(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0106809
(43) 공개일자 2022년07월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 63/205 (2013.01)
H04L 63/0435 (2013.01)
(21) 출원번호 10-2022-7021970
(22) 출원일자(국제) 2021년01월10일
심사청구일자 2022년06월30일
(85) 번역문제출일자 2022년06월27일
(86) 국제출원번호 PCT/IB2021/050141
(87) 국제공개번호 WO 2021/156686
국제공개일자 2021년08월12일
(30) 우선권주장
16/782,400 2020년02월05일 미국(US)

(71) 출원인
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
기블린, 크리스토퍼
스위스 취리히 8803, 뤼쉴리콘, 조이머스트라세 4, 아이비엠 리서치 지엠비에이치
(74) 대리인
허정훈

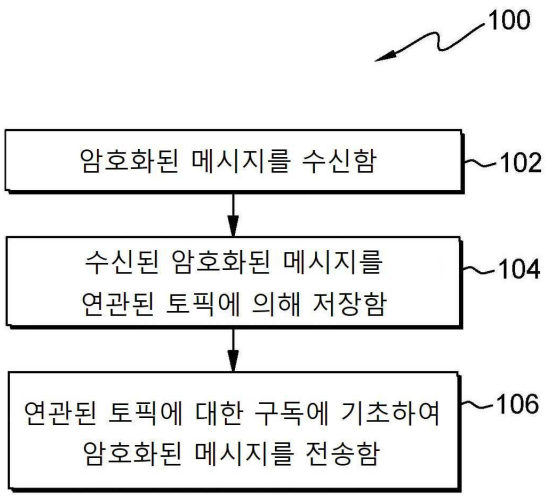
전체 청구항 수 : 총 23 항

(54) 발명의 명칭 **메시지 큐들에 대한 암호화**

(57) 요 약

게시-구독 메시지 큐에서의 타겟, 토픽-기반 암호화가 제공된다. 메시지들을 저장하고 수신하기 위해 암호화 정책들에 의해 구동되는 토픽-기반 암호화는 활동 추적 및 로깅하는 단계를 사용하여 저장된 암호화된 메시지들과 연관된 특정 토픽들의 기밀성을 보장한다. 게시자와 소비자 모두의 인증을 통해 암호화를 보장하고 암호 해독 키들은 기밀로 사용된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0442 (2013.01)
H04L 63/062 (2013.01)
H04L 63/0823 (2013.01)
H04L 63/105 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨터-구현 방법에 있어서, 상기 컴퓨터-구현 방법은:

제 1 메시지와 연관된 제 1 토픽이 토픽-기반 암호화 정책(a topic-based encryption policy)을 참조하여 제 1 암호화 레벨을 요구한다고 결정하는 단계;

제 1 암호화된 메시지를 생산하기 위해 상기 제 1 암호화 레벨에 따라 상기 제 1 메시지를 암호화하기 위해서 암호화 키를 제 1 주체(entity)에 제공하는 단계;

상기 제 1 암호화된 메시지를 상기 제 1 토픽에 따라 메시지 큐잉 시스템에 저장하는 단계;

상기 제 1 암호화된 메시지를 포함하는 상기 제 1 토픽과 연관된 메시지들에 대한 요청을 제 2의 주체로부터 수신하는 단계;

상기 제 1 토픽을 참조하여 상기 토픽-기반 암호화 정책에 따라 상기 암호화된 메시지에 대응하는 암호 해독 키를 식별하는 단계; 및

상기 암호 해독 키를 사용하여 소비자에 의한 암호 해독을 위해 상기 제 1 암호화된 메시지를 상기 제 2의 주체에 전송하는 단계를 포함하는

컴퓨터-구현 방법.

청구항 2

제 1항에 있어서, 상기 방법은:

상기 제 1 암호화된 메시지를 생산하기 위해서 상기 암호화 키를 상기 제 1 주체에 제공하는 단계 및 상기 제 1 암호화된 메시지에 대한 상기 암호 해독 키를 상기 제 2의 주체에 전송하는 단계를 로깅 시스템에 기록하는 단계를 더 포함하는

컴퓨터-구현 방법.

청구항 3

제 2항에 있어서, 상기 방법은:

상기 토픽-기반 암호화 정책에 대한 업데이트에 응답하여, 상기 업데이트를 상기 로깅 시스템에 기록하는 단계를 더 포함하는

컴퓨터-구현 방법.

청구항 4

제 1항에 있어서, 상기 방법은:

상기 제 1 토픽이 메시지 큐잉 시스템에서의 저장을 위해 암호화를 요구하는지를 결정하기 위한 요청을, 상기 제 1 주체로부터, 수신하는 단계를 더 포함하는

컴퓨터-구현 방법.

청구항 5

제 1항에 있어서, 상기 방법은:

상기 제 2의 주체에 대한 인증 자격 증명들을(authenticating credentials) 할당하는 것을 포함하는 상기 제 2의 주체를 위한 구독 계정(a subscription account)을 설정하는 단계; 및

상기 제 2의 엔터티가 상기 구독 계정을 통해 상기 제 1 토픽에 대해 구독할 때 상기 요청을 수신하는 단계를 더 포함하는

컴퓨터-구현 방법.

청구항 6

제 1항에 있어서, 상기 암호 해독 키는 상기 토픽-기반 암호화 정책에 의해서 제 1 토픽에 할당되는

컴퓨터-구현 방법.

청구항 7

컴퓨터 프로그램 제품에 있어서, 상기 컴퓨터 프로그램 제품은 그 안에 한 세트의 명령들을 갖는 컴퓨터-판독가능 스토리지 매체를 포함하고, 상기 명령들은, 프로세서에 의해서 실행될 때, 상기 프로세서가:

제 1 메시지와 연관된 제 1 토픽이 토픽-기반 암호화 정책(a topic-based encryption policy)을 참조하여 제 1 암호화 레벨을 요구한다고 결정하는 단계;

제 1 암호화된 메시지를 생산하기 위해 상기 제 1 암호화 레벨에 따라 상기 제 1 메시지를 암호화하기 위해서 암호화 키를 제 1 주체(entity)에 제공하는 단계;

상기 제 1 암호화된 메시지를 상기 제 1 토픽에 따라 메시지 큐잉 시스템에 저장하는 단계;

상기 제 1 암호화된 메시지를 포함하는 상기 제 1 토픽과 연관된 메시지들에 대한 요청을 제 2의 주체로부터 수신하는 단계;

상기 제 1 토픽을 참조하여 상기 토픽-기반 암호화 정책에 따라 상기 암호화된 메시지에 대응하는 암호 해독 키를 식별하는 단계; 및

상기 암호 해독 키를 사용하여 소비자에 의한 암호 해독을 위해 상기 제 1 암호화된 메시지를 상기 제 2의 주체에 전송하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 수행하도록 하는

컴퓨터 프로그램 제품.

청구항 8

제 7항에 있어서, 상기 프로세서가:

상기 제 1 암호화된 메시지를 생산하기 위해서 상기 암호화 키를 상기 제 1 주체에 제공하는 단계 및 상기 제 1 암호화된 메시지에 대한 상기 암호 해독 키를 상기 제 2의 주체에 전송하는 단계를 로깅 시스템에 기록하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 프로그램 제품.

청구항 9

제 8항에 있어서, 상기 프로세서가:

상기 토픽-기반 암호화 정책에 대한 업데이트에 응답하여, 상기 업데이트를 상기 로깅 시스템에 기록하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 프로그램 제품.

청구항 10

제 7항에 있어서, 상기 프로세서가:

상기 제 1 토픽이 메시지 큐잉 시스템에서의 저장을 위해 암호화를 요구하는지를 결정하기 위한 요청을, 상기 제 1 주체로부터, 수신하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 프로그램 제품.

청구항 11

제 7항에 있어서, 상기 프로세서가:

상기 제 2의 주체에 대한 인증 자격 증명들을(authenticating credentials) 할당하는 것을 포함하는 상기 제 2의 주체를 위한 구독 계정(a subscription account)을 설정하는 단계; 및

상기 제 2의 엔터티가 상기 구독 계정을 통해 상기 제 1 토픽에 대해 구독할 때 상기 요청을 수신하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 프로그램 제품.

청구항 12

제 7항에 있어서, 상기 암호 해독 키는 상기 토픽-기반 암호화 정책에 의해서 제 1 토픽에 할당되는

컴퓨터 프로그램 제품.

청구항 13

컴퓨터 시스템에 있어서, 상기 컴퓨터 시스템은:

프로세서 세트; 및

프로그램 명령들이 그 안에 저장되어 있는 컴퓨터 판독 가능한 스토리지 매체를 포함하고;

상기 프로세서 세트는 상기 프로그램 명령들을 실행하며, 상기 프로그램 명령들은 상기 프로세서 세트가:

제 1 메시지와 연관된 제 1 토픽이 토픽-기반 암호화 정책(a topic-based encryption policy)을 참조하여 제 1 암호화 레벨을 요구한다고 결정하는 단계;

제 1 암호화된 메시지를 생산하기 위해 상기 제 1 암호화 레벨에 따라 상기 제 1 메시지를 암호화하기 위해서 암호화 키를 제 1 주체(entity)에 제공하는 단계;

상기 제 1 암호화된 메시지를 상기 제 1 토픽에 따라 메시지 큐잉 시스템에 저장하는 단계;

상기 제 1 암호화된 메시지를 포함하는 상기 제 1 토픽과 연관된 메시지들에 대한 요청을 제 2의 주체로부터 수신하는 단계;

상기 제 1 토픽을 참조하여 상기 토픽-기반 암호화 정책에 따라 상기 암호화된 메시지에 대응하는 암호 해독 키를 식별하는 단계; 및

상기 암호 해독 키를 사용하여 소비자에 의한 암호 해독을 위해 상기 제 1 암호화된 메시지를 상기 제 2의 주체에 전송하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 수행하도록 하는

컴퓨터 시스템.

청구항 14

제 13항에 있어서, 상기 프로세서 세트가:

상기 제 1 암호화된 메시지를 생산하기 위해서 상기 암호화 키를 상기 제 1 주체에 제공하는 단계 및 상기 제 1 암호화된 메시지에 대한 상기 암호 해독 키를 상기 제 2의 주체에 전송하는 단계를 로깅 시스템에 기록하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 시스템.

청구항 15

제 14항에 있어서, 상기 프로세서가:

상기 토픽-기반 암호화 정책에 대한 업데이트에 응답하여, 상기 업데이트를 상기 로깅 시스템에 기록하는 단계

에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 시스템.

청구항 16

제 13항에 있어서, 상기 프로세서가:

상기 제 1 토픽이 메시지 큐잉 시스템에서의 저장을 위해 암호화를 요구하는지를 결정하기 위한 요청을, 상기 제 1 주체로부터, 수신하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 시스템.

청구항 17

제 13항에 있어서, 상기 프로세서가:

상기 제 2의 주체에 대한 인증 자격 증명들을(authenticating credentials) 할당하는 것을 포함하는 상기 제 2의 주체를 위한 구독 계정(a subscription account)을 설정하는 단계; 및

상기 제 2의 엔터티가 상기 구독 계정을 통해 상기 제 1 토픽에 대해 구독할 때 상기 요청을 수신하는 단계에 의해서 게시-구독(publish-subscribe) 메시징 큐에서의 토픽-기반 암호화를 더 수행하도록 하는

컴퓨터 시스템.

청구항 18

제 13항에 있어서, 상기 암호 해독 키는 상기 토픽-기반 암호화 정책에 의해서 제 1 토픽에 할당되는

컴퓨터 시스템.

청구항 19

컴퓨터-구현 방법에 있어서, 상기 컴퓨터-구현 방법은:

제 1 메시지와 연관된 제 1 토픽이 토픽-기반 암호화 정책(a topic-based encryption policy)을 참조하여 제 1 암호화 레벨을 요구한다고, 생산자에 의해서, 결정하는 단계;

암호화된 메시지를 생산하기 위해 상기 제 1 암호화 레벨에 따라 상기 제 1 메시지를, 상기 생산자에 의해서, 암호화하는 단계;

상기 암호화된 메시지를 상기 제 1 토픽에 따라 메시지 큐잉 시스템에 저장하는 단계;

상기 제 1 메시지를 포함하는 상기 제 1 토픽과 연관된 메시지들에 대한 구독을 소비자로부터 수신하는 단계;

상기 제 1 토픽을 참조하여 상기 토픽-기반 암호화 정책에 따라 상기 암호화된 메시지에 대응하는 암호 해독 키를, 상기 소비자에 의해서, 식별하는 단계; 및

상기 제1 메시지를 재생하기 위해 상기 암호 해독 키를 사용하여 상기 암호화된 메시지를, 상기 소비자에 의해서, 암호 해독하는 단계를 포함하는

컴퓨터-구현 방법.

청구항 20

제 19항에 있어서, 상기 방법은:

상기 생산자로부터 상기 제 1 토픽과 연관된 상기 제 1 메시지를 수신하는 단계를 더 포함하는

컴퓨터-구현 방법.

청구항 21

제 19항에 있어서, 상기 메시지 큐잉 시스템은 카프카(Kafka) 시스템인

컴퓨터-구현 방법.

청구항 22

제 19항에 있어서, 상기 암호 해독 키를 식별하는 단계는:

상기 제 1 토픽과 연관된 메시지들에 대한 상기 구독이 암호화된 메시지들을 포함하는지를 결정하기 위해 상기 토픽-기반 암호화 정책을 참조하는 단계를 포함하는

컴퓨터-구현 방법.

청구항 23

제 19항에 있어서,

상기 암호화된 메시지는 메시지 인증 코드(a message authentication code)를 포함하고; 그리고

메시지들에 대한 상기 구독은 상기 메시지 인증 코드가 상기 소비자에 의해서 제공될 때만 상기 암호화된 메시지를 포함하는

컴퓨터-구현 방법.

발명의 설명

기 술 분 야

[0001] [0001] 본 발명은 일반적으로 메시지 큐잉 시스템들에 관한 것이며 보다 구체적으로 메시지 큐잉 시스템에서 안전한 방식으로 메시지들을 처리하는 것(handling)에 관한 것이다.

배 경 기 술

[0002] [0002] 기업들 내, 기업들 간, 기업들에서 소비자들로, 뿐만 아니라 소비자들에서 소비자들로의 메시지 및 정보 교환을 관리하는 것은 정보 기술의 핵심 능력들(core competencies) 중 하나이다. 메시징 시스템들은 수십 년 동안 데이터를 메시지들로 저장, 전달 및 배포하기 위해 널리 사용되어 왔다. 최근에, 카프카(Kafka)와 같은 메시징 시스템들은 또한 데이터베이스의 한 형태로 간주되고 있다. 이 개발과 동시에, 이런 메시징 시스템들은 클라우드 컴퓨팅 시스템들에서 점점 더 실체화되고 있다(instantiated). (참고: "KAFKA"라는 상기 용어는 전 세계의 다양한 관할 구역들에서 상표권들(trademark rights)의 적용을 받을 수 있고 그러한 상표권들이 존재할 수 있는 범위 내에서 상기 상표에 의해 적절하게 표시된 제품들 또는 서비스들을 여기서 참조하기 위해서만 사용된다.)

발명의 내용

해결하려는 과제

[0003] [0003] 보안 키 관리(a secure key management) 및 데이터 전송 시스템은 전이 시스템(a transition system), 데이터 소비자 네트워크 디바이스, 사용자 네트워크 디바이스, 및 데이터 전송 네트워크를 포함하는 것으로 알려져 있다. 전송 관리 시스템은 데이터 전송 네트워크를 통해 사용자 네트워크 디바이스로부터 사용자 특정의(user-specific) 데이터를 수신하고 데이터 소비자 네트워크 디바이스에 의해서 제공되는 독점적 프로세스에 따라 사용자 특정의 데이터를 처리하는 것에 대응하는 서비스에 대한 요청을 수신하도록 구성된다.

[0004] [0004] 또한, 게시/구독(publish/subscribe) 메시징 시스템을 사용하기 위해 네트워크 구성 정책들을 전파하는 시스템에 대해서도 알려져 있다. 운영 중에, 시스템은, 게시/구독 메시징 시스템을 통해서, 정책 서버로부터 구성 정책의 제 1 표현을 포함하는 하나 또는 그 이상의 메시지들을 수신한다.

과제의 해결 수단

[0005] [0005] 본 발명의 일 실시 예에서, 방법, 컴퓨터 프로그램 제품 및 시스템은: (i) 제 1 메시지와 연관된 제 1 토픽이 토픽-기반 암호화 정책(a topic-based encryption policy)을 참조하여 제 1 암호화 레벨을 요구한다고 결정하는 단계; (ii) 제 1 암호화된 메시지를 생산하기 위해 상기 제 1 암호화 레벨에 따라 상기 제 1 메시지를

암호화하기 위해서 암호화 키를 제 1 주체(entity)에 제공하는 단계; (iii) 상기 제 1 암호화된 메시지를 상기 제 1 토픽에 따라 메시지 큐잉 시스템에 저장하는 단계; (iv) 상기 제 1 암호화된 메시지를 포함하는 상기 제 1 토픽과 연관된 메시지들에 대한 요청을 제 2의 주체로부터 수신하는 단계; (v) 상기 제 1 토픽을 참조하여 상기 토픽-기반 암호화 정책에 따라 상기 암호화된 메시지에 대응하는 암호 해독 키를 식별하는 단계; 및 (vi) 상기 암호 해독 키를 사용하여 소비자에 의한 암호 해독을 위해 상기 제 1 암호화된 메시지를 상기 제 2의 주체에 전송하는 단계를 포함한다.

[0006] [0006] 본 발명의 다른 실시 예에 따라, 게시/구독 메시지 큐잉 시스템(a publish/subscribe message queueing system)에서 타겟, 정책-기반 암호화(a targeted, policy-based encryption)를 위한 컴퓨터 구현 방법이 제공될 수 있다. 상기 방법은 메시지 큐잉 시스템에 의해서 암호화된 메시지를 수신하는 단계- 상기 메시지는 암호화 정책 시스템 및 토픽-관련 암호화 키를 저장하는 키 관리 시스템을 참조하여 암호화됨-, 수신된 토픽-관련 암호화된 메시지를 저장하는 단계, 및 상기 토픽에 대한 구독에 기초하여 상기 암호화된 메시지를 전송하는 단계를 포함할 수 있다.

[0007] [0007] 본 발명의 또 다른 실시 예에 따라, 게시-구독 메시지 큐에서 타겟, 정책-기반 암호화를 위한 시스템이 제공될 수 있다. 상기 시스템은 암호화된 메시지를 수신하도록 구성된 메시지 큐잉 시스템- 상기 메시지는 암호화 정책 시스템 및 토픽-관련 암호화 키를 저장하는 키 관리 시스템을 참조하여 암호화됨-, 수신된 토픽-관련 암호화된 메시지를 저장하는 수단, 및 상기 토픽에 대한 구독에 기초하여 상기 암호화된 메시지를 전송하는 수단을 포함할 수 있다.

[0008] [0008] 더 나아가, 실시 예들은 컴퓨터 또는 모든 명령 실행 시스템과 함께 사용하기 위해, 또는 연결하여 사용하기 위해 프로그램 코드를 제공하는 컴퓨터 사용 가능 또는 컴퓨터 판독 가능 매체로부터 액세스 가능한, 관련 컴퓨터 프로그램 제품의 형태를 취할 수 있다. 이 설명의 목적상, 컴퓨터 사용 가능 또는 컴퓨터 판독 가능한 매체는 명령 실행 시스템, 장치 또는 디바이스와 함께 사용하기 위해, 또는 연결하여 사용하기 위해 프로그램을 저장, 통신, 전파 또는 운반하는 수단을 포함할 수 있는 모든 장치일 수 있다.

도면의 간단한 설명

[0009] [0009] 본 발명의 실시 예들은 다양한 주제들(subject-matters)을 참조하여 기술된다는 점에 주의해야 한다. 특히, 일부 실시 예들이 방법 유형 청구항들을 참조하여 기술되는 반면, 다른 실시 예들은 장치 유형 청구항들을 참조하여 기술된다. 그러나, 이 기술 분야에서 통상의 지식을 가진 자들은 전술한 그리고 다음의 설명으로부터, 달리 언급하지 않은 한, 하나의 유형의 주제에 속하는 특징들의 모든 조합에 더하여, 또한 다양한 주제들과 관련된 특징들 사이의 모든 조합, 특히, 방법 유형 청구항들의 특징들, 및 장치 유형 청구항들의 특징들 사이의 모든 조합이, 상기 설명은 이 문서 내에서 개시될 것이 고려된다는 점을 이해할 것이다.

[0010] 위에서 정의된 실시 예들, 및 본 발명의 추가 실시 예들은, 이후 기술될 실시 예들의 예들로부터 명백하고, 실시 예들의 예들을 참조하여 설명되지만, 본 발명이 이에 한정되지 않는다.

[0011] 본 발명의 일부 실시 예들은 다음 도면들을 참조하여, 예시적인 방식으로만, 설명될 것이다.

[0012] 도 1은 게시-구독(publish-subscribe) 메시지 큐에서 타겟, 정책-기반(policy-based) 암호화를 위한 제 1-실시 예(first-embodiment) 방법의 플로차트이다.

[0013] 도 2는 도 1의 제 1-실시 예 방법을 지원하는 제 1-실시 예 시스템의 개략도(schematic view)이다.

[0014] 도 3은 도 2의 제 1-실시 예 시스템을 사용하여 제 1-실시 예 방법의 적어도 부분들을 구현하기 위한 동작들의 플로차트이다.

[0015] 도 4는 게시/구독 메시지 큐에서 타겟, 정책-기반 암호화를 위한 제 1-실시 예 시스템의 머신 로직(예를 들어, 소프트웨어) 부분의 개략도이다.

[0016] 도 5는 게시-구독 메시지 큐에서 타겟, 정책-기반 암호화를 위한 제 2-실시 예 방법의 플로차트이다.

[0017] 도 6은 본 발명에 따른 컴퓨팅 시스템의 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0010] [0018] 게시-구독 메시지 큐에서 타겟, 토픽-기반(topic-based) 암호화가 제공된다. 메시지들을 저장하고 수신하기 위해 암호화 정책들에 의해서 구동되는 토픽-기반 암호화는 활동 추적과 로깅을 사용하여 저장된 암호화된

메시지와 연관된 특정 토픽들의 기밀성을 보장한다. 게시자와 소비자 모두의 인증은 암호화 및 암호 해독 키들이 기밀로 사용되는 것을 보장한다.

[0011] [0019] 메시징 시스템들이 개인 정보나 금융 데이터와 같은, 매우 민감한 데이터를 이동할 때, 규제 요건들, 개인 정보 보호 정책들(privacy policies), 및/또는 모범 사례들(best practices) 때문에 메시징 서버에서의 데이터의 암호화가 종종 요구될 수 있다.

[0012] [0020] 일부 메시징 시스템들은 메시징 서버를 통해서 전달되어 있도록 의도되어 있는 모든 데이터를 저장한다. 이런 저런 이유들로, 이들 메시징 시스템들은 데이터베이스들과 유사하다. 이러한 유형의 메시징 시스템의 경우, 중요한 정보의 완전한 세트가 메시징 서버 상에서 존재하고 저장될 수 있기 때문에 암호화된 스토리지에 대한 필요성이 높아진다. 암호화되지 않은 경우, 전체의 중요한 데이터 세트가 허용되지 않은(non-allowed) 액세스에 노출될 수 있다.

[0013] [0021] 일부 메시징 시스템들은 메시징 서버 상에서 저장된 데이터의 원시 암호화(native encryption)를 지원할 수 있다. 그러나, 메시징 시스템들이 서버 상의 암호화된 스토리지를 지원한다 하더라도, 데이터의 오리지널 생산자가 반드시 암호화의 수단을 컨트롤할 필요가 없고 특히 암호화 키들을 컨트롤할 필요는 없다.

[0014] [0022] 종종, 저장 데이터 암호화(encryption-at-rest)는 메시징 서버 상의 디스크 또는 파일 시스템 암호화로 해결된다. 이런 접근법들은 디스크가 분실되거나 도난 되었을 때 노출을 방지할 수 있지만, 이런 접근법들은 일반적으로 사용자들이 메시징 서버 상의 모든 파일들에 대한 읽기 및 액세스 권한을 가지고 있을 때 암호 해독된 데이터에 대한 액세스를 방지하지는 못한다. 따라서, 파일 시스템은 그러한 사용자들은 읽기 권한을 소유하고 있기 때문에 그들을 위해 데이터를 암호 해독할 것이다. 이러한 소위 "시스템 관리자 공격(sysadmin attack)"을 방지하기 위해, 최선의 보안 방책(best security practice)은 중요한 데이터가 암호화되도록 의무화하는 것이며(mandate), 즉, 대응하는 암호 해독 키들에서 데이터베이스나 애플리케이션 레벨이 시스템 관리자들(system administrators)에게 액세스 가능하지 않게 의무화하는 것이다.

[0015] [0023] 이 설명의 맥락에서, 다음의 규약, 용어들 및/또는 표현들이 사용될 수 있다:

[0016] [0024] "정책-기반 암호화(policy-based encryption)"라는 용어는 규칙들의 저장소(a repository of rules)가, 예를 들어 암호화 정책 데이터베이스에서 이용 가능할 수 있다는 것을 의미할 수 있다. 메시지 큐에서 특정 토픽과 관련된 메시지들의 암호화를 위한 요건으로서, 암호화 정책 데이터베이스를 참조하고 플래그를 요청함으로써, 암호화 정책 데이터베이스는 요청자에게 선택된 토픽과 관련된 메시지들이 암호화되거나 암호화되어야 함을 알릴 수 있다. "메시지를 암호화하는 단계(encrypting a message)"는 메시지를 평문(plain text)으로 읽을 수 없게 만드는 프로세스를 의미한다 점에 또한 주목해야 한다. 암호화된 메시지는 암호 해독이 완료된 후에만 이해 가능할 수 있다.

[0017] [0025] "암호화"라는 용어는 폭 넓은 의미로 이해될 수 있다는 점에 또한 유의해야 한다. 다시 말해, 암호화는 메시지 무결성 및 부인 방지 속성들(non-repudiation properties)을 제공하는 디지털 서명들 및 MAC들과 같은 기타 암호화 연산들(operations)을 또한 포함한다.

[0018] [0026] "메시지 큐"(또는 메시징 큐)라는 용어는 프로세스 간(inter-process) 통신을 가능하게 하는 데이터 스토리지 조직(a data storage organization), 또는 동일한 프로세스 내에서 스레드 간(inter-thread) 통신을 위한 데이터 스토리지 조직을 의미할 수 있다. 메시지 큐는 메시지들, 예를 들어 정의된 시퀀스의 메시지들을 위한 큐를 사용할 수 있다. 이 방식은 비동기 통신 프로토콜이 설정될 수 있게 한다. 이는 메시지의 발신자와 수신자는 동시에(at the same time) 메시지 큐와 상호 작용할 필요가 없다는 점을 의미한다. 발신자에 의해서 큐 상으로 배치된 메시지들은 상기 큐 상에 저장되고 수신되며 및/또는 수신자는 저장된 메시지들을 찾아올(검색할) 수 있다. 다양한 회사들로부터 또는 오픈 소스 구현들로서 대규모의 다양한 상업적 메시지 큐잉 시스템들이 존재할 수 있다. 때때로 상기 메시지 큐잉 시스템은 또한 메시지 브로커를 의미할 수도 있다.

[0019] [0027] 따라서, 메시지 큐잉은 하나의 메시징 패턴을 가능하게 할 수 있으며, 이 메시징 패턴에서는, 여기서 게시자들 또는 메시지 생산자들이라 하는, 메시지들의 발신자들은 메시지를, 여기서 메시지 소비자라 하는, 특정 수신자 에게 직접 보내도록 프로그램 하지 않는다. 이 설명의 맥락에서, "생산자" 및 "소비자"라는 용어들은 컴퓨터를 운영하는 인간 사용자 또는 메시지 큐잉 시스템의 메시지들을 생산, 암호화, 구독, 수신, 및/또는 암호 해독하는 프로그램 명령들에 따라 운영하는 컴퓨터 프로그램을 의미할 수 있다. 대신, 게시된 메시지들은 모든 구독자에 대한 지식 없이, 다양한 클래스들 또는 토픽들 로 분류될 수 있다. 구독자들은 이들 메시지 클래스들 중 하나 또는 그 이상에 관심을 표시할 수 있고, 특정의 관심 토픽과 같은, 그들이 관심을 갖는 그러한 메시지

들만 수신할 수 있으며, 그러한 메시지들을 수신함에 있어서, 구독자들은 어떤 메시지 생산자가 그 메시지를 생성했는지는 알 필요가 없다.

[0020] [0028] "암호화된 메시지"라는 용어는 평문(clear text)으로는 존재하지 않지만 암호화 키에 의해서 인코드 된 데이터를 의미할 수 있다. 암호화에 대한 다양한 방법들이 알려져 있다. 본 발명의 제안된 개념은 상기 선택된 암호화 방법과는 무관하다. 암호화된 메시지는 암호 해독 후에만 평문으로 읽을 수 있다.

[0021] [0029] "암호화 정책 시스템(encryption policy system)"이라는 용어는 메시지들에 적용될, 예를 들어, 메시지 큐잉 시스템으로 주어진 토픽을 전송하기 위한 암호화 연산들 및 연관된 키 자료를 정의하는 정보의 정책 데이터베이스 또는 정보의 보관소를 의미할 수 있다. 구체적으로 무단 액세스에 대해서 보호되어야 할 각 토픽에 대해 다음 정보의 적어도 일부를 포함하는 기록이 존재할 수 있다: (i) 메시지 서버 주소(들); (ii) 토픽 이름; (iii) 토픽 식별자; (iv) 암호화 알고리즘(들); (v) 암호화/암호 해독 단계(들); (vi) 암호 스위트(cipher suite)(예: 각각의 애플리케이션 프로그래밍 인터페이스들); (vii) 키 관리 서비스; (viii) 서비스 주소; (ix) 키 식별자; 및/또는 (x) 암호화/암호 해독에 대한 선택적인 초기화 정보.

[0022] [0030] "키 관리 시스템"이라는 용어는 메시지들에 대한 대칭 암호화/암호 해독을 위한 -특히, 비대칭 암호화를 위한- 암호화 및 암호 해독 키들의 쌍들을 위한 스토리지 시스템을 의미할 수 있다. 키 관리 시스템은 암호화 정책 시스템의 선택된 규칙(메시지 발신자 측에서) 또는 선택된 토픽(메시지 소비자 측에서)에 기초하여 특정 암호화 키를 제공할 수 있다.

[0023] [0031] "구독(subscription)"이라는 용어는 명시된 클래스 또는 토픽의 메시지들에 대해 표시된 관심을 의미할 수 있다. 구독을 갖는 메시지 소비자는 토픽 또는 클래스별로 메시지 큐에서 저장된 메시지들을 수신할 수 있다.

[0024] [0032] "토픽(topic)"이라는 용어는 복수의 메시지들에 대한 테마 또는 헤드라인을 의미할 수 있다. 토픽들은 다양한 규칙들, 예를 들어, 동일하거나 유사한 컨텐츠와 관련된 규칙들, 특정 기간과 관련된 규칙들, 및/또는 저자와 관련된 규칙들에 따라 체계화될 수 있다(organized).

[0025] [0033] "카프카(Kafka)"(또는 카프카 시스템)라는 용어는, -특히 0.9.0 또는 그 이상의 버전에서- 아파치 소프트웨어 재단(Apache Software Foundation)가 소유하는 알려진 오픈-소스 스트림-처리 소프트웨어 플랫폼(open-source stream-processing software platform)을 의미할 수 있다. 카프카는 실시간(real-time)으로 데이터 피드들을 처리하기 위해서 통합된, 높은-처리량(high-throughput)의, 저지연(low-latency) 플랫폼을 제공하는 것을 목표로 한다. 카프카는 토픽들에서 수신된 메시지들을 체계화하여 관련된 데이터베이스에 그것들을 저장하는 메시지 큐잉 시스템으로서 또한 사용될 수 있다. 카프카 시스템 외에, 본 발명의 제안된 방법 및 관련된 시스템이 또한 다른 메시지 큐잉 시스템들로 구현될 수 있다. (참고: " KAFKA", " APACHE" 및 " APACHE SOFTWARE FOUNDATION"이라는 용어는 전 세계의 다양한 관할 구역들에서 상표권들의 적용을 받을 수 있으며 그러한 상표권들이 존재할 수 있는 범위 내에서 상기 상표들에 의해서 적절하게 표시된 제품들 또는 서비스들을 참조하기 위해서만 여기에서 사용된다.)

[0026] [0034] "메시지 생산자(message producer)"라는 용어는 메시지의 창작자(originator)(또는 창작자 운영 시스템)을 의미할 수 있다. 창작자는 또한 게시자(publisher)를 의미할 수도 있다.

[0027] [0035] "메시지 소비자(message consumer)"라는 용어는 메시지의 수신자를 의미할 수 있다. "(메시지) 생산자" 및 "(메시지) 소비자"라는 용어들은 카프카 시스템과 관련될 수 있다는 점에 유의한다.

[0028] [0036] 본 발명의 일부 실시 예들은 종래 기술의 현재 상태 관련하여 다음과 같은 사실들, 잠재적인 문제들 및/또는 개선되어야 할 잠재적인 영역들을 인식한다: (i) 네트워크 구성 정책들을 전파하는 종래의 시스템들은 메시지 브로커 시스템들에서 토픽-관련(topic-related) 메시지들의 종단간 암호화(an end-to-end encryption(E2EE): 데이터가 한 종단 시스템이나 디바이스에서 다른 종단 시스템이나 디바이스로 전송되는 동안 제3자가 데이터에 액세스하는 것을 방지하는 보안 통신 방법)를 허용하지 않는다. 그래서 시스템 관리자 공격들을 피할 수 있는 가능성이 여전히 없고, 따라서, 전통적인 메시지 큐잉 시스템들에서 이들 결함들, 특히 메시지 큐잉 시스템 내의 데이터를 보호해야 한다는 점에서 이들 결점들을 극복해야 할 필요가 있을 수 있다; (ii) 종단간 데이터 보호-생산자에서 소비자까지의 데이터 보호-는, 메시지 큐잉 서버 상의 데이터베이스들에서 저장된 메시지들이 암호화된 상태를 유지하고 데이터베이스에서 암호화된 형태로 저장된다는 점에서, 생산자로부터 메시지 큐잉 시스템으로 전송되는 메시지들을 해독하지 않고도 보장될 수 있다. 따라서 보안 정책에 따라 암호화를 요청하고 메시지 큐잉 시스템에 의해서 수신되는 메시지는 승인되지 않은 사람(또는 승인되지 않은

시스템들)에 의해 핵세스될 가능성은 없다; (iii) 메시지 큐잉 시스템, 암호화 정책 시스템, 및/또는 관련된 키 관리 시스템 및/또는 서비스를 조합하면 게시/구독 환경에서 토픽-관련 메시지들의 보안 측면들을 고유하게 컨트롤할 수 있다; (iv) 메시지 큐잉 서버의 관리자들은, 데이터베이스의 토픽들에 대한 읽기 권한으로부터 관리자를 제외할 수 있는, 암호화 정책 시스템에 따라 메시지 큐잉 시스템의 데이터베이스에서 명시된 토픽들의 암호화된 메시지들에 액세스하는 것으로부터 배제될 수 있다; (v) 컨트롤은 단순하게 메시지 생산자에게 위임되는 것이 아니고 암호화 정책 시스템에 의해서 컨트롤되며, 암호화 정책 시스템은 메시지 생산자들과 메시지 수신자들을 위한 규칙들을 다음과 같은 방식으로 독립적으로 정의할 수 있다. 즉 메시지 생산자는 키 관리 시스템 또는 암호화 정책 시스템과 관련된-그러나 반드시 동일할 필요는 없음- 서비스로부터 암호화 키를 단순히 요청할 수 있고 메시지는 그 다음에 메시지 큐잉 시스템을 통해 메시지를 전송하기 전에 메시지 생산자의 측에서 암호화될 수 있다(그 다음 예를 들어, 메시지의 암호 해독은 - 권한이 있을 경우- 소비자 측에서만 실시될 수 있으므로 메시지는 메시지 생산자부터 메시지 수신자까지 전송되는 내내 암호화된 상태로 남아있게 된다); (vi) 메시지는, 메시지 큐잉 시스템의 데이터베이스에서 암호화를 요구하는 토픽들과 어떠한 암호화도 요구할 수 없는 다른 토픽들이 있을 수 있는, 그러한 메시지 큐잉 시스템에 토픽-관련 메시지로서 저장될 수 있다; 및/또는 (vii) 메시지의 생산자 및/또는 암호화 데이터베이스 시스템 키 사용자는 암호화가 메시지 큐잉 시스템의 운영자에게 위임되지 않게 되도록 암호화/암호 해독 프로세스를 완전히 컨트롤 할 수 있다(예를 들어, 카프카와 같은-표준 메시지 큐잉 시스템이 사용될 수 있고-동시에-토픽들에서 메시지들의 암호화는 보장될 수 있다).

[0029] [0037] 다음에서, 도면들에 대한 상세 설명이 제공된다. 도면들에서 모든 명령들은 개략적이다. 먼저, 게시-구독 메시징 큐에서 타겟, 정책-기반 암호화를 위한 독창적인 컴퓨터-구현 방법(computer-implemented method)의 일 실시 예의 블록도가 주어진다. 그 뒤에, 추가적인 실시 예들뿐만 아니라, 게시-구독 메시징 큐에서 타겟, 정책-기반 암호화를 위한 시스템의 실시 예들이 기술될 것이다.

[0030] [0038] 도 1은 타겟, 특히 토픽 레벨 상의 타겟, 게시-구독 메시지 큐에서의 정책-기반 암호화를 위한, 제 1실시 예 방법의 플로차트(100)을 도시한다. 메시지 큐는 카프카 시스템 또는 현재 알려져 있거나 개발될 다른 메시징 시스템을 사용하여 구현될 수 있다. 상기 방법은 메시지 큐 시스템에 의해 암호화된 메시지를 수신하는 단계(102)를 포함한다. 이에 의해서, 메시지는 암호화되는데, 암호화 정책 시스템과 토픽-관련 암호화 키를 저장하는 키 관리 시스템을 참조함으로써 메시지 생산자 또는 관련 메시지 생산 시스템에 의해 구체적으로 암호화된다. 이와 달리, 정책 기반 암호화는 클래스 레벨 상에서 타겟 될 수 있다.

[0031] [0039] 방법(100)은 또한 수신된 토픽-관련 암호화된 메시지를 저장하는 단계(104), 및 메시지와 관련된 토픽에 대한 구독에 기초하여 암호화된 메시지를, 메시지 소비자의 요청에 따라 게시/구독 방식으로 구체적으로 전송하는 단계(106)를 포함한다. 이와 달라, 메시지 클래스의 노션(notion)이 메시지들의 체계를 세우는 것을 위한 그리고 구독들을 위한 기초들이 될 수 있다. 본 명세서에 있어서, 클래스라는 용어는 메시지들의 긴급성, 기밀 상태, 및 통찰력의 레벨과 같은, 토픽들로서 쉽게 이해되지 않을 수 있는 특성들을 포함한다.

[0032] [0040] 도 2는 도 1의 제 1-실시 예 방법을 지원하는 제 1-실시 예 시스템의 개략도(200)이다. 메시지 생산자(202)는 특정 토픽에 관한 메시지가 암호화되어야 하는지를 결정하기 위해서 암호화 정책 시스템(210)의 암호화 정책을 참조한다. 생산자(202)는, 키 관리 시스템이 액세스 컨트롤 모듈(213)을 통해 액세스 권한을 부여하는 키 관리 시스템(212)으로부터, 병렬로 또는 요청에 의해서, 메시지를 위한 암호화 키를 수신한다. 이 예에서, 메시지 생산자는 키 관리 API(애플리케이션 프로그래밍 인터페이스)(214)를 사용하여 키 관리 시스템과 상호 작용할 수 있다. 키 관리 시스템과 암호화 정책 시스템은 액세스 컨트롤 모듈들(211 및 213)을 통해 로깅 시스템(216)에 키 액세스 트랜잭션들 및 정책 변화들을 기록한다. 기록하는 내용에는 수신된 요청들, 수락, 거부, 대응 타임 스탬프들, 권한 레벨들(authorization levels), 검색된 토픽들, 및/또는 제공된 키들이 포함될 수 있다. 키 관리 시스템은 또한 생산자들 및 소비자들을 위한 특정 토픽들에 대해 액세스 컨트롤을 관리할 수 있다. 메시지(도시되지 않음)는 그 다음에, 메시지 생산자(204)의 암호화 인터페이스(203)에 의해서 암호화되어, 특정한 암호화된 형태로 메시지 브로커(204)에 전송되어, 파일 시스템(206)에 명시된 토픽 또는 클래스로서 암호화된 형태로 저장된다. 본 발명의 일부 실시 예들에서, 파일 시스템(206)은 카프카 클러스터의 형태이다. 본 발명의 일부 실시 예들에서, 암호화 및 암호 해독은 브로커 레벨, 예를 들어, 브로커(204) 내에서 수행되므로, 키 액세스는 상기 브로커에서 통합된다. 게시/구독 모드에서, 브로커(204)는, 소비자(208)가 구독하는, 토픽과 관련된 암호화된 메시지를, 소비자에게 전송한다. 메시지를 수신하는 것에 응답하여, 소비자(208)는 구독 된 토픽과 관련된 메시지가 암호화되었는지를 결정하기 위해 암호화 정책 시스템(210)으로 체크한다. 만일 암호화되었다면, 소비자는 요청에 의해서 앞서 언급한(above-mentioned) 암호화 키와 관련된 암호 해독 키를 수신하며, 여기에서 상기 요청은 구독된 토픽을 키 관리 시스템(212)에 대한 입력 파라미터로서 사용하여 이루어진다. 암

호화/암호 해독은 대칭(암호화 및 암호 해독 키가 동일하다)이거나 비대칭(예를 들어, 퍼블릭 키 하부구조와 유사하게, 암호화 및 암호 해독 키가 서로 다르다)일 수 있다. 암호화/암호 해독 메커니즘은 AES-256 고급 보안 표준을 준수하거나 또는 상기 키(들)는 모든 적절한 암호화 표준과 호환될 수 있다. 본 발명의 일부 실시 예들에서, 상기 브로커는 메시지 큐잉 시스템일 수 있다. 본 발명의 일부 실시 예들에서, 상기 키 관리 시스템은 키 관리 서비스로 운영될 수 있다.

[0033] [0041] 암호 해독 키를 수신하면, 메시지 소비자는 수신된 메시지(도시되지 않음)를 해독하는데, 메시지 소비자(208)의 암호 해독 인터페이스(209)와 수신된 암호 해독 키(도시되지 않음)를 사용하여 해독한다.

[0034] [0042] 도 3은 도 2의 제 1-실시 예 시스템을 사용하여 제 1-실시 예 방법의 적어도 일부분들을 구현하기 위한 동작들을 포함하는 프로세스의 플로차트(300)이다. 초기 단계(302)에서, 메시지 생산자 또는, 간단하게, 생산자는 브로커(204)를 통해 구독 된 토픽에 할당된 메시지를 파일 시스템(206)으로 전송할 준비를 한다. 전송에 앞서, 단계(304)에서, 생산자는 구독된 토픽을 입력 변수로 사용하여 암호화 정책 시스템(210)을 체크한다. 이 예에서, 구독된 토픽은 암호화 정책 시스템 또는 데이터베이스에 따라 암호화를 요구한다. 그 다음에 생산자는 키 관리 시스템(212)으로부터 암호화 정책에서 참조된 암호화 키를 요청한다. 키 관리 서비스에서 액세스 컨트롤 정책이 생산자를 위해 키에 대한 액세스를 허용한다고 가정하면-즉, 생산자가 명시된 토픽에 대한 메시지를 파일 시스템으로 전송하는 것이 허용된다면-상기 키는 생산자에 대한 요청 응답으로 키 관리 서비스에 의해서 반환된다.

[0035] [0043] 동시에, 생산자에 의한 키 요청은 로깅 시스템(216)의 감사 추적에 로그인 된다.

[0036] [0044] 다음에, 단계(306)에서, 생산자는 키 관리 시스템으로부터 검색된 키를 사용하여 발신 메시지 몸체(outgoing message body)를 암호화하고 암호화된 메시지는 브로커(204)를 통해 명시된 토픽 하에서 파일 시스템(206)으로 전송된다. 단계(308)에서, 브로커는 메시지를 수신하고 수신된 메시지는 암호화된 형태로 파일 시스템의 타겟 토픽에 저장한다.

[0037] [0045] 그 다음, 단계(310)에서, 브로커는 명시된 토픽의 메시지들에 관한 요청을 소비자로부터 수신한다. 소비자 요청은 로깅 시스템(216)과 같은 메시지 로깅 시스템에 저장된다. 상기 로깅 시스템은, 단일 시스템으로서 정책과 액세스가 동일 시스템 내에서 추적되도록, 액세스 컨트롤 모듈(213)에 의해서 키 관리 시스템(212)과 연관되고 액세스 컨트롤 모듈(211)에 의해서 암호화 정책 시스템(210)과 연관된다. 이와 달리, 별도의 로깅 시스템들이 두 개의 시스템들과 연관될 수 있다. 브로커는 단계(312)에서 생산자로부터 수신된 메시지를 전송함으로써 상기 요청에 응답한다. 단계(314)에서, 소비자는 명시된 토픽에 할당된 메시지를 암호화된 형태로 수신한다.

[0038] [0046] 그 다음, 단계(316)에서, 소비자는 암호화 정책 데이터베이스 시스템을 체크하여 토픽과 관련된 메시지가 암호화되었는지를 결정하고, 만일 암호화되었다면, 메시지를 암호 해독하는 데 필요한 키를 키 관리 시스템으로부터 요청한다. 단계(318)에서, 소비자가 키 관리 시스템으로부터 암호 해독 키를 수신한 후, 소비자 시스템은 수신된 메시지를 암호 해독한다. 먼저, 관리 시스템 또는 암호화 정책 시스템에서, 소비자가, 액세스 컨트롤 정책에 따라, 소비자가 암호 해독 키를 수신할 수 있음이 검증된다. 요청하는 소비자들은 각각의 감사 서비스, 동작 추적기(activity tracker), 로깅 시스템, 및/또는 주문된 추적(ordered trail)으로부터 금지된다는 점에 주의해야 한다. 마지막으로, 소비자는 키 관리 시스템으로부터 수신한 키를 사용하여 메시지를 암호 해독한다.

[0039] [0047] 본 발명을 완전하게 설명하기 위해, 도 4는 게시/구독 메시지 큐에서 타겟, 정책-기반 암호화를 위한 제 1-실시 예 시스템의 머신 로직(예를 들어, 소프트웨어) 부분의 개략도(400)를 도시한다. 상기 머신 로직 부분은 암호화된 메시지를 수신하도록 구성된 메시지 큐잉 시스템(402)을 포함하며, 여기서 메시지는 암호화 정책 시스템(404)과 토픽-관련 암호화 키를 저장하는 키 관리 시스템(406)을 참조하여 암호화된다. 또한, 메시지는, 암호화 시스템(410)과 같은, 생산자의 암호화 시스템에 의해서 암호화될 수도 있다.

[0040] [0048] 상기 머신 로직 부분은 또한 수신된 토픽-관련 암호화된 메시지(the received topic-related encrypted message)를 데이터베이스(408)에서 저장하기 위한 수단을 포함할 수 있다. 즉, 메시지들 중 하나의 그룹은 하나의 토픽 하에 또는 하나의 토픽과 관련되어 저장될 수 있고, 다른 그룹은 다른 토픽에 또는 다른 토픽과 관련되어 저장될 수 있다. 데이터베이스(408)는 메시지 큐잉 시스템(402)에 링크되거나 또는 메시지 큐잉 시스템(402)의 물리적 부분일 수 있다.

[0041] [0049] 마지막으로, 상기 머신 로직 부분은 메시지의 할당된 토픽에 대한 구독에 기초하여 암호화된 메시지를 소비자에게 전송하기 위한 수단을 포함한다. 상기 전송은 암호 해독 시스템(412)과 같은 암호 해독 시스템이 설

치된 메시지 수신자(도시되지 않음)로 향해질 수 있다.

[0042] [0050] 본 발명의 일부 실시 예들은 다음의 특징들, 특성들 및/또는 이점들 중 하나를, 또는 그 이상을, 포함할 수 있다: (i) 본 발명의 다양한 실시 예들을 실시할 때 메시지 큐잉 시스템은 카프카 시스템이 될 수 있고, 특히 버전 0.9.0의 또는 보다 높은 버전의 카프카 시스템이 될 수 있으며 모든 다른 메시지 큐잉 시스템도 배치될 수 있다; (ii) 본 발명의 방법들은 기본 메시지 큐잉 시스템(the underlying message queuing system)에 대해 애그노스틱(agnostic) 할 수 있다; (iii) 상기 방법은 또한, 메시지 생산자가 메시지 큐잉 시스템에 특정 토픽과 관련된 메시지를 전송하기 전에 그 것이 암호화되어야 하는지를 결정할 수 있도록, 메시지 생산자가 토픽-관련 메시지를 전송하기 전에 암호화 정책 시스템을, 참조하는 단계를 포함할 수 있다; (iv) 상기 방법은, 메시지 생산자에 의해서, 암호화 정책 데이터베이스가 토픽-관련 메시지의 암호화-즉, 선택된 토픽에 기초한 메시지의 암호화를 시행하는 규칙을 포함한다고 결정하는 것에 기초하여, 만일 메시지 생산자가 암호화 키를 수신하도록 허용되었고 암호화 키가 키 관리 시스템으로부터 메시지 생산자에 의해 요청될 수 있었다면(예를 들어, 보안 액세스 방법을 사용하여) 키 관리 시스템으로부터 암호화 키를 수신하는 단계를 포함할 수 있다; (v) 키 관리 시스템과 암호화 정책 시스템은 동일 보안 시스템에서 구현될 수 있다(예를 들어, 키 관리 시스템은 암호화 정책 시스템의 서비스일 수 있다 보안 규칙들 및 암호화와 암호 해독을 위한 관련된 키의 중앙 컨트롤, 특히 메시지 큐잉 시스템 운영자의 컨트롤 밖에 있는 중앙 컨트롤이 제공될 수 있다.); 및/또는 (vi) 키 관리 시스템과 암호화 정책 시스템은 다양한 위치들에서 액세스될 수 있다(예를 들어, 암호화 데이터베이스 시스템과 키 관리 시스템은, 보안 아키텍처가 제공된 보안 레벨을 더욱 높일 수 있도록, 서로 독립적으로 구현될 수 있다)(암호화 데이터베이스 시스템과 키 관리 시스템에 액세스를 하기 위해서 서로 다른 인증 방법들이 사용되어야 할 수 있다는 점에 유의해야 할 수 있다).

[0043] [0051] 본 발명의 일부 실시 예들은 다음과 같은 특징들, 특성들 및/또는 장점들 중 하나를, 또는 그 이상을, 포함할 수 있다: (i) 암호화 정책 시스템을 참조하는 전송된 메시지, 특히 메시지 큐잉 시스템으로부터 전송된 메시지를, 메시지 소비자에 의해서, 수신하는 것에 기초하여 수신된 메시지가 암호화되었는지를 결정하는 동작을 포함할 수 있고, 이 동작에서 메시지 소비자는 메시지 큐잉 시스템으로부터 암호화된 메시지와 암호화되지 않은 메시지를 구별할 수 있고 메시지 수신자는 그들을 다르게 취급하지 못할 수 있다; (ii) 수신된 메시지가 암호화되었다고 결정하는 것에 기초하여 암호 해독 키를, 특히 키 관리 시스템으로부터, 특히 메시지 소비자에 의한 관련 요청 후에, 수신하는 동작을 포함할 수 있고, 이 동작에서 암호 해독 키는 메시지가 암호화된 암호화 키와 관련되어야 하며, 암호 해독 키들은 토픽별로 저장될 수 있기 때문에, 메시지 수신자는 토픽을 참조로써 암호 해독 키를 요청할 수 있고, 그 다음 메시지 수신자는 수신된 암호 해독 키를 사용하여 수신된 메시지를 해독할 수 있다; (iii) 암호화/암호 해독 키(들)는 대칭 암호화 또는 비대칭 암호화에 사용될 수 있다; (iv) 암호화 정책 시스템에 대한 액세스들을 로깅하는 동작을 포함할 수 있다; (v) 키 관리 시스템에 대한 액세스들을 로깅하는 동작을 포함할 수 있고, 이에 의해서, 보안 감사 추적은 키 관리 시스템뿐만 아니라, 암호화 정책 시스템에 대해서도 설정될 수 있으며, 그 결과 모든 액세스들, 키 검색들, 및 변화들이 항 시 추적 가능할 수 있고, 이에는 승인되지 않은 사용자들 또는 시스템들의 액세스 시도들을 포함한다; (vi) 모든 액세스들, 키 검색들, 및 변화들은 메시지 소비자에게 전송된 메시지가 암호 해독되었는지(예를 들어 특정의, 식별가능한 사용자에 의해서 읽을 수 있게 되었는지)에 관계없이 추적될 수 있다; (vii) 수신된 암호화된 메시지는, 메시지 큐잉 시스템에 의해서, 디지털 방식으로 서명될 수 있다; 및/또는 (viii) 메시지 큐잉 시스템에 의해서 수신된 암호화된 메시지는 메시지 인증 코드, 특히 HMAC(keyed-Hash Message Authentication Code)를 포함하는데, 이는 암호화된 메시지의 서명자의 무결성뿐만 아니라, 메시지의 무결성을 보장하기 위해서이다(예를 들어, 메시지 생산자에서 메시지 소비자로 전송되는도중에 어떤 비트도 변화되지 않았음이 증명될 수 있다).

[0044] [0052] 도 5는 본 발명에 따라 제 2의 방법을 도시하는 플로차트(600)를 도시한다.

[0045] [0053] 처리는 단계(S602)에서 시작되며, 여기에서 키 관리 시스템은 제 1 암호화 레벨을 결정한다. 상기 암호화 레벨은 암호화의 유형 및/또는 정도를 의미한다. 암호화 레벨들은 암호화 정책에 따라 토픽-기반 목록 상에 제공된다. 메시지들은 메시지의 연관된 토픽에 따라 암호화된다.

[0046] [0054] 처리는 단계(S604)로 진행되며, 여기에서 키 관리 시스템은 암호화 키를 카프카와 같은 메시지 큐잉 시스템의 파일 시스템에서 메시지를 저장하고자 하는 사용자에게 제공한다. 본 발명의 일부 실시 예들에서, 키 액세스는 키가 제공되기 전에 사용자가 인증되어야 하도록 컨트롤된다.

[0047] [0055] 처리는 단계(S606)로 진행되며, 여기에서 키 관리 시스템은 암호화된 메시지를 저장한다. 사용자는 주어진 토픽과 연관된 메시지를 암호화하고 암호화된 메시지를 브로커에게 제공하여 암호화된 메시지가 메시지 큐잉

시스템의 파일 시스템에 저장되게 한다.

[0048] [0056] 처리는 단계(S608)로 진행되며, 여기에서 키 관리 시스템은 암호화된 메시지에 대한 요청을 수신한다. 소비자들은 메시지 큐잉 시스템을 구독하고 관심있는 특정 토픽들을 선택할 수 있다. 구독된 토픽과 연관된 메시지가 저장될 때, 소비자는 상기 메시지를 요청할 수 있다. 본 발명의 일부 실시 예들에서, 소비자는 특정한 토픽 상에 관한 메시지의 통지를 수신하고 상기 통지 후에 요청을 제출한다. 이와 달리, 요청은 특정한 토픽을 구독하는 각 소비자를 위해 자동으로 생성될 수 있다.

[0049] [0057] 처리는 단계(S610)으로 진행되며, 여기에서 키 관리 시스템은 암호화된 메시지에 대응하는 암호 해독 키를 식별한다. 암호 해독 키들은 토픽에 따라 저장되므로, 특정한 토픽 상에 주어진 메시지에 대해서, 암호 해독 키는 암호화 정책 시스템을 통해 식별될 수 있다.

[0050] [0058] 처리는 단계(S612)에서 종료되며, 여기에서 키 관리 시스템은 소비자에게 암호화된 메시지와 그에 대응하는 암호 해독 키를 전송한다. 본 발명의 일부 실시 예들에서, 암호화된 메시지는 소비자에게 전송되고, 암호 해독 키가 필요하다고 결정하는 것에 기초하여, 암호 해독 키가 소비자에게 전송된다. 이와 달리, 소비자가 암호화된 메시지를 수신하고 메시지를 암호 해독하기 위해 암호 해독 키를 요청할 수 있다.

[0051] [0059] 본 발명의 실시 예들은 프로그램 코드를 저장 및/또는 실행하기에 적합한 플랫폼에 관계없이 사실상 모든 유형의 컴퓨터와 함께 구현될 수 있다. 도 6은, 일례로서, 제안된 방법과 관련된 프로그램 코드를 실행하기에 적합한 컴퓨팅 시스템(500)을 보여준다.

[0052] [0060] 컴퓨팅 시스템(500)은 적절한 컴퓨터 시스템의 하나의 예일뿐이며, 컴퓨터 시스템(500)이 구현될 수 있는지 및/또는 전술한 기능들 중 하나를 수행할 수 있는지 여부에 관계없이, 본 명세서에 설명된 본 발명의 실시 예들의 사용 범위 또는 기능에 관하여 어떠한 제한도 제안하려는 의도가 없다. 컴퓨터 시스템(500)에는, 수많은 다른 범용 또는 특수 목적 컴퓨팅 시스템 환경들 또는 구성들과 함께 작동하는, 컴포넌트들이 있다. 컴퓨터 시스템/서버(500)과 함께 사용하기에 적합할 수 있는 잘 알려진 컴퓨팅 시스템들, 환경들 및/또는 구성들의 예들은, 개인용 컴퓨터 시스템들, 서버 컴퓨터 시스템들, 씬 클라이언트들, 씩 클라이언트들, 핸드-헬드 또는 노트북 디바이스들, 멀티프로세서 시스템들, 마이크로프로세서 기반 시스템들, 셋톱 박스들, 프로그래밍 가능한 소비자 전자 제품들, 네트워크 PC들, 미니 컴퓨터 시스템들, 메인프레임 컴퓨터 시스템들 및 위의 시스템들 또는 디바이스들, 등을 포함하는 분산 클라우드 컴퓨팅 환경들, 등을 포함하나, 이들에 국한되지 않는다. 컴퓨터 시스템/서버(500)은, 컴퓨터 시스템(500)에 의해 실행되는, 프로그램 모듈들과 같은, 컴퓨터 시스템 실행 명령들의 일반적인 맥락에서 설명될 수 있다. 일반적으로, 프로그램 모듈들은 특정 작업들을 수행하거나 또는 특정 추상 데이터 유형들을 구현하는 루틴들, 프로그램들, 객체들, 컴포넌트들, 로직, 데이터 구조들, 등을 포함할 수 있다. 컴퓨터 시스템/서버(500)은 통신망을 통해 링크되는 원격 처리 디바이스들에 의해 작업들이 수행되는 분산형 클라우드 컴퓨팅 환경들에서 실시될 수 있다. 분산 클라우드 컴퓨팅 환경에서, 프로그램 모듈들은, 메모리 스토리지 디바이스들을 포함하는, 로컬 및 원격 컴퓨터 시스템 스토리지 매체 모두에 위치할 수 있다.

[0053] [0061] 도면에 도시된 바와 같이, 컴퓨터 시스템/서버(500)은 범용 컴퓨팅 디바이스의 형태로 도시된다. 컴퓨터 시스템/서버(500)의 컴포넌트들은, 하나 또는 그 이상의 프로세서들 또는 처리 유닛들(502), 시스템 메모리(504) 및 시스템 메모리(504)를 포함한 다양한 시스템 컴포넌트들을 프로세서(502)에 결합하는 버스(506)를 포함할 수 있으나 이에 한정되지 않는다. 버스(506)는, 메모리 버스 또는 메모리 컨트롤러, 주변장치 버스, 가속 그래픽 포트, 다양한 버스 아키텍처들 중 어느 하나를 사용하는 프로세서 또는 로컬 버스를 포함하는, 여러 유형들의 버스 구조들 중 하나 또는 그 이상을 나타내는 통신 패브릭이다. 예를 들어, 그러한 아키텍처들은 ISA(산업 표준 아키텍처) 버스, MCA(마이크로 채널 아키텍처) 버스, EISA(향상된 ISA) 버스, VESA(비디오 전자 표준 협회) 로컬 버스, 및 PCI(주변 컴포넌트 상호 연결) 버스를 포함하나, 이에 한정되지 않는다. 컴퓨터 시스템/서버(500)은 일반적으로 다양한 컴퓨터 시스템 판독 가능 매체를 포함한다. 그러한 매체는 컴퓨터 시스템/서버(500)에서 액세스할 수 있는 모든 사용 가능한 매체일 수 있으며 휘발성 및 비휘발성 매체, 착탈식 및 비-착탈식 매체를 모두 포함한다.

[0054] [0062] 시스템 메모리(504)은, 예컨대 랜덤 액세스 메모리(RAM)(508) 및/또는 캐시 메모리(510)와 같은, 휘발성 메모리의 형태의 컴퓨터 시스템 판독 가능한 매체를 포함할 수 있다. 컴퓨터 시스템/서버(500)는 또한, 다른 착탈식/비-착탈식, 휘발성/비휘발성 컴퓨터 시스템 스토리지 매체를 포함할 수 있다. 예를 들어, 스토리지 시스템(512)는 비-착탈식, 비휘발성 자기 매체(도시되지 않음 일반적으로 "하드 드라이브"라고 불림)를 읽고 쓰기 위해 제공될 수 있다. 비록 도시되지는 않았지만, 착탈식 비휘발성 자기 디스크에서 읽고 쓰기 위한 자기 디스크 드라이브(예: 플로피 디스크)와 CD-ROM, DVD-ROM 또는 기타 광학 미디어와 같은 착탈식 비휘발성 광 디스크에서

읽거나 쓰기 위한 광 디스크 드라이브가 제공될 수 있다. 그러한 경우들에서, 각각은 하나 또는 그 이상의 데이터 매체 인터페이스들에 의해 버스(506)에 연결될 수 있다. 이러한 경우, 각각은 하나 또는 그 이상의 데이터 미디어 인터페이스에 의해 버스(506)에 연결될 수 있다. 아래에서 더 도시되고 설명될 수 있 바와 같이, 메모리(504)는 본 발명의 실시 예들의 기능들을 수행하도록 구성된 프로그램 모듈들의 세트(예를 들어, 적어도 하나)를 갖는 적어도 하나의 프로그램 제품을을 포함할 수 있다.

[0055] [0063] 프로그램 모듈(516)의 세트(적어도 하나)를 갖는 프로그램/유틸리티는, 예를 들어, 메모리(504)에 저장될 수 있으며, 이들은 운영 체제뿐만 아니라 하나 또는 그 이상의 애플리케이션 프로그램들, 다른 프로그램 모듈들 및 프로그램 데이터를 포함하나, 이들에 제한되지는 않는다. 각각의 운영 체제들, 하나 또는 그 이상의 애플리케이션 프로그램들, 다른 프로그램 모듈들, 프로그램 데이터 또는 이들의 조합들은 네트워킹 환경의 구현을 포함할 수 있다. 프로그램 모듈(516)은 일반적으로 본 명세서에 설명된 바와 같이 본 발명의 실시 예들의 기능 및/또는 방법을 수행한다.

[0056] [0064] 컴퓨터 시스템/서버(500)는 키보드, 포인팅 디바이스, 디스플레이(520) 등과 같은, 하나 또는 그 이상의 외부 디바이스들(518); 사용자가 컴퓨터 시스템/서버(500)와 상호작용할 수 있게 하는 하나 또는 그 이상의 디바이스들; 및/또는 컴퓨터 시스템/서버(500)가 하나 또는 그 이상의 다른 컴퓨팅 디바이스들과 통신할 수 있게 하는 모든 디바이스들(예를 들어, 네트워크 카드, 모뎀 등)과 통신 할 수 있다. 그러한 통신은 입/출력(I/O) 인터페이스들(514)를 통해 발생할 수 있다. 또한, 컴퓨터 시스템/서버(500)는 근거리 통신망(LAN), 일반 광역 통신망(WAN), 및/또는 네트워크 어댑터(522)를 통한 공공 네트워크(예를 들어, 인터넷)와 같은, 하나 또는 그 이상의 네트워크들과 통신할 수 있다. 묘사된 바와 같이, 네트워크 어댑터(522)는 버스(506)을 통해 컴퓨터 시스템/서버(500)의 다른 컴포넌트들과 통신할 수 있다. 비록 도시되지는 않았지만, 다른 하드웨어 및/또는 소프트웨어 컴포넌트들도 컴퓨터 시스템/서버(500)과 함께 사용될 수 있다는 것을 이해해야 한다. 예들은 마이크로코드, 디바이스 드라이버들, 중복 처리 유닛들, 외장 디스크 드라이브 어레이들, RAID 시스템들, 테이프 드라이브들 및 데이터 아카이브 스토리지 시스템들 등을 포함하지만, 이에 한정되지는 않다.

[0057] [0065] 추가적으로, 발행-구독 메시징 큐에서 타겟 정책-기반 암호화를 위한 시스템(400)의 적어도 일부들은 버스 시스템(506)에 첨부될 수 있다. 완전한 시스템(400)은 시스템의 다양한 부분들, 예를 들어, 메시지 생산자 시스템, 메시지 수신자 시스템, 데이터베이스 시스템, 핵심 메시지 큐 시스템, 키 관리 시스템 및 암호화 정책 시스템을 위한 복수의 다양한 컴퓨팅 시스템(500)을 필요로 할 수 있다.

[0058] [0066] 본 발명의 다양한 실시 예들의 설명들은 예시의 목적으로 제공되는 것이며, 개시된 실시 예들이 전부라거나 이들에 한정하려는 의도가 있는 것은 아니다. 많은 수정들 및 변형들이 설명된 실시 예들의 범위와 정신을 벗어남이 없이 이 기술 분야에서 통상의 지식을 가진 자에게는 명백할 것이다. 여기서 사용된 용어들은 실시 예들의 원리들, 실제 애플리케이션 또는 시장에서 발견된 기술들에 대한 기술적 개선을 가장 잘 설명하기 위해 또는 이 기술 분야에서 통상의 지식을 가진 자들이 여기서 개시된 실시 예들을 이해할 수 있도록 하기 위해 선택되었다

[0059] [0067] 본 발명은 시스템, 방법 및/또는 컴퓨터 프로그램 제품일 수 있다. 컴퓨터 프로그램 제품은 컴퓨터 판독 가능 스토리지 매체(또는 매체)를 포함할 수 있으며, 이 매체 상에 프로세서가 본 발명의 실시 예들을 수행하도록 하는 컴퓨터 판독 가능 프로그램 명령들을 갖는다.

[0060] [0068] 상기 매체는 전파 매체를 위한 전자, 자기, 광학, 전자기, 적외선 또는 반도체 시스템일 수 있다. 컴퓨터 판독 가능한 매체의 예로는 반도체 또는 고체 메모리, 자기 테이프, 착탈가능 컴퓨터 디스켓, RAM(Random-Access Memory), 읽기 전용 메모리(ROM), 강성 자기 디스크 및 광 디스크를 들 수 있다. 현재 광디스크의 예들로는 CD-ROM, CD-R/W, DVD, 블루레이 디스크 등이 있다.

[0061] [0069] 상기 컴퓨터 판독 가능 스토리지 매체는 명령 실행 장치에 의해 사용될 명령들을 유지 및 저장할 수 있는 유형의(tangible) 디바이스일 수 있다. 상기 컴퓨터 판독 가능 스토리지 매체는, 예를 들면, 전자 스토리지 디바이스, 자기 스토리지 디바이스, 광 스토리지 디바이스, 전자기 스토리지 디바이스, 반도체 스토리지 디바이스, 또는 전술한 것들의 모든 적절한 조합일 수 있으며, 그러나 이에 한정되지는 않는다. 컴퓨터 판독 가능 스토리지 매체의 더 구체적인 예들의 비포괄적인 목록에는 다음이 포함될 수 있다: 휴대용 컴퓨터 디스켓, 하드 디스크, 랜덤 액세스 메모리(RAM), 판독-전용 메모리(ROM), 소거 및 프로그램가능 판독-전용 메모리(EPROM 또는 플래시 메모리), 정적 랜덤 액세스 메모리(SRAM), 휴대용 컴팩트 디스크 판독-전용 메모리(CD-ROM), 디지털 다용도 디스크(DVD), 메모리 스틱, 플로피 디스크, 천공-카드들 또는 명령들이 기록된 홈에 있는 융기된 구조들 같이 머신적으로 인코드 된 장치, 및 전술한 것들의 모든 적절한 조합. 본 명세서에서 사용될 때, 컴퓨터 판독

가능 스토리지 매체는 무선 전파들이나 다른 자유롭게 전파되는 전자기파들, 도파관이나 기타 전송 매체(예를 들어, 광섬유 케이블을 통해 전달되는 광 펄스들)를 통해 전파되는 전자기파들, 또는 선(wire)을 통해 전송되는 전기 신호들 같이 그 자체로 일시적인(transitory) 신호들로 해석되지는 않는다.

[0062] [0070] 본 명세서에 기술되는 컴퓨터 판독 가능 명령들은, 예를 들어, 인터넷, 근거리 통신망, 광역 통신망 및/또는 무선 네트워크 등의 통신망(네트워크)을 통해 컴퓨터 판독 가능 스토리지 매체로부터 각각 컴퓨팅/처리 디바이스들로 또는 외부 스토리지 디바이스로부터 외부 컴퓨터로 다운로드 될 수 있다. 상기 통신망은 구리 전송 케이블들, 광 전송 섬유들, 무선 전송, 라우터들, 방화벽들, 스위치들, 게이트웨이 컴퓨터들 및/또는 엣지 서버들을 포함할 수 있다. 각 컴퓨팅/처리 유닛 내 네트워크 어댑터 카드 또는 네트워크 인터페이스는 상기 통신망으로부터 컴퓨터 판독 가능 프로그램 명령들을 수신하고 그 컴퓨터 판독 가능 프로그램 명령들을 각각의 컴퓨팅/처리 디바이스 내의 컴퓨터 판독 가능 스토리지 매체에 저장하기 위해 전송한다.

[0063] [0071] 본 발명의 연산들을 실행하기 위한 컴퓨터 판독 가능 프로그램 명령들은 Smalltalk, C++ 또는 그와 유사 언어 등의 객체 지향 프로그래밍 언어와 "C" 프로그래밍 언어 또는 그와 유사한 프로그래밍 언어 등의 종래의 절차적 프로그래밍 언어들을 포함하여, 하나 또는 그 이상의 프로그래밍 언어들을 조합하여 작성된(written) 어셈블러 명령들, 명령-세트-아키텍처(ISA) 명령들, 머신 명령들, 머신 종속 명령들, 마이크로코드, 펌웨어 명령들, 상태-셋팅 데이터, 집적회로를 위한 구성 데이터, 또는 소스 코드나 목적 코드일 수 있다. 상기 컴퓨터 판독 가능 프로그램 명령들은 전적으로 사용자의 컴퓨터상에서, 부분적으로 사용자의 컴퓨터상에서, 독립형(stand-alone) 소프트웨어 패키지로서, 부분적으로 사용자의 컴퓨터상에서 그리고 부분적으로 원격 컴퓨터상에서 또는 전적으로 원격 컴퓨터나 서버상에서 실행될 수 있다. 위에서 마지막의 경우에, 원격 컴퓨터는 근거리 통신망(LAN) 또는 광역 통신망(WAN)을 포함한 모든 종류의 네트워크를 통해서 사용자의 컴퓨터에 접속될 수 있고, 또는 이 접속은 (예를 들어, 인터넷 서비스 제공자를 이용한 인터넷을 통해서) 외부 컴퓨터에 이루어질 수도 있다. 일부 실시 예들에서, 예를 들어 프로그램 가능 로직 회로, 필드-프로그램 가능 게이트 어레이들(FPGA), 또는 프로그램 가능 로직 어레이들(PLA)을 포함한 전자 회로는 본 발명의 실시 예들을 수행하기 위해 전자 회로를 맞춤화 하도록 상기 컴퓨터 판독 가능 프로그램 명령들의 상태 정보를 활용하여 상기 컴퓨터 판독 가능 프로그램 명령들을 실행할 수 있다.

[0064] [0072] 본 발명의 특징들이 본 발명의 실시 예들에 따른 방법들, 장치들(시스템들), 및 컴퓨터 프로그램 제품들의 플로 차트 예시도들 및/또는 블록도들을 참조하여 기술된다. 플로 차트 예시도들 및/또는 블록도들의 각 블록과 플로 차트 예시도들 및/또는 블록도들 내 블록들의 조합들은 컴퓨터 판독 가능 프로그램 명령들에 의해 구현될 수 있다는 것을 이해할 수 있을 것이다.

[0065] [0073] 이들 컴퓨터 판독 가능 프로그램 명령들은 범용 컴퓨터, 특수목적용 컴퓨터, 또는 기타 프로그램가능 데이터 처리 유닛의 프로세서에 제공되어 머신(machine)을 생성하고, 그렇게 하여 그 명령들이 상기 컴퓨터 또는 기타 프로그램가능 데이터 처리 유닛의 프로세서를 통해서 실행되어, 상기 플로 차트 및/또는 블록도의 블록 또는 블록들에 명시된 기능들/동작들을 구현하기 위한 수단을 생성할 수 있다. 이들 컴퓨터 판독 가능 프로그램 명령들은 또한 컴퓨터 판독 가능 스토리지 매체에 저장될 수 있으며, 컴퓨터, 프로그램가능 데이터 처리 유닛 및/또는 기타 디바이스들에 지시하여 명령들이 저장된 상기 컴퓨터 판독 가능 스토리지 매체가 상기 플로 차트 및/또는 블록도의 블록 또는 블록들에 명시된 기능/동작의 특징들을 구현하는 명령들을 포함하는 제조품(an article of manufacture)을 포함하도록 특정한 방식으로 기능하게 할 수 있다.

[0066] [0074] 상기 컴퓨터 판독 가능 프로그램 명령들은 또한 컴퓨터, 기타 프로그램가능 데이터 처리 유닛, 또는 다른 디바이스에 로드 되어, 상기 컴퓨터, 기타 프로그램가능 장치 또는 다른 디바이스에서 일련의 동작 단계들이 수행되게 하여 컴퓨터 구현 프로세스를 생성하며, 그렇게 하여 상기 컴퓨터, 기타 프로그램가능 장치, 또는 다른 디바이스 상에서 실행되는 명령들이 플로 차트 및/또는 블록도의 블록 또는 블록들에 명시된 기능들/동작들을 구현할 수 있다.

[0067] [0075] 도면들 내 플로 차트 및 블록도들은 본 발명의 여러 실시 예들에 따른 시스템들, 방법들 및 컴퓨터 프로그램 제품들의 가능한 구현들의 아키텍처, 기능(functionality), 및 연산(operation)을 예시한다. 이와 관련하여, 상기 플로 차트 또는 블록도들 내 각 블록은 상기 명시된 로직 기능(들)을 구현하기 위한 하나 또는 그 이상의 실행 가능한 명령들을 포함한 모듈, 세그먼트 또는 명령들의 일부분을 나타낼 수 있다. 일부 다른 실시 예들에서, 상기 블록에 언급되는 기능들은 도면들에 언급된 순서와 다르게 일어날 수도 있다. 예를 들면, 연속으로 도시된 두 개의 블록들은 실제로는 사실상 동시에 실행될 수도 있고, 또는 이 두 블록들은 때때로 관련된 기능에 따라서는 역순으로 실행될 수도 있다. 블록도들 및/또는 플로 차트 예시도의 각 블록, 및 블록도들 및/또

는 플로 차트 예시도 내 블록들의 조합들은 특수목적용 하드웨어 및 컴퓨터 명령들의 명시된 기능들 또는 동작들, 또는 이들의 조합들을 수행하는 특수목적용 하드웨어-기반 시스템들에 의해 구현될 수 있다는 것에 또한 주목해야 한다.

[0068] [0076] 본 명세서에서 사용되는 용어는 특정 실시 예들만을 설명하기 위한 것으로, 본 발명을 제한하기 위한 것은 아니다. 여기서 사용되는 단수 형태 표현은 문맥이 달리 명확하게 지시하지 않는 한 복수 형태도 포함하도록 의도된다. 또한 본 명세서에서 "포함한다" 및/또는 "포함하는"이라는 용어는 명시된 특징들, 정수들, 단계들, 동작들, 엘리멘트들 및/또는 컴포넌트들의 존재를 명시하지만 하나 또는 그 이상의 다른 특징들, 정수들, 단계들, 동작들, 엘리멘트들, 컴포넌트들 및/또는 그들의 그룹의 존재 또는 추가를 배제하지 않는다는 것을 이해할 수 있다.

[0069] [0077] 아래 청구항들 내 모든 수단들 또는 단계 플러스 기능 엘리멘트들의 대응하는 구조들, 재료들, 동작들 및 등가물들은 구체적으로 청구된 다른 청구항과 결합하여 기능을 수행하기 위한 모든 구조들, 재료들 또는 동작들을 포함하도록 의도되었다. 본 발명의 설명들은 예시와 설명의 목적으로 제공되는 것이며, 개시된 형태의 발명이 전부라거나 이들에 한정하려는 의도가 있는 것은 아니다. 많은 수정들 및 변형들이 설명된 실시 예들의 범위와 정신을 벗어남이 없이 이 기술 분야에서 통상의 지식을 가진 자에게는 명백할 것이다. 실시 예들은 본 발명의 원리들, 및 실제 애플리케이션을 가장 잘 설명하기 위해 또는 이 기술 분야에서 통상의 지식을 가진 자들이 다양한 변형들을 갖는 다양한 실시 예들에 대한 발명을, 고려된 특정 용도에 적합하게, 이해할 수 있도록 하기 위해 선택 및 설명된다.

[0070] [0078] 본 명세서에서 도움이 되는 정의들은 다음과 같다:

[0071] [0079] 본 발명: "본 발명"이라는 용어에 의해서 설명되는 주제가 출원 시의 청구항들에 의해서, 또는 특허 중간 처리 후 최종으로 특허 결정될 수 있는 청구항들에 의해서 커버된다는 것을 절대적으로 표시하는 것은 아니다; "본 발명"이라는 용어는 새로운 것으로 여겨지는 본 문서의 공개들에 대해서 독자가 일반적인 느낌을 받도록 돕기 위해 사용되지만, "본 발명"이라는 용어의 사용에 의해 표시된 이러한 이해는 잠정적이고 일시적인 것이며 특허 심사 중간 과정에서 관련 정보가 개발되고 청구항들이 잠재적으로 개정됨으로써 변화될 수 있다.

[0072] [0080] 실시 예: 위의 "본 발명"의 정의에서 살펴본 바와 같이, 유사한 주의가 "실시 예"라는 용어에도 적용될 수 있다.

[0073] [0081] 및/또는: 포함한다는 것을 의미하거나 또는; 예를 들어, A, B "및/또는" C라고 할 때 이는 A 또는 B 또는 C 중 적어도 하나가 참이고 적용 가능하다는 것을 의미한다.

[0074] [0082] 사용자/구독자: 다음을 포함하지만, 이에 반드시 국한되지는 않는다: (i) 단일의 개인; (ii) 사용자 또는 구독자로써 활동하기에 충분한 지능을 가진 인공지능 주체; 및/또는 (iii) 관련된 사용자들 또는 구독자들의 그룹.

[0075] [0083] 모듈/서브-모듈(Sub-Module): 어떤 종류의 기능을 수행하기 위해 작동하는 하드웨어, 펌웨어 및/또는 소프트웨어의 모든 세트이고, 모듈이: (i) 단일 로컬 근접 위치에 위치하는지, (ii) 넓은 영역을 걸쳐 분포되는지, (iii) 대규모 소프트웨어 코드 내 단일 근접 위치에 위치하는지, (iv) 단일 소프트웨어 코드 내에 위치하는지; (v) 단일 스토리지 디바이스, 메모리 또는 매체에 위치하는지; (vi) 기계적으로 연결되었는지; (vii) 전기적으로 연결되었는지; 및/또는 (vii) 데이터 통신에서 연결되었는지는 상관 없다.

[0076] [0084] 컴퓨터: 중요한 데이터 처리 및/또는 머신-판독가능(machine-readable) 명령을 읽는 능력을 갖는 모든 디바이스로서 다음을 포함하지만, 이들에 국한되지는 않는다: 데스크톱 컴퓨터들, 메인프레임 컴퓨터들, 랩톱 컴퓨터들, 필드-프로그램 가능 게이트 어레이(field-programmable gate array: FPGA) 기반 디바이스들, 스마트 폰들, 개인 정보 단말기들(personal digital assistants: PDAs), 신체-장착형(body-mounted) 또는 삽입형 컴퓨터들, 임베드된 디바이스 스타일 컴퓨터들, 주문형 집적 회로(application-specific integrated circuit: ASIC) 기반 디바이스들.

[0077] [0085] 본 발명의 일부 실시 예들은 다음의 발명 개념들 중 하나 또는 그 이상과 관련된다.

[0078] [0086] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화를 위한 컴퓨터-구현 방법에 있어서, 상기 방법은: (i) 메시지 큐잉 시스템에 의해서 암호화된 메시지를 수신하는 단계 - 상기 메시지는 암호화 정책 시스템과 토픽-관련 암호화 키를 저장하는 키 관리 시스템을 참조하여 암호화됨-; (ii) 수신된 암호화된 메시지를 저장하는 단계; 및 (iii) 토픽에 대한 구독에 기초하여 상기 암호화된 메시지를 전송하는 단계를 포함한다.

[0079] [0087] 메시지 큐잉 시스템은 카프카 시스템이다.

[0080] [0088] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화는 토픽-관련 메시지를 전송하기 전에 암호화 정책 시스템을, 메시지 생산자에 의해서, 참조하는 동작을 포함한다.

[0081] [0089] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화는 상기 암호화 정책 데이터베이스가 토픽-관련 메시지의 암호화를 시행하는 규칙을 포함한다고, 메시지 생산자에 의해서, 결정하는 동작과 만일 상기 메시지 생산자가 암호화 키를 수신하도록 허가되었다면 상기 키 관리 시스템으로부터 암호화 키를 수신하는 동작을 포함한다.

[0082] [0090] 키 관리 시스템 및 암호화 정책 시스템은 동일 보안 시스템에서 구현된다.

[0083] [0091] 키 관리 시스템 및 암호화 정책 시스템은 서로 다른 위치들에서 액세스할 수 있다.

[0084] [0092] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화는, 전송된 메시지를, 메시지 소비자에 의해서, 수신하는 것에 기초하여, 상기 암호화 정책 시스템을 참조하는 동작과 상기 수신된 메시지가 암호화되었는지를 결정하는 동작을 포함한다.

[0085] [0093] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화는 다음 동작들을 포함한다: (i) 수신된 메시지가 암호화되었다고 결정하는 것에 기초하여, 암호 해독 키를, 메시지 소비자에 의해서, 수신하는 동작; (ii) 수신된 메시지를 암호 해독하는 동작.

[0086] [0094] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화는 상기 암호화 정책 시스템에 대한 액세스들을 로깅하는 동작을 포함한다.

[0087] [0095] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화는 상기 키 관리 시스템에 대한 액세스들을 로깅하는 동작을 포함한다.

[0088] [0096] 메시지 큐잉 시스템에 의해서 수신된 암호화된 메시지는 디지털 서명된다.

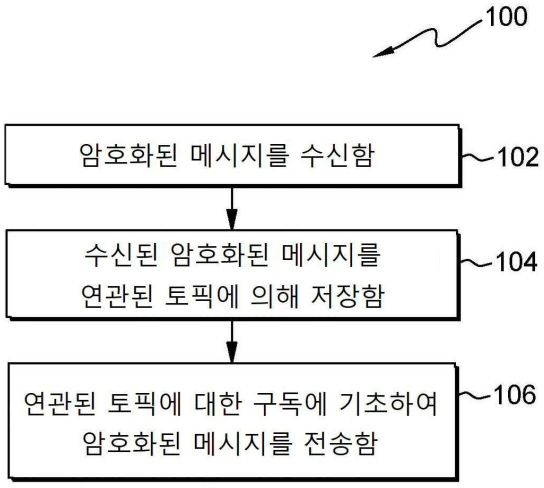
[0089] [0097] 메시지 큐잉 시스템에 의해서 수신된 암호화된 메시지는 메시지 인증 코드를 포함한다.

[0090] [0098] 게시-구독 메시지 큐에서의 타겟, 정책-기반 암호화를 위한 컴퓨터 시스템에 있어서, 상기 컴퓨터 시스템은: (i) 암호화된 메시지를 수신하기 위해 구성된 메시지 큐잉 시스템 - 상기 메시지는 암호화 정책 시스템과 토픽-관련 암호화 키를 저장하는 키 관리 시스템을 참조하여 암호화됨-; (ii) 수신된 암호화된 메시지를 저장하기 위한 수단; 및 (iii) 토픽에 대한 구독에 기초하여 상기 암호화된 메시지를 전송하기 위한 수단을 포함한다.

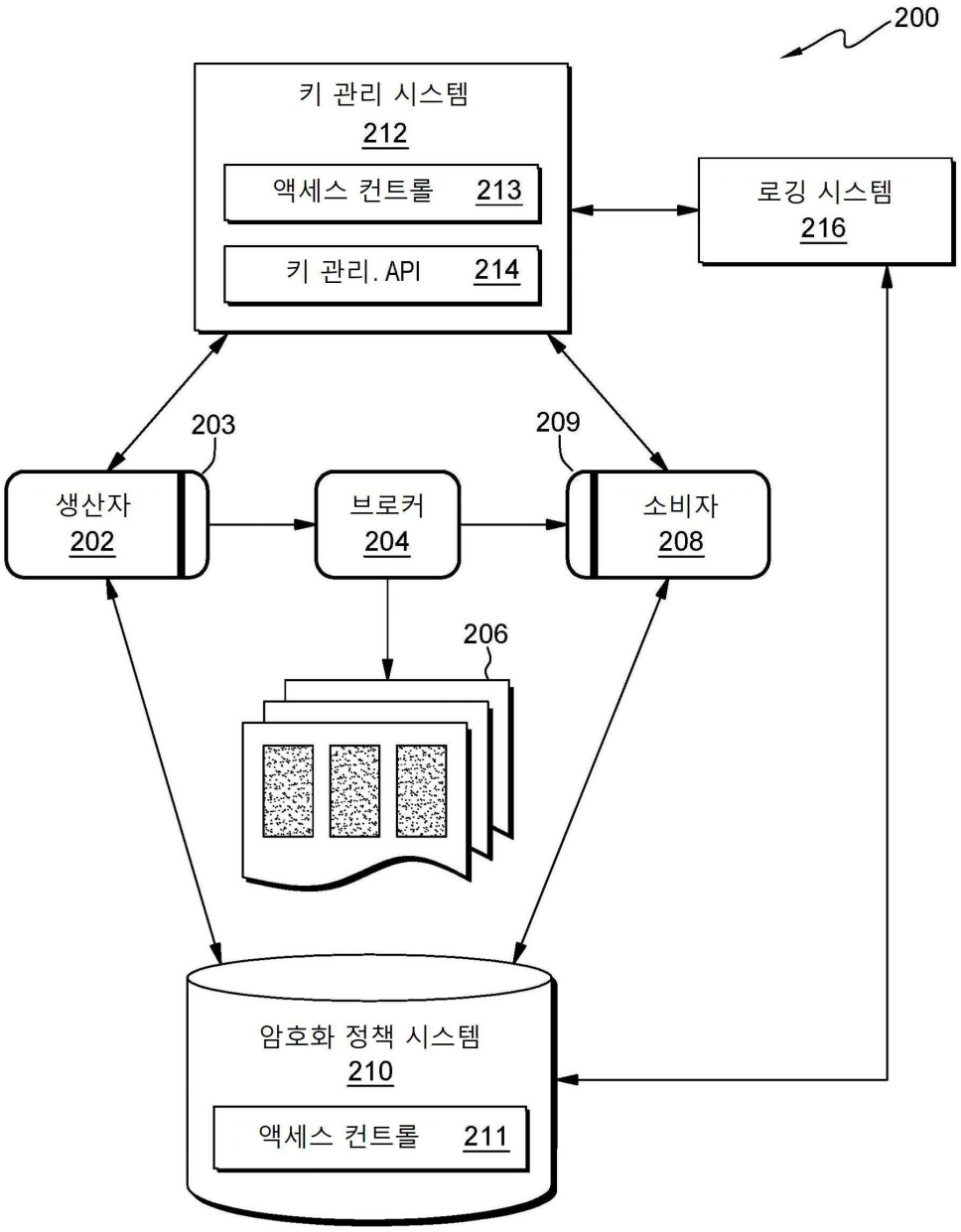
[0091] [0099] 게시-구독 메시징 큐에서의 타겟, 정책-기반 암호화를 위한 컴퓨터 시스템에 있어서, 상기 컴퓨터 시스템은: 상기 암호화 정책 데이터베이스가 토픽-관련 메시지의 암호화를 시행하는 규칙을 포함한다고, 메시지 생산자에 의해서, 결정하는 것에 기초하여, 만일 상기 메시지 생산자가 암호화 키를 수신하도록 허가되었다면 상기 키 관리 시스템으로부터 암호화 키를 수신하도록 구성된다.

도면

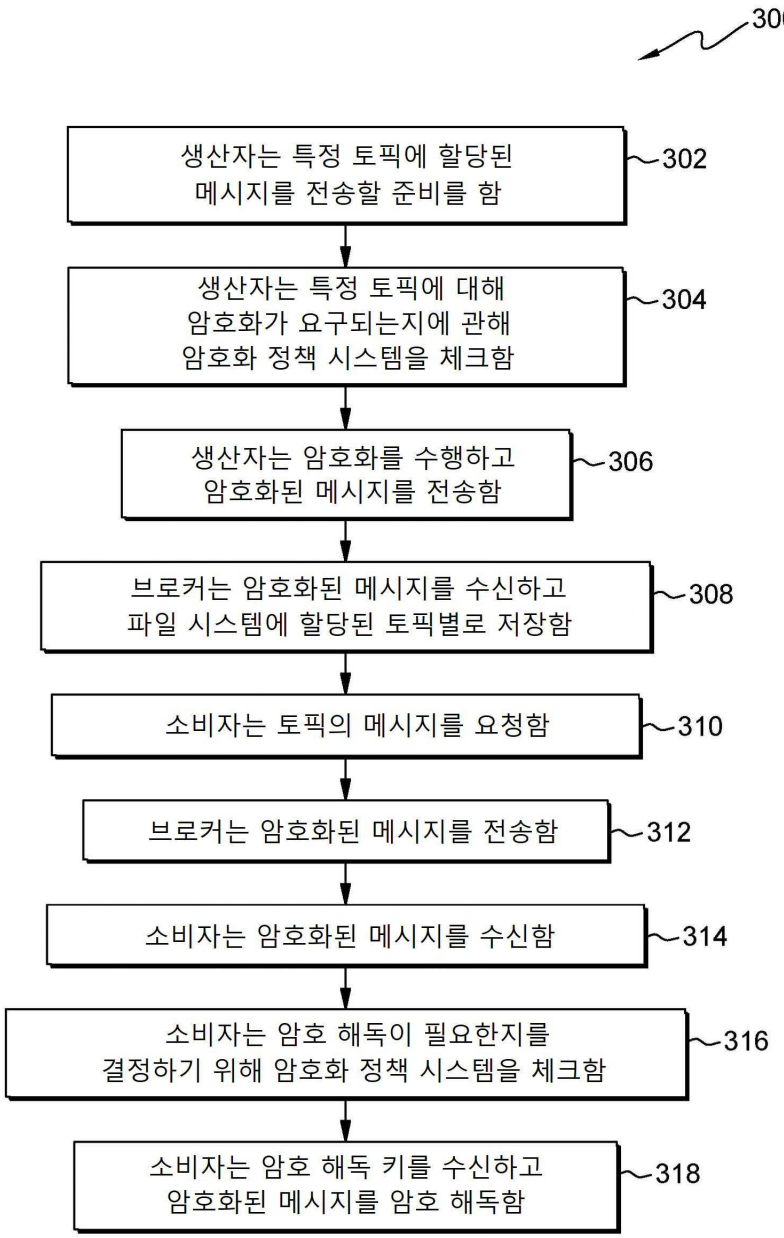
도면1


100
암호화된 메시지를 수신함
102
수신된 암호화된 메시지를
연관된 토픽에 의해 저장함
104
연관된 토픽에 대한 구독에 기초하여
암호화된 메시지를 전송함
106

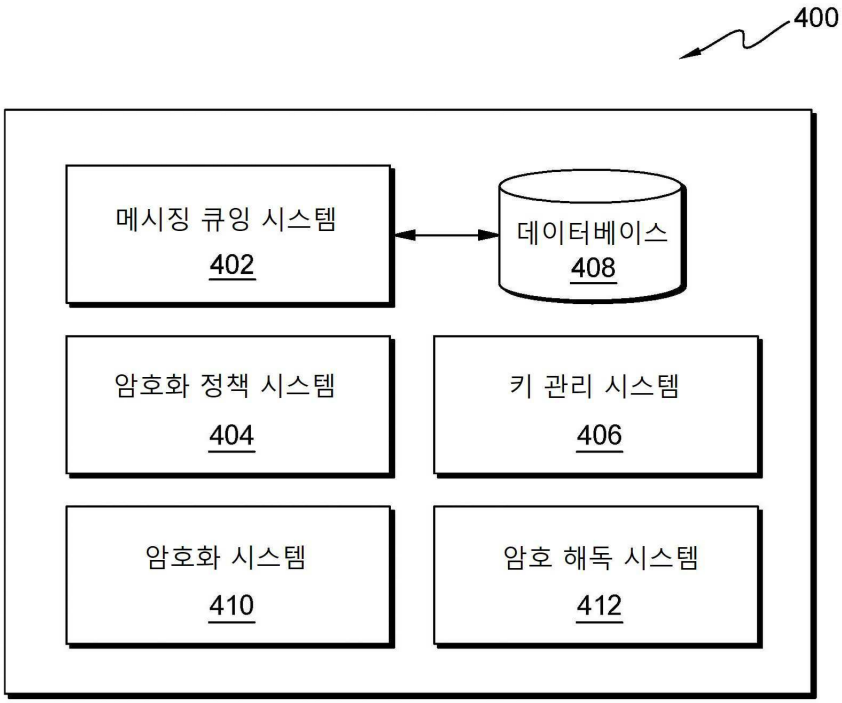
도면2


200
키 관리 시스템
212
액세스 컨트롤 213
키 관리. API 214
로깅 시스템
216
203
209
생산자
202
브로커
204
소비자
208
206
암호화 정책 시스템
210
액세스 컨트롤 211

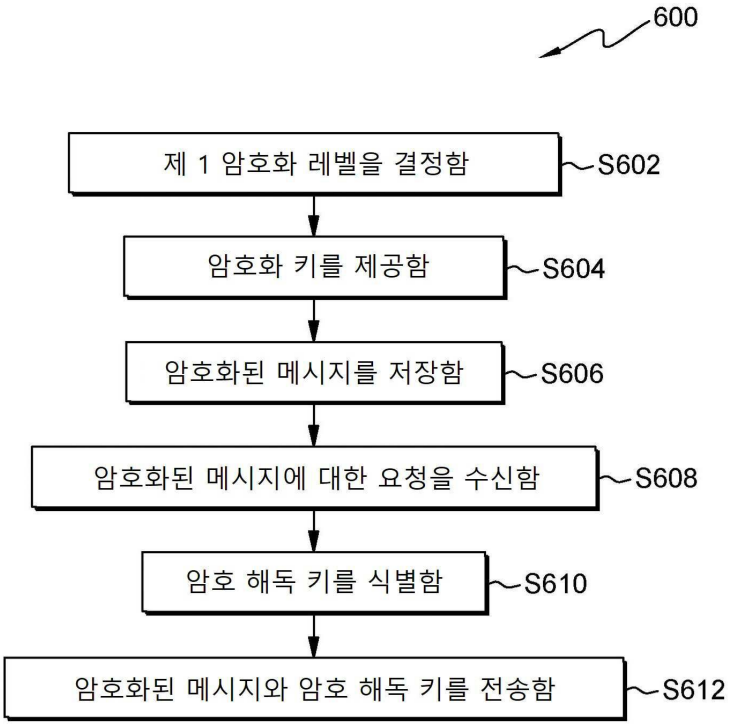
도면3


300
생산자는 특정 토픽에 할당된 메시지를 전송할 준비를 함
302
생산자는 특정 토픽에 대해 암호화가 요구되는지에 관해 암호화 정책 시스템을 체크함
304
생산자는 암호화를 수행하고 암호화된 메시지를 전송함
306
브로커는 암호화된 메시지를 수신하고 파일 시스템에 할당된 토픽별로 저장함
308
소비자는 토픽의 메시지를 요청함
310
브로커는 암호화된 메시지를 전송함
312
소비자는 암호화된 메시지를 수신함
314
소비자는 암호 해독이 필요한지를 결정하기 위해 암호화 정책 시스템을 체크함
316
소비자는 암호 해독 키를 수신하고 암호화된 메시지를 암호 해독함
318

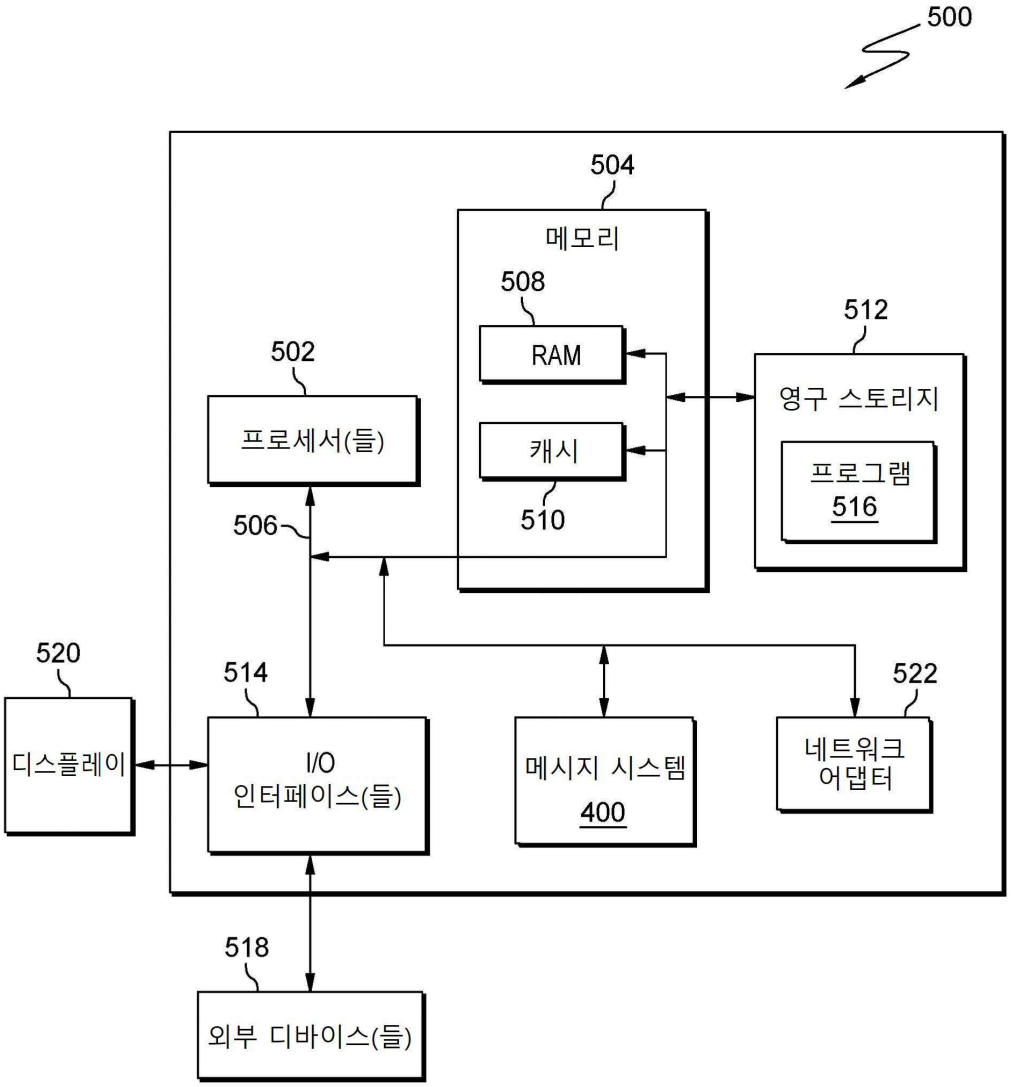
도면4


400
메시징 큐잉 시스템
402
데이터베이스
408
암호화 정책 시스템
404
키 관리 시스템
406
암호화 시스템
410
암호 해독 시스템
412

도면5


600
제 1 암호화 레벨을 결정함
S602
암호화 키를 제공함
S604
암호화된 메시지를 저장함
S606
암호화된 메시지에 대한 요청을 수신함
S608
암호 해독 키를 식별함
S610
암호화된 메시지와 암호 해독 키를 전송함
S612

도면6


500
504
메모리
508
RAM
캐시
510
512
영구 스토리지
프로그램
516
502
프로세서(들)
506
520
디스플레이
514
I/O
인터페이스(들)
메시지 시스템
400
522
네트워크
어댑터
518
외부 디바이스(들)