환경감시 시스템의 정보 인증 서브 시스템 설계 및 구현

신동명°, 김영덕, 최용락
대전대학교 컴퓨터공학과
e-mail:dmshin@zeus.taejon.ac.kr

Implementation of Information Authentication Sub-System for The Environmental Telemetry Monitoring System

Dong-Myung Shin°, Yeong-Deok Kim, Yong-Rak Choi
Dept. of Computer Science, Taejon University

요 약

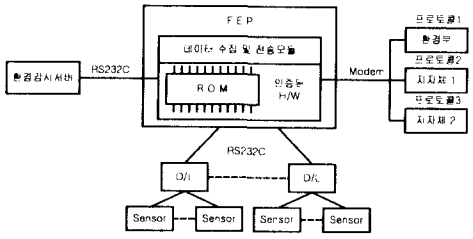
환경부나 지방자치단체에서는 환경문제를 사전에 예방할 수 있는 체계를 마련하기 위하여 오염물질 배출업체가 환경감시 시스템을 통하여 환경오염물질의 배출상태를 실시간으로 측정하여 공시하도록 의무화 하고있다. 그러나 환경단체나 지역주민들은, 환경부나 지방자치단체에 제공된 환경정보에 대한 신뢰감이 부족한 현실이다. 본 논문에서는 환경정보의 신뢰성 제공을 위하여 암호학적 인증 메커니즘을 이용한 환경정보 인증 서브 시스템을 설계, 구현하였다. 제시한 환경정보 인증시스템에서는 클라이언트/서버간 인증, 환경정보에 대한 무결성 보장 및 접근통제, 감사기록의 기능을 제공한다.

1. 서론

국내외적으로 환경관리에 대한 관심이 고조되고 있는데 반해, 환경 관리 단체인 각 기관에서 공시하는 환경정보에 대한 지역주민들의 신뢰도가 낮은 현실이다. 이러한 원인은 환경정보의 수집과정 및 공시과정에서 원천 데이터의 변조가능성에 관한 것들에 기인한다. 환경정보의 분석, 자료처리, 자료제공 등의 업무는 매우 복잡하고 정리 및 통계처리에 많은 시간이 소요되므로 지역주민들이 필요로 하는 정보를 신속 정확하게 제공하기에는 어려움이 있고 그에 따라 환경정보에 대한 불신임이 확대되고 있다. 또한, 기존의 모뎀 통신방식과 하드웨어에 의한 인증처리 방식[1,2]은 정보 요구기관별로 각각의 프로토콜에 의하여 정보를 제공해야 하며, 단편적인 인증기능만을 수행한다. 따라서, 환경정보자원 관리시스템에서 제공하는 정보를 시스템적으로 인증할 수 있는 PKI 기반의 인증 서브 시스템을 개발하여 정보의 효과적인 처리와 동시에 대외 신뢰도를 높여 환경관리에 대한 투명성을 확보 할 필요가 있다.

2. 환경감시 시스템 분석

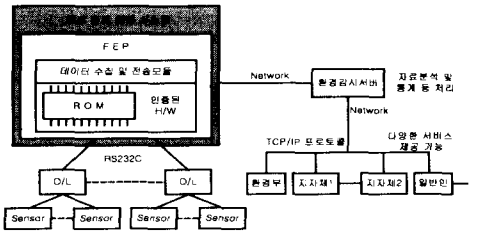
기존의 환경감시시스템은 (그림 1)에서와 같이 환경부나 지자체에 FEP에서 수집한 원시 데이터를 직접 전송함으로써, 환경정보의 통계처리 및 분석을 위한 부가적인 처리장치가 환경부나 지자체에도 중복적으로 필요하게 되었다.



(그림 1) H/W 방식에 의한 환경정보 인증

현재 모뎀을 이용한 통신방법에는 회선의 특성상 정보의 재전송 및 축적전송 기능이 필수적으로 요구되고 있다[1,2]. 그러나 축적전송 및 재전송 과정에서 전송정보의 신뢰성이 매우 떨어지게 된다. 통신장비의 전원차단, 기능정지, 파손, 재전송을 위해 축적하는 데이터에 대한 불법 수정 및 저장정보의 손실 등의 신뢰성 위협형태가 나타날 수 있다[3].

이러한 문제를 해결하기 위해서 네트워크 통신망을 이용한 환경정보의 전송이 필요하고, 네트워크상에서의 여러 가지 보안 위협 요소를 고려한 (그림 2)와 같은 암호학적 인증 메커니즘이 제공되어야 한다. 특히 환경정보의 전송에 있어, 전송정보의 무결성, 발신처 인증, 부인봉쇄, 접근통제, 감사기록 등의 정보보호 서비스가 필수적으로 제공되어야 한다.



(그림 2) 암호학적 인증메커니즘에 의한 환경정보 인증 시스템 설계

3. 환경정보 인증시스템 설계

■ 환경감시 시스템 설계시 고려사항

- 환경감시 서버에 접속하여 다양한 서비스를 제공받고자 할 때 반드시 적절한 수준의 접근통제 서비스가 제공되어야 한다.
- 원시 환경정보의 직접적 공개나 가공한 형태의 자료를 공개할 수 있는데, 두 경우 모두 제공하는 데이터가 변조되지 않았음을 입증하는 처리가 필요하다.

■ 환경감시 시스템의 개선 사항

- 환경정보 인증시스템에서는 원시데이터와 UTC, 접근통제 정보, 각 기관의 서명을 함께 저장하며, 별도의 신뢰된 하드웨어의 사용 없이 원시정보의 무결성을 증명할 수 있다.
- 하드웨어적인 방식으로만 환경정보를 인증했기 때문에 생기는 직접적인 입출력 접근의 제한, 저장영역과 공간의 제약을 받지 않는다.
- 환경정보에 서명정보를 부가하여 시스템적으로 정보인증 서비스를 수행함으로써 위의 하드웨어적인 제한과 공간적 제약을 벗어나 인증된 환경정보를 폭넓게 공개할 수 있고 다양한 접근서비스를 제공할 수 있게 된다.

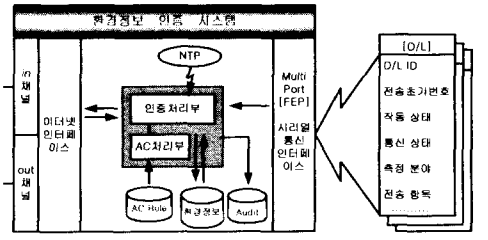
3.1 환경정보 인증시스템의 기능 설계

제시한 환경정보 인증 시스템은 PKI 기반의 공개키 인증서를 사용하여 환경감시 서버와 환경부, 지자체 감시 시스템간의 인증기능을 수행하여, 예상된 클라이언트와 서버로부터 환경정보가 제공되었음을 보장하고, D/L(Data Logger)에서 수집된 원시 환경정보가 부서간의 결탁이나 운영자의 조작에 의해 변조되지 않았음을 증명할 수 있는 정보의 무결성을 보장하는 환경정보 인증시스템을 설계하였다. 또한 환경정보의 무결성 보장을 위해 환경정보자원 관리시스템의 사용자에 대한 오퍼레이션의 권한을 명시하는 접근통제가 제공된다.

1) 인증처리 절차

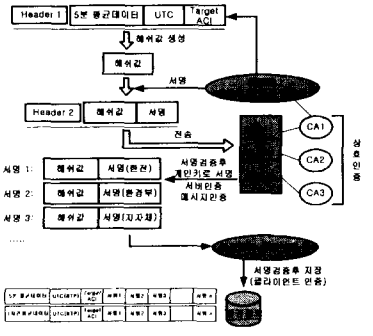
D/L에서 수집된 5분·1시간 평균 환경정보와 NTP 서버에서 입력받은 UTC(Universal Time Coordinated)시간과 환경부나 지자체 등의 각 부서의 서명을 갖는 필드로 구성되어 있다.

각 서명필드는 인증받고자 하는 부서의 수에 따라 확장할 수 있다. Target ACI 필드에는 평균 데이터에 대한 접근통제 정보를 기록한다.



(그림 3) 환경정보 인증시스템

D/L을 통하여 수집한 5분 평균 환경정보는 UTC 시간을 부가한 후 해쉬값을 생성하고, 환경정보 인증시스템의 개인키로 서명하여 해쉬값과 서명값을 환경정보 수집기관(환경부, 지자체) 등에 전송한다. 각 부서는 환경정보의 해쉬값을 보게 되므로, 실제 어떤 값을 갖는지 알 수 없고, 환경정보 인증시스템의 서명을 통하여, 인증시스템을 인증할 수 있다. 각 부서는 해쉬값에 서명을 통하여 환경정보 인증시스템에 보낸다. (그림 4)와 같은 인증처리 흐름도에 따라 환경정보 인증시스템은 서명검증 후 데이터 베이스에 원시 환경정보와 함께 각 부서의 서명을 저장한다.



(그림 4) 환경정보 인증처리 흐름도

각 부서의 인증서 검증과정이 끝나면 EIAS는 다음의 절차를 따라서 환경정보에 대한 인증처리를 수행하게 된다.

- EIAS는 Field_Data를 구성하고 해쉬값을 계산한다.

  ① EIAS : Field_Data 구성, 해쉬값 계산

  $$Field\_Data = \{Header, DATA_5, UTC, ACI_{target}\}$$

  $$Hash\_Value = H[Header||DATA_5||UTC||ACI_{target}]$$

- EIAS는 해쉬 결과에 대해 EIAS의 개인키 KREIAS로 암호화하여 서명한 후 Field_Data 대신 Field_Data의 해쉬값과 해쉬값에 대한 서명을 한전, 환경부, 지자체 등에 전송한다.

  ② EIAS -> KEPCO, ENV_MINISTRY, RI_ORGAN

  $$H(Field\_Data)_{KR_{EIAS}}[H(Field\_Data)]$$

검증된 EIAS의 공개키를 이용하여 EIAS가 전송한 메시지를 검증한다. 메시지의 검증은 예상된 EIAS로부터 메시지가 왔고,

메시지가 중간에 변경되지 않았음을 나타낸다.

③ KEPCO, ENV_MINISTRY, R1_ORGAN

$$D_{KU_{EIAS}}[E_{KR_{EIAS}}[H(Field\_Data) = H(Field\_Data)]$$

각 부서는 EIAS의 메시지 검증 후, 자신의 서명을 붙여 EIAS에 전송한다.

④ KEPCO, ENV_MINISTRY, R1_ORGAN -> EIAS

KEPCO : $H(Field\_Data), E_{KR_{KEPCO}}[H(d_{KR_{EIAS}}[H(Field\_Data)])]$

ENV_MINISTRY :

$$H(Field\_Data), E_{KR_{ENV\ MINISTRY}}[H(d_{KR_{EIAS}}[H(Field\_Data)])]$$

R1_ORGAN :

$$H(Field\_Data), E_{KR_{R1\ ORGAN}}[H(d_{KR_{EIAS}}[H(Field\_Data)])]$$

EIAS는 각 부서의 서명 검증 후, 데이터베이스에 인증정보가 부가된 환경정보를 저장한다. 각 부서의 서명을 검증함으로써 EIAS에 대한 클라이언트들을 인증할 수 있다. 저장된 환경정보와 인증정보는 환경관리 시스템이나 환경감시시스템에 접근하여 환경정보를 요청하는 클라이언트들에 의해 사용된다.

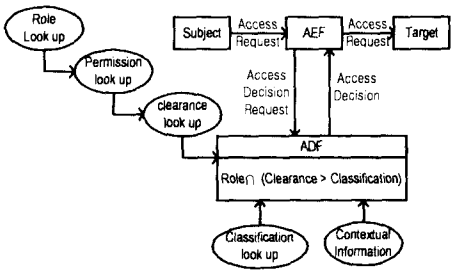
⑤ EIAS : 인증정보가 부가된 환경정보 저장

$$Field\_Data \,||\, E_{KR_{KEPCO}}[H(d_{KR_{EIAS}}[H(Field\_Data)])] \,||\, E_{KR_{ENV\ MINISTRY}}[H(d_{KR_{EIAS}}[H(Field\_Data)])] \,||\, E_{KR_{R1\ ORGAN}}[H(d_{KR_{EIAS}}[H(Field\_Data)])]$$

2) 접근통제

ACI 정보로는 환경정보 관리기관 부서 정보와 부서내의 신분식별자(ID), 수행 오퍼레이션, 평균데이터 내의 항목이 포함된다. 환경정보에의 접근통제 절차로는 (그림 5)에서와 같이 사용자(Subject)의 역할을 검색하고 역할에 따른 타겟(Target)에의 접근권한을 검사한다. 다음으로 타겟에 대하여 사용자의 접근수준(Clearance)을 검색한 후 타겟에 대한 허용등급(Classification)과 비교한다[5].

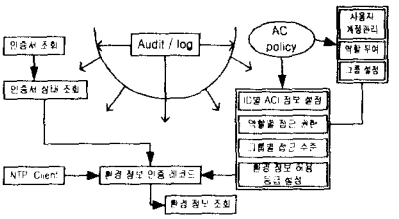
접근권한결정 규칙으로 Role ∩ (Clearance > Classification)을 적용하고 ADF(Access Control Decision Function)에서 접근통제 규칙과 배경 정보(Contextual Information)를 종합하여 타겟에 대한 요청 오퍼레이션의 권한을 결정한다.



(그림 5) 접근통제 절차

3) 감사기록

감사기록의 기능들이 효과적으로 수행이 되기 위해서는 신분확인을 통한 주체의 식별자가 올바로 확인이 되어야 하고, 주체의 식별자에 따른 객체의 식별자, 접근통제, 무결성 및 비밀성 등의 보안관련 메커니즘에서 감사대상이 되는 사건에 대한 정확한 감사정보를 기록해야 한다. 또한, 감사자료에 대한 접근통제가 함께 이루어 져야 한다. 제안한 환경정보 인증시스템에서는 (그림 6)과 같이 인증서 조회, 인증서 상태 조회, 사용자 계정관리, 역할부여, ACI 정보 설정 등 인증시스템 전반에



(그림 6) 인증시스템의 감사기록 영역

걸쳐 일어나는 사건(Event)들을 기록한다.

4. 수행환경

인터넷환경에서 클라이언트쪽은 JRE가 설치된 웹브라우저를 사용하고, 서버쪽은 레드햇 리눅스에 아파치 웹서버와 MySQL 데이터베이스 서버를 설치하였다. 인증시스템의 수행방식은 HTTP 프로토콜을 사용하여 클라이언트와 서버간에 통신을 수행하고 관리자는 윈도우즈 환경에서 웹브라우저를 통해 환경정보관리 시스템인 서버에 로그온하여 사용자 계정, 역할, 접근권한, 감사기록 설정 등을 수행하게 된다.

5. 결론

본 논문에서는 모뎀통신 환경에 의한 환경감시시스템을 인터넷을 이용한 정보처리 및 분배시스템 환경으로 전환하고 정보의 신뢰성 향상을 위한 구체적인 해결방안을 위하여 정보보호기술을 도입한 환경정보 인증시스템을 설계, 구현하였다.

향후 SSL, TLS, IPsec과 같은 인터넷 보안 프로토콜을 적용하여 안전한 통신체계를 마련하고 Java 코드에 대한 인증기능, 감사기록 정보의 무결성 방안 등에 대해 더 심도있게 연구할 필요가 있다. 구현한 환경정보 인증 시스템은 환경관리시스템뿐만 아니라, 환경부나 지자체에 환경정보를 의무적으로 제공해야 하는 공해물질 배출 사업장에 대해 신뢰성 있는 환경정보의 제공을 위한 인증 서브 시스템의 형태로 광범위하게 적용될 수 있다.

참고문헌

[1] 환경관리공단, "TMS구성에 따른 권장규격", 1998
[2] 환경관리처, "환경감시시스템 운영서", 1997.12
[3] William Stalling, Network and Internetwork Security, Prentice Hall, 1995
[4] ISO/IEC DIS 10181-2, Information technology- Open Systems Interconnection - Security Frameworks for Open Systems: Authentication Framework, 1993.
[5] Mohammed I., Dilts D.M., "Design for dynamic user-role-based security", Computer & Security, 1994