(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년03월02일
(11) 등록번호 10-1018924
(24) 등록일자 2011년02월23일

(51) Int. Cl.
G06F 21/00 (2006.01) *H04L 9/32* (2006.01)
G06F 15/16 (2006.01)
(21) 출원번호 10-2009-0013405
(22) 출원일자 2009년02월18일
심사청구일자 2009년02월18일
(65) 공개번호 10-2010-0094127
(43) 공개일자 2010년08월26일
(56) 선행기술조사문헌
전자공학회지 30권6호, 권한관리를 위한 기반기술 (2003.06.)*
RFC 3281, An Internet Attribute Certificate Profile for Authorization, IETF PKIX Working Group (2002.04.)*
M. Menzel et al. Journal of Information Assurance and Security 2, pp.155-160, 2007
US20060248599 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
성균관대학교산학협력단
경기 수원시 장안구 천천동 300 성균관대학교내
(72) 발명자
최형기
서울특별시 서초구 반포본동 반포아파트 53동 106호
한찬규
서울특별시 관악구 봉천4동 1557-22
(74) 대리인
특허법인이상

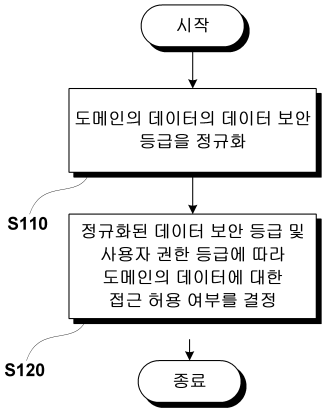
전체 청구항 수 : 총 17 항 심사관 : 경연정

(54) 교차 도메인 상에서의 데이터 접근 방법, 이를 수행하는 시스템 및 이를 수행하는 프로그램을 기록한 기록매체

(57) 요 약

데이터 보안 레벨 협상을 이용한 교차 도메인 상에서의 데이터 접근 방법, 이를 수행하는 시스템 및 이를 수행하는 프로그램을 기록한 기록매체가 개시된다. 교차 도메인 상에서의 데이터 접근 방법은, (a) 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계 및 (b) 도메인의 데이터에 접근하는 경우 정규화된 데이터 보안 등급 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계를 포함한다. 따라서 보안 정책이 서로 상이한 도메인 간의 정보 전송 시 데이터 보안 수준 및 사용자의 권한 수준에 따라 허용되는 정보만이 안전하게 전송될 수 있고, 따라서 교차 도메인 상에서의 호환성을 확보할 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

(a) 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계; 및

(b) 상기 도메인의 데이터에 접근하는 경우 정규화된 상기 데이터 보안 등급 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계를 포함하고,

상기 (a) 단계는 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 (a) 단계는 서로 다른 도메인 간에 k(k는 군집의 수)를 합의한 후 k-means 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 4

제1항에 있어서,

상기 (a) 단계는 상기 군집화 기법이 아닌 도메인 신뢰 등급을 고려하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 5

제4항에 있어서,

상기 (a) 단계는 상기 군집화 기법이 아닌 상기 데이터 보안 등급 및 상기 도메인 신뢰 등급의 곱에 기초하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 6

제4항에 있어서,

상기 도메인 신뢰 등급은 Web of Trust 기법에 의하여 결정되는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 7

제1항에 있어서,

상기 데이터 보안 등급은, 데이터에 접근하기 위해 요구되는 인증 방법, 접근 권한 확인 수준, 키 분배 방법 및 암호화 방법 중 적어도 하나에 대한 정보를 포함하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 8

제1항에 있어서,

상기 (b) 단계는, 속성 인증서를 제시받고, 상기 속성 인증서에 포함된 사용자 권한 등급 및 상기 도메인의 데이터의 정규화된 데이터 보안 등급에 따라 상기 도메인의 데이터에 대한 접근 허용 여부를 결정하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 9

제1항에 있어서,

상기 (b) 단계는, 사용자 권한 등급에 대한 정보를 포함하는 속성 인증서를 이용하여 상기 도메인의 데이터에 접근하는 것을 제어하되,

상기 속성 인증서는, 속성 증명서 발급자 식별자, 속성 증명서 유효 기간 및 사용자 권한 등급에 대한 정보를 포함하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 방법.

청구항 10

다른 도메인의 데이터의 데이터 보안 등급에 상응하여 군집화 기법을 이용하여 자기 도메인의 데이터의 데이터 보안 등급을 정규화하고, 자기 도메인의 사용자 또는 네트워크 노드에게 속성 인증서를 발급하며, 다른 도메인의 호스트가 제시하는 속성 인증서 및 상기 다른 도메인의 호스트가 접근을 시도하는 자기 도메인의 데이터의 정규화된 데이터 보안 등급을 비교하여 상기 다른 도메인의 호스트의 데이터 접근을 제어하는 속성 인증서 발급자; 및

자기 도메인의 속성 인증서 발급자로부터 발급받은 속성 인증서를 다른 도메인에 제시하고, 상기 속성 인증서에 포함된 사용자 권한 등급에 따라 다른 도메인의 데이터에 접근하는 호스트를 포함하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 11

삭제

청구항 12

제10항에 있어서,

상기 속성 인증서 발급자는 인증기관을 통하여 다른 도메인의 속성 인증서 발급자와 k를 합의한 후 k-means 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 13

제10항에 있어서,

상기 속성 인증서 발급자는 상기 군집화 기법이 아닌 도메인 신뢰 등급을 고려하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 14

제13항에 있어서,

상기 속성 인증서 발급자는 상기 군집화 기법이 아닌 상기 데이터 보안 등급 및 상기 도메인 신뢰 등급의 곱에 기초하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 15

제13항에 있어서,

상기 속성 인증서 발급자는 Web of Trust 기법을 이용하여 상기 도메인 신뢰 등급을 결정하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 16

제10항에 있어서,

상기 데이터 보안 등급은, 데이터에 접근하기 위해 요구되는 인증 방법, 접근 권한 확인 수준, 키 분배 방법 및 암호화 방법 중 적어도 하나에 대한 정보를 포함하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 17

제10항에 있어서,

상기 속성 인증서는, 속성 증명서 발급자 식별자, 속성 증명서 유효 기간 및 사용자 권한 등급에 대한 정보를 포함하는 것을 특징으로 하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 18

다른 도메인의 데이터의 데이터 보안 등급에 상응하여 군집화 기법을 이용하여 자기 도메인의 데이터의 데이터 보안 등급을 정규화하고, 다른 도메인의 사용자 또는 네트워크 노드에게 속성 인증서를 발급하며, 다른 도메인의 호스트가 제시하는 속성 인증서 및 상기 다른 도메인의 호스트가 접근을 시도하는 자기 도메인의 데이터의 정규화된 데이터 보안 등급을 비교하여 상기 다른 도메인의 호스트의 데이터 접근을 제어하는 속성 인증서 발급자; 및

다른 도메인의 속성 인증서 발급자로부터 발급받은 속성 인증서를 다른 도메인에 제시하고, 상기 속성 인증서에 포함된 사용자 권한 등급에 따라 다른 도메인의 데이터에 접근하는 호스트를 포함하는 교차 도메인 상에서의 데이터 접근 시스템.

청구항 19

교차 도메인 상에서의 데이터 접근 방법을 수행하는 디지털 처리 장치에 의해 실행될 수 있는 명령어의 프로그램이 유형적으로 구현되어 있으며, 상기 디지털 처리 장치에 의해 판독될 수 있는 프로그램을 기록한 기록매체는,

(a) 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계; 및

(b) 상기 도메인의 데이터에 접근하는 경우 정규화된 상기 데이터 보안 등급 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계를 포함하고,

상기 (a) 단계는 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화하는 것을 특징으로 하는 프로그램을 기록한 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 네트워크 보안에 관한 것으로, 더욱 상세하게는 교차 도메인 상에서의 데이터 접근 방법, 이를 수행하는 시스템 및 이를 수행하는 프로그램을 기록한 기록매체에 관한 것이다.

배 경 기 술

[0002] 인터넷이 원활한 의사소통을 위한 새로운 매개체로 자리 잡음에 따라, 국내외 기관 및 기업은 물론, 개인 이용자들에 의한 인터넷 수요량은 그 양이 매해 폭발적으로 증가하고 있다. 최근 들어 인터넷은 기존의 클라이언트-서버 간 통신 외에, 접근 권한 또는 보안 권한이 서로 다른 다수의 네트워크가 결합된 형태로 발전하게 되었다. 이러한 상황에서 서로 다른 보안 수준의 도메인 간, 다시 말해서 교차 도메인(Cross-Domain) 상에서의 사용자 접속 및 데이터 전송이 수시로 발생하고 있다.

[0003] 교차 도메인 상에서는 개인정보, 인터넷 페이지, 이메일, 대용량 파일 등 다양한 종류의 정보의 교환이 발생하는데, 이러한 정보 교환을 위해서는 각 도메인 간의 데이터 보안 등급이 협의 또는 일치되어 있어야 한다. 따라서 교차 도메인 상에서 가장 중요한 것은 데이터의 보안 수준과 사용자의 권한 수준에 맞게 데이터를 교환하는 것인데, 모바일 환경 또는 All IP 네트워크 환경과 같은 동적 네트워크 환경에서 데이터 별로 상호 협의를 한다는 것은 사실상 불가능하다.

[0004] 종래의 도메인 간 정보 교환 기법은 다양한 보안 등급의 도메인이 존재하는 교차 도메인에서는 범용적인 해결책을 제시하지 못하고 있다. 정보를 교환하는 도메인 간의 신뢰 관계가 형성되지 못하면, 네트워크 공격 발생시 파급효과가 크다. 따라서 보안 등급 또는 보안 정책이 서로 다른 도메인 간에 호환성을 유지하면서도 안전한 정보 교환을 할 수 있는 방법이 요구되고 있다.

발명의 내용

해결 하고자하는 과제

[0005] 따라서 본 발명의 제1 목적은 보안 정책이 서로 다른 교차 도메인 상에서 데이터 보안 등급을 호환시킬 수 있는 교차 도메인 상에서의 데이터 접근 방법을 제공하는 것이다.

[0006] 그리고 본 발명의 제2 목적은 상기와 같은 방법을 수행하는 데이터 접근 시스템을 제공하는 것이다.

[0007] 또한 본 발명의 제3 목적은 상기와 같은 방법을 수행하는 디지털 처리 장치에 의해 실행될 수 있는 명령어의 프로그램이 유형적으로 구현되어 있으며, 상기 디지털 처리 장치에 의해 판독될 수 있는 프로그램을 기록한 기록매체를 제공하는 것이다.

과제 해결수단

[0008] 상술한 본 발명의 제1 목적을 달성하기 위한 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법은, (a) 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계 및 (b) 상기 도메인의 데이터에 접근하는 경우 정규화된 상기 데이터 보안 등급 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계를 포함한다.

[0009] 상기 (a) 단계는 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0010] 상기 (a) 단계는 서로 다른 도메인 간에 k(k는 군집의 수)를 합의한 후 k-means 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0011] 상기 (a) 단계는 도메인 신뢰 등급을 고려하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0012] 상기 (a) 단계는 상기 데이터 보안 등급 및 상기 도메인 신뢰 등급의 곱에 기초하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0013] 상기 도메인 신뢰 등급은 Web of Trust 기법에 의하여 결정될 수 있다.

[0014] 상기 데이터 보안 등급은, 데이터에 접근하기 위해 요구되는 인증 방법, 접근 권한 확인 수준, 키 분배 방법 및 암호화 방법 중 적어도 하나에 대한 정보를 포함할 수 있다.

[0015] 상기 (b) 단계는, 속성 인증서를 제시받고, 상기 속성 인증서에 포함된 사용자 권한 등급 및 상기 도메인의 데이터의 정규화된 데이터 보안 등급에 따라 상기 도메인의 데이터에 대한 접근 허용 여부를 결정할 수 있다.

[0016] 상기 (b) 단계는, 사용자 권한 등급에 대한 정보를 포함하는 속성 인증서를 이용하여 상기 도메인의 데이터에 접근하는 것을 제어하되, 상기 속성 인증서는, 속성 증명서 발급자 식별자, 속성 증명서 유효 기간 및 사용자 권한 등급에 대한 정보를 포함할 수 있다.

[0017] 상술한 본 발명의 제2 목적을 달성하기 위한 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 시스템은, 다른 도메인의 데이터의 데이터 보안 등급에 상응하여 자기 도메인의 데이터의 데이터 보안 등급을 정규화하고, 자기 도메인의 사용자 또는 네트워크 노드에게 속성 인증서를 발급하며, 다른 도메인의 호스트가 제시하는 속성 인증서 및 상기 다른 도메인의 호스트가 접근을 시도하는 자기 도메인의 데이터의 정규화된 데이터 보안 등급을 비교하여 상기 다른 도메인의 호스트의 데이터 접근을 제어하는 속성 인증서 발급자 및 자기 도메인의 속성 인증서 발급자로부터 발급받은 속성 인증서를 다른 도메인에 제시하고, 상기 속성 인증서에 포함된 사용자 권한 등급에 따라 다른 도메인의 데이터에 접근하는 호스트를 포함할 수 있다.

[0018] 상기 속성 인증서 발급자는 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0019] 상기 속성 인증서 발급자는 인증기관을 통하여 다른 도메인의 속성 인증서 발급자와 k를 합의한 후 k-means 군집화 기법을 이용하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0020] 상기 속성 인증서 발급자는 도메인 신뢰 등급을 고려하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0021] 상기 속성 인증서 발급자는 상기 데이터 보안 등급 및 상기 도메인 신뢰 등급의 곱에 기초하여 상기 데이터 보안 등급을 정규화할 수 있다.

[0022] 상기 속성 인증서 발급자는 Web of Trust 기법을 이용하여 상기 도메인 신뢰 등급을 결정할 수 있다.

[0023] 상기 데이터 보안 등급은, 데이터에 접근하기 위해 요구되는 인증 방법, 접근 권한 확인 수준, 키 분배 방법 및 암호화 방법 중 적어도 하나에 대한 정보를 포함할 수 있다.

[0024] 상기 속성 인증서는, 속성 증명서 발급자 식별자, 속성 증명서 유효 기간 및 사용자 권한 등급에 대한 정보를 포함할 수 있다.

[0025] 상술한 본 발명의 제2 목적을 달성하기 위한 본 발명의 다른 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 시스템은, 다른 도메인의 데이터의 데이터 보안 등급에 상응하여 자기 도메인의 데이터의 데이터 보안 등급을 정규화하고, 다른 도메인의 사용자 또는 네트워크 노드에게 속성 인증서를 발급하며, 다른 도메인의 호스트가 제시하는 속성 인증서 및 상기 다른 도메인의 호스트가 접근을 시도하는 자기 도메인의 데이터의 정규화된 데이터 보안 등급을 비교하여 상기 다른 도메인의 호스트의 데이터 접근을 제어하는 속성 인증서 발급자 및 다른 도메인의 속성 인증서 발급자로부터 발급받은 속성 인증서를 다른 도메인에 제시하고, 상기 속성 인증서에 포함된 사용자 권한 등급에 따라 다른 도메인의 데이터에 접근하는 호스트를 포함한다.

[0026] 상술한 본 발명의 제3 목적을 달성하기 위한 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법을 수행하는 디지털 처리 장치에 의해 실행될 수 있는 명령어의 프로그램이 유형적으로 구현되어 있으며, 상기 디지털 처리 장치에 의해 판독될 수 있는 프로그램을 기록한 기록매체는, (a) 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계 및 (b) 상기 도메인의 데이터에 접근하는 경우 정규화된 상기 데이터 보안 등급 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계를 수행하는 프로그램을 기록한다.

효 과

[0027] 상기와 같은 교차 도메인 상에서의 데이터 접근 방법, 이를 수행하는 시스템 및 이를 수행하는 프로그램을 기록한 기록매체에 따르면, 보안 정책이 서로 상이한 도메인 간의 정보 전송 시 데이터 보안 수준 및 사용자의 권한 수준에 따라 허용되는 정보만이 안전하게 전송될 수 있고, 교차 도메인 상에서의 호환성을 확보할 수 있다.

[0028] 그리고 동적으로 보안 등급을 설정할 수 있으므로 All IP 네트워크 환경 또는 모바일 환경 등과 같은 네트워크 보안 환경이 동적으로 변동되는 상황에서 데이터 및 사용자 별 상호 협의를 통하여 안전한 데이터 전송을 수행할 수 있다.

발명의 실시를 위한 구체적인 내용

[0029] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0030] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0031] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0032] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0033] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이

속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0034] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 이하, 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0035] 본 발명의 실시예에 대하여 설명하기에 앞서, 본 발명에서 사용되는 용어들에 대하여 우선 설명한다.

[0036] "데이터 보안 등급"이란 도메인 내의 각 데이터에 대하여 부여되는 값으로서, 도메인의 관리 범위 내에 있는 특정 데이터로의 접근 시 요구되는 보안 정책을 수치화한 결과를 의미한다. 예를 들어, 도메인의 데이터에 대한 보안 정책은 인증 방법, 접근 권한 확인 수준, 키 분배 방법 및 암호화 방법에 대한 정책을 포함할 수 있다.

[0037] 인증 방법에는 사용자 비밀번호, 대칭키(Symmetric Key), 공개키(Public Key), One Time 비밀번호, 그래픽(Graphical) 비밀번호, 바이오메트릭스 (Biometrics) 등이 있고, 후자로 갈수록 높은 보안 수준에 해당한다.

[0038] 접근 권한 확인 수준에는 세션(Session) 별 확인, 연결(Connection) 별 확인, 패킷(Packet) 별 확인, 로그(Log) 또는 리뷰(Reviewing) 지원 등이 있고, 후자로 갈수록 높은 보안 수준에 해당한다.

[0039] 키 분배 방법에는 인증서버 키 전달, 도메인 간 키 교환, 키 실시간 전달, 세션 별 신선성(Freshness) 보장, 연결 별 신선성 보장, 패킷 별 신선성 보장 등이 있고, 후자로 갈수록 높은 보안 수준에 해당한다.

[0040] 암호화 방법에는 DES(Data Encryption Standard) 등의 대칭키 암호화, RSA 등의 비대칭키 암호화, 워터마킹(Watermarking) 지원, 부인방지(Nonrepudiation) 지원, 프라이버시 보호 등이 있고, 후자로 갈수록 높은 보안 수준에 해당한다.

[0041] 상기와 같은 각 보안 정책의 보안 기법에 대하여 보안 수준에 따라 차등적으로 점수를 부여할 수 있다.

[0042] 도 1은 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 이용되는 데이터 보안 등급 점수배정의 예를 설명하기 위한 예시도이다.

[0043] 도 1을 참조하면, 인증 방법에 있어서, 사용자 비밀번호 기법에는 0.1, 대칭키 기법에는 0.2, 공개키 기법에는 0.4, One Time 비밀번호 기법에는 0.5, 그래픽 비밀번호 기법에는 0.7, 바이오메트릭스 기법에는 1.0과 같은 방식으로 점수를 부여할 수 있다. 이 경우 지원하는 가장 높은 보안 수준에 해당되는 점수를 부여받게 된다. 즉, 인증 방법에 있어서, 사용자 비밀번호 기법, 대칭키 기법, 공개키 기법, One Time 비밀번호 기법, 그래픽 비밀번호 기법 및 바이오메트릭스 기법 모두를 지원하는 경우에는 1.0점을 부여하고, One Time 비밀번호 기법까지만 지원하는 경우에는 0.5점을 부여한다.

[0044] 접근 권한 확인 수준, 키 분배 방법, 암호화 방법에 속하는 각 보안 기법에 대해서도 상술한 바와 유사하게 점수를 부여할 수 있다. 따라서, 특정 도메인의 데이터에 대한 보안 정책이 상기 네가지 보안 정책으로 구성된다면, 상기 도메인에 속하는 데이터에 대한 데이터 보안 등급은 네개의 값으로 구성되는 벡터의 형태를 가지게 된다. 즉, 데이터 보안 등급 벡터 D_S = (x, y, z, u) = (인증 방법 점수, 접근 권한 확인 수준 점수, 키 분배 방법 점수, 암호화 방법 점수)가 될 수 있다.

[0045] "도메인 신뢰 등급"이란 도메인 자체의 신뢰 수준을 나타내는 수치로서, Web of Trust 구조에 속해 있는 각 도메인은 인증기관(Certificate Authority, CA)으로부터 자신의 도메인 신뢰 등급을 얻을 수 있다. 도메인 신뢰 등급은 통상 0.1 ~ 1.0 범위의 값을 가지며, 특히 0.1점, 0.5점, 1.0점과 같이 설정될 수 있다. 신뢰할 수 없는 도메인에 대하여는 0점의 도메인 신뢰 등급을 설정하며, 이 경우 보안 등급 협상 또는 해당 도메인으로의 데이터 송신을 거절한다.

[0046] Web of Trust란 각 사용자들끼리 서로 간의 신뢰 수준을 측정하고, 인증서를 발행하는 기법이다. 각 사용자는 다른 사용자의 인증서 또는 키에 대한 신뢰 수준을 결정할 수 있고, 이것이 파생되어 다른 신뢰관계를 생성할 수 있다. Web of Trust에서는 소개자 신뢰 수준, 인증서 신뢰 수준, 키 적합성 신뢰 수준 등을 고려하여 전체적인 신뢰 수준을 결정할 수 있다. 소개자가 소개해준 인증서의 신뢰 수준은 보통 소개자의 신뢰 수준과 같게 설정된다. 예를 들어, 도메인 A가 완전히 신뢰하는 인증기관에 의해 도메인 B가 인증(Sign)되었다면, 도메인 A는

도메인 B를 완전히 신뢰할 수 있으므로, 도메인 B에 대한 인증서 신뢰 수준 또는 키 적합성 신뢰 수준을 1점으로 결정할 것이다. Web of Trust에 대한 상세한 사항은 관련 공지기술 및 기술문헌으로부터 용이하게 파악될 수 있으므로 이하 설명은 생략한다.

[0047] "데이터 접근 등급"이란 도메인 내의 특정 데이터에 접근하는 경우 상기 도메인에 의해 요구되는 접근 수준 또는 권한 수준을 의미하는 값으로서, 특히 데이터 보안 등급과 도메인 신뢰 등급의 조합으로부터 산출될 수 있다. 예를 들어, 데이터 보안 등급 벡터와 도메인 신뢰 등급 수치의 스칼라 곱으로서 데이터 접근 등급을 정의할 수 있다. 즉, 데이터 보안 등급 벡터 $D_S = (x, y, z, u)$와, 도메인 신뢰 등급 t에 대하여, 데이터 접근 등급 벡터 $D_A = tD_S = (tx, ty, tz, tu)$가 되게 된다.

[0048] "사용자 권한 등급"이란 사용자 또는 네트워크 노드(Network Node)가 특정 도메인 내의 데이터에 접근할 수 있는 권한 수준을 의미하는 값으로서, 데이터 접근 등급에 대응되어 사용자가 특정 도메인 내의 데이터에 접근할 수 있도록 허용된 한계 수준을 나타낸다. 다시 말해서, 소정의 사용자 권한 등급을 가진 사용자는 특정 도메인에서 그 사용자 권한 등급과 동일하거나 그보다 낮은 데이터 접근 등급 이하의 데이터는 모두 접근할 수 있지만, 그 사용자 권한 등급보다 높은 데이터 접근 등급의 데이터에는 접근할 수 없다.

[0049] 사용자 권한 등급은 데이터 접근 등급에 대응되어 사용자 권한 등급 벡터 또는 하나의 수치 형태를 취할 수 있다. 사용자 권한 등급의 값 설정은 데이터 접근 등급을 구성하는 인증 방법 등의 구체적인 보안 정책의 조합별로 세부적으로 결정될 수도 있고, 또는 데이터 접근 등급을 전체적으로 평가하였을 때 비보안(Unclassified), 비밀(Confidential), 기밀(Secret) 또는 일급비밀(Top Secret) 중 어느 수준에 있는지에 따라 그에 대응되는 미리 정하여진 수개의 값 중에서 결정될 수도 있다. 예를 들어, 비보안 데이터만 접근할 수 있는 사용자의 경우에는 사용자 권한 등급 벡터 $U_A = (a, b, c, d) = (0, 0, 0, 0)$, 비밀 데이터까지 접근할 수 있는 사용자의 경우에는 사용자 권한 등급 벡터 $U_A = (a, b, c, d) = (0.2, 0.3, 0.4, 0.1)$과 같이 결정할 수 있다. 사용자 권한 등급은 각 도메인이 다른 도메인과의 합의 없이 자유롭게 결정할 수 있다.

[0050] 이하에서는 데이터 보안 등급, 데이터 접근 등급, 사용자 권한 등급은 벡터의 형태를 가지고, 도메인 신뢰 등급은 스칼라의 형태를 가지는 것으로 예를 들어 설명한다.

[0051] 도 2는 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법을 설명하기 위한 흐름도이다.

[0052] 도 2를 참조하면, 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법은 크게 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계(S110)와, 도메인의 데이터에 접근하는 경우 데이터 접근 등급(정규화된 상기 데이터 보안 등급) 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계(S120)를 포함한다.

[0053] 먼저, 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계(S110)에 대해 설명한다.

[0054] 교차 도메인 환경에서는 각 도메인의 보안 정책이 다를 수 있고, 어느 한 도메인에서의 "보안 등급 1"이 요구하는 보안 수준이 다른 도메인에서의 "보안 등급 1"이 요구하는 보안 수준과 일치하지 않을 수 있다. 예를 들어, 도메인 A는 데이터 보안 등급을 A등급 ~ Z등급 총 26개 등급으로 나누는 반면에, 도메인 B는 데이터 보안 등급을 가등급 ~ 하등급 총 14개 등급으로 나눈다면, 도메인 A의 A등급과 도메인 B의 가등급은 보안 수준이 정확히 동등하다고 볼 수 없다. 따라서 도메인 A의 어느 사용자가 도메인 B의 데이터에 접근하려고 하거나, 그 반대의 경우에 안전한 데이터 전송을 보장하기 위해 도메인 A의 데이터 보안 등급과 도메인 B의 데이터 보안 등급을 서로 맞추는 정규화 과정이 필요하다. 이하에서 교차 도메인 환경의 예로서 서로 다른 도메인 A와 도메인 B가 존재하는 경우를 예로 들어 설명한다.

[0055] 교차 도메인 환경에서 도메인의 데이터의 데이터 보안 등급을 정규화하는 방법으로서 군집화 기법(Clustering Algorithm)이 사용될 수 있다. 상기 데이터 보안 등급을 정규화하는 방법은 특정한 방법에 제한되지 아니하고, 도메인 A가 정의한 데이터 보안 등급을 도메인 B가 정의한 데이터 보안 등급으로 대응(Mapping)시킬 수 있는 가능한 모든 종류의 방법이 될 수 있다. 이하에서는 상기 데이터 보안 등급을 정규화하는 방법으로서 군집화 기법을 예로 들어 설명한다.

[0056] 군집화 기법을 사용하는데에 있어서, 도메인 A와 도메인 B는 군집의 수 k를 합의한 후 각 도메인의 데이터에 대하여 군집화 과정을 수행할 수 있다. k-means 기법이 이러한 방식에 해당한다. 상기 합의 과정은 인증기관(CA)을 통하여 이루어질 수 있다. 상기 군집화 기법은 특정한 기법에 제한되지 아니하고, 도메인 A가 정의한 데이터

보안 등급의 일군을 도메인 B가 정의한 데이터 보안 등급의 일군으로 대응시킬 수 있는 가능한 모든 종류의 기법이 될 수 있다. 이하에서는 상기 군집화 기법으로서 k-means 기법을 예로 들어 설명한다.

[0057] k-means 기법에서 k를 선택하는 방법으로는 임의 선택 기법, Furthest First 기법(D. Hochbaum, D. Shmoys, A best possible heuristic for the k-center problem, Mathematics of Operations Research, 10(2):180-184, 1985) 등의 방법을 사용할 수 있고, 여러 k값에 대하여 k-means 기법을 실행한 후 가장 군집화 결과가 좋은 k를 선택할 수도 있다.

[0058] k-means 군집화 기법에 대해 이하에서 설명한다. k-means 군집화 기법은 n개의 데이터를 n보다 작은 k개의 군집으로 재구성하는데, 구체적인 과정은 아래와 같다.

[0059] (단계 1) 각 군집을 대표하는 총 k개의 중간값을 선택한다.

[0060] (단계 2) n개의 데이터에 대하여 가장 가까운 거리의 중간값을 발견하고, 그 중간값의 군집에 배정한다.

[0061] (단계 3) 각 군집에 배정된 데이터로부터 총 k개의 중간값을 계산한다.

[0062] (단계 4) 중간값이 미리 정하여진 기준에 부합할 때까지 단계 2 및 단계 3을 반복한다.

[0063] 단계 2에서의 거리는 유클리디안 거리(Euclidean Divergence)일 수 있고, 단계 4에서의 미리 정하여진 기준은 더 이상 중간값의 변화가 없이 수렴하는 경우일 수 있다.

[0064] 도 3은 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 k-means 기법을 설명하기 위한 개념도이다. 여기서 k는 3인 것으로 가정한다.

[0065] 도 3의 (a)를 참조하면, 흰색 원으로 도시된 총 12개의 데이터와, 회색 원으로 도시된 총 3개의 중간값이 나타나 있다. 회색 원 안의 숫자 i는 그 회색 원으로 도시된 중간값이 군집 i의 중간값임을 나타낸다. 이와 같이 3개의 군집을 대표하는 3개의 중간값을 선택하는 과정이 상기 단계 1에 해당한다.

[0066] 도 3의 (b)를 참조하면, 12개의 데이터 각각에 대하여 가장 가까운 거리의 중간값을 발견하고, 그 중간값이 대표하는 군집에 배정하는 과정이 나타나 있다. 흰색 원 안의 숫자 i는 그 흰색 원으로 도시된 데이터가 군집 i에 배정된 데이터임을 나타낸다. 이와 같이 12개의 데이터를 3개의 군집에 배정하는 과정이 상기 단계 2에 해당한다.

[0067] 도 3의 (c)를 참조하면, 각 군집 별로 배정된 데이터의 중간값을 계산하여 새로운 k개의 중간값을 산출하는 과정이 나타나 있다. 점선 윤곽선을 가진 회색 원이 현재 중간값을 나타내고, 실선 윤곽선을 가진 회색 원이 새로이 계산된 중간값을 나타낸다. 군집 1의 경우 배정된 데이터가 1개였으므로, 그 데이터 값 자체가 군집 1의 중간값이 된다. 도 2의 (c)에서 군집 1의 데이터가 따로 도시되어 있지 아니하나, 군집 1의 중간값과 동일한 데이터가 존재한다. 군집 2 및 군집 3의 경우도 마찬가지로 각 군집에 속해 있는 데이터 값으로부터 중간값을 산출한다. 이와 같이 3개의 군집에 배정된 총 12개의 데이터로부터 3개의 중간값을 계산하는 과정이 상기 단계 3에 해당한다.

[0068] 도 3의 (d)를 참조하면, 상기 단계 3을 거쳐서 새로이 계산된 중간값이 나타나 있다. 중간값이 더 이상 변동되지 않을 때까지 군집화 과정을 계속 하는 것으로 정하였다면, 도 2의 (b)와 (d)에서 보는 바와 같이 중간값의 변동이 발생하였으므로, 상기 단계 2 및 상기 단계 3을 추가로 더 반복하게 된다. 이와 같은 과정이 상기 단계 4에 해당한다.

[0069] 데이터 보안 등급은 하나의 수치 형태 또는 복수의 수치로 구성된 벡터 형태를 가질 수 있다. 따라서 데이터 보안 등급이 어떤 형태를 취하더라도 유클리디안 거리 등의 거리 기준에 따라 상술한 군집화 기법 또는 k-means 기법을 수행할 수 있다.

[0070] 상술한 바와 같이 데이터 보안 등급에 대해 군집화를 수행한 후, 군집화된 데이터별 데이터 보안 등급을 도메인 신뢰 등급과 조합함으로써 정규화된 데이터 보안 등급, 다시 말해서 최종적인 데이터 접근 등급을 산출한다. 예를 들어, 군집화된 데이터별 데이터 보안 등급과 도메인 신뢰 등급의 곱을 데이터 접근 등급으로 정의할 수 있다. 상기 군집화된 데이터별 데이터 보안 등급이 벡터 형태인 경우 도메인 신뢰 등급과의 스칼라 곱으로 정의할 수 있다.

[0071] 도 4는 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 데이터 접근 등급을 설명하기 위한 개념도이다.

[0072] 도 4를 참조하면, 도메인 A와 도메인 B는 군집의 수를 2로 합의하였음을 알 수 있고, 각 도메인에 속하는 데이터에 대한 데이터 접근 등급이 나타나 있다. 도메인 A의 데이터 a, b는 군집 1에, 데이터 c는 군집 2에 배정되었다. 도메인 B의 모든 데이터 가, 나, 다, 라는 군집 2에 배정되었다. 데이터 c와 데이터 가는 동등한 데이터 접근 등급을 가지지만, 데이터 a와 데이터 가는 동등한 데이터 접근 등급을 가지지 않는다. 예를 들어, 데이터 a를 접근할 수 있는 권한을 가진 사용자는 데이터 가, 나, 다, 라를 접근할 수 있지만, 데이터 가를 접근할 수 있는 권한을 가진 사용자는 데이터 c를 접근할 수 있을 뿐 데이터 a, b를 접근할 수는 없다.

[0073] 다시 도 2를 참조하면, 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계(S110)를 마친 후, 도메인의 데이터에 접근하는 경우 데이터 접근 등급(정규화된 상기 데이터 보안 등급) 및 사용자 권한 등급에 따라 허용 여부를 결정하는 단계(S120)를 수행한다.

[0074] 누구나 아무런 제한 없이 데이터에 접근할 수 있는 Public 도메인과 달리, 일정한 보안 정책에 따라 데이터 접근을 제어하는 Protected 도메인에는 속성 증명서 발급자(Attribute Certificate Issuer) 네트워크 노드가 존재한다.

[0075] 속성 증명서 발급자는, 자신이 속한 도메인의 모든 사용자 또는 네트워크 노드에게 데이터 접근 권한에 대한 정보를 포함하는 속성 증명서(Attribute Certificate)를 발급한다. 또는 속성 증명서 발급자는 자신이 속한 도메인의 데이터에 다른 도메인의 사용자가 접근하고자 하는 경우 상기 다른 도메인의 사용자 또는 상기 다른 도메인의 네트워크 노드에게 데이터 접근 권한에 대한 정보를 포함하는 속성 증명서를 발급할 수 있다. 다시 말해서, 사용자 또는 네트워크 노드는 접근하려고 하는 도메인의 속성 증명서 발급자로부터 직접 속성 인증서를 발급받거나, 또는 접근하려고 하는 도메인의 속성 증명서 발급자와 신뢰 관계가 구축된 자신이 속한 도메인의 속성 인증서 발급자로부터 발급받을 수 있다.

[0076] 도 5는 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 이용되는 속성 인증서를 설명하기 위한 개념도이다.

[0077] 도 5를 참조하면, 속성 인증서는 속성 인증서 버전, 데이터에 접근하려고 하는 사용자 식별자, 접근하려고 하는 데이터가 속한 도메인 또는 데이터에 접근하려고 하는 사용자가 속한 도메인의 속성 인증서 발급자 식별자, 암호화 또는 무결성 알고리즘 식별자, 인증서 일련번호, 속성 인증서 유효기간, 사용자 권한 등급에 대한 정보를 포함할 수 있다.

[0078] 상기 사용자는 발급된 상기 속성 인증서를 자신이 접근하고자 하는 데이터가 속한 도메인에 제시하는데, 특히 상기 도메인의 가드(Guard)가 상기 속성 인증서에 기재된 사용자 권한 등급과 접근하고자 하는 데이터의 데이터 접근 등급을 비교하여 접근 여부를 결정할 수 있다. 이 경우 상기 사용자는 발급된 상기 속성 인증서에 기재되어 있는 사용자 권한 등급과 동일하거나 그보다 낮은 등급의 데이터에 접근할 수 있다.

[0079] 도메인 또는 도메인의 가드는 상기 사용자가 접근 요청한 데이터의 데이터 접근 등급 벡터 D_A = (tx, ty, tz, tu)와 상기 사용자가 제시한 속성 인증서에 명시된 속성, 즉 사용자 권한 등급 벡터 U_A = (a, b, c, d)를 대조하여 접근 허용 여부를 결정한다. 이 경우 difference = min(a tx, b ty, c tz, d tu)를 정의하고, difference < 0 이면 접근을 불허할 수 있다. 즉, 사용자 권한 등급 벡터의 어느 한 요소라도 데이터 접근 등급의 대응되는 요소의 보안 수준에 미치지 못하면 데이터 접근이 불허된다. 예를 들어, 사용자가 접근 요청한 데이터의 데이터 접근 등급 벡터가 D_A = (0.5, 0.5, 0.5, 0.5)인데 사용자가 제시한 속성 인증서에 명시된 사용자 권한 등급 벡터 U_A = (0.4, 0.6, 0.7, 0.5)이면 difference = -0.1이 되므로 상기 사용자의 데이터 접근은 허용되지 않는다.

[0080] 도 6은 본 발명의 일 실시예에 따른 k-means 기법을 이용한 교차 도메인 상에서의 데이터 접근 방법을 설명하기 위한 흐름도이다.

[0081] 도 2를 참조하여 설명한 바와 같이, 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법은 크게 도메인의 데이터의 데이터 보안 등급을 정규화하는 단계(S110)와, 도메인의 데이터에 접근하는 경우 사용자 권한 등급에 따라 허용 여부를 결정하는 단계(S120)를 포함한다.

[0082] 도 6을 참조하면, 상기 도메인의 데이터의 데이터 보안 등급 정규화 단계(S110)은 도메인 간에 군집의 수 k를 합의하는 단계(S111), 각 도메인의 데이터에 대하여 데이터 보안 등급을 기준으로 k 군집화를 수행하는 단계(S113) 및 각 도메인의 데이터에 대하여 데이터 보안 등급과 도메인 신뢰 등급의 조합으로부터 데이터 접근 등

급을 산출하는 단계(S115)를 포함할 수 있다.

[0083] 상기 도메인의 데이터에 접근하는 경우 사용자 권한 등급에 따라 허용 여부를 결정하는 단계(S120)는 사용자 권한 등급을 명시하는 속성 인증서를 발급하는 단계(S121), 도메인의 데이터에 접근하는 사용자로부터 발급한 속성 인증서를 제시 받는 단계(S123), 속성 인증서에 명시된 사용자 권한 등급이 데이터의 데이터 접근 등급과 동일하거나 높은지 판단하는 단계(S125) 및 도메인의 데이터에 접근을 허용하는 단계(S127)를 포함할 수 있다.

[0084] 상기 군집 수 합의 단계(S111), 군집화 수행 단계(S113), 데이터 접근 등급 산출 단계(S115), 속성 인증서 발급 단계(S121), 속성 인증서 제시 받는 단계(S123), 사용자 권한 등급과 데이터 접근 등급 대조 단계(S125) 및 도메인 데이터 접근 허용 단계(S127)에 대하여는 상기 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 상기 도메인의 데이터의 데이터 보안 등급 정규화 단계(S110) 및 상기 도메인의 데이터에 접근하는 경우 사용자 권한 등급에 따라 허용 여부를 결정하는 단계(S120)에 대하여 도 1 내지 도 5을 참조하여 설명한 바와 동일하게 이해될 수 있으므로 이하 설명을 생략한다.

[0085] 도 7은 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 시스템의 구성을 나타내는 블록도이다.

[0086] 도 7을 참조하면, 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 시스템은 속성 인증서 발급자(210), 호스트(220) 및 가드(Guard, 230)를 포함한다. Protected 도메인은 다른 Public 도메인 또는 다른 Protected 도메인과의 연결에 있어서 에지 라우터(Edge Router, 240)를 경유할 수 있다. 다른 Protected 도메인, 예를 들어 도 7에 도시된 Protected 도메인 B도, 마찬가지로 속성 인증서 발급자(310), 호스트(320) 및 가드(330)를 포함할 수 있다.

[0087] 구체적으로 속성 인증서 발급자(Attribute Certificate Issuer, 210)는 다른 도메인의 데이터의 데이터 보안 등급에 상응하여 자기 도메인의 데이터의 데이터 보안 등급을 정규화하고, 다른 도메인 또는 자기 도메인에 속하는 사용자 또는 호스트(220, 320) 등의 네트워크 노드에게 속성 인증서를 발급한다.

[0088] 속성 인증서 발급자(210)는 데이터 보안 등급을 정규화함에 있어서 군집화 기법을 이용할 수 있다. 이 경우 군집화 기법으로서 k-means 기법을 이용하는 경우 인증기관(Certificate Authoirty, CA, 250)을 통하여 군집의 수 k를 합의 할 수 있다.

[0089] 속성 인증서 발급자(210)는 도메인 신뢰 등급을 고려하여 상기 데이터 보안 등급을 정규화할 수 있는데, 이때 도메인 신뢰 등급은 군집화된 데이터 보안 등급에 일종의 가중치를 부가하는 의미를 가진다. 이 경우, 예를 들어, 속성 인증서 발급자(210)는 데이터 보안 등급 및 도메인 신뢰 등급의 곱을 데이터 접근 등급으로 정의할 수 있다.

[0090] 속성 인증서 발급자(210)는 도메인 신뢰 등급을 결정함에 있어서 Web of Trust 구조의 최상위 기관인 인증기관(Certificate Authority, CA)으로부터 자신의 도메인 신뢰 등급을 얻을 수 있다.

[0091] 호스트(Host, 220)는 다른 도메인의 속성 인증서 발급자(310) 또는 자기 도메인의 속성 인증서 발급자(210)로부터 발급받은 속성 인증서를 다른 도메인의 가드(330)에 제시하고, 상기 속성 인증서에 포함된 사용자 권한 등급에 따라 다른 도메인의 데이터, 예를 들어 다른 도메인의 호스트(320)의 데이터에 접근한다.

[0092] 가드(Guard, 230)는 다른 도메인의 호스트(320)가 제시하는 속성 인증서 및 상기 다른 도메인의 호스트(320)가 접근을 시도하는 자기 도메인의 데이터, 예를 들어 자기 도메인의 호스트(220)의 데이터의 정규화된 데이터 보안 등급을 비교하여 상기 다른 도메인의 호스트(320)의 데이터 접근을 제어할 수 있다. 또는 가드(230)는 다른 도메인의 호스트(320)가 제시하는 속성 인증서를 자기 도메인의 속성 인증서 식별자(210)으로 전달하고, 자기 도메인의 속성 인증서 식별자(210)가 유사한 방식으로 상기 다른 도메인의 호스트(320)의 데이터 접근을 제어할 수 있다.

[0093] 가드(230)는 각기 다른 보안레벨을 가진 교차 도메인 시스템에서 정보를 공유하고, 전달하는 보안 메커니즘을 제어한다. 통상적으로 가드(230)는 데이터 안전성(Sanitation), 데이터 필터링(Review), Protected 네트워크와 Public 네트워크 간의 연결, 재전송, 접근 제한 및 보안에 관한 기능을 지원한다. 가드에 대한 상세한 사항은 관련 공지기술 및 기술문헌으로부터 용이하게 파악될 수 있으므로 이하 설명은 생략한다(Jeremy Epstein, "Architecture and concepts of the ARGuE Guard", 15th Annual Computer Security Applications Conference, (ACSAC), December 1999).

[0094] 전체적으로 요약하면, 도메인 A의 속성 인증서 발급자(210)와 도메인 B의 속성 인증서 발급자(310)는, 인증기관(CA, 250)을 통하여 군집화 기법에서 미리 결정되어야 하는 군집의 수 k를 합의하는 등의 과정을 통하여, 도메인 A와 도메인 B의 데이터 보안 등급을 정규화한다. 또한 인증기관(CA, 250)을 통하여 각자의 속성 인증서를 신뢰한다.

[0095] 도메인 B의 호스트(320)가 도메인 A의 호스트(220)의 데이터에 접근하려고 하는 경우, 도메인 B의 호스트(320)는 속성 인증서를 발급받는다. 이 경우 도메인 B의 호스트(320)는 상기 속성 인증서를 도메인 A의 속성 인증서 발급자(210)로부터 발급받거나, 도메인 A의 속성 인증서 발급자(210)와 정규화 과정을 통하여 신뢰 관계를 형성한 도메인 B의 속성 인증서 발급자(310)로부터 발급받을 수 있다.

[0096] 도메인 B의 호스트(320)는 발급 받은 속성 인증서를 도메인 A의 가드(230)에 제시하고, 도메인 A의 가드(230)가 속성 인증서에 명시된 사용자 권한 등급과 도메인 B의 호스트(320)가 접근하려고 하는 도메인 A의 데이터의 데이터 접근 등급을 비교하여 접근 허용 여부를 결정하거나, 도메인 A의 가드(230)로부터 상기 속성 인증서를 전달 받은 도메인 A의 속성 인증서 발급자(210)가 유사한 방식으로 접근 허용 여부를 결정할 수 있다. 도메인 A의 가드(230)는 도메인 A의 속성 인증서 발급자(220)를 통하여 데이터 접근 등급에 관한 정보를 얻을 수 있다. 도메인 A의 가드(230) 또는 속성 인증서 발급자(210)가 접근을 허용한 경우, 도메인 B의 호스트(320)는 도메인 A의 호스트(220)의 데이터에 접근할 수 있다.

[0097] 상기 속성 인증서 발급자(210), 상기 호스트(220), 상기 가드(230), 상기 데이터 보안 등급, 상기 도메인 신뢰 등급, 상기 사용자 권한 등급, 상기 속성 인증서에 대하여는 상기 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 상기 도메인의 데이터의 데이터 보안 등급 정규화 단계(S110) 및 상기 도메인의 데이터에 접근하는 경우 사용자 권한 등급에 따라 허용 여부를 결정하는 단계(S120)에 대하여 도 1 내지 도 6을 참조하여 설명한 바와 유사하게 이해될 수 있으므로 이하 설명을 생략한다.

[0098] 이상 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

[0099] 도 1은 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 이용되는 데이터 보안 등급 점수배정의 예를 설명하기 위한 예시도이다.

[0100] 도 2는 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법을 설명하기 위한 흐름도이다.

[0101] 도 3은 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 k-means 기법을 설명하기 위한 개념도이다.

[0102] 도 4는 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 데이터 접근 등급을 설명하기 위한 개념도이다.

[0103] 도 5는 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 방법에서 이용되는 속성 인증서를 설명하기 위한 개념도이다.

[0104] 도 6은 본 발명의 일 실시예에 따른 k-means 기법을 이용한 교차 도메인 상에서의 데이터 접근 방법을 설명하기 위한 흐름도이다.

[0105] 도 7은 본 발명의 일 실시예에 따른 교차 도메인 상에서의 데이터 접근 시스템의 구성을 나타내는 블록도이다.

[0106] * 도면의 주요부분에 대한 부호의 설명 *

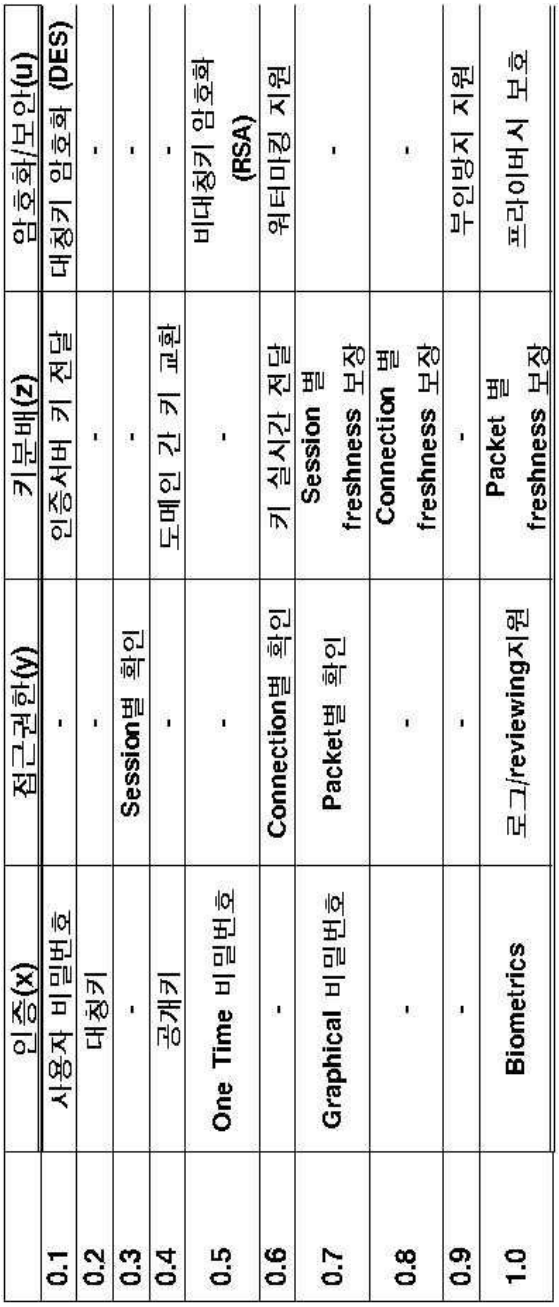
[0107] 210, 310 : 속성 인증서 발급자 220, 320 : 호스트

[0108] 230, 330 : 가드 240 : 에지 라우터

[0109] 250 : 인증기관

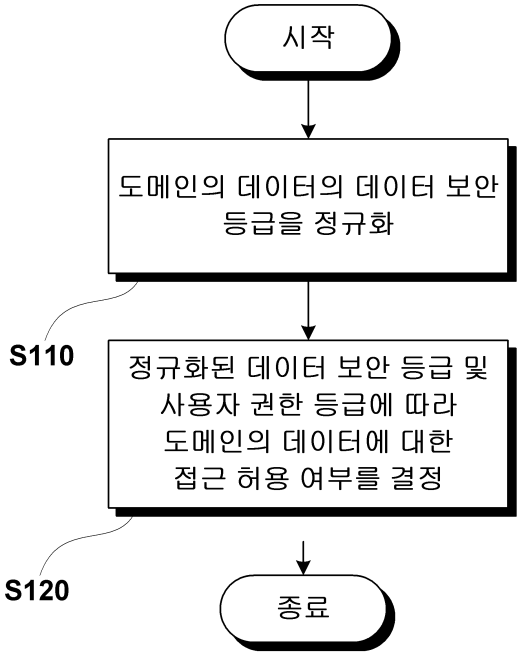
도면

도면1

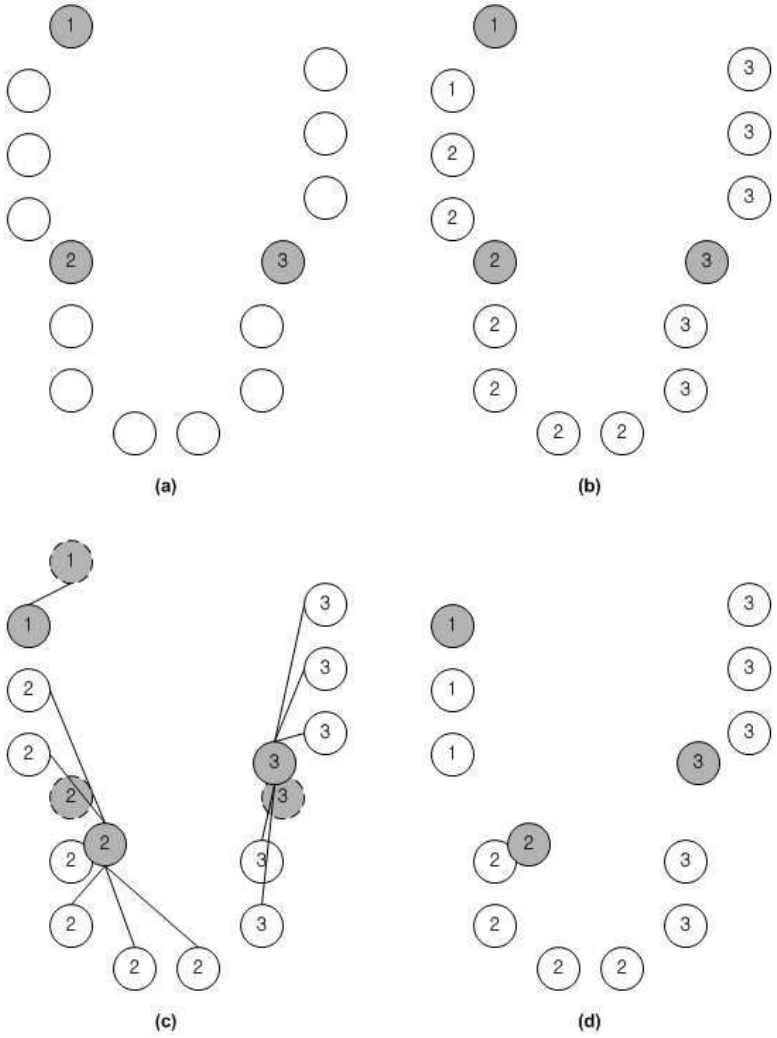


	인증(x)	접근권한(y)	키분배(z)	암호화/보안(u)
0.1	사용자 비밀번호	-	인증서버 키 전달	대칭키 암호화 (DES)
0.2	대칭키	-	-	-
0.3	-	Session별 확인	-	-
0.4	공개키	-	도메인 간 키 교환	-
0.5	One Time 비밀번호	-	-	비대칭키 암호화 (RSA)
0.6	-	Connection별 확인	키 실시간 전달	워터마킹 지원
0.7	Graphical 비밀번호	Packet별 확인	Session 별 freshness 보장	-
0.8	-	-	Connection 별 freshness 보장	-
0.9	-	-	-	부인방지 지원
1.0	Biometrics	로그/reviewing지원	Packet 별 freshness 보장	프라이버시 보호

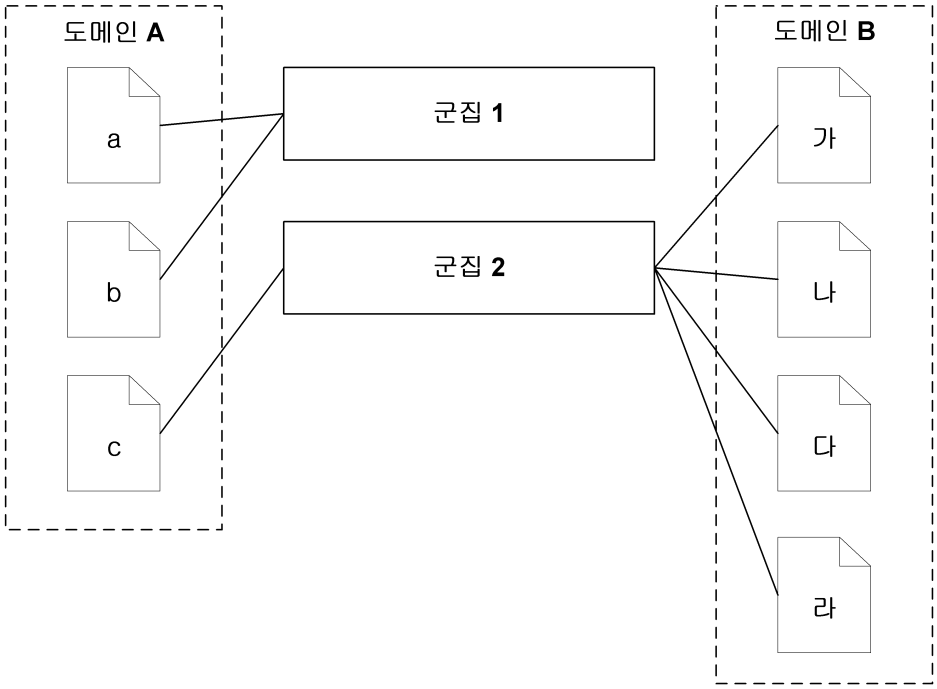
도면2


시작
도메인의 데이터의 데이터 보안 등급을 정규화
S110
정규화된 데이터 보안 등급 및 사용자 권한 등급에 따라 도메인의 데이터에 대한 접근 허용 여부를 결정
S120
종료

도면3



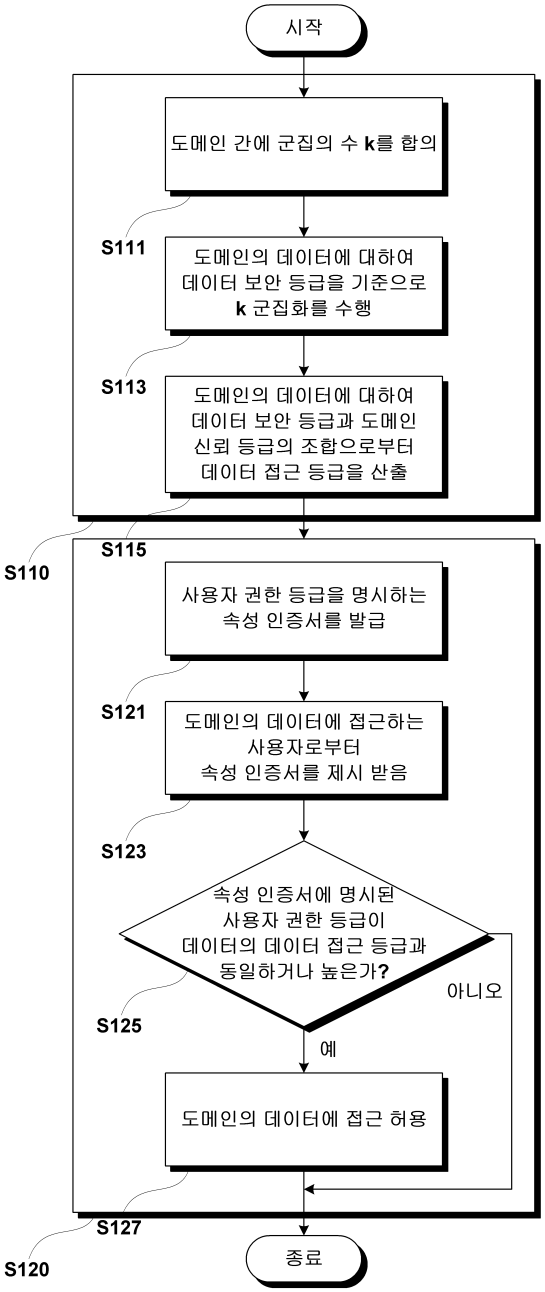
도면4



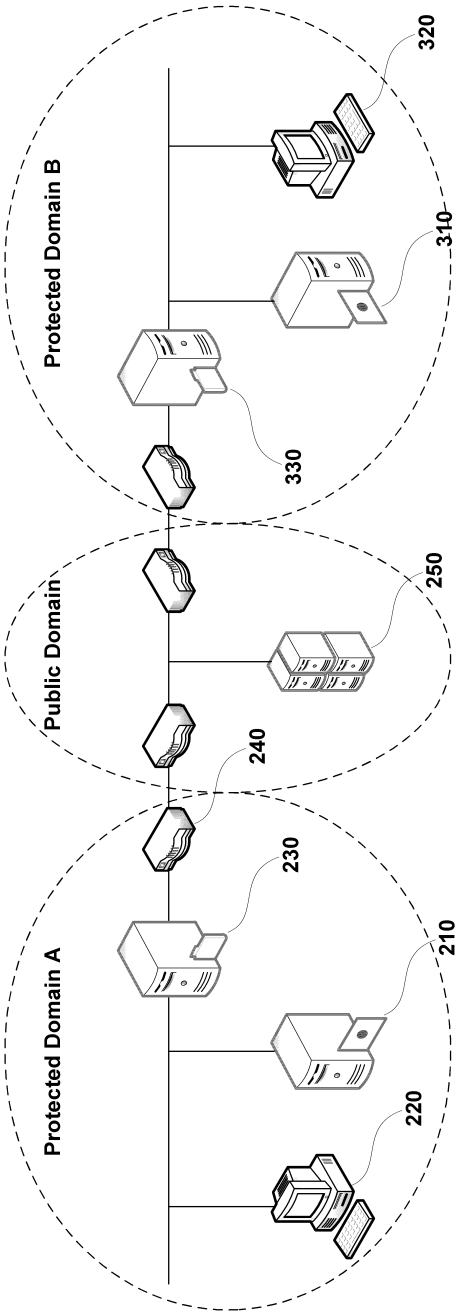
도면5

```
AttributeCertificate ::= {
        version;                    // 속성 인증서 버전
        holder;                     // 데이터에 접근하려고 하는 사용자 ID
        issuer;                     // 속성 인증서 발급자 ID
        cipher_integrity;           // 암호화 알고리즘 ID
        serialNumber;               // 인증서 일련번호
        attrCertValidityPeriod;     // 속성 인증서 유효기간
        attributes;                 // 사용자 권한 등급
}
```

도면6


시작
도메인 간에 군집의 수 k를 합의
S111
도메인의 데이터에 대하여 데이터 보안 등급을 기준으로 k 군집화를 수행
S113
도메인의 데이터에 대하여 데이터 보안 등급과 도메인 신뢰 등급의 조합으로부터 데이터 접근 등급을 산출
S110
S115
사용자 권한 등급을 명시하는 속성 인증서를 발급
S121
도메인의 데이터에 접근하는 사용자로부터 속성 인증서를 제시 받음
S123
속성 인증서에 명시된 사용자 권한 등급이 데이터의 데이터 접근 등급과 동일하거나 높은가?
아니오
S125
예
도메인의 데이터에 접근 허용
S127
S120
종료

도면7


Protected Domain B
Public Domain
Protected Domain A
320
310
330
250
240
230
210
220