propose efficient distributed data Management based on XOR operation. The contribution of this paper is to provide a secure algorithm that manages efficiently distributed data in the field of private data in smart grid environment.

■ keyword : | Smart Grid | Smart Grid Security | Privacy Protection | Secret Sharing | Vulnerability |

* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임. (No. 2010-0028122)

접수번호 : #100420-004
접수일자 : 2010년 04월 20일
심사완료일 : 2010년 06월 14일
교신저자 : 송유진, e-mail : song@dongguk.ac.kr

I. 서 론

최근 국내외적 이슈 가운데 하나인 녹색성장(Green Growth)은 지구온난화의 문제로 이산화탄소(CO_2) 배출을 줄이기 위한 산업적 노력과 이와 관련된 기술 및 산업을 성장 동력의 기회로 만들자는 취지이다. 이러한 녹색성장을 위한 그린 IT 실현에서 주요 기술의 하나로 스마트 그리드(Smart Grid)가 주목을 받고 있다.

스마트 그리드는 전기 에너지의 효율적 사용을 목적으로 전력망에 IT기술을 도입 및 융합하여 전력의 송·배전을 지능화하는 지능형 전력망을 뜻한다[1][20]. 스마트 그리드 시스템은 공급자, 네트워크, 소비자 간의 에너지 송·배전에 대한 연계, 자동화 및 조정 가능성을 높인다. 또한, 스마트 그리드 기술은 소비자의 에너지 사용을 실시간으로 감시하고 비사용 기간 동안(예를 들어 보다 많은 전력자원이 필요한 근무일 동안) 차단 요구에 응답할 가정용 기기와 통신함으로써, 에너지 효율을 가정으로까지 확대해 준다.

스마트 그리드 시스템은 에너지 효율을 크게 높일 수 있다. 하지만 스마트 그리드 시스템의 개발에는 여러 기회와 혜택도 존재하지만 동시에 사생활 침해의 우려도 있다. 소비자들의 상세한 전력 사용 내역이 자동 전송됨에 따라 개인 정보의 유출 가능성이 발생되거나 개인의 에너지 사용에 대한 정보가 경찰이나 보험회사 등의 제3자에게 유출될 위험 요소가 존재하는 등의 스마트 그리드의 프라이버시(개인정보 노출) 문제에 대한 논란이 발생할 수 있다. 이에, 스마트 그리드의 보안 체계로서 송·배전 보호, AMI(Advanced Metering Infrastructure, 고도화된 검침 기반 시설, 지능형 원격검침)·서비스 보안, 보안관제 기술, 보안기반 기술, 시스템 보안기술 등의 체계화된 보안 프레임워크 기술 연구와 보안에 대한 법, 제도, 조직, 기술 등의 정보보호정책 관점에서의 지원방안이 필요하다[2-4].

스마트 그리드의 개인정보 데이터는 외부의 데이터 센터에 저장되기도 한다. 여기서, 고객 사용자가 PC를 사용하여 전력량 등의 개인정보를 읽는 것 외에 서비스 관리자나 고객 자신이 유비쿼터스 단말을 이용하여 접근권한 범위내에서 정보를 확인하고 조회 및 입력하게 된다. 이때, 개인정보의 보안상 위험성을 고려하여 데이터를 암호화 하여 관리할 수 있다. 그러나 암호화 방식은 암·복호화에 많은 시간이나 메모리를 필요로 한다. 현재 암호화 방식은 비밀정보 전체가 암호화되기 때문에 키가 해독될 경우, 비밀정보가 완전하게 유출될 수 있다. 따라서 키 분배 및 관리의 어려움이 존재한다. 따라서 이러한 한계를 극복할 수 있는 방식으로써 비밀분산방식이 적용될 수 있다.

이와같이, 비밀분산 방식[5]은 키 분배 등 키관리가 필요하지 않고 원 데이터를 분산 저장했을 경우, 분산된 정보인 Share 크기와 원 데이터의 크기가 같게 되어 저장해야 할 데이터양이 증가하게 된다. 또한, 암호화하기 전에 평문에 적절한 변환을 수행(암호화 모드)하여 기존 암호화 방식의 효율성을 저하시키지 않고 안전성을 향상시킬 수 있다는 것이 알려져 있다[6-9][18].

이에, 본 논문에서는 그린 IT 전략 중 스마트 그리드 기술에서 개인정보보호의 요소를 살펴보고, 프라이버시 보호 필요성과 요구사항에 대해 분석한다. 그리고, All-Or-Nothing Transform(AONT) 암호화 모드의 특성을 이용하여 스마트 그리드 환경에서의 안전한 개인정보보호를 제공하기 위한 데이터 분산 보안 관리방안을 제안한다.

II. 스마트 그리드와 개인정보보호

1. 개요

스마트 그리드란 IT 기반의 미래형 차세대 전력망으로 센서, 통신 네트워크, 자동제어 등의 IT 기술을 전력망에 도입함으로써 전력 인프라의 융통성, 보안성, 신뢰성, 효율성, 안전성 등을 향상시키고, 전력의 생산 및 소비정보를 유틸리티와 소비자 간의 양방향, 실시간 통신을 가능하게 함으로써 에너지 효율을 최적화하는 차세대 전력망 기술이다[1][20]. 발전소와 송·배전 시설과 전력 소비자를 정보통신망으로 연결하고 양방향으로 공유하는 정보를 통하여 전력시스템 전체가 하나의 체계 내에서 효율적으로 작동하도록 설계한다[10][21]. 이 기술을 통하여 전력 낭비를 줄이는 동시에 재생에너지 사용을

활성화하고 이산화탄소 배출도 줄여 지구 온난화 방지에도 효과가 있어 선진국들의 관심과 투자가 이루어지고 있다.

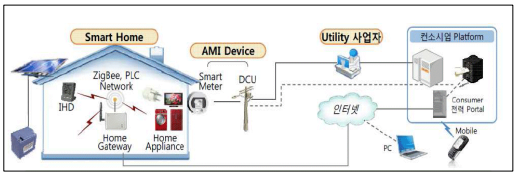

그림 1. 스마트 그리드의 통신 구조

[그림 1]은 전기의 생산과 공급, 제어를 위한 통신 네트워크와 센서 시스템, 각종 지능형 설비, 계측 장비 등을 망라한 통합 네트워크로 구성되는 일반적인 스마트 그리드 통신 구조를 보여주고 있다[20]. 위의 [그림 1]과 같이 스마트 그리드에서는 양방향으로 통합된 통신기술(Communication)이 핵심 기반 기술이며, 이러한 통신 기술을 바탕으로 스마트 미터기와 관련된 미터링(Metering) 기술, 전력의 송·배전과 관련되는 고급 제어 기술(Advanced Control), 그리고 정보의 효과적인 전달과 기기간의 호환성을 위한 인터페이스(Interface)가 스마트 그리드를 구성한다고 볼 수 있다.

스마트 그리드에서 IT는 스마트 그리드의 특징인 자기 복구(Self-healing), 수요반응(Demand Response), 보안, 전력 품질보장, 그리고 전력 거래 등을 실현시키는 필수 도구이며, 양방향 유·무선 통합 통신망, 센서 네트워크, 알고리즘 기반 관리, 프레임워크 S/W 등의 IT 기술이 전력망의 지능화를 가능하게 한다[11].

현재까지 전력망은 폐쇄형, 단독망 운영관리로 보안이 크게 문제되지 않았지만, IT가 결합됨에 따라 정보통신 네트워크 기기에서 발생하고 있는 보안 문제가 나타날 수 있는 우려가 높다. 고객의 프라이버시 노출, 정보 도용, 사용요금 조작은 물론, 전력 시스템의 마비까지 기존 전력망에서 나타나지 않았던 새로운 보안 위협의 가능성이 나타난다. 스마트 그리드의 대상이 국가주요기반시설인 전력망이기 때문에, 스마트 그리드의 추진에 있어 주요기반시설보호 등의 보안이 중요한 요소로 고려될 필요가 있으며, 스마트 가전기기 보안, 측정/제어 정보 무결성, 장치간 상호인증, 크로스 서비스 공격, 분산 서비스 거부 공격 방지, 제어시스템의 침해사고 탐지/대응/복구 등의 보안 대책이 필요하다. 또한, 스마트 그리드 전반적으로 새로운 국면의 기술적인 보안 대책이 마련되어야 함은 물론, 스마트 그리드 구축과정으로부터 밀착성 있게 구현되어야 한다.

2. 스마트 그리드에서의 개인정보

'개인 정보'란 개인 신상에 관한 모든 기록을 말한다. 스마트 그리드의 맥락에서, 에너지 사용과 개인적으로 식별 가능한 정보를 연계하면 개인 정보로서 또 하나의 연계된 정보가 생성된다. 기존 그리드의 현대화는 (제3자와 유틸리티 공급자에 의한 개인정보 수집, 사용, 공개를 늘리는 경향이 있는) 최종 사용자와 관련된 요소 및 활동과 관련이 있다[4]. 이러한 요소와 활동의 내용을 살펴보면 스마트 미터기, 스마트 가전제품, 동적요금제, 소비자 접근, 부하 관리 등이 있다.

3. 스마트 그리드에서의 개인정보보호 요구사항

지금까지 스마트 그리드의 일부가 되는 조직을 위한 몇 가지 실제 개인정보 보호 기준을 만들 필요성에 대해 설명해 왔다. 이를 바탕으로 스마트 그리드의 개인정보 보호 요구사항[1][4][11]은 다음과 같다.

- 동의 및 선택 : 조직은 개인정보의 수집, 사용 및 공개에 대해 동의를 구해야 한다.
- 통지 및 목적사양 : 조직은 개인정보의 수집 시점, 사용, 공유의 목적 등에 대해 통지를 해야 한다.
- 개인 참여 및 접근 : 조직은 해당 개인정보를 알아보기 위해 물어 볼 수 있도록 개인 및 가구에 대한 프로세스를 제공해야 한다.
- 정보의 품질, 무결성, 정확성 : 조직은 개인정보와 스마트 미터기로부터 수집한 기타 정보의 정확성, 완전성, 통지에서 식별된 목적에 적합성, 그리고 조직의 통제 안에서 정보의 일생동안 정확성을 기하기 위해 문서화한 정책, 절차, 기준 및 진행중인 훈련 및 의사소통을 동원하여 모든 노력을 해야 한다.
- 사용 제한 : 스마트 그리드 네트워크와 시스템 내에서의 정보는 수집된 목적으로만 사용되고 공개되어

야 하며, 이 정보를 받을 권한이 부여된 자들에 한해서 공개되어야 한다.

- 보존 및 폐기 정책/관행 : 스마트 미터기의 정보와 해당 개인 정보는 수집 목적을 완성하기 위해 그것을 필요로 하는 기간 동안만 보관해야 한다.
- 투명성 및 개방성 : 문서화된 개인정보보호 정책은 스마트 그리드 시스템과 네트워크의 일부인 개인 및 가구가 사용할 수 있어야 한다.
- 수집 제한 : 명시된 목적을 완수하는 데 필요한 정보만이 개인과 가구로부터 수집되어야 한다.
- 보안 및 안전장치 : 스마트 미터기 네트워크의 일원인 조직은 도난, 손실로부터 모든 형태로 개인 정보를 보호해야 하고, 무단 접근, 공개, 복사, 사용 또는 수정을 막아야 한다.
- 회계 및 관리 : 각 조직은 공식적으로 지위, 팀, 부서 또는 개인을 지정해서 정보보안과 개인정보보호 정책 및 관행이 존재하고 따르게 되도록 보장해야 한다.
- 감시 및 강화 : 스마트 그리드는 네트워크 및 시스템의 일원인 각 조직은 그 조직의 개인정보보호 정책 및 절차 준수 여부를 모니터링해야 한다.

Ⅲ. 스마트 그리드에서의 개인정보보호 관리 방안

본 장에서는 스마트 그리드 환경의 프라이버시를 고려한 개인정보보호 관리방안을 분석한다. 개인정보의 수집에 대해 프라이버시를 최대한 보장하면서 다양한 서비스마다 각기 다른 개인 프라이버시 정보의 접근에 대해 적응적이고 동적으로 정보 이용 범위를 제공하는 지능형 개인정보보호 에이전트 및 접근제어 기술 개발이 요구된다. 이를 위해 다음과 같은 사항이 고려되어야 한다.

- 개인정보의 접근/사용시 상황정보를 토대로 사용자의 개인설정의 동적인 적용에 따라 프라이버시 정책 제공을 통한 개인정보 특성에 따른 정보공개의 판정 메커니즘을 제공해야 한다.
- 클라이언트-서버 통합 지능형 프라이버시 보호 서비스가 제공되어야 한다.
- 프라이버시 정책에 의한 접근 판단 및 동적 상황에 근거한 접근제어를 통한 개인정보에 대한 수집 에이전트로부터 불법 접근 제안, 동적 개인정보가 이용되어야 한다.
- 개인 신상정보와 분리된 상황인식 데이터 관리를 통한 적응적 개인정보가 이용되어야 한다.

1. 개인정보의 분산 저장 관리

스마트 그리드의 여러 응용 서비스에서 시스템에 저장된 개인의 정보가 악의적인 해킹에 노출되는 경우가 있을 수 있고, 여러 기관에서의 개인정보보호를 위한 보안관리가 허술하고 과도한 개인정보 열람 등으로 프라이버시가 침해당할 수 있다. 이에 대한 대책으로서 개인정보의 안전한 분산 저장관리 기능이 요구되고 있다. 이에, 스마트 그리드 개인정보의 안전한 저장 및 관리를 위한 기술적 대책으로서 비밀정보 분산(Secret Sharing) 기술에 의해 기밀성을 유지함으로써 개인정보의 안전한 저장이 가능하고, 시간이 흐르면 해독될 우려가 있는 암호화, 전자서명의 약점을 극복하고 안전하게 장기간의 저장을 늦은 비용으로 처리하기 위한 분산, 저장 기능을 적용할 수 있다. 또한, 스마트 그리드 관리자에 의한 개인정보의 부정이용에 대한 대응방안으로 개인정보의 분산 기능을 이용할 수 있다.

2. 개인정보의 추출 관리

최근 정보기술의 발달로 기술적이고 교묘한 방법으로 개인정보를 추출하거나 개인정보를 자동적으로 추론하는 등의 기법으로 개인의 프라이버시를 침해하고 있다. 근래 활용되고 있는 데이터 마이닝의 목적은 구매정보 등의 개인 정보를 대량으로 모아 관련 상품 구매분석 등 일반적으로 성립되는 규칙을 찾아내는 것이다. 일반화된 규칙 자체를 공개하는 것은 프라이버시 상 문제는 없지만 데이터 마이닝의 과정에서 개인정보가 정보 마이닝 엔진에 보내짐으로써 프라이버시 침해 우려가 발생될 수 있다. 이를 방지하기 위해 스마트 그리드의 전기사용량, 결제이력 등 관련 개인정보를 열람하고자 하는 목적, 대상 및 서비스의 목적에 따라 차등적으로 개인정보의 범위를 선택적으로 추출해주는 기술인 프라이버시 보호 데이터마이닝 기술이 필요하다. 이러한 기술은 결제 이력,

개인연령 등의 통계적 분포로부터 개인의 결제내용, 신상정보를 직접 모으지 않고 이러한 숫자에 난수를 부가해 랜덤화하여 수집한 것으로부터 원래의 결제 이력, 연령 분포를 복원함으로써 개인의 프라이버시를 보호할 수 있다.

본 논문에서는 이러한 요구사항 중에 스마트 그리드 상의 소비자 정보를 안전하게 분산 관리하는 것을 중심으로 개인정보를 안전하고 효율적으로 저장하기 위해 AONT 특성을 갖는 비밀분산을 적용한 데이터관리 구조를 제안한다.

본 논문의 방안은 기밀성이 높은 개인정보 데이터, 고객의 개인정보를 포함하는 스마트 그리드 전력사용량 등의 영업 비밀 데이터가 외부에 일부가 유출되더라도 가용성을 유지할 수 있고 효율적으로 분산 관리하는 방식으로서의 이용이 기대된다.

IV. 안전한 분산 데이터 관리 구조

1. 관련연구

본 연구에서는 기존의 AONT 암호화 모드와 배타적 논리합(XOR) 기반의 (k,n) 임계치 비밀분산 방식을 이용하여 AONT기반 비밀분산 방식을 제안하는 것으로 해당 연구기법을 살펴보면 다음과 같다.

1.1 암호화 모드

① OAEP 암호화 모드[12]

OAEP(Optimal Asymmetric Encryption Padding)는 1994년 Bellare와 Rogaway에 의해 도입되었다. [그림 2]는 OAEP 암호화 모드를 나타낸다. 사용자는 우선, 보안 파라미터 k를 입력으로 암호화 모드 $f:\{0,1\}^k \rightarrow \{0,1\}^k$로 한다. 평문의 크기는 n비트로 하고, $n = k - k_0 - k_1$이 되는 k_0, k_1을 선택한다. 여기서, $H: \{0,1\}^{n+k_1} \rightarrow \{0,1\}^{k0}$는 해쉬 함수이고 $G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n+k_1}$는 generator로 한다. 평문은 $m \in \{0,1\}^n$이고 $r \in \{0,1\}^{k_0}$은 랜덤하게 선택하고 $\{0\}^{k_1}$을 선택한다.

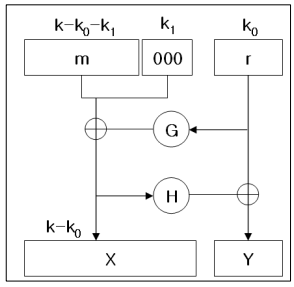

그림 2. OAEP 암호화 모드

우선, 랜덤하게 선택된 $r \in \{0,1\}^{k_0}$에 대해 함수 G연산을 수행한다. 그리고 평문 $m \in \{0,1\}^n$과 선택된 $\{0\}^{k_1}$를 비트연결을 한 후, 두 결과값에 대해 $\oplus$(XOR) 연산을 수행하여 결과값 X을 얻는다. 이를 수식 1과 같이 표현할 수 있다.

$$X = (m \| 0^{k1}) \oplus G(r) \quad (1)$$

그리고 결과값 X에 대해 함수 H를 수행하고 수식 1에서 선택한 $r \in \{0,1\}^{k_0}$과 $\oplus$(XOR) 연산을 수행하여 결과값 Y을 얻는다. 이를 수식 2와 같이 표현할 수 있다.

$$Y = r \oplus H(X) \quad (2)$$

최종적으로 계산된 결과값 X, Y에 대해 비트연결을 수행하여 수식 3과 같은 결과값 c를 얻을 수 있다.

$$c = f(X \| Y) \quad (3)$$

② AONT 암호화 모드[6-9][18]

AONT(All-or-Nothing Transform)방식은 RSA 암호 방식의 발명자인 Rivest에 의해 제안된 개념으로 원래는 RSA암호의 강도를 높이기 위해 OAEP라는 Preprocessor에 이용된 방식이다.

평문 데이터에 대해 AONT연산을 수행하면 원래의 데이터와 동일한 크기의 출력데이터를 얻을 수 있으며, 출력데이터의 모든 비트가 모아지면 원래의 데이터를 복원할 수 있다.

AONT방식[18]은 해쉬 함수 h와 의사 난수 생성기 g를 이용한다. h는 $\{0,1\}^{\ell(s-1)} \rightarrow \{0,1\}^{\ell}$인 hash function 이고 g는 $\{0,1\}^{\ell} \rightarrow \{0,1\}^{\ell(s-1)}$인 generator로 한다. 여기서, s는 평문블록수이다. 평문블록을

$m_1, m_2, ..., m_s (m_i \in \{0,1\}^\ell)$로 했을 때, 의사평문블록 $x_1, x_2, ..., x_s$는 다음과 같이 계산된다.

우선, 평문블록 $m_1 \| m_2 \| ... \| m_{s-1}$에 대해 함수 h를 수행하여 μ_s를 계산한다. 이는 수식 4와 같이 표현될 수 있다.

$$\mu_s = h(m_1 \| m_2 \| ... \| m_{s-1}) \quad (4)$$

계산된 μ_s와 평문블록 m_s에 대해 $\oplus$(XOR) 연산을 수행하고 함수 g를 수행한 후, 평문 블록 $m_1 \| m_2 \| ... \| m_{s-1}$과 $\oplus$(XOR) 연산을 수행하여 의사평문블록 $x_1 \| x_2 \| ... \| x_{s-1}$를 얻는다. 이는 수식 5와 6과 같이 표현될 수 있다.

$$g (\mu_s \oplus m_s) \quad (5)$$

$$x_1 \| x_2 \| ... \| x_{s-1} = (m_1 \| m_2 \| ... \| m_{s-1}) \oplus g (\mu_s \oplus m_s) \quad (6)$$

그리고 의사평문블록 x_s를 구하기 위해 평문 블록 $m_1 \| m_2 \| ... \| m_{s-1}$에 대해 h함수를 수행하고 수식 4에서 계산된 μ_s와 평문블록 m_s를 $\oplus$(XOR) 연산을 수행하고 두 결과값에 대해 다시 $\oplus$(XOR) 연산을 수행한다. 이를 수식 7과 같이 표현할 수 있다.

$$x_s = (\mu_s \oplus m_s) \oplus h(x_1 \| x_2 \| ... \| x_{s-1}) \quad (7)$$

[그림 3]은 AONT 알고리즘에서 s = 4 인 경우를 나타낸다.

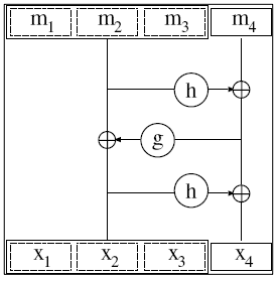

그림 3. AONT 암호화 모드

1.2 배타적 논리합(XOR) 임계치 비밀분산 방식

비밀분산 방식은 1979년에 Shamir[5]에 의해 제안되었다. 그 중 다항식 보간법을 사용하는 Shamir의 (k, n) 임계치 비밀분산 방식은 비밀정보를 n개의 분산정보로 분할하여 n개의 분산 정보 중 임의의 k개가 모이면 원래의 비밀정보를 복원할 수 있는 방식이다. 이때, 정보의 분산 · 복원시 k-1차 다항식을 처리해야 한다. 하지만 다항식 연산은 계산부하의 크기가 실제 어플리케이션에 적용할 때 문제가 되고 있다. 문헌 [13-16][19]에서 XOR 연산만으로 비밀정보의 분산 · 복원을 할 수 있는 고속의 임계치 비밀분산 방식을 제안하였다. 본 논문에서는 고속으로 비밀정보의 분산 · 복원이 가능한 배타적 논리합을 이용한다. 한편, Kurihara[15]등 [16]는 2008년 XOR 기반의 (k,n) 임계치 비밀분산 방식을 제안하였다. 이 방식은 임계치 k값을 확장할 수 있는 알고리즘으로, 평문 S와 비밀분산 연산에 필요한 랜덤숫자를 발생시켜 이에 대한 XOR을 취함으로 비밀 분산 조각을 생성한다.

2. 제안기법 : AONT기반 개인정보 분산관리

본 장에서는 스마트 그리드에서 개인정보를 안전하게 관리하기 위하여 AONSS(All-Or-Nothing Secret Sharing) 비밀분산방식을 적용한다. 우선, 본 제안방식은 분산 데이터베이스 시스템에서 비밀분산 방식을 사용하여 분산된 데이터를 DB에 할당하는 방식이다. 따라서 기밀성과 신뢰성이 높은 분산 데이터베이스를 구축할 수 있다. 보통의 분산 데이터베이스의 경우, 데이터베이스가 공격되면 데이터베이스에 저장된 데이터는 도난, 변조의 위험성이 있다. 본 제안방식에서는 비밀분산 방식을 이용하여 DB 서버에 저장된 데이터가 임계치 이하만큼 도난된 경우, 원래의 관계 테이블을 복원하는 것은 불가능하고 도난된 데이터로부터 부분정보도 얻을 수 없기 때문에 기밀성이 높다. 우선, 대용량 데이터 베이스를 활용하기 위한 Neptune 구조를 살펴본다.

2.1 Neptune[22]

Neptune은 페타바이트 규모의 대용량 데이터를 분산관리하기 위한 시스템으로 데이터 모델, 오퍼레이션, 서버 구성 등 대용량 데이터를 정형화된 포맷으로 분산클러스터 환경에 저장하는 시스템이다. Neptune설계의 기본 개념은 구글의 Bigtable[17]를 도입하였다.

[그림 4]는 Neptune 아키텍처를 나타내고 있으며, NeptuneMaster, TabletServer, ChangelogServer 3개의

데몬 서버와 클라이언트 API로 구성되어 있다.

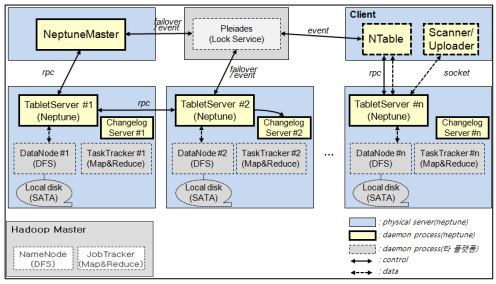

그림 4. Neptune 아키텍처

- NeptuneMaster : Tablet을 TabletServer에 할당하는 역할을 수행함. 여기서, Tablet은 하나의 큰 테이블을 여러 개의 작은 단위로 분산한 것을 의미함.
- TabletServer : 사용자 데이터와 테이블 관리용 데이터(ROOT, META 테이블)를 관리하면서, 클라이언트에게 데이터 입력/조회 등과 같은 데이터 서비스를 제공하는 데이터 서비스와 Tablet을 관하는 것임.
- ChangelogServer : 데이터 입력과 관련된 트랙젝션 로그를 디스크에 저장한 다음, TabletServer에 장애가 발생했을 때 데이터 복구를 지원하는 기능을 수행함.

Neptune의 데이터 모델은 모든 데이터가 row key, colum key로 정렬된 multi-dimensional sorted map이다. 모든 데이터는 테이블이라고 하는 논리적인 저장소에 저장된다. 각 테이블은 n개의 row로 구성되어 있고 각 row는 중복되지 않는 유일한 식별자인 rowkey필드를 가진다.

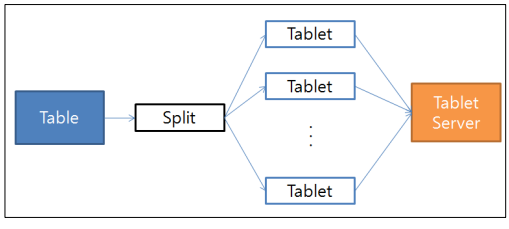

그림 5. Table 분리

[그림 5]는 Table 분리 과정을 나타내는데 테이블은 rowkey 범위로 분리(split)하여 관리하며, 분리된 단위를 Tablet이라고 한다. 하나의 Table은 n개의 row를 가질 수 있으며 Tablet으로 분리될 수 있는 최소 단위는 하나의 row이다. 데이터의 분산은 Tablet 단위로 분리된다.

각 Tablet은 NeptuneMaster에 의해 TabletServer에게 할당되고 TabletServer는 할당 받은 Tablet을 로딩하여 데이터 서비스를 수행한다. Tablet의 rowkey 범위, 할당된 서버 등과 같은 Tablet 정보는 시스템에서 관리하는 ROOT, META 두 개의 테이블에 저장되어 관리된다.

- META 테이블 : 사용자 테이블의 Tablet 정보를 저장함.
- ROOT 테이블 : META 테이블의 Tablet에 대한 정보를 저장함. 이 테이블은 분리되지 않는 특별한 테이블임.

2.2 AONSS

AONSS(All-or-Nothing Secret Shairng)는 AONT 변환 및 비밀분산(SS) 방식을 적용한 개념이다. 따라서 암호화방식과 같은 암복호키의 관리가 필요없다. [그림 6]은 AONSS의 흐름을 나타낸다.

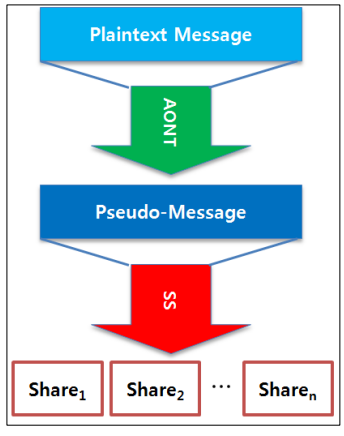

그림 6. AONSS 흐름도

- 평문을 AONT 방식을 통해 변화시킨다.
- 변화된 Pseudo-Message를 XOR기반 SS방식을 이

용하여 분산시킨다. 여기서, 평문과 분산된 정보(Share)의 합은 같다.

- 분산된 Share는 각 DB에 저장관리 되고 복원시에는 분산되 Share를 이용하여 복원한다.

AONSS는 XOR 연산에 기반하고 있어 속도측면에서 기존 비밀분산 방식 보다 빠르다. 그리고 기존 비밀분산 방식에 비해 용장성(redundancy)을 최소화 할 수 있으며, 평문과 Share 크기에 대한 가변성을 가지고 있다. 또한 평문과 분산된 Share 합의 크기가 동일하여 대용량 데이터베이스의 안전한 관리를 위해 적합하다.

본 논문에서는 대용량 데이터베이스의 안전한 보안 관리를 위해서 키를 사용하지 않는 비밀분산 방식을 이용하여 용량의 증가가 없는 AONSS 방식을 적용한다.

2.3 제안 구조

본 방식은 대용량 분산 데이터 관리 시스템인 Neptune을 기반으로 AONSS를 이용한 TA(Tablet Agent)에 의해 분산 데이터의 안전한 관리를 가능하도록 하는 분산 데이터 보안관리 구조를 제안한다. 이를 적용하기 위해 Neptune에서 테이블을 분리한 후, 데이터를 분산 저장할 경우, 분산 및 복원 기능을 수행하는 TA를 시스템에 추가한다. [그림 7]은 제안구조의 흐름을 나타내며, 이 구조의 특징은 데이터 크기가 불변이고 XOR연산에 의해 처리속도가 빠른 장점이 있다.

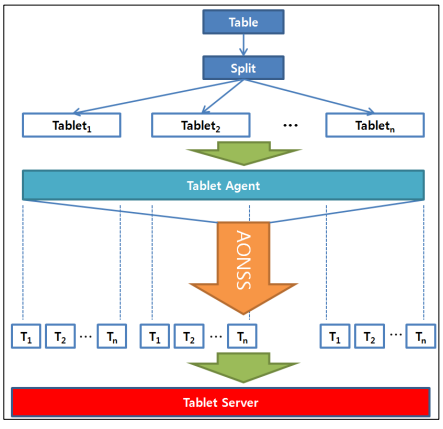

그림 7. 제안구조

본 방식은 Neptune에 기반하고 있기 때문에 우선, 테이블을 Split하는 단계와 Split된 Tablet를 분산하는 단계로 이루어진다. 여기서, AONSS를 기반으로 하는 분산단계는 Tablet 에이전트(TA, Tablet Agent)에 의해 실행된다.

① 하나의 테이블을 rowkey범위로 Split한다. 여기서, Split된 단위를 Tablet라고 한다.

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

③ 분산된 Share(T_1,T_2....Tn)들은 NeptuneMaster에 의해 TabletServer에 할당된다. 복원시에는 할당된 Share들로부터 TA에 의해 Tablet이 복원된다.

본 장에서는 AONT 변환과 배타적 논리합(XOR) 연산을 이용한 새로운 알고리즘을 제안한다. 제안하는 알고리즘은 [그림 8]과 같다.

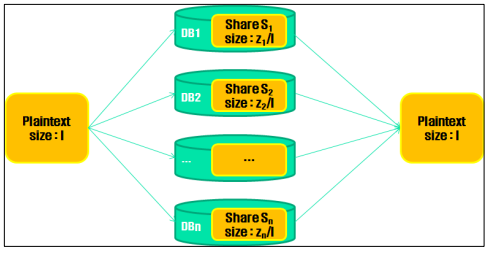

그림 8. 제안하는 개인정보 분산 알고리즘

제안하는 방식은 l의 사이즈를 가진 평문 P에 대하여 $\frac{z_n}{l}$의 사이즈를 갖는 개인정보 조각 S_n을 생성하며, 전체 개인정보 조각 사이즈의 합계와 평문의 사이즈는 같으며, 수식 8과 같이 표현될 수 있다.

$$Z_1 + Z_2 +,...,+ Z_n = l \tag{8}$$

기존의 Shamir의 방식이나 Kurihara가 제안한 비밀분산 방식에 비하여 큰 장점을 갖는다. 즉, 기존 비밀 분산 방식은 각 조각 사이즈의 합계가 평문사이즈×n과 같으

므로, 데이터베이스 저장시 각 데이터베이스마다 평문과 동일한 저장공간을 필요로 하나, 제안하는 알고리즘은 각 개인정보 조각의 사이즈의 합계가 평문과 동일하여 각 데이터베이스당 평균 n/l만큼의 저장공간을 필요로 한다. 이러한 특성은 대용량 데이터베이스에 매우 적합하다.

V. 결 론

향후 지능형 전력망이 갈수록 복잡해지고 서로 연결됨에 따라 유틸리티 공급업체의 사이버 보안 위협을 위한 노력이 점차로 중요하게 될 것이다. 스마트 그리드 시스템에 기존의 암호화 방식만으로 보안성을 유지하기는 현실적으로 어려우며, 이를 보완하기 위하여 데이터 분산 보안관리가 매우 안전한 방법으로 각광받고 있다. 그러나 기존의 비밀분산 방식을 여기에 적용할 경우, 비밀분산 정보가 기존 데이터의 크기와 동일하게 되어 스마트 그리드 시스템과 같은 대용량 데이터 처리에 적용하는데 적합하지 않다. 본 논문에서는 AONT 암호화 모드의 특성을 이용하여 스마트 그리드 환경에서의 안전한 개인정보보호를 제공하기 위한 효율적인 개인정보 데이터의 분산 보안 관리방안을 제안하였다. 본 논문에서 제안된 알고리즘은 처리속도 측면에서 데이터의 고속 분산 및 복원이 가능하며, 각 비밀조각 사이즈의 총합이 평문과 동일하여 스마트 그리드 시스템의 대용량 데이터 관리에 매우 적합하다.

향후 과제로써 효율성 측면에서 실제 구현을 통해 기존의 암호화 모드, XOR방식과 제안방식의 비교분석을 통한 증명이 필요할 것이다. 본 논문의 연구결과는 대용량 데이터를 안전하고 효율적으로 분산 보안 관리하는 개방형 분산 환경에서의 여러 응용 서비스에서 이용될 것으로 기대된다.

참 고 문 헌

[1] U. S. Department of Commerce, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)," pp.83-84, 2009(9).

[2] P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security and Privacy, Vol.7, No.3, pp.75-77, 2009.

[3] C. Wolf and W. Maxwell, "Smart Grids And Privacy," Communications & Strategies, No.76, pp.127-130, 2009.

[4] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the Smart Grid: Embedding Privacy in the Design of Electricity Conservation," The Future of Privacy Forum, 2009(11).

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

[6] R. L. Rivest, "All-or-nothing encryption and the package transform," Fast Software Encryption FSE '97, Lecture Notes in Computer Science, Vol.1267, pp.210-218, 1997.

[7] D. R. Stinson, "Something about all or nothing (transform)," Designs, Codes and Cryptography, Vol.22, pp.133-138, 2001.

[8] H. Kuwakado and H. Tanaka, "Strongly non-separable encryption mode for throwing a media away," Technical Report of IEICE, Vol.103, No.417, pp.15-18, 2003.

[9] V. Boyko, "On the security properties of OAEP as an all-or-nothing transform," Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science, Vol.1666. pp.503-518, 1999.

[10] Office of Electricity Delivery and Energy Reliability, "A System view of the modern Grid," NETL, 2007.

[11] U. S. Department of Commerce, "(Draft) NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements," September 2009.

[12] M. Bellare, P. Rogaway, "Optimal asymmetric encryption," Lecture Notes in Computer Science Advanced in Cryptology EUROCRYPT '94, Vol.950, pp.92-111, 1994.
[13] M. Tada, Y. Fujii, N. Hosaka, K. Tochikubo, and T. Kato, "A secret sharing scheme with threshold 3," Proc. CSS2005, pp.637-642, 2005.
[14] Y. Fujii, M. Tada, N. Hosaka, K. Tochikubo, and T. Kato, "A fast (2, n)-threshold scheme and its application," Proc. CSS2005, pp.631-636, 2005.
[15] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A fast (3, n)-threshold secret sharing scheme using exclusive-or operations," IEICE Trans. Fundamentals, vol.E91-A, No.1. pp.127-138, 2008.
[16] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. TanakavA, "New (k, n)-Threshold Secret Sharing Scheme and Its Extension," 11th Information Security Conference ISC '08, 2008.
[17] F. Chang, J. Dean, S. Ghemawat, W. Hsieh, D. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. Gruber, "Bigtable: A Distributed Storage System for Structured Data," In Proc. of the 7th OSDI, 2006.
[18] 桑門秀典, 神戶大學, "暗号システムの安全性を向上させる暗号化モードに關する硏究(継續)", 電氣通信普及財団, 硏究調査報告, No.19, pp.236, 2004.
[19] 石津晴崇, 荻原利彦, "電子データの長期保管に關する一考察", 電子情報通信學會2004年總合大會講演論文集, D-9-10, 2004.
[20] 이일우, 한동원, "IT기반의 스마트 그리드 기술", 한국정보기술학회지, 제7권, 제1호, pp.25-30, 2009.
[21] 박찬국, "전력인프라 사이버보안 이슈와 정책 대응", 주간기술동향, 제1398호, pp.1-10, 2009.
[22] 김형준, "Neptune : 대용량 분산 데이터 관리 시스템," NHN, 2008.
[23] 박남제, "안전한 모바일 RFID리더를 위한 개방형 임베디드 소프트웨어 플랫폼 구현방안", 한국통신학회논문지, 제35권, 제5호, pp.785-793, 2010.

저 자 소 개

박 남 제(Namje Park) 정회원

- 2000년 8월 : 동국대학교 정보산업학과(이학사)
- 2003년 8월 : 성균관대학교 정보호호학과(공학석사)
- 2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
- 2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
- 2009년 1월 ~ 2009년 12월 : University of California, Los Angeles (UCLA) 공과대학 Post-Doc.
- 2009년 3월 ~ 2009년 12월 : University of California, Los Angeles (UCLA) WINMEC 연구센터 Staff Researcher
- 2010년 1월 ~ 2010년 8월 : Arizona State University (ASU) 컴퓨터공학과 Research Scientist
- 2010년 9월 ~ 현재 : 제주대학교 교육대학 컴퓨터교육전공 교수

<관심분야> : 암호이론, 융합기술보안, 모바일컴퓨팅, RFID/USN, 스마트 그리드, 컴퓨터교육

송 유 진(Youjin Song) 정회원

- 1982년 2월 : 한국항공대학교 전자공학 학사
- 1987년 8월 : 경북대학교 대학원 석사
- 1995년 3월 : 일본 Tokyo Institute of Technology 정보보호학 박사
- 1988년 ~ 1996년 : 한국전자통신연구원 선임연구원
- 2003년 12월 ~ 2005년 2월 : University of North Carolina at Charlotte 연구교수
- 2006년 7월 ~ 8월 : 일본 정보보호대학원(IISEC) 객

원교수
- 1996년 ~ 현재 : 동국대학교 정보경영학과/대학원 교수
- 2005년 ~ 현재 : 동국대학교 부설 전자상거래연구소 소장
- 1998년~ 현재 : 한국정보보호학회 이사/영남지부장
- 2006년~ 현재 : 국제 e-비즈니스학회 이사
- 2006년~ 현재 : 한국사이버테러정보전학회 이사
- 2001년 : ICISC2001 운영위원장 역임
- 2003년 : 하계 CISC2003 프로그램 위원장
- 2006년 : CISC-S2006 공동 프로그램 위원장
- 2007년 : 한국정보시스템학회 추계학술발표대회 공동조직위원장

<관심분야> : IT 융합보안(의료보안, 스마트그리드 보안) Cloud Security and Privacy, Secret Sharing, Context Aware Application Security

박 광 용(Kwangyong Park) **준회원**

- 2008년 2월 : 동국대학교 전자상거래과(이학사)
- 2008년 3월 : 동국대학교 전자상거래 협동과정 기술전공(석사과정)

<관심분야> : 암호이론, 데이터베이스 보안, 유비쿼터스 프라이버시 보호