(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0016530
(43) 공개일자 2018년02월14일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 20/10* (2012.01)
(52) CPC특허분류
G06Q 20/4016 (2013.01)
G06Q 20/108 (2013.01)
(21) 출원번호 10-2018-7000584
(22) 출원일자(국제) 2016년07월08일
심사청구일자 2018년01월08일
(85) 번역문제출일자 2018년01월08일
(86) 국제출원번호 PCT/US2016/041515
(87) 국제공개번호 WO 2017/011307
국제공개일자 2017년01월19일
(30) 우선권주장
14/796,244 2015년07월10일 미국(US)

(71) 출원인
마스터카드 인터내셔날, 인코포레이티드
미합중국 뉴욕주, 퍼체이스, 퍼체이스 스트리트 2000 (우편번호:10577)
(72) 발명자
나이다마누리, 스리니바사라오
미국, 몬타나주 63005, 체스터필드, 우드클리프 플레이스 드라이브 333
허트, 대릴
미국, 몬타나주 63385, 웬츠빌 엥글리시 마너 드라이브 415
(74) 대리인
김영철, 김 순 영

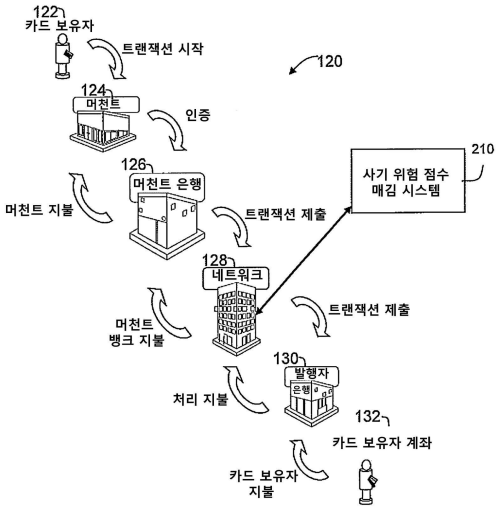
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **대리 기능성을 위한 상호 처리 전자 신호**

(57) 요 약

잠재적인 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 상호 처리 사기 위험 점수 매김 시스템이 서술된다. 추가적으로, 잠재적인 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 방법 및 컴퓨터 판독가능 저장 매체가 서술된다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/405 (2013.01)

명 세 서

청구범위

청구항 1

잠재적인 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 상호 처리 사기 위험 점수 매김 시스템으로서, 상기 사기 위험 점수 매김 시스템은 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치, 상기 메시지 프로세서 컴퓨팅 장치에 연결된 제1 점수 매김 컴퓨팅 장치, 및 상기 메시지 프로세서 컴퓨팅 장치에 연결된 제2 점수 매김 컴퓨팅 장치를 포함하며, 상기 사기 위험 점수 매김 시스템은:

제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를 수신하고;

상기 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는지를 결정하며;

제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 상기 제1 카드 보유자 계좌에 연관된 제1 프로파일에 기초하여 상기 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 상기 제1 인증 요청 메시지를 상기 제1 점수 매김 컴퓨팅 장치로 전송하고;

제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신하며;

상기 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는지를 결정하고; 그리고

제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 상기 제2 카드 보유자 계좌에 연관된 제2 프로파일에 기초하여 상기 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 상기 제2 인증 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치로 전송하도록 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 2

제1항에 있어서,

상기 제1 카드 보유자 계좌에 연관된 제1 프로파일을 업데이트하기 위해 제1 프로파일 업데이트 요청 메시지를, 상기 제1 점수 매김 컴퓨팅 장치에 의해, 생성하고;

상기 제1 프로파일 업데이트 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치로 전송하며;

상기 제2 카드 보유자 계좌에 연관된 제2 프로파일을 업데이트하기 위해 제2 프로파일 업데이트 요청 메시지를, 상기 제2 점수 매김 컴퓨팅 장치에 의해, 생성하고; 그리고

상기 프로파일 업데이트 요청 메시지를 상기 제1 점수 매김 컴퓨팅 장치로 전송하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 3

제1항에 있어서,

제1 점수 매김 컴퓨팅 장치가 동작하지 않는지 결정하고;

상기 제1 데이터베이스와 상기 제2 데이터베이스 간에 데이터를 복제하기 위한 임의의 프로세스를 종료하며;

짝수 및 홀수 번호가 부여된 은행 식별 번호 모두에 연관된 프로파일 업데이트 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치에서 생성하고 상기 제1 점수 매김 컴퓨팅 장치가 동작하는 경우 상기 제1 점수 매김 컴퓨팅 장치에 의한 처리를 위해 상기 프로파일 업데이트 요청 메시지를 저장하며;

이어서 상기 제1 점수 매김 컴퓨팅 장치가 동작하는지를 결정하고;

저장된 프로파일 업데이트 요청 메시지 모두를 상기 제2 점수 매김 컴퓨팅 장치로부터 상기 제1 점수 매김 컴퓨팅 장치로 전송하며; 그리고

상기 제2 데이터베이스에 저장된 제2 규칙 세트를 상기 제1 데이터베이스에 저장된 제1 규칙 세트와 동기화하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 4

제1항에 있어서,

상기 제1 인증 요청 메시지를 전송하는 것은 실시간 및 근 실시간(near real time) 인증 요청 메시지 중 적어도 하나를 상기 제1 점수 매김 컴퓨팅 장치로 전송하는 것을 더 포함하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 5

제1항에 있어서,

각각의 수신된 인증 요청 메시지에 대한 인증 응답 메시지를, 상기 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치에 의해, 생성하고;

상기 인증 요청 메시지에 기초하여 대응하는 카드 보유자 프로파일을 업데이트하며; 그리고

상기 업데이트된 카드 보유자 프로파일을 상기 제1 데이터베이스 및 제2 데이터베이스에 저장하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 6

제1항에 있어서,

상기 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치는 프로파일 업데이트 요청 메시지에 응답하여, 상기 프로파일 업데이트 요청 메시지를 상기 제1 데이터베이스 또는 제2 데이터베이스에 저장하지 않고, 카드 보유자 프로파일을 업데이트하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 7

제1항에 있어서,

카드 보유자 인구 통계(demographics) 및 비금전(nonmonetary) 데이터를 상기 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치에서 수신하고; 그리고

상기 수신된 카드 보유자 인구 통계 및 비금전 데이터를 사용하여 카드 보유자 프로파일을 업데이트하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 8

제1항에 있어서,

상기 제1 데이터베이스에 저장된 제1 규칙이 상기 제2 데이터베이스에 저장된 제2 규칙과 매칭하지 않는지 결정하고; 그리고

상기 제1 규칙을 상기 제2 규칙과 동기화하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 9

제1항에 있어서,

상기 제1 데이터베이스와 상기 제2 데이터베이스 간에 데이터를 미리 정의된 인터벌에서 복제하도록 더 구성되는 상호 처리 사기 위험 점수 매김 시스템.

청구항 10

잠재적 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 방법으로서, 상기 방법은 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치, 상기 메시지 프로세서 컴퓨팅 장치에 연결된 제1 점수 매김 컴퓨팅 장치, 및 상기 메시지 프로세서 컴퓨팅 장치에 연결된 제2 점수 매김 컴퓨팅 장치를 포함한 상호 처리 사기 위험 점수 매김

시스템에 의해 실시되며, 상기 방법은:

제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를, 상기 상호 처리 사기 위험 점수 매김 시스템에 의해, 수신하는 단계;

상기 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는지를, 상기 상호 처리 사기 위험 점수 매김 시스템에 의해, 결정하는 단계;

제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 상기 제1 카드 보유자 계좌에 연관된 제1 프로파일에 기초하여 상기 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 상기 제1 인증 요청 메시지를, 상기 상호 처리 사기 위험 점수 매김 시스템에 의해, 상기 제1 점수 매김 컴퓨팅 장치로 전송하는 단계;

제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를, 상기 상호 처리 사기 위험 점수 매김 시스템에 의해, 수신하는 단계;

상기 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는지를, 상기 상호 처리 사기 위험 점수 매김 시스템에 의해, 결정하는 단계; 및

제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 상기 제2 카드 보유자 계좌에 연관된 제2 프로파일에 기초하여 상기 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 상기 제2 인증 요청 메시지를, 상기 상호 처리 사기 위험 점수 매김 시스템에 의해, 상기 제2 점수 매김 컴퓨팅 장치로 전송하는 단계를 포함하는 방법.

청구항 11

제10항에 있어서,

상기 제1 카드 보유자 계좌에 연관된 제1 프로파일을 업데이트 하기 위해 제1 프로파일 업데이트 요청을, 상기 제1 점수 매김 컴퓨팅 장치에 의해, 생성하는 단계;

상기 제1 프로파일 업데이트 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치로 전송하는 단계;

상기 제2 카드 보유자 계좌에 연관된 제2 프로파일을 업데이트하기 위해 제2 프로파일 업데이트 요청 메시지를, 상기 제2 점수 매김 컴퓨팅 장치에 의해, 생성하는 단계; 및

상기 프로파일 업데이트 요청 메시지를 상기 제1 점수 매김 컴퓨팅 장치로 전송하는 단계를 더 포함하는 방법.

청구항 12

제10항에 있어서,

상기 제1 점수 매김 컴퓨팅 장치가 동작하지 않는지 결정하는 단계;

상기 제1 데이터베이스와 상기 제2 데이터베이스 간에 데이터를 복제하기 위한 임의의 프로세스를 종료하는 단계;

짝수 및 홀수 번호가 부여된 은행 식별 번호 모두에 연관된 프로파일 업데이트 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치에서 생성하고 상기 제1 점수 매김 컴퓨팅 장치가 동작하는 경우 상기 제1 점수 매김 컴퓨팅 장치에 의한 처리를 위해 상기 프로파일 업데이트 요청 메시지를 저장하는 단계;

이어서 상기 제1 점수 매김 컴퓨팅 장치가 동작하는지를 결정하는 단계;

저장된 프로파일 업데이트 요청 메시지 모두를 상기 제2 점수 매김 컴퓨팅 장치로부터 상기 제1 점수 매김 컴퓨팅 장치로 전송하는 단계; 및

상기 제2 데이터베이스에 저장된 제2 규칙 세트를 상기 제1 데이터베이스에 저장된 제1 규칙 세트와 동기화하는 단계를 더 포함하는 방법.

청구항 13

제10항에 있어서,

상기 제1 인증 요청 메시지를 전송하는 단계는 실시간 및 근 실시간(near real time) 인증 요청 메시지 중 적어

도 하나를 상기 제1 점수 매김 컴퓨팅 장치로 전송하는 단계를 더 포함하는 방법.

청구항 14

제10항에 있어서,

각각의 수신된 인증 요청 메시지에 대한 인증 응답 메시지를, 상기 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치에 의해, 생성하는 단계;

상기 인증 요청 메시지에 기초하여 대응하는 카드 보유자 프로파일을 업데이트하는 단계; 및

상기 업데이트된 카드 보유자 프로파일을 상기 제1 데이터베이스 및 제2 데이터베이스에 저장하는 단계를 더 포함하는 방법.

청구항 15

제10항에 있어서,

프로파일 업데이트 요청 메시지에 응답하여, 상기 프로파일 업데이트 요청 메시지를 상기 제1 데이터베이스 또는 제2 데이터베이스에 저장하지 않고, 카드 보유자 프로파일을 업데이트하는 단계를 더 포함하는 방법.

청구항 16

제10항에 있어서,

카드 보유자 인구 통계 및 비금전 데이터를 상기 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치에서 수신하는 단계; 및

상기 수신된 카드 보유자 인구 통계 및 비금전 데이터를 사용하여 카드 보유자 프로파일을 업데이트하는 단계를 더 포함하는 방법.

청구항 17

제10항에 있어서,

상기 제1 데이터베이스에 저장된 제1 규칙이 상기 제2 데이터베이스에 저장된 제2 규칙과 매칭하지 않는지를 결정하는 단계; 및

상기 제1 규칙을 제2 규칙과 동기화하는 단계를 더 포함하는 방법.

청구항 18

제10항에 있어서,

상기 제1 데이터베이스와 상기 제2 데이터베이스 간에 데이터를 미리 정의된 인터벌에서 복제하는 단계를 더 포함하는 방법.

청구항 19

컴퓨터 실행 가능한 명령어가 구현된 컴퓨터 판독가능 저장 매체로서, 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치, 상기 메시지 프로세서 컴퓨팅 장치에 연결된 제1 점수 매김 컴퓨팅 장치 및 상기 메시지 프로세서 컴퓨팅 장치에 연결된 제2 점수 매김 컴퓨팅 장치를 포함한 상호 처리 사기 위험 점수 매김 시스템의 하나 이상의 프로세서에 의해 실행되는 경우, 상기 컴퓨터 실행 가능 명령어는 상기 사기 위험 점수 매김 시스템이:

제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를 수신하고;

상기 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는지를 결정하며;

제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 상기 제1 카드 보유자 계좌에 연관된 제1 프로파일에 기초하여 상기 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 상기 제1 인증 요청 메시지를 상기 제1 점수 매김 컴퓨팅 장치로 전송하고;

제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신하며;

상기 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는지를 결정하고; 그리고

제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 상기 제2 카드 보유자 계좌에 연관된 제2 프로파일에 기초하여 상기 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 상기 제2 인증 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치로 전송하게 하는 컴퓨터 판독가능 저장 매체.

청구항 20

제19항에 있어서,

상기 컴퓨터 판독가능 명령어는 추가적으로 상기 사기 위험 점수 매김 시스템이:

상기 제1 카드 보유자 계좌에 연관된 제1 프로파일을 업데이트하기 위해 제1 프로파일 업데이트 요청 메시지를, 상기 제1 점수 매김 컴퓨팅 장치에 의해, 생성하고;

상기 제1 프로파일 업데이트 요청 메시지를 상기 제2 점수 매김 컴퓨팅 장치로 전송하며;

상기 제2 카드 보유자 계좌에 연관된 제2 프로파일을 업데이트하기 위해 제2 프로파일 업데이트 요청 메시지를, 상기 제2 점수 매김 컴퓨팅 장치에 의해, 생성하고; 그리고

상기 프로파일 업데이트 요청 메시지를 상기 제1 점수 매김 컴퓨팅 장치로 전송하게 하는 컴퓨터 판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 출원은 2015년 7월 10일자로 출원된 미국 특허 출원 제14 / 796,244호의 우선권을 주장하며, 그 내용은 본 명세서에서 그 전체가 참고로 인용된다.

[0002] 본 발명은 컴퓨터 네트워크를 통해 전송된 전자 신호를 처리하는 것에 관한 것으로서, 보다 상세하게는 대리 기능성(redundancy)을 제공하는 상호 처리(co-processing)를 사용하여 전자 거래 신호와 연관된 사기 점수(fraud scores)를 계산하는 것에 관한 것이다.

배 경 기 술

[0003] 당사자들 간에 금융 거래를 처리하는 적어도 공지된 지불 처리 네트워크는 사기 점수 매김 시스템 (fraud scoring system) 을 사용한다. 이러한 사기 점수 매김 시스템은 전자 거래와 연관된 데이터를 하나 이상의 미리 정의된 규칙에 대해 비교하여 전자 트랜잭션이 사기성(예를 들어, 계정 소유자가 아닌 다른 사람이 시도한 구매)인지 결정한다. 이러한 사기 평점 시스템이 동작 불능이 되는 경우, 예를 들면 유지 보수가 수행되는 경우, 지불 처리 네트워크는 전자 거래가 사기성이 있는지 여부를 신속하게 결정할 수 있는 능력에 방해를 겪는다.

발명의 내용

해결하려는 과제

[0004] 잠재적인 사기에 대하여 전자 지불 트랜잭션을 점수 매김하는 사기 위험 점수 매김 시스템 및 상기 사기 위험 점수 매김 시스템에 의해 실시되는 방법이 제공된다.

과제의 해결 수단

[0005] 일 측면에 있어서, 잠재적인 사기에 대하여 전자 지불 트랜잭션을 점수 매김하는 사기 위험 점수 매김 시스템이 제공된다. 사기 위험 점수 매김 시스템은 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치, 메시지 프로세서 컴퓨팅 장치에 연결된 제1 점수 매김 컴퓨팅 장치 및 메시지 프로세서 컴퓨팅 장치에 연결된 제2 점수 매김 컴퓨팅 장치를 포함한다. 사기 위험 점수 매김 시스템은 제1 지불 트랜잭션에 대한 제1 인증 요청 (authorization request) 메시지를 수신하도록 구성된다. 사기 위험 점수 매김 시스템은 추가적으로 제1 인증

요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는지를 결정하고, 제1 데이터 베이스에 의해 저장된 제1 규칙 세트에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수와 제1 카드 보유자 계좌와 연관된 제1 프로파일을 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송하며, 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신하고, 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는 지를 결정하며, 그리고 제2 데이터베이스에 의해 저장된 제2 규칙 세트에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수와 제2 카드 보유자 계좌와 연관된 제2 프로파일을 생성하기 위해 2 인증 요청 메시지를 제2 컴퓨팅 장치로 전송하도록 구성된다.

[0006] 다른 측면에 있어서, 잠재적인 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 방법이 제공된다. 상기 방법은 사기 위험 점수 매김 시스템에 의해 실시되며, 상기 사기 위험 점수 매김 시스템은 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치, 메시지 프로세서 컴퓨팅 장치에 연결된 제1 점수 매김 컴퓨팅 장치, 및 메시지 프로세서 컴퓨팅 장치에 연결된 제2 점수 매김 컴퓨팅 장치를 포함한다. 상기 방법은 제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를, 사기 위험 점수 매김 시스템에 의해, 수신하는 단계를 포함한다. 상기 방법은 추가로 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는 지를, 사기 점수 매김 시스템에 의해, 결정하는 단계, 제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 제1 카드 보유자 계좌와 연관된 제1 프로파일에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로, 사기 위험 점수 매김 시스템에 의해, 전송하는 단계, 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를, 사기 점수 매김 시스템에 의해, 수신하는 단계, 제2 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는 지를, 사기 점수 매김 시스템에 의해, 결정하는 단계, 및 제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌와 연관된 제2 프로파일에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치로, 사기 점수 매김 시스템에 의해, 전송하는 단계를 포함한다.

[0007] 또 다른 측면에 있어서, 컴퓨터 실행 가능한 명령어가 구현된 컴퓨터 판독가능 저장매체가 제공된다. 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치, 메시지 프로세서 컴퓨팅 장치에 연결된 제1 점수 매김 컴퓨팅 장치, 및 메시지 프로세서 컴퓨팅 장치에 연결된 제2 점수 매김 컴퓨팅 장치를 포함한 사기 위험 점수 매김 시스템의 하나 이상의 프로세서에 의해 실행되는 경우, 상기 컴퓨터 실행 가능한 명령어는 사기 위험 점수 매김 시스템이: 제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를 수신하고, 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는 지를 결정하며, 제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 제1 카드 보유자 계좌와 연관된 제1 프로파일에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송하고, 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신하며, 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는 지를 결정하고, 그리고 제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌와 연관된 제2 프로파일에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치로 전송하게 한다.

발명의 효과

[0008] 본 명세서에 서술된 시스템 및 방법은 전자 지불 처리 네트워크가 전자 지불 트랜잭션 신호의 매우 견고하고 고장에 내성이 있는 전자 지불 트랜잭션의 사기 점수 매김을 제공하여 지불 처리 네트워크가 특정 지불 트랜잭션이 사기성인지 여부를, 지불 구매가 이미 완료된 이후가 아니라, 트랜잭션이 처리되는 동안 결정할 수 있게 하는 기술적 이점을 제공한다. 보다 구체적으로, 본 명세서에 서술된 시스템 및 방법은 사기 점수 매김 시스템 상에서 유지 보수가 수행되는 동안에도 지불 네트워크가 그러한 사기 점수 매김을 수행할 수 있게 한다. 이와 같이 매우 신뢰할 수 있고 견고한 사기 점수 매김을 가능하게 함으로써, 본 명세서에 서술된 시스템 및 방법은 지불 네트워크 트랜잭션이 사기 때문에 거절되어야 하는 지불 트랜잭션을 수정(예를 들어, 조정을 적용)하기 위해 다른 방식으로 전송 및 처리될 필요가 있는 추가 트랜잭션의 양을 감소시켜 지불 네트워크 인프라가 보다 효율적으로 동작할 수 있게 한다.

도면의 간단한 설명

[0009] 도 1 내지 도 9는 본 명세서에 서술된 방법 및 시스템의 예시적인 실시예를 도시한다.

도 1은 머천트(merchants) 및 카드 발행사가 반드시 일대일 관계를 가질 필요가 없는 카드에 의한 지불 트랜잭션을 가능하게 하는 예시적인 다자 지불 카드 산업 시스템을 도시하는 개략도이다.

도 2는 본 발명의 일 예시적인 실시예에 따른 지불 처리 서버 컴퓨팅 장치, 사기 위험 점수 매김 컴퓨팅 장치, 및 복수의 컴퓨팅 장치를 포함하는 예시적인 지불 처리 시스템의 간략한 블록도이다.

도 3은 본 발명의 일 예시적인 실시예에 따른 복수의 컴퓨팅 장치를 포함한 지불 처리 시스템의 서버 구조의 상세한 블록도이다.

도 4는 본 발명의 일 예시적인 실시예에 따른 도 2 및 도 3에 도시된 클라이언트 시스템의 구성을 묘사한다.

도 5는 본 발명의 일 예시적인 실시예에 따른 도 2 및 도 3에 도시된 서버 시스템의 구성을 묘사한다.

도 6은 본 발명의 일 예시적인 실시예에 따른 사기 위험 점수 매김 서버에 의한 데이터의 라우팅 및 저장에 대한 데이터 흐름도이다.

도 7은 사기 위험 점수 매김 서버에 의해 처리되고 저장된 인구 통계(demographic) 및 비금융 정보(non-financial information)에 대한 데이터 흐름도이다.

도 8은 본 발명의 일 예시적인 실시예에 따른 잠재적인 사기에 대하여 전자 지불 트랜잭션을 점수 매김하는 사기 위험 점수 매김 서버에 의해 실시되는 예시적인 프로세스의 흐름도이다.

도 9는 도 2에 도시된 시스템에서 사용될 수 있는 하나 이상의 예시적인 컴퓨팅 장치의 컴포넌트의 도면이다.

발명을 실시하기 위한 구체적인 내용

[0010] 상기 시스템은 본 명세서에 서술된 잠재적인 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 사기 위험 점수 매김 시스템을 포함한다. 보다 상세하게는, 사기 위험 점수 매김 시스템은 전자 지불 트랜잭션이 사기성인지 결정할 때 방해를 제거하기 위해 분산 처리(distributed processing)를 사용한다. 사기 위험 점수 매김 시스템은 지불 네트워크와 통신하는 메시지 프로세서 컴퓨팅 장치를 포함한다. 사기 위험 점수 매김 시스템은 또한 지불 네트워크에 연결된 제1 점수 매김 컴퓨팅 장치 및 지불 네트워크에 연결된 제2 점수 매김 컴퓨팅 장치를 포함한다. 사기 위험 점수 매김 시스템은 제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를 수신하도록 구성된다. 추가적으로, 사기 위험 점수 매김 시스템은 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호(BIN, bank identification number)를 포함한 제1 카드 보유자 계좌 번호를 포함하는지를 결정한다. 사기 위험 점수 매김 시스템은 제1 데이터베이스에 저장된 제1 규칙 세트 및 제1 카드 보유자 계좌와 연관된 제1 프로파일에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송한다. 추가적으로, 사기 위험 점수 매김 시스템은 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신한다. 또한, 사기 위험 점수 매김 시스템은 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는지를 결정한다. 사기 위험 점수 매김 시스템은 제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌와 연관된 제2 프로파일에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치로 전송한다.

[0011] 일부 실시예에서, 사기 점수 매김 시스템은 제1 카드 보유자 계좌와 연관된 제1 프로파일을 업데이트하기 위해 제1 프로파일 업데이트 요청 메시지를, 제1 점수 매김 컴퓨팅 장치에 의해, 생성하도록 더 구성된다. 추가적으로, 사기 점수 매김 시스템은 제1 프로파일 업데이트 요청 메시지를 제2 점수 매김 컴퓨팅 장치로 전송한다. 뿐만 아니라, 사기 점수 매김 시스템은 제2 카드 보유자 계좌와 연관된 제2 프로파일을 업데이트 하기 위해 제2 프로파일 업데이트 요청 메시지를 생성하고, 상기 프로파일 업데이트 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송한다.

[0012] 일부 실시예에서, 사기 위험 점수 매김 시스템은 제1 점수 매김 컴퓨팅 장치가 동작하지 않는 지를 결정하고, 대비 프로세스(fallback process)를 수행한다. 구체적으로, 사기 위험 점수 매김 시스템은 제1 데이터베이스와 제2 데이터베이스 간에 데이터를 복제하는 임의의 프로세스를 종료한다. 추가적으로, 사기 위험 점수 매김 시스템은 홀수 및 짝수 번호가 부여된 은행 식별 번호와 연관된 프로파일 업데이트 요청 메시지를 제2 점수 매김 컴퓨팅 장치에서 생성하고 제1 점수 매김 컴퓨팅 장치가 동작 가능한 경우 제1 점수 매김 컴퓨팅 장치에 의한 처리를 위해 프로파일 업데이트 요청 메시지를 저장한다. 이어서, 사기 위험 점수 매김 시스템은 제1 점수 매김 컴퓨팅 장치가 동작하는 지를 결정하고 저장된 프로파일 업데이트 요청 메시지 모두를 제2 점수 매김 컴퓨팅 장

치에서 제1 점수 매김 컴퓨팅 장치로 전송한다. 추가적으로, 사기 위험 점수 매김 시스템은 제2 데이터베이스에 저장된 제2 규칙 세트를 제1 데이터베이스에 저장된 제1 규칙 세트와 동기화한다.

[0013] 일부 실시예에서, 인증 요청 메시지는 실시간 또는 근 실시간 인증 요청 메시지이다. 추가적으로, 일부 실시예에서, 사기 위험 점수 매김 시스템은 수신된 각각의 인증 요청 메시지에 대한 인증 응답 메시지를, 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치에 의해, 생성하도록 구성된다. 추가적으로, 사기 위험 점수 매김 시스템은 인증 요청 메시지에 기초하여 해당하는 카드 보유자 프로파일을 업데이트하고 업데이트된 카드 보유자 프로파일을 제1 데이터베이스 및 제2 데이트베이스에 저장한다.

[0014] 적어도 일부 실시예에서, 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치는 프로파일 업데이트 요청 메시지를 제1 데이터베이스 및 제2 데이터베이스에 저장하지 않고 프로파일 업데이트 요청 메시지에 응답하여 카드 보유자 프로파일을 업데이트한다. 추가적으로, 일부 실시예에서, 사기 점수 매김 시스템은 카드 보유자 인구 통계(demographics) 및 비금전적인(nonmonetary) 데이터를 제1 점수 매김 컴퓨팅 장치 및 제2 점수 매김 컴퓨팅 장치에서 수신하고, 수신된 카드 보유자의 인구 통계 및 비금전적 데이터를 사용하여 카드 보유자 프로파일을 업데이트한다.

[0015] 일부 실시예에서, 사기 위험 점수 매김 시스템은 제1 데이터베이스에 저장된 제1 규칙이 제2 데이터베이스에 저장된 제2 규칙과 매칭하지 않는 지를 결정함으로써 제1 데이터베이스 및 제2 데이터베이스 간의 규칙을 동기화하고, 제1 규칙을 제2 규칙과 동기화한다. 추가적으로, 일부 실시예에서, 사기 위험 점수 매김 시스템은 제1 데이터베이스 및 제2 데이터베이스 간에 데이터를 미리 정의된 인터벌(예를 들어, 하루에 한 번, 시간당 한 번, 분당 한 번, 또는 초당 한 번)에서 복제하도록 구성된다.

[0016] 보다 구체적으로, 본 발명은 분산 처리(예를 들어, 상호 처리(co-processing))를 사용하여 사기 위험 점수 매김 시스템(“사기 탐지 시스템”)에 대한 높은 이용가능성을 제공하는 아키텍처(architecture)를 제공한다. 인증 시스템(B24)은 다음과 같이 사기 위험 점수 매김 시스템의 기본 사이트 및 보조 사이트로 트랜잭션을 전송한다. 인증 시스템은 홀수 은행 식별 번호(“BINs”, bank identification numbers)가 있는 카드 보유자 계좌와 관련된 실시간(101) 및 근 실시간(near real time)(102) 트랜잭션 모두를 기본 사이트의 점수 매김 엔진으로 전송한다. 기본 사이트의 점수 매김 엔진(scoring engine)은 또한 짝수 BIN를 갖는 카드 보유자의 계좌에 대한 프로파일 업데이트(108) 트랜잭션을 수신한다. 인증 시스템은 짝수 BIN를 갖는 카드 보유자에 대한 트랜잭션을 보조 사이트의 보조 점수 매김 엔진으로 전송한다. 보조 점수 매김 엔진은 짝수 BIN를 갖는 카드 보유자 계좌에 대한 실시간(101) 및 근 실시간(102) 트랜잭션 모두를 수신한다. 보조 사이트에서의 점수 매김 엔진은 추가적으로 홀수 BIN를 갖는 카드 보유자 계좌에 대한 프로파일 업데이트(108) 트랜잭션을 수신한다. 사기 위험 점수 매김 시스템은 프로파일 업데이트 트랜잭션을 처리하고 카드 보유자 프로파일만 업데이트한다. 상기 업데이트는 이 시점에서 데이터베이스에 기록되지 않는다. 이것은 카드 보유자 프로파일이 두 사이트에 대한 최신 상태를 보장한다. 추가적으로, 사기 위험 점수 매김 시스템은 101/102 트랜잭션을 처리하고 해당하는 인증 응답을 지불 네트워크(128)로 송신하며, 그리고 사례 작성을 위해 카드 보유자 프로파일 및 데이터베이스를 업데이트할 것이다. 카드 보유자 인구 통계 및 비금전적 정보는 카드 보유자 인구 통계 정보를 업데이트하기 위해 기본 및 보조 사이트로 전달된다. 사례 매니지먼트를 지원하기 위해, 시스템 데이터는 기본 사이트와 보조 사이트 모두에서 이용가능하다. 사례 매니지먼트를 위해서, 기본 사이트 및 보조 사이트 모두가 이용가능하지만, 처리는 한 사이트에서만 이루어지며 다른 사이트는 상시 대기(hot standby) 모드에 있을 것이다. 데이터베이스 간의 복제는 양방향이고 1초 미만으로 동작한다. 규칙 복제자 프로세스는 변경을 위해 규칙 저장소를 지속적으로 모니터링한다. 규칙에 변경이 있는 경우, 규칙 복제자는 규칙을 반대 사이트에 복제하고 규칙 배치를 시뮬레이트하여 규칙 배치를 동기화한다.

[0017] 인프라 유지 보수로 인해 기본 사이트에서 보조 사이트로 페일오버(failover)하는 경우, 다음의 프로세스가 수행된다. 첫째, 인증 트랜잭션 트래픽이 기본 사이트에서 정지된다. 둘째, 사기 위험 점수 매김 서버, 사례 매니저, 및 전문가 애플리케이션이 기본 사이트에서 정지된다. 그 다음, 보조 사이트에서 기본 사이트로의 데이터베이스 복제가 정지된다. 추가적으로 기본 사이트 데이터베이스의 모든 데이터가 보조 사이트의 데이터베이스로 복제된다. 일단 모든 데이터가 기본 사이트에서 보조 사이트로 복제되면, 양방향 복제가 정지된다. 그 다음, 모든 홀수 BIN 트랜잭션은 보조 사이트로 라우팅된다. 이 시점에서, 보조 사이트가 실행될 것이고 그것은 기본 사이트로부터 라우팅되었던 모든 홀수 BIN 트랜잭션을 수신할 것이다. 그 다음, 홀수 및 짝수 BIN 프로파일 업데이트 트랜잭션은 기본 사이트 상의 프로파일을 업데이트하기 위해 생성된다. 이런 메시지들은 기본 사이트가 처리를 위해 이용 가능할 때까지 보류된다. 추가적으로, 웹 애플리케이션은 HTTP 요청을 보조 사이트에서 수신하여 사례를 처리하고 규칙을 배치한다. 일단 기본 사이트 유지 보수가 완료되면, 모든 프로파일 업데이트 트랜잭

션은 기본 사이트 프로파일을 업데이트하기 위해 릴리즈된다. 일단 프로파일이 업데이트되면, 상기 시스템은 규칙이 보조 사이트의 최신임을 확인한다. 일단 위의 프로세스가 완료되면, 기본 사이트는 트래픽을 정상화하기 위해 이용가능하다. 위의 동작가능한 페일 오버 프로세스를 사용하여, 사기 위험 점수 매김 시스템은 임의의 유지 보수 도중에 중단 없어 높은 이용 가능성이 있다.

[0018] 본 명세서에 서술된 방법 및 시스템은 컴퓨터 소프트웨어, 펌웨어, 하드웨어 또는 이들의 임의의 조합 또는 이들의 서브 세트를 포함하는 컴퓨터 프로그래밍 또는 엔지니어링 기술을 사용하여 실시될 수 있으며, 상기 기술 효과는 (a) 제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를 수신하는 단계; (b) 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는 지를 결정하는 단계; (c) 제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 제1 카드 보유자 계좌에 연관된 제1 프로파일에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송하는 단계; (d) 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신하는 단계; (e) 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는 지를 결정하는 단계; 및 (f) 제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌에 연관된 제2 프로파일에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치로 전송하는 단계 중 적어도 하나를 수행함으로써 성취된다. 본 명세서에 서술된 기술 효과는 분산 처리를 사용하여 컴퓨터 네트워크를 통해 전송된 전자 신호를 처리하는 기술 분야에 적용된다.

[0019] 본 명세서에 서술된 시스템 및 방법은 전자 지불 처리 네트워크가 전자 지불 트랜잭션 신호의 매우 견고하고 고장에 내성이 있는 전자 지불 트랜잭션의 사기 점수 매김을 제공하여 지불 처리 네트워크가 특정 지불 트랜잭션이 사기성인지 여부를, 지불 구매가 이미 완료된 이후가 아니라, 트랜잭션이 처리되는 동안 결정할 수 있게 하는 기술적 이점을 제공한다. 보다 구체적으로, 본 명세서에 서술된 시스템 및 방법은 사기 점수 매김 시스템 상에서 유지 보수가 수행되는 동안에도 지불 네트워크가 그러한 사기 점수 매김을 수행할 수 있게 한다. 이와 같이 매우 신뢰할 수 있고 견고한 사기 점수 매김을 가능하게 함으로써, 본 명세서에 서술된 시스템 및 방법은 지불 네트워크 트랜잭션이 사기 때문에 거절되어야 하는 지불 트랜잭션을 수정(예를 들어, 조정을 적용)하기 위해 다른 방식으로 전송 및 처리될 필요가 있는 추가 트랜잭션의 양을 감소시켜 지불 네트워크 인프라가 보다 효율적으로 동작할 수 있게 한다.

[0020] 본 명세서에 언급된 시스템이 사용자에 관한 개인 정보를 수집하거나 개인 정보를 사용할 수 있는 상황에서, 사용자는 프로그램 또는 기능이 사용자 정보를 수집하는지 여부를 제어하는 기회를 제공 받을 수 있다. 나아가, 특정 데이터는 저장되거나 사용되기 전에, 개인 식별 정보가 제거되도록, 하나 이상의 방식으로 취급될 수 있다. 예를 들어, 사용자의 신원이 개인 식별 정보가 사용자를 위해 결정되지 않도록 처리되거나 또는 사용자의 특정 위치가 결정되지 않도록 사용자의 지리적 위치는 위치 정보가 획득된 곳 (예: 도시, 우편 번호 또는 주 수준)으로 일반화될 수 있다. 따라서, 사용자는 정보가 사용자에 대해 어떻게 수집되고 시스템에 의해 사용되는지에 대한 제어를 가질 수 있다.

[0021] 본 명세서에 사용된, 용어 "트랜잭션 카드", "금융 트랜잭션 카드" 및 "지불 카드"는 신용 카드, 직불 카드(debit card), 선불 카드(prepaid card), 후불 카드(charge card), 회원 카드, 홍보 카드(promotional card), 단골 고객 카드(frequently flyer card), 신원 카드, 기프트 카드와 같은 임의의 적합한 트랜잭션 카드, 및/또는 모바일 폰, 스마트 폰, 휴대 정보 단말기(PDAs, personal digital assistants), 키 포브(key fobs) 및/또는 컴퓨터와 같은 지불 계좌 정보를 보유할 수 있는 임의의 다른 장치를 지칭한다. 각 유형의 트랜잭션 카드는 트랜잭션 수행을 위한 지불 방법으로 사용될 수 있다.

[0022] 일 실시예에서, 컴퓨터 프로그램이 제공되며, 프로그램은 컴퓨터 판독 가능 매체 상에 구현된다. 일 실시예에서, 상기 시스템은 서버 컴퓨터에 연결될 필요 없이 단일 컴퓨터 시스템상에서 실행된다. 또 다른 예시적인 실시예에서, 상기 시스템은 Windows® 환경에서 실행된다 (Windows는 워싱턴 주 레드먼드 시의 Microsoft Corporation의 등록 상표이다). 또 다른 실시예에서, 상기 시스템은 메인 프레임 환경 및 UNIX® 서버 환경에서 실행된다(UNIX는 뉴욕 주 뉴욕에 위치한 AT & T의 등록 상표이다). 이 애플리케이션은 유연하고 주요 기능을 손상시키지 않으면서 다양한 환경에서 실행되도록 설계되었다. 일부 실시예에서, 상기 시스템은 복수의 컴퓨팅 장치 사이에 분산된 다수의 컴포넌트를 포함한다. 하나 이상의 컴포넌트는 컴퓨터 판독 가능 매체에 구현된 컴퓨터 실행 가능 명령어의 형태일 수 있다. 상기 시스템 및 프로세스는 본 명세서에 서술된 특정 실시예에 한정되지 않는다. 나아가, 각 시스템 및 각 프로세스의 컴포넌트는 독립적으로 실행될 수 있으며 본 명세서에 서술된 다른 컴포넌트 및 프로세스와 분리될 수 있다. 각 컴포넌트 및 프로세스는 다른 어셈블리 패키지 및 프로세스와

함께 사용할 수도 있다.

[0023] 다음의 상세한 설명은 한정으로서가 아닌 예시적인 것으로서 본 발명의 실시예를 설명한다. 본 개시는 산업, 상업 및 주거 애플리케이션에서 제3자에 의한 금융 트랜잭션 데이터를 처리하는 일반적인 애플리케이션을 갖는 것으로 고려된다.

[0024] 본 명세서에 사용된 바와 같이, 단수로 인용되고 "a" 또는 "an"이라는 단어가 선행된 컴포넌트 또는 단계는 복수의 요소 또는 단계의 제외가 명시적으로 인용되지 않는 한, 복수의 요소 또는 단계를 제외하지 않는 것으로 이해되어야 한다. 또한, 본 발명의 "예시적인 실시예" 또는 "일 실시예"에 대한 언급은 인용된 특징을 포함하는 부가적인 실시예의 존재를 제외하는 것으로 의도되지 않는다.

[0025] 도 1은 머천트 및 카드 발행자가 반드시 일대일 관계를 가질 필요가 없는 카드에 의한 지불 트랜잭션을 가능하게 하는 예시적인 다자 지불 카드 시스템(120)을 도시한 개념도이다. 본 명세서는 마스터카드 지불 카드 시스템 지불 네트워크(MasterCard® payment card system payment network)(128)를 사용한 신용 카드 지불 시스템(또한 “상호 교환” 또는 “상호 교환 네트워크”라고 지칭됨)과 같은, 지불 카드 시스템(120)에 관한 것이다. 마스터카드 지불 카드 시스템 지불 네트워크(128)는 마스터카드 인터네셔널 인코퍼레이티드(MasterCard International Incorporated®)의 회원인 금융 기관 사이에 금융 트랜잭션 데이터를 교환하기 위해 마스터카드 인터네셔널 인코퍼레이티드가 공표한 독점적인 통신 표준이다. (마스터카드는 뉴욕의 퍼치스에 위치한 마스터카드 인터네셔널 인코퍼레이티드의 등록상표이다.)

[0026] 지불 카드 시스템(120)에서, 발행자(130)와 같은 금융 기관은 카드 보유자(122)의, 신용 카드 계좌 또는 직불 카드 계좌와 같은, 지불 계좌 카드를 발행한다. 상기 카드 보유자(122)는 지불 계좌 카드를 사용하여 머천트(124)로부터의 구매에 대한 지불을 입찰한다. 지불 계좌 카드로 지불을 수락하기 위해, 머천트(124)는 일반적으로 금융 지불 시스템의 일부인 금융 기관과의 계좌를 개설해야 한다. 이 금융 기관은 일반적으로 “머천트 은행” 또는 “취득 은행(acquirer bank)” 또는 단순히 “취득자(acquirer)”로 지칭된다. 카드 보유자(122)가 지불 계좌 카드(또한 금융 트랜잭션 카드로 알려짐)로 구입에 대한 지불을 입찰하는 경우, 머천트(124)는 구입 금액에 대한 취득자(126)로부터의 인증을 요청한다. 상기 요청은 전화를 통해 수행될 수 있으나, 일반적으로 상호 작용 지점(point-of-interaction) 단말의 사용을 통해 수행된다. 상기 상호 작용 지점 단말은 지불 계좌 카드 또는 EMV 칩의 마그네틱 스트라이프에서 카드 보유자의 계좌 정보를 읽고 취득자(126)의 트랜잭션 처리 컴퓨터와 전자적으로 통신한다. 대안적으로, 취득자(126)는 제3자가 대신 트랜잭션 처리를 수행하도록 인증할 수 있다. 이 경우, 상호 작용 지점 단말은 제3자와 통신하도록 구성될 것이다. 이러한 제3자는 일반적으로 “머천트 프로세서” 또는 “취득 프로세서(acquiring processor)”로 지칭된다. 일부 경우에서, 머천트(예를 들어, 머천트(124))는 카드 보유자(예를 들어, 카드 보유자(122))에 연관된 지불 카드 정보를 저장하고 지불 카드 자체로부터 카드 보유자의 계좌 정보를 읽는 대신에 저장된 지불 카드 정보를 사용하여 취득자(126)로부터의 승인을 요청한다.

[0027] 일부 실시예에서, 지불 네트워크(128)의 컴퓨터 시스템은 사기 위험 점수 매김 시스템(210)과 통신하며, 본 명세서에서 보다 상세하게 서술된 바와 같이, 사기 위험 점수 매김 시스템은 각각의 점수 매김 엔진을 갖는 다수의 사이트를 포함할 수 있다. 사기 위험 점수 매김 시스템(210)은 인증 요청 메시지를 지불 네트워크(128)의 컴퓨터로부터 수신하고 하나 이상의 규칙을 적용하여 트랜잭션이 사기성인 가능성 여부(예를 들어, 사기 위험 점수)를 결정한다. 보다 구체적으로, 사기 위험 점수 매김 시스템(210)은 카드 보유자의 프로파일, 트랜잭션 내역, 지출 패턴, 구입 위치, 구입 시간, 구입 금액 및/또는 기타 요인들에 기초하여 사기 위험 점수를 계산한다. 그 후, 사기 위험 점수 매김 시스템(210)은 사기 위험 점수를 지불 네트워크(128)의 컴퓨터로 전송한다. 사기 위험 점수에 기초하여, 지불 네트워크(128)의 컴퓨터는 인증 요청 메시지를 발행자(130)에게 전송하지 않고 트랜잭션을 거절하거나, 또는 사기 위험 점수와 함께 인증 요청 메시지를 발행자(130)에게 전송할 수 있다.

[0028] 보다 구체적으로, 후자의 경우에서, 지불 카드 시스템 지불 네트워크(128)를 사용하여, 취득자(126)의 컴퓨터들 또는 머천트 프로세서가 발행자(130)의 컴퓨터들과 통신하여 카드 보유자의 계좌(132)가 양호한지 여부 및 구입이 카드 보유자의 이용 가능한 신용 한도(credit line) 또는 계좌 잔액에 의해 커버되는지 여부를 결정할 것이다. 이들 결정에 기초하여 상기 인증을 위한 요청은 거절되거나 수락될 수 있다. 상기 요청이 수락되는 경우, 인증 코드가 머천트(124)로 발행된다.

[0029] 인증을 위한 요청이 수락되는 경우, 이용가능한 신용 한도 또는 이용가능한 카드 보유자의 계좌(132)의 잔액이 감소된다. 일반적으로, 요금은 카드 보유자의 계좌로 즉시 포스팅되지 않는다. 왜냐면 마스터카드 인터네셔널 인코퍼레이티드와 같은 은행카드 협회는 상품이 배송되거나 서비스가 배달될 때까지 머천트가 요금을 부과하거

나 “포획”할 수 없도록 하는 규칙을 발표했기 때문이다. “머천트가 상품 또는 서비스를 배송 또는 배달하는 경우, 머천트(124)는 예를 들어 상호 작용 단말 상의 적절한 데이터 입력 절차에 의해 트랜잭션을 포획한다. 카드 보유자가 그것이 포획되기 이전에 트랜잭션을 취소하는 경우, “보이드(void)”가 생성된다. 카드 보유자가 트랜잭션이 포획된 이후 상품을 리턴하는 경우, “신용(credit)”이 생성된다.

[0030] PIN 직불 카드 트랜잭션에서, 인증을 위한 요청이 발행자에 의해 승인되는 경우, 카드 보유자의 계좌(132)는 감소된다. 일반적으로, 요금은 카드 보유자의 계좌(132)로 즉시 포스팅된다. 그런 다음 은행카드 협회는 ATM의 경우 상품/서비스, 또는 정보 또는 현금의 유통을 위해 승인을 취득 프로세서로 전송한다.

[0031] 트랜잭션이 포획된 이후, 트랜잭션이 머천트(124), 취득자(126) 및 발행자(130) 사이에서 클리어되고 처분된다. 클리어링이란 당사자 간의 조화 목적으로 재무 데이터를 전달하는 것을 지칭한다. 처분(Settlement)은 트랜잭션과 관련된 머천트의 계좌, 취득자(126), 및 발행자(130) 간의 자금의 이체를 지칭한다.

[0032] 도 2는 본 발명의 일 실시예에 따른 예시적인 지불 처리 시스템(200)의 간략한 블록도이다. 예시적인 실시예에서, 시스템(200)은 지불 처리 서버 컴퓨팅 장치(202), 클라이언트 시스템(204) 또는 클라이언트 컴퓨팅 장치로 지칭되는, 지불 처리 서버 컴퓨팅 장치(202)에 연결된 복수의 클라이언트 서브 시스템들, 및 본 명세서에서 사기 위험 점수 매김 시스템으로 지칭되는 사기 위험 점수 매김 서버(210)를 포함한다. 일 실시예에서, 클라이언트 시스템(204)은 웹 브라우저를 포함한 컴퓨터로서, 지불 처리 서버 컴퓨팅 장치(202)는 인터넷을 사용하여 클라이언트 시스템(204)에 액세스 가능하다. 클라이언트 시스템(204)은 근거리 통신망(LAN) 및/또는 광역 통신망(WAN, wide area network), 다이얼-인 연결(dial-in connections), 케이블 모뎀, 무선 연결 및 전용 초고속 ISDN (special high-speed ISDN) 회선과 같은 네트워크를 포함한 많은 인터페이스를 통해 인터넷으로 상호 연결된다. 클라이언트 시스템(204)은 노트북 컴퓨터, 웹 기반 폰, 휴대 정보 단말기(PDA), 또는 다른 웹-연결가능한 장비와 같은 모바일 컴퓨팅 장치를 포함한, 인터넷에 상호 연결이 가능한 임의의 장치일 수 있다. 일 실시예에서, 클라이언트 컴퓨팅 장치(204)는 판매 시점(POS, point-of-sale) 장치, 카드 보유자 컴퓨팅 장치(예를 들어, 스마트폰, 태블릿, 또는 다른 컴퓨팅 장치), 또는 지불 처리 서버 컴퓨팅 장치(202)와 통신 가능한 임의의 다른 컴퓨팅 장치를 포함한다. 데이터베이스 서버(206)는 아래에서 보다 상세하게 서술되는 바와 같이, 다양한 문제에 관한 정보를 포함한 데이터베이스(208)에 연결된다. 일 실시예에서 데이터베이스(208)는 지불 처리 서버 컴퓨팅 장치(202) 상에 저장되고 클라이언트 시스템(204) 중 하나를 통해 지불 처리 서버 컴퓨팅 장치(202)에 로깅(logging)함으로써 클라이언트 시스템(204) 중 하나의 잠재 사용자에 의해 액세스될 수 있다. 임의의 대안적인 실시예에서, 데이터베이스(208)는 지불 처리 서버 컴퓨팅 장치(202)로부터 원격으로 저장되고 비-집중화(non-centralized)될 수 있다.

[0033] 도 3은 본 발명의 일 실시예에 따른 지불 처리 시스템(200)의 서버 구조의 예시적인 실시예의 상세한 블록도이다. 지불 처리 시스템(200)은 지불 처리 서버 컴퓨팅 장치(202), 클라이언트 시스템(204) 및 사기 위험 점수 매김 서버(210)를 포함한다. 지불 처리 서버 컴퓨팅 장치(202)는 데이터베이스 서버(206), 애플리케이션 서버(302), 웹 서버(304), 팩스 서버(306), 사전 서버(dictionary server)(308), 및 메일 서버(mail server)(310)를 포함한다. 디스크 저장부(312)는 데이터베이스 서버(206) 및 사전 서버(308)에 연결된다. 서버들(206, 302, 304, 306, 308 및 310)은 근거리 통신망(LAN)(314)으로 연결된다. 또한, 시스템 관리자의 워크스테이션(316), 사용자 워크스테이션(318) 및 감독자의 워크스테이션(320)은 LAN(314)에 연결된다. 대안적으로, 워크스테이션(316, 318 및 320)은 인터넷 링크를 사용하여 LAN(314)에 연결되거나 인트라넷을 통해 연결된다. 일부 실시예들에서, 사기 위험 점수 매김 서버(210)는 지불 처리 서버 컴퓨팅 장치(202)로부터 원격이지만, 통신에 관해서는 연결된다. 다른 실시예에서, 사기 위험 점수 매김 서버(210)는 지불 처리 서버 컴퓨팅 장치(202)에 통합된다.

[0034] 각 워크스테이션(316, 318 및 320)은 웹 브라우저를 갖는 개인용 컴퓨터이다. 워크스테이션에서 수행되는 기능은 통상적으로 각각의 워크스테이션(316, 318 및 320)에서 수행되는 것으로 설명됨에도 불구하고, 이러한 기능은 LAN(314)에 연결된 많은 개인용 컴퓨터 중 하나에서 수행될 수 있다. 워크 스테이션들(316, 318 및 320)은 LAN(314)에 액세스하는 개인들에 의해 수행될 수 있는 상이한 유형의 기능에 대한 이해를 용이하게 하기 위해서만 별도의 기능에 연관되고 있는 것으로 설명된다.

[0035] 지불 처리 서버 컴퓨팅 장치(202)는 인터넷 연결(326)을 사용하여 취득자(322) 및 발행자(324)를 포함한 다양한 엔티티들 및 제3자(예를 들어, 감사자(auditors))와 통신 가능하게 연결되도록 구성된다. 서버 시스템(202)은 또한 하나 이상의 머천트(336)와 통신 가능하게 연결된다. 상기 예시적인 실시예에서 통신은 인터넷을 사용하여 수행되는 것으로 설명되나, 임의의 다른 광대역 통신망(WAN) 유형 통신이 다른 실시예들에서 활용될 수 있다. 즉, 상기 시스템 및 프로세스는 인터넷을 사용하여 실시되는 것으로 제한되지 않는다. 또한, WAN(328) 보다는,

근거리 네트워크(314)가 WAN(328) 대신에 사용될 수 있다. 위에서 서술한 바와 같이, 일부 실시예들에서, 사기 위험 점수 매김 서버(210)는 지불 처리 서버 컴퓨팅 장치(202)로부터 원격이나, 통신 가능하게 연결된다. 다른 실시예들에서, 사기 위험 점수 매김 서버(210)는 지불 처리 서버 컴퓨팅 장치(202)에 통합된다.

[0036] 상기 예시적인 실시예에서, 워크스테이션(330)을 갖는 임의의 인증된 개인 또는 엔티티는 시스템(200)에 액세스할 수 있다. 클라이언트 시스템 중 적어도 하나는 원거리에 위치한 매니저 워크스테이션(322)을 포함한다. 워크스테이션들(330 및 332)은 웹 브라우저를 갖는 개인용 컴퓨터를 포함한다. 또한, 팩스 서버(306)는 전화 링크를 사용하여 클라이언트 시스템(332)을 포함한, 원격으로 위치된 클라이언트 시스템과 통신한다. 팩스 서버(306)는 다른 클라이언트 시스템들(316, 318 및 320)과 마찬가지로 통신하도록 구성된다.

[0037] 도 4는 클라이언트 컴퓨팅 장치(402)의 예시적인 구성을 설명한다. 클라이언트 컴퓨팅 장치(402)는 (도 3에 도시된) 클라이언트 시스템들(“클라이언트 컴퓨팅 장치들”)(204, 316, 318 및 320), 워크스테이션(330), 매니저 워크스테이션(332), 및 제3자 컴퓨팅 장치(334)를 포함할 수 있으나, 이에 제한되진 않는다.

[0038] 클라이언트 컴퓨팅 장치(402)는 실행 명령어를 위한 프로세서(405)를 포함한다. 일부 실시예에서, 실행 가능한 명령어는 메모리 영역(410)에 저장된다. 프로세서(405)는 하나 이상의 처리부(예를 들어, 멀티 코어 구성)를 포함할 수 있다. 메모리 영역(410)은 실행 가능한 명령어와 같은 정보 및/또는 다른 데이터가 저장되고 검색되게 하는 임의의 장치이다. 메모리 영역(410)은 하나 이상의 컴퓨터 판독가능 매체를 포함할 수 있다.

[0039] 클라이언트 컴퓨팅 장치(402)는 또한 정보를 사용자(401)(예를 들어, 카드 보유자(122))에게 제공하는, 적어도 하나의 미디어 출력 컴포넌트(415)를 포함한다. 미디어 출력 컴포넌트(415)는 정보를 사용자(401)에게 운반 가능한 임의의 컴포넌트이다. 일부 실시예에서, 미디어 출력 컴포넌트(415)는 비디오 어댑터 및/또는 오디오 어댑터와 같은 출력 어댑터(adapter)를 포함한다. 출력 어댑터는 프로세서(405)에 동작 가능하게 연결되고, 디스플레이 장치(예를 들어, 액정 디스플레이(LCD), 유기 발광 다이오드(OLED, organic light emitting diode) 디스플레이, 음극선관(CRT, cathode ray tube), 또는 “전자 잉크(electronic ink)” 디스플레이)와 같은 출력 장치에 동작 가능하게 연결될 수 있다.

[0040] 일부 실시예에서, 클라이언트 컴퓨팅 장치(402)는 사용자(401)로부터 입력을 수신하는 입력 장치(420)를 포함한다. 입력 장치(420)는 예를 들어, 키보드, 포인팅 장치, 마우스, 스타일러스(stylus), 터치 감지 패널(예를 들어, 터치 패드 또는 터치 스크린), 카메라, 자이로스코프, 가속도계, 위치 탐지기, 및/또는 오디오 입력 장치를 포함할 수 있다. 터치 스크린과 같은 단일 컴포넌트는 미디어 출력 컴포넌트(415)의 출력 장치 및 입력 장치(420) 모두로 기능할 수 있다.

[0041] 클라이언트 컴퓨팅 장치(402)는 또한 서버 시스템(202) 또는 머천트에 의해 동작되는 웹 서버와 같은 원격 장치에 통신 가능하게 연결 가능한 통신 인터페이스(425)를 포함할 수 있다. 통신 인터페이스(425)는 예를 들어, 유선 또는 무선 네트워크 어댑터, 또는 모바일 폰 네트워크(예를 들어, GSM(Global System for Mobile communications), 3G, 4G 또는 블루투스) 또는 다른 모바일 데이터 네트워크(예를 들어, WIMAX(Worldwide Interoperability for Microwave Access))와 함께 사용하기 위한 무선 데이터 송수신기를 포함할 수 있다.

[0042] 메모리 영역(410)에 저장되는 것은 예를 들어, 사용자 인터페이스를 미디어 출력 컴포넌트(415)를 통해 사용자 인터페이스에 제공하고, 선택적으로 입력을 입력 장치(420)로부터 수신 및 처리하기 위한 컴퓨터 판독 가능 명령어들이다. 사용자 인터페이스는 다른 가능성 중에서도 웹 브라우저 및 클라이언트 애플리케이션을 포함할 수 있다. 웹 브라우저는 사용자(401)가 미디어 및 머천트에 연관된 웹 서버로부터의 웹 사이트 또는 웹 페이지 상에 통상적으로 구현된 다른 정보를 표시하고 상호 작용할 수 있게 한다. 클라이언트 애플리케이션은 사용자(401)가 예를 들어 머천트에 연관된, 서버 애플리케이션과 상호 작용하게 한다.

[0043] 도 5는 서버 컴퓨팅 장치(502)의 예시적인 구성을 설명한다. 서버 컴퓨팅 장치(502)는 (도 2 및 도 3에 도시된) 지불 처리 서버 컴퓨팅 장치(502), 데이터베이스 서버(206), 애플리케이션 서버(302), 웹 서버(304), 팩스 서버(306), 사전 서버(308), 메일 서버(310), 및 사기 위험 점수 매김 서버(210)에 포함된 하나 이상의 컴퓨팅 장치를 대표한다.

[0044] 서버 컴퓨팅 장치(502)는 명령어를 실행하는 프로세서(504)를 포함한다. 명령어는, 예를 들어 메모리 영역(506)에 저장될 수 있다. 프로세서(504)는 (예를 들어, 멀티 코어 구성의) 하나 이상의 처리부를 포함할 수 있다.

[0045] 프로세서(504)는 서버 컴퓨팅 장치(502)가 클라이언트 컴퓨팅 장치(402) 또는 다른 서버 컴퓨팅 장치(502)와 같은 원격 장치와 통신 가능하도록 통신 인터페이스(508)에 동작 가능하게 연결된다. 예를 들어, 통신 인터페이스(508)는 도 2 및 도 3에 도시된 것처럼, 클라이언트 시스템(204)으로부터의 요청을 인터넷을 통해 수신할 수 있

다.

[0046] 프로세서(504)는 또한 저장 장치(510)에 동작 가능하게 연결된다. 저장 장치(510)는 데이터를 저장 및/또는 검색하기 위해 적합한 임의의 컴퓨터 동작 하드웨어(computer-operated hardware)이다. 일부 실시예에서, 저장 장치(510)는 서버 컴퓨팅 장치(502)에 통합된다. 예를 들어, 서버 컴퓨팅 장치(502)는 저장 장치(510)로 하나 이상의 하드 디스크 드라이버를 포함할 수 있다. 일부 실시예에서, 저장 장치(510)는 서버 컴퓨팅 장치(502)의 외부에 있고 복수의 서버 컴퓨팅 장치(502)에 의해 액세스될 수 있다. 예를 들어, 저장 장치(510)는 RAID(redundant array of inexpensive disks) 구성에 하드 디스크 또는 솔리드 스테이트 디스크와 같은 다수의 저장 장치를 포함할 수 있다. 저장 장치(510)는 SAN(storage area network) 및/또는 NAS(network attached storage) 시스템을 포함할 수 있다.

[0047] 일부 실시예에서, 프로세서(504)는 저장 장치(510)에 저장 인터페이스(512)를 통해 동작 가능하게 연결된다. 저장 인터페이스(512)는 저장 장치(510)에 대한 액세스를 프로세서(504)에 제공할 수 있는 임의의 컴포넌트다. 저장 인터페이스(512)는, 예를 들어 ATA(Advanced Technology Attachment) 어댑터, SATA(Serial ATA) 어댑터, SCSI(Small Computer System Interface) 어댑터, RAID 컨트롤러, SAN 어댑터, 네트워크 어댑터 및/또는 저장 장치(510)에 대한 액세스를 프로세서(504)에 제공하는 임의의 컴포넌트를 포함할 수 있다.

[0048] 메모리 영역(410 및 506)은 동적 RAM(dynamic RAM) 또는 정적 RAM(static RAM)과 같은 RAM(random access memory), ROM(read-only memory), ERPROM(erasable programmable read-only memory), EEPROM(electrically erasable programmable read-only memory), 및 NVRAM(non-volatile RAM)을 포함할 수 있으나, 이에 제한되진 않는다. 위의 메모리 유형은 단지 예시적인 것으로서, 컴퓨터 프로그램의 저장을 위해 사용할 수 있는 메모리 유형을 제한하진 않는다.

[0049] 도 6은 사기 위험 점수 매김 서버(210)에 의한 데이터의 라우팅 및 저장에 대한 데이터 흐름도(600)이다. 사기 위험 점수 매김 서버(210)는 제1(“기본(primary)”) 사이트(602)와 제2(“보조(secondary)”) 사이트(604)를 포함한다. 또한, 적어도 일부 실시예에서, 사기 위험 점수 매김 서버(210)는 홀수가 부여된 은행 식별 번호(BIN, bank identification number)를 포함한 카드 보유자 계좌(132)에 관련된 제1 트랜잭션 메시지(620)(예를 들어, 인증 요청 메시지)를 제1 점수 매김 엔진(608)으로 보내고, 짝수가 부여된 BIN 을 포함한 카드 보유자의 계좌(132)에 관련된 제2 트랜잭션 메시지(622)(예를 들어, 인증 요청 메시지)를 제2 점수 매김 엔진(610)으로 보내는 인증 시스템(601)을 포함한다. 일부 실시예에서, 인증 시스템(601)은 지불 처리 서버 컴퓨팅 장치(202)에 포함된다. 적어도 일부 실시예에서, 트랜잭션 메시지(620 및 622)는 실시간(101 트랜잭션 메시지) 또는 근실시간(즉, 102 트랜잭션 메시지)이다. 제1 점수 매김 엔진(608)은 제1 데이터베이스(612)에 연결되고 제1 트랜잭션 메시지(620)에 적어도 부분적으로 기초하여, 카드 보유자 프로파일, 트랜잭션 내역, 및 사기 위험 점수를 제1 데이터베이스(612)에 저장한다. 유사하게, 제2 점수 매김 엔진(610)은 제2 데이터베이스(614)에 연결되고 카드 보유자 프로파일, 트랜잭션 내역, 및 사기 위험 점수를 제2 데이터베이스(614)에 저장한다. 데이터는 제1 데이터베이스(612) 및 제2 데이터베이스(614) 사이에서 전송된 복제 메시지(634)를 통해 두 데이터베이스 사이에서 복제된다. 적어도 일부 실시예에서, 데이터베이스(208)(도 2)는 하나 이상의 제1 데이터베이스(612) 및 제2 데이터베이스(614)를 포함한다.

[0050] 사기 위험 점수 매김 서버(210)는 추가적으로 메시지 프로세서(606)를 포함한다. 상기 메시지 프로세서(606)는 인구 통계(demographics) 메시지와 같은, 제1 비-금융 요청 메시지(616)를 제1 점수 매김 엔진(608)으로 전송하고 인구 통계와 같은 제2 비-금융 요청 메시지(618)를 제2 점수 매김 엔진(610)으로 전송한다. 적어도 일부 실시예에서, 제1 비금융 요청 메시지(616) 및 제2 비금융 요청 메시지(618)는 동일하다. 제1 점수 매김 엔진(608)은 짝수 BIN와 관련된 트랜잭션에 대한 제1 프로파일 업데이트 메시지(624)(즉, 108 메시지)를 수신하고 제2 점수 매김 엔진(610)은 홀수 BIN와 관련된 트랜잭션에 대한 제2 프로파일 업데이트 메시지(626)를 수신한다. 추가적으로, 제1 점수 매김 엔진(608)은 트랜잭션(예를 들어, 제1 트랜잭션(620))에 대한 사기 위험 점수를 결정하기 위해 제1 규칙(628)을 액세스하고 업데이트하며, 제2 점수 매김 엔진(610)은 트랜잭션(예를 들어, 제2 트랜잭션(622))에 대한 사기 위험 점수를 결정하기 위해 제2 규칙(630)을 액세스하고 업데이트한다. 사기 위험 점수 매김 서버(210)는 추가적으로 제1 규칙(628)을 제2 규칙(630)으로 복제하는 규칙 복제자(632)를 포함한다.

[0051] 위에서 서술한 바와 같이, 사기 위험 점수 매김 서버(210)는 계산된 사기 점수를 각각의 제1 점수 매김 엔진(608) 및 제2 점수 매김 엔진(610)으로부터 지불 네트워크의 지불 처리 서버 컴퓨팅 장치(202)로 전송한다. 일부 실시예에서, 지불 처리 컴퓨팅 장치(202)는 계산된 사기 점수가 미리 정의된 임계 값을 초과하는 것을 결정하고 인증 요청 메시지를 해당 발행자(130)에게 전송하지 않고 해당 지불 트랜잭션을 거부한다. 일부 실시예에

서, 지불 처리 서버 컴퓨팅 장치(202)는 인증 요청 메시지와 함께 사기 위험 점수를 발행자(130)로 전송하여 상기 트랜잭션이 사기일 가능성을 발행자에게 알려준다. 사기 위험 점수 매김 서버(210)가 각각의 점수 매김 엔진(608 및 610)을 갖는 다수의 사이트(602 및 604)를 포함한다면, 사기 위험 점수 매김 서버(210)가 하나의 점수 매김 엔진을 갖는 단 하나의 사이트를 포함하는 경우 보다 견고하고 신뢰성이 있다. 추가적으로, 사기 위험 점수 매김 서버(210)는, 본 명세서에서 보다 상세하게 서술되는, 사이트(602 및 604) 중 하나가, 예를 들어 유지보수로 인하여, 작동 불능이 되는 경우에 방해 없는 사기 위험 점수 매김 서비스를 제공하는 대비(fallback)(“페일오버(failover)”) 프로세스를 수행하도록 구성된다.

[0052] 도 7 은 사기 위험 점수 매김 서버(210)에 의해 처리되고 저장된 인구 통계 및 비금융 정보에 대한 데이터 흐름도(700)이다. 사기 위험 점수 매김 서버(210)는 위에서 서술한 바와 같이, 인구 통계 및 비금융 정보를 사용하여 카드 보유자 프로파일(916)을 업데이트하고, 사기 위험 점수 매김 서버(210)에 의해 사용되어 사기 위험 점수를 계산한다. 카드 매니지먼트 시스템(702), 예를 들어 지불 처리 서버 컴퓨팅 장치(202)는 비금융 메시지(예를 들어, 제1 비금융 요청(616))를 비금융 메시지 큐(704)로 전송한다. 메시지 프로세서(606)는 비금융 요청 메시지(616)를 사기 큐 매니저(706)로 전송한다. 도 6에 참조로 서술된 바와 같이, 사기 큐 매니저는 추가적으로 하나 이상의 핸드쉐이크 메시지(708)를 제1 점수 매김 엔진(608)으로부터 수신하고 비금융 요청(616)을 제1 점수 매김 엔진(608)으로 전송한다. 추가적으로, 도 6에 도시된 바와 같이, 제1 점수 매김 엔진(608)은 비금융 요청 메시지(616)에 적어도 부분적으로 기초하여 제1 데이터베이스(612)를 액세스하고 업데이트한다.

[0053] 도 8은 잠재적인 사기에 대한 전자 지불 트랜잭션을 점수 매김하는 사기 위험 점수 매김 서버(210)에 의해 실시된 예시적인 프로세스(800)의 흐름도이다. 사기 위험 점수 매김 서버(210)는 제1 지불 트랜잭션에 대한 제1 인증 요청 메시지(예를 들어, 제1 트랜잭션 메시지(620))를 수신한다(802). 추가적으로, 사기 위험 점수 매김 서버(210)는 제1 인증 요청 메시지(620)가 홀수가 부여된 BIN을 포함한 제1 카드 보유자 계좌 번호(132)를 포함하는지를 결정한다(804). 추가적으로, 사기 위험 점수 매김 서버(210)는, 제1 데이터베이스에 의해 저장된 제1 규칙 세트(예를 들어, 제1 규칙(628)) 및 제1 카드 보유자 계좌(132)에 연관된 제1 프로파일(예를 들어 프로파일(916))에 기초한 제1 인증 요청 메시지(620)에 대한 제1 사기 위험 점수(예를 들어, 사기 위험 점수(920))를 생성하기 위해, 제1 인증 요청 메시지(620)를 제1 점수 매김 컴퓨팅 장치(예를 들어, 제1 점수 매김 엔진(608))로 전송한다(806).

[0054] 추가적으로, 사기 위험 점수 매김 서버(210)는 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지(예를 들어, 제2 트랜잭션 메시지(622))를 수신한다. 또한, 사기 위험 점수 매김 서버(210)는 제2 인증 요청 메시지(622)가 짝수 번호가 부여된 BIN을 포함하는 제2 카드 보유자 계좌 번호(132)를 포함하는 지를 결정한다(810). 추가적으로, 사기 위험 점수 매김 서버(210)는, 제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌(132)에 연관된 제2 프로파일(916)에 기초한 제2 인증 요청 메시지(622)에 대한 제2 사기 위험 점수(920)를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치(예를 들어, 제2 점수 매김 엔진(610))로 전송한다(812).

[0055] 일부 실시예에서, 사기 점수 매김 시스템은 제1 카드 보유자 계좌(132)에 연관된 제1 프로파일(예를 들어, 카드 보유자 프로파일(916))을 하기 위해 제1 프로파일 업데이트 요청 메시지(예를 들어, 프로파일 업데이트 요청 메시지(624))를, 제1 점수 매김 컴퓨팅 장치(예를 들어, 제1 점수 매김 엔진(608))에 의해, 생성하도록 더 구성된다. 추가적으로, 사기 점수 매김 시스템(210)은 제1 프로파일 업데이트 요청 메시지(624)를 제2 점수 매김 컴퓨팅 장치(예를 들어, 제2 점수 매김 엔진(610)으로 전송한다. 또한, 사기 점수 매김 시스템은 제2 카드 보유자 계좌(132)에 연관된 제2 프로파일(예를 들어, 카드 보유자 프로파일(916))을 업데이트하기 위해 제2 프로파일 업데이트 요청 메시지(예를 들어, 프로파일 업데이트 요청 메시지(626))를, 제2 점수 매김 컴퓨팅 장치(예를 들어, 제2 점수 매김 엔진(610))에 의해, 생성하고, 프로파일 업데이트 요청 메시지(626)를 제1 점수 매김 컴퓨팅 장치(608)로 전송한다.

[0056] 일부 실시예에서, 사기 위험 점수 매김 시스템(210)은 제1 점수 매김 컴퓨팅 장치(608)가 동작하는지 결정하고, 대비 프로세스(fallback process)를 수행한다. 구체적으로, 사기 위험 점수 매김 시스템(210)은 제1 데이터베이스(612) 및 제2 데이터베이스(614) 간에 데이터를 복제하기 위한 임의의 프로세스를 종료한다. 추가적으로, 사기 위험 점수 매김 시스템(210)은 짝수 번호가 부여된 은행 식별 번호 및 홀수 번호가 부여된 은행 식별 번호 모두에 연관된 프로파일 업데이트 요청 메시지를 제2 점수 매김 컴퓨팅 장치(610)에서 생성하고, 제1 점수 매김 컴퓨팅 장치(608)가 동작하는 경우 제1 점수 매김 컴퓨팅 장치(608)에 의한 처리를 위해 프로파일 업데이트 요청 메시지(624 및 626)를 저장한다. 이어서, 사기 위험 점수 매김 시스템(210)은 제1 점수 매김 컴퓨팅 장치(210)가 동작하는지를 결정하고 저장된 프로파일 업데이트 요청 메시지 모두(624 및 626)를 제2 점수 매김 컴퓨

팅 장치(610)로부터 제1 점수 매김 컴퓨팅 장치(608)로 전송한다. 추가적으로, 사기 위험 점수 매김 시스템(210)은 제2 데이터베이스에 저장된 제2 규칙 세트(예를 들어, 제2 규칙(630))을 제1 데이터베이스에 저장된 제1 규칙 세트(예를 들어, 제1 규칙(628))와 동기화한다.

[0057] 일부 실시예에서, 인증 요청 메시지(620 및 622)는 실시간 또는 근 실시간 인증 요청 메시지이다. 추가적으로, 일부 실시예에서, 사기 위험 점수 매김 시스템(210)은 제1 점수 매김 컴퓨팅 장치(608) 및 제2 점수 매김 컴퓨팅 장치(610)에 의해 수신된 각각의 인증 요청 메시지에 대한 인증 응답 메시지를 생성하도록 구성된다. 추가적으로, 사기 위험 점수 매김 시스템(210)은 인증 요청 메시지에 기초하여 대응하는 카드 보유자 프로파일(916)을 업데이트하고, 업데이트된 카드 보유자 프로파일을 제1 데이터베이스(612) 및 제2 데이터베이스(614)에 저장한다.

[0058] 적어도 일부 실시예에서, 제1 점수 매김 컴퓨팅 장치(608) 및 제2 점수 매김 컴퓨팅 장치(610)는 프로파일 업데이트 요청 메시지(624 및 626)에 응답하여 카드 보유자 프로파일(916)을 업데이트하고 프로파일 업데이트 요청 메시지를 제1 데이터베이스(612) 및 제2 데이터베이스(614)에 저장하지 않는다. 추가적으로, 일부 실시예에서, 사기 위험 점수 매김 시스템(210)은 카드 보유자 인구 통계(demographics) 및 비통화(nonmonetary) 데이터(616 및 618)를 제1 점수 매김 컴퓨팅 장치(608) 및 제2 점수 매김 컴퓨팅 장치(610)에서 수신하고, 수신된 카드 보유자 인구 통계 및 비통화 데이터(616 및 618)를 사용하여 카드 보유자 프로파일(916)을 업데이트한다.

[0059] 일부 실시예에서, 사기 위험 점수 매김 시스템(210)은 제1 데이터베이스에 저장된 제1 규칙(628)이 제2 데이터베이스에 저장된 제2 규칙(630)과 매칭하지 않는지를 결정함으로써 제1 데이터베이스(612) 및 제2 데이터베이스(614) 사이의 규칙을 동기화하고 제1 규칙을 제2 규칙과 동기화한다. 일부 실시예에서, 사기 위험 점수 매김 시스템(210)은 제1 데이터베이스(612) 및 제2 데이터베이스(614) 간의 데이터(예를 들어, 복제 메시지(634))를 미리 정의된 인터벌에서 복제하도록 구성된다.

[0060] 도 9는 설명된 시스템 및 방법의 실시예에서 사용될 수 있는 하나 이상의 예시적인 컴퓨팅 장치, 예를 들어 사기 위험 점수 매김 서버(210)의 컴포넌트의 도면(900)이다. 도 9는 적어도 일부 실시예에서 제1 데이터베이스(612), 제1 규칙 세트(628), 제2 데이터베이스(614) 및 제2 규칙 세트(630)를 나타내는, 데이터베이스(208)의 데이터의 구성을 더 도시한다. 데이터베이스(208)는 특정 임무를 수행하는, 사기 위험 점수 매김 서버(210) 내의 몇몇 개별 컴포넌트와 통신한다.

[0061] 사기 위험 점수 매김 서버(210)는 제1 지불 트랜잭션에 대한 제1 인증 요청 메시지를 수신하는 제1 인증 요청 수신 컴포넌트(902)를 포함한다. 추가적으로, 사기 위험 점수 매김 서버(210)는 제1 인증 요청 메시지가 홀수 번호가 부여된 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는지를 결정하는 홀수 BIN 결정 컴포넌트(904)를 포함한다. 또한, 사기 위험 점수 매김 서버(210)는 제1 데이터베이스에 의해 저장된 제1 규칙 세트 및 제1 카드 보유자 계좌에 연관된 제1 프로파일에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송하는 제1 인증 요청 전송 컴포넌트(906)를 포함한다. 추가적으로, 사기 위험 점수 매김 서버(210)는 제2 지불 트랜잭션에 대한 제2 인증 요청 메시지를 수신하는 제2 인증 요청 수신 컴포넌트(908)를 수신한다. 사기 위험 점수 매김 서버(210)는 제2 인증 요청 메시지가 짝수 번호가 부여된 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는 지를 결정하는 짝수 BIN 결정 컴포넌트(910)를 포함한다. 추가적으로, 사기 위험 점수 매김 서버(210)는 제2 데이터베이스에 의해 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌에 연관된 제2 프로파일에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치로 전송하는 제2 인증 요청 전송 컴포넌트를 포함한다.

[0062] 예시적인 실시예에서, 데이터베이스(208)의 데이터는, 트랜잭션 내역 섹션(914), 카드 보유자 프로파일 섹션(916), 규칙 섹션(918) 및 사기 위험 점수 섹션(920)을 포함하는 복수의 섹션으로 구획되나, 이에 제한되진 않는다. 데이터베이스(208)에 저장된 이들 섹션은 상술한 기능 및 프로세스에 따라 정보를 검색하기 저장하기 위해 상호 접속된다.

[0063] 본 명세서에서 사용되는 프로세서라는 용어는 중앙 처리 장치, 마이크로프로세서, 마이크로 컨트롤러, 축소 명령 세트 회로 (RISC, reduced instruction set circuits), 주문형 집적 회로 (ASIC, application specific integrated circuits), 논리 회로 및 본 명세서에 설명된 기능을 실행할 수 있는 임의의 다른 회로 또는 프로세서를 지칭한다.

[0064] 본 명세서에 사용되는, "소프트웨어" 및 "펌웨어"라는 용어는 상호 교환 가능하며, RAM 메모리, ROM 메모리,

EPROM 메모리, EEPROM 메모리 및 비휘발성 RAM(NVRAM, non-volatile RAM) 메모리를 포함하는, 프로세서 (405, 504)에 의한 실행을 위해 메모리에 저장된 임의의 컴퓨터 프로그램을 포함한다. 상기 메모리 유형은 단지 예일 뿐이며, 따라서 컴퓨터 프로그램의 저장에 사용 가능한 메모리의 유형에 대하여 제한하지 않는다.

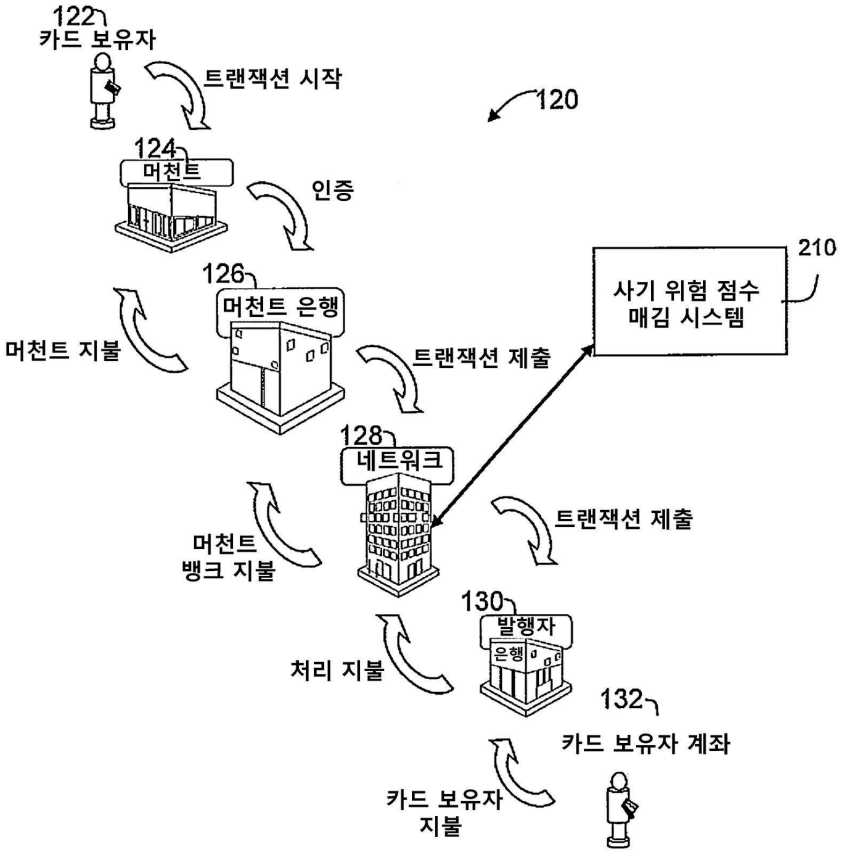
[0065] 전술한 명세서에 기초하여 이해되는 바와 같이, 위에서 서술한 본 발명의 실시예는 컴퓨터 소프트웨어, 펌웨어, 하드웨어 또는 이들의 임의의 조합 또는 서브 세트를 포함하는 컴퓨터 프로그래밍 또는 엔지니어링 기술을 이용하여 구현될 수 있다. 컴퓨터 판독 가능 및/또는 컴퓨터 실행 가능 명령어를 갖는 이러한 임의의 결과적인 컴퓨터 프로그램은 하나 이상의 컴퓨터 판독 가능 매체 내에 구현되거나 제공되어, 논의된 본 발명의 실시예에 따른 컴퓨터 프로그램 제품, 즉 제조 물품(article of manufacture)을 생성 할 수 있다. 이러한 컴퓨터 프로그램 (프로그램, 소프트웨어, 소프트웨어 응용 또는 코드로도 알려짐)은 프로그램 가능 프로세서에 대한 머신 명령어를 포함하며, 고도한 절차 및/또는 객체 지향 프로그래밍 언어, 및/또는 어셈블리/머신 언어에서 구현될 수 있다. 본 명세서에 사용된 바와 같이, "머신 판독 가능 매체", "컴퓨터 판독 가능 매체" 및 "컴퓨터 판독 가능 매체"라는 용어는 머신 명령어를 머신 판독가능 신호로서 수신하는 머신 판독 가능 매체를 포함한, 머신 명령어 및/또는 데이터를 컴퓨터 시스템에 제공하기 위해 사용되는 임의의 컴퓨터 프로그램 제품, 기구 및/또는 장치(예를 들어, 자기 디스크, 광학 디스크, 메모리, 프로그램 가능 논리 소자(PLDs))를 지칭한다. 그러나, "머신 판독 가능 매체", "컴퓨터 판독 가능 매체" 및 "컴퓨터 판독 가능 매체"는 일시적인 신호를 포함하지 않는다 (즉, 그들은 "비일시적(non-transitory)"이다). "머신 판독 가능 신호"라는 용어는 머신 명령어 및/또는 데이터를 프로그램 가능 프로세서에 제공하기 위해 사용되는 모든 신호를 지칭한다.

[0066] 위에서 서술한 방법 및 시스템의 실시예는 전자 지불 트랜잭션이 사기성인지 여부를 결정할 때 방해를 제거하기 위해 분산 처리를 사용하는 사기 위험 점수 매김 시스템을 제공한다. 그 결과, 본 명세서에서 서술된 방법 및 시스템은 전자 지불 처리 네트워크가 전자 지불 트랜잭션 신호의 매우 견고하고 고장에 내성이 있는 사기 점수 매김을 제공할 수 있게 하여 지불 처리 네트워크가 지불 구매가 이미 완료된 후가 아니라, 트랜잭션이 처리되는 동안 특정 지불 트랜잭션이 사기성인지 여부를 결정할 수 있게 한다. 보다 구체적으로, 본 명세서에서 서술된 시스템 및 방법은 사기 위험 점수 매김 시스템에서 유지 보수가 수행되는 동안에도 지불 네트워크가 그러한 사기 위험 점수 매김을 수행할 수 있게 한다. 이와 같이 매우 신뢰성 있고 견고한 사기 점수 매김을 제공함으로써, 본 명세서에 서술된 시스템 및 방법은 사기 때문에 거절되어야 하는 지불 트랜잭션을 수정(예를 들어, 조정을 적용)하기 위해 다른 방식으로 전송 및 처리될 필요가 있는 추가 트랜잭션의 양을 감소시켜 지불 네트워크 인프라가 보다 효율적으로 동작할 수 있게 한다.

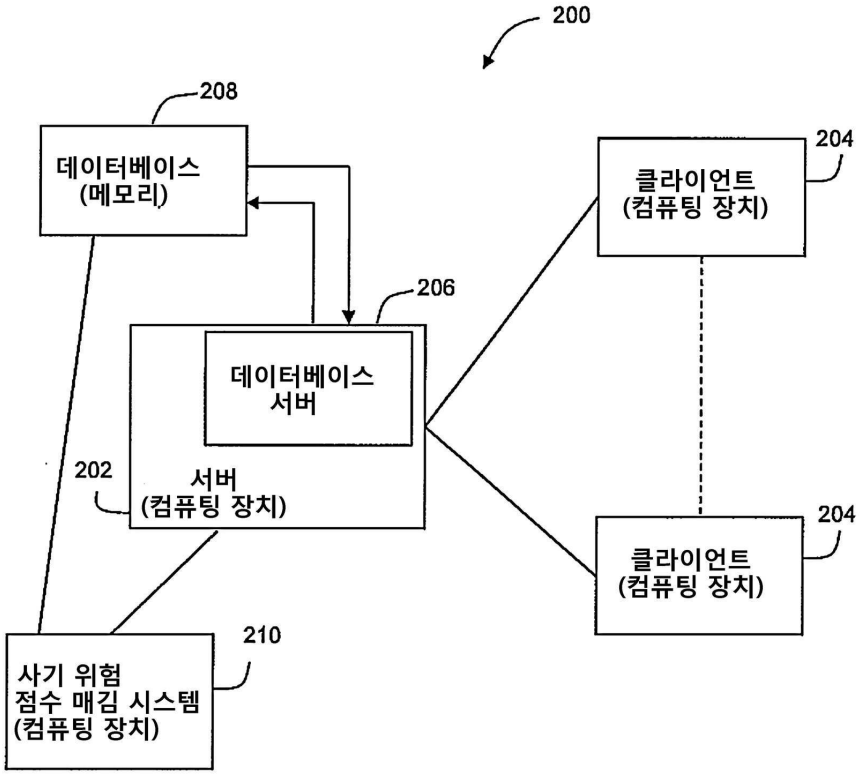
[0067] 이 작성된 설명은 임의의 장치 또는 시스템을 제작 및 사용하고 임의의 통합된 방법을 수행하는 것을 포함하여, 통상의 기술자가 본 발명을 실시할 수 있게 하는, 최적의 형태를 포함한 예를 사용한다. 본 발명의 특허 가능한 범위는 특허 청구 범위에 의해 정의되며, 통상의 기술자에게 발생할 수 있는 다른 예를 포함할 수 있다. 그러한 다른 예는 청구항의 문자 그대로의 언어와 다르지 않은 구조적 요소를 갖는 경우 또는 청구 범위의 문자 그대로의 언어와 실질적이지 않은 차이를 갖는 등가의 구조 요소를 포함하는 경우 청구 범위 내에 있는 것으로 의도된다.

도면

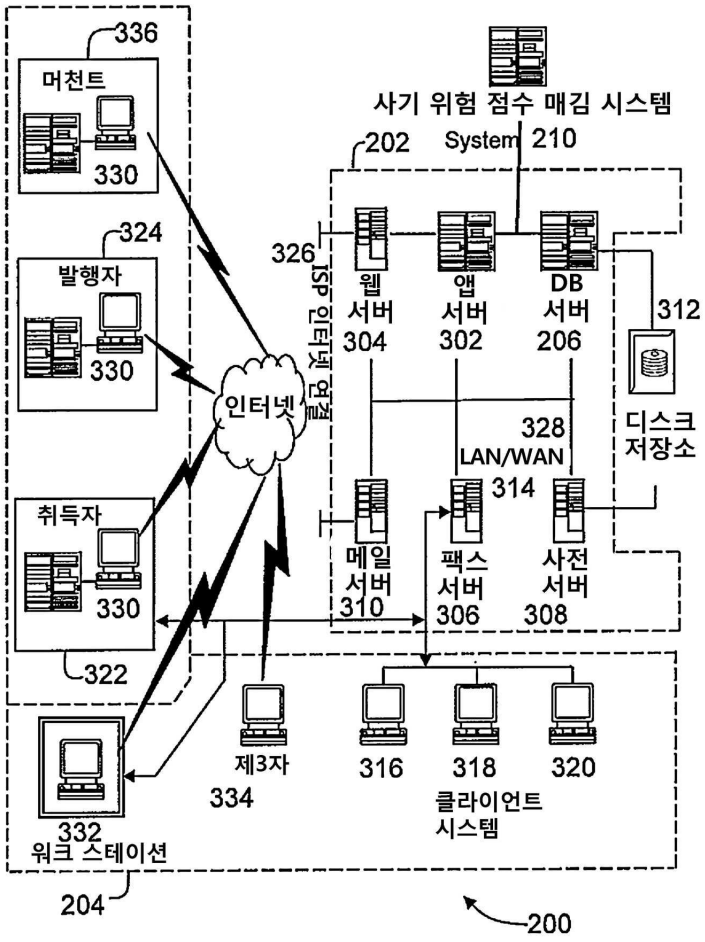
도면1


122
카드 보유자
트랜잭션 시작
120
124
머천트
인증
126
머천트 은행
210
사기 위험 점수
매김 시스템
머천트 지불
트랜잭션 제출
128
네트워크
트랜잭션 제출
머천트
뱅크 지불
130
발행자
은행
처리 지불
132
카드 보유자 계좌
카드 보유자
지불

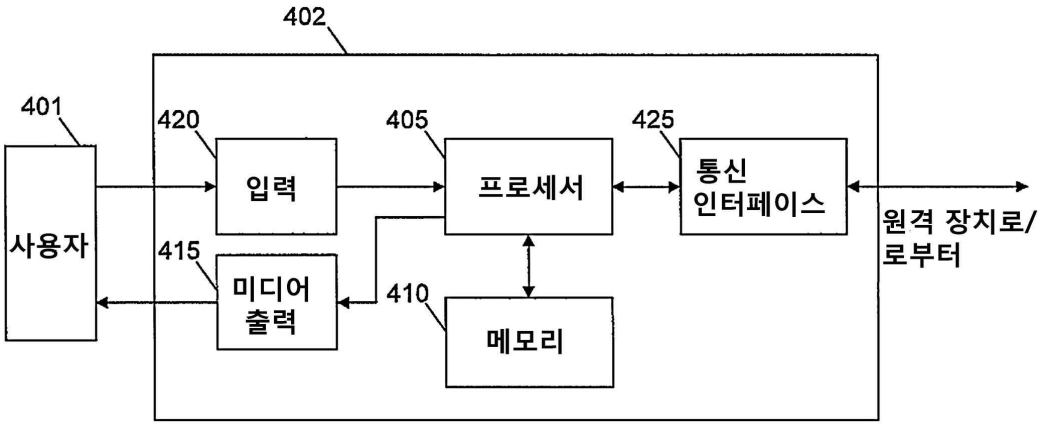
도면2


200
208
데이터베이스
(메모리)
204
클라이언트
(컴퓨팅 장치)
206
데이터베이스
서버
202
서버
(컴퓨팅 장치)
204
클라이언트
(컴퓨팅 장치)
210
사기 위험
점수 매김 시스템
(컴퓨팅 장치)

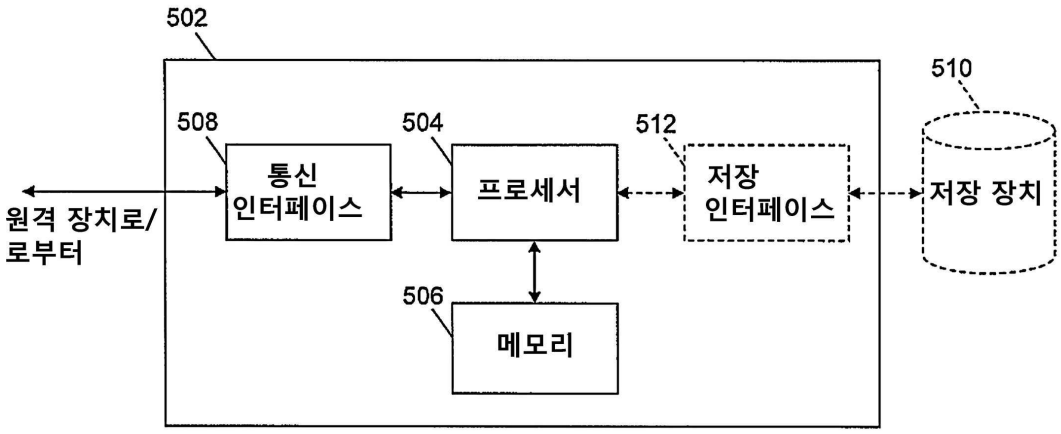
도면3


336
머천트
330
324
발행자
330
취득자
330
322
332
워크 스테이션
204
인터넷
326
ISP 인터넷 연결
사기 위험 점수 매김 시스템
202
System 210
웹 서버 304
앱 서버 302
DB 서버 206
312
디스크 저장소
328
LAN/WAN
314
메일 서버 310
팩스 서버 306
사전 서버 308
제3자
334
316
318
320
클라이언트 시스템
200

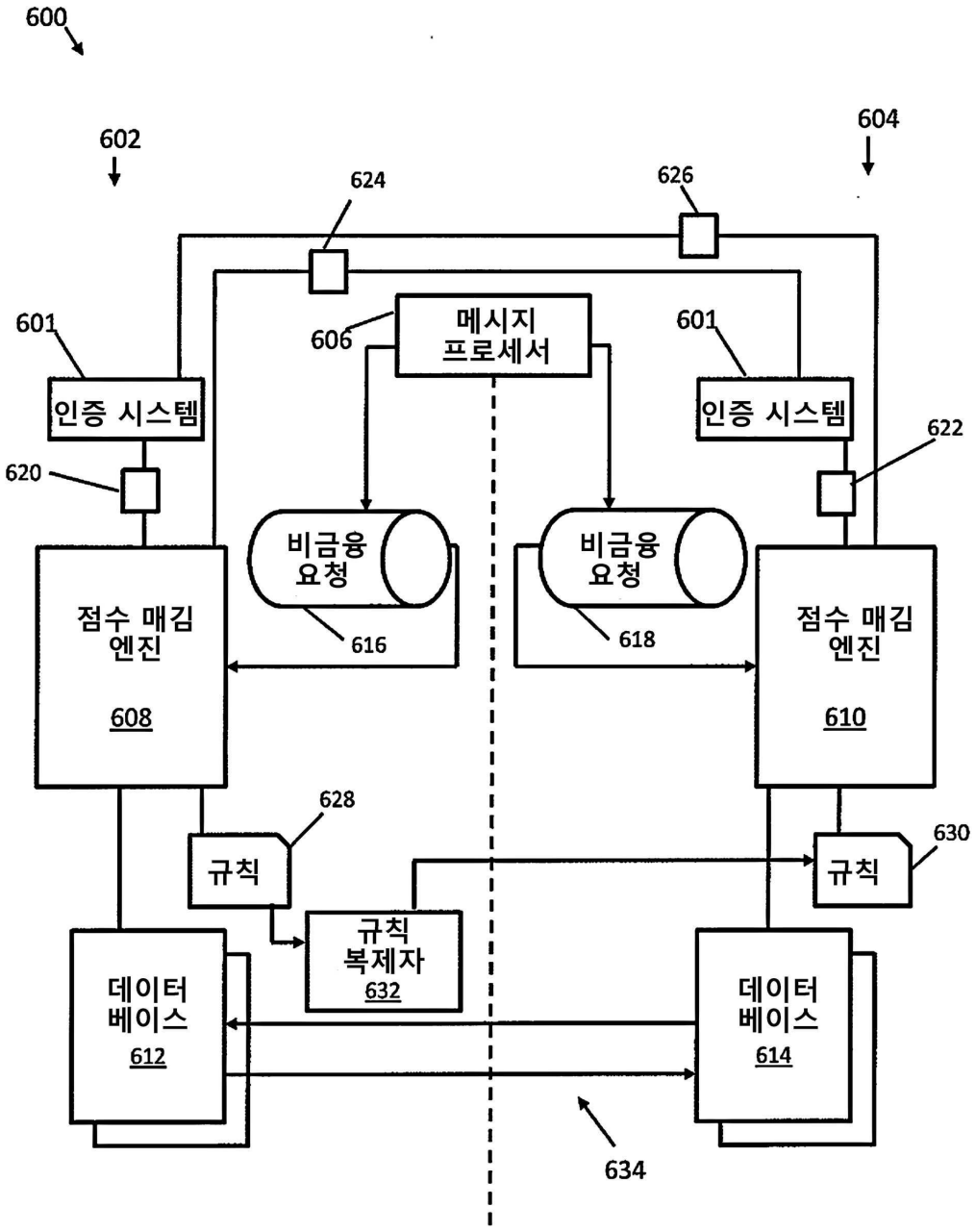
도면4


402
401
사용자
420
입력
405
프로세서
425
통신 인터페이스
원격 장치로/로부터
415
미디어 출력
410
메모리

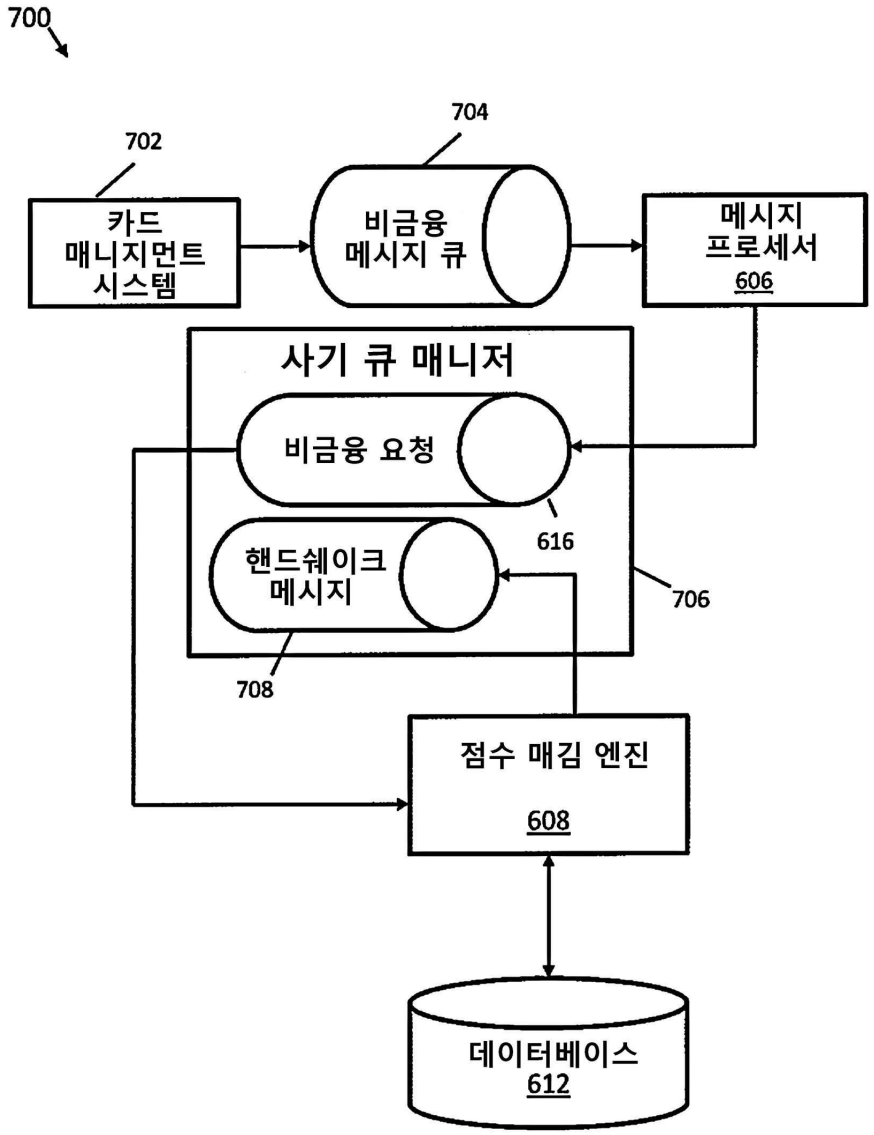
도면5


502
508
통신
인터페이스
504
프로세서
512
저장
인터페이스
510
저장 장치
원격 장치로/
로부터
506
메모리

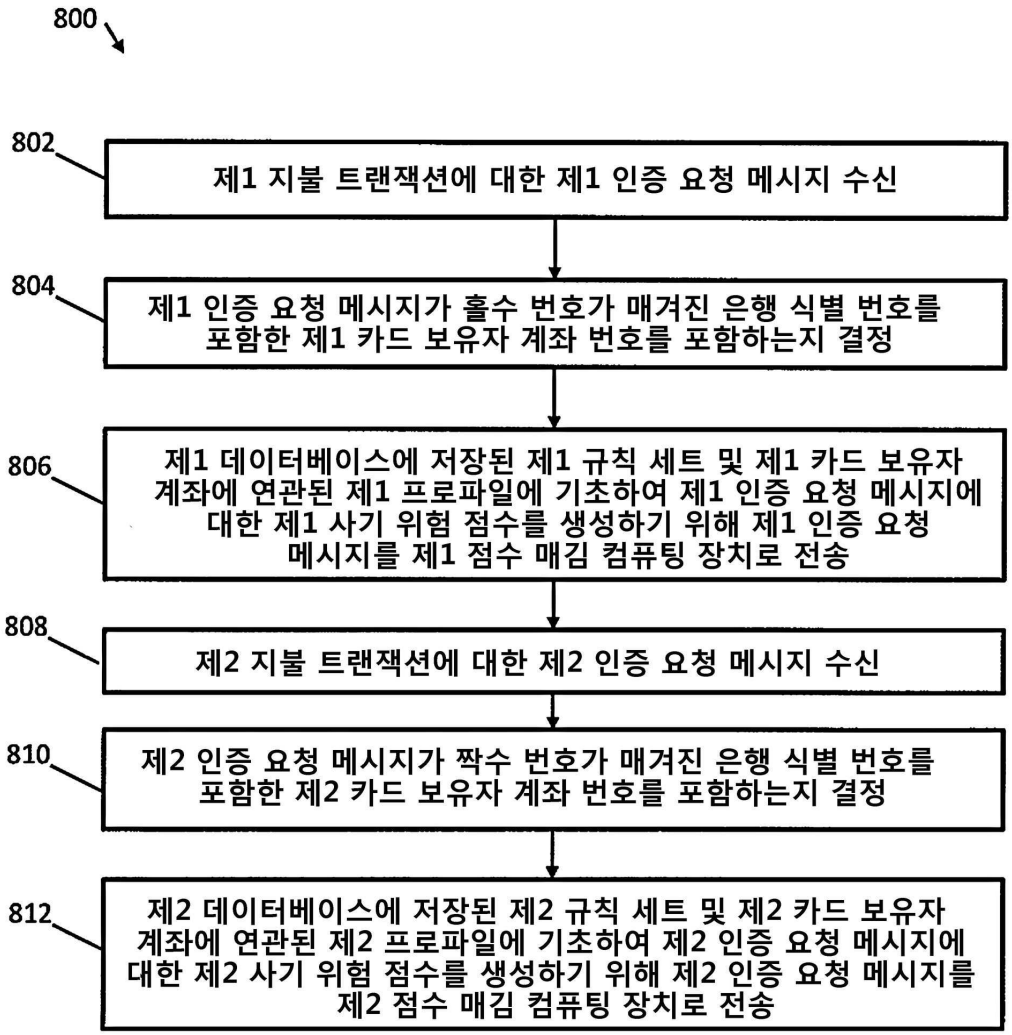
도면6


600
602
604
624
626
601
606
메시지
프로세서
601
인증 시스템
인증 시스템
622
620
비금융
요청
비금융
요청
점수 매김
엔진
608
616
618
점수 매김
엔진
610
628
630
규칙
규칙
규칙
복제자
632
데이터
베이스
612
데이터
베이스
614
634

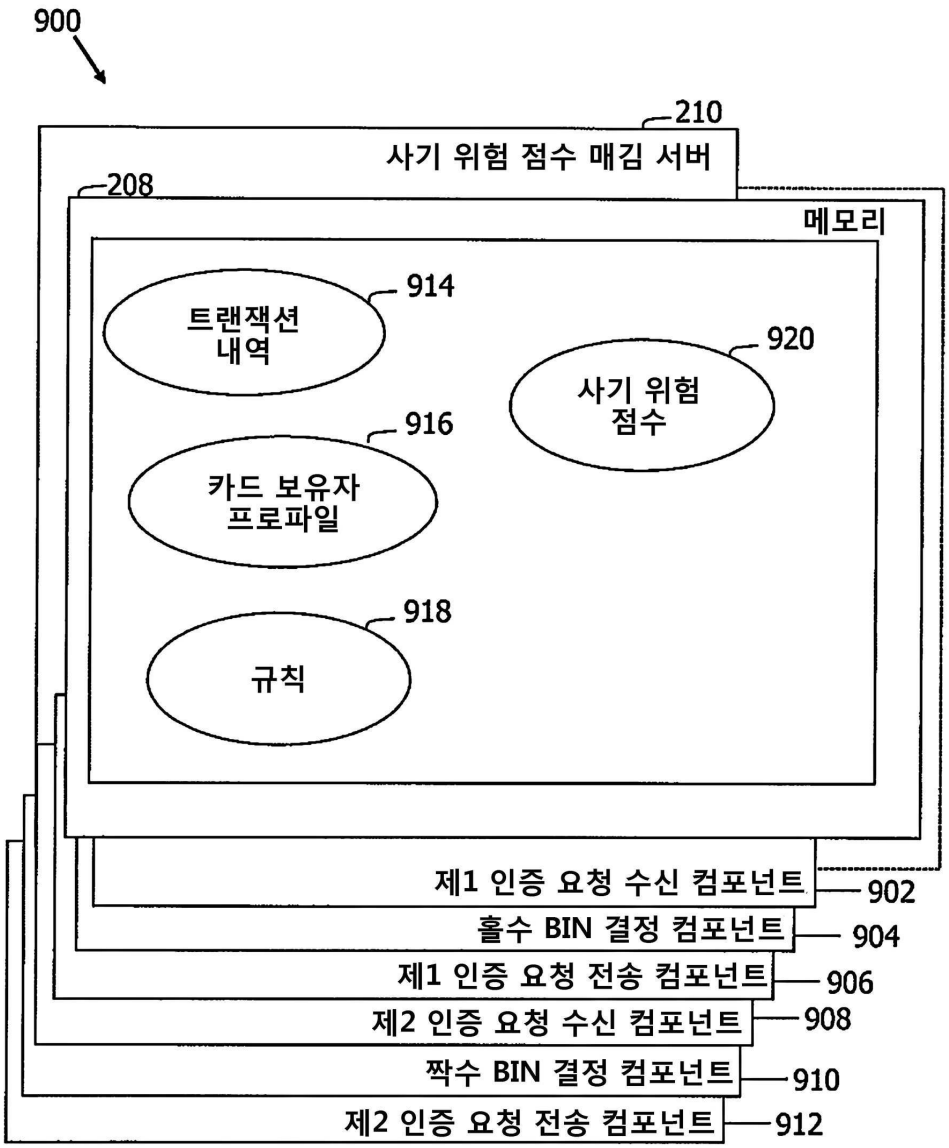
도면7


700
702
704
카드
매니지먼트
시스템
비금융
메시지 큐
메시지
프로세서
606
사기 큐 매니저
비금융 요청
616
핸드쉐이크
메시지
706
708
점수 매김 엔진
608
데이터베이스
612

도면8


800
802
제1 지불 트랜잭션에 대한 제1 인증 요청 메시지 수신
804
제1 인증 요청 메시지가 홀수 번호가 매겨진 은행 식별 번호를 포함한 제1 카드 보유자 계좌 번호를 포함하는지 결정
806
제1 데이터베이스에 저장된 제1 규칙 세트 및 제1 카드 보유자 계좌에 연관된 제1 프로파일에 기초하여 제1 인증 요청 메시지에 대한 제1 사기 위험 점수를 생성하기 위해 제1 인증 요청 메시지를 제1 점수 매김 컴퓨팅 장치로 전송
808
제2 지불 트랜잭션에 대한 제2 인증 요청 메시지 수신
810
제2 인증 요청 메시지가 짝수 번호가 매겨진 은행 식별 번호를 포함한 제2 카드 보유자 계좌 번호를 포함하는지 결정
812
제2 데이터베이스에 저장된 제2 규칙 세트 및 제2 카드 보유자 계좌에 연관된 제2 프로파일에 기초하여 제2 인증 요청 메시지에 대한 제2 사기 위험 점수를 생성하기 위해 제2 인증 요청 메시지를 제2 점수 매김 컴퓨팅 장치로 전송

도면9


900
210
사기 위험 점수 매김 서버
208
메모리
914
트랜잭션 내역
920
사기 위험 점수
916
카드 보유자 프로파일
918
규칙
제1 인증 요청 수신 컴포넌트
902
홀수 BIN 결정 컴포넌트
904
제1 인증 요청 전송 컴포넌트
906
제2 인증 요청 수신 컴포넌트
908
짝수 BIN 결정 컴포넌트
910
제2 인증 요청 전송 컴포넌트
912