

**T.C.
TÜRK PATENT VE MARKA KURUMU
Patent Dairesi Başkanlığı**

Sayı : 39616753- 2017/21525 /

Konu : Patent

**ZELİHA ÖZSOY (3 TEK PATENT MARKA DANIŞMANLIK A.Ş.)
ÇANKAYA MAH. MAHMUT YESARI SOK. NO:8/5 ÇANKAYA/ANKARA**

İlgi: 25/12/2017 tarihli patent başvurunuz.

İlgide kayıtlı başvurunuzla ilgili olarak Kurumumuz tarafından düzenlenen tekniğin bilinen durumu konusundaki Araştırma Raporu ve Ekleri ilişkide gönderilmiştir.

6769 sayılı Sinai Mülkiyet Kanununun 98 inci maddesinin birinci fıkrası ve anılan Kanunun Uygulanmasına Dair Yönetmeliğin 102 nci maddesinin birinci fıkrası hükümleri uyarınca bildirim tarihinden itibaren üç ay içinde ücretinin de ödenerek inceleme talebinde bulunulması gerekmektedir. Aksi takdirde başvurunuz geri çekilmiş sayılacaktır.

Saygılarımla.

Zü'lal YAVUZ
Kurum Başkanı a.
Sinai Mülkiyet Uzmanı

Ek: Araştırma Raporu ve Ekleri

NOTLAR:

1- Türk Patent ve Marka Kurumunun sunduğu hizmetlere ilişkin ücretlerde, ödemenin yapıldığı tarih itibariyle yürürlükte olan Ücret Tebliğinin dikkate alınması gerekmektedir.

2- Başvurunun korunması için gerekli olan yıllık ücretler üçüncü yıldan başlamak üzere her yıl vadesinde ödenir. Vade tarihi, başvuru tarihine tekabül eden ay ve gündür. Yıllık ücretler, vadesinde ödenmediği takdirde ek ücretle birlikte vadeyi takip eden altı ay içinde de ödenebilir. Yıllık ücretlerin bu süre içinde de ödenmemesi halinde başvurular geçersiz sayılır.

Evrak bilgisine <http://www.turkpatent.gov.tr> adresinden, "grgt4A1B9F08" DYS No ve Evrak tarihinden erişebilirsiniz.

"e-imzalıdır"

Cevaplarda; ilgili yazının çıktıgı daire, tarih ve sayının tam olarak yazılması rica olunur.

Başvuru Sahibi:

TURKCELL TEKNOLOJİ ARAŞTIRMA VE GELİŞTİRME ANONİM ŞİRKETİBaşvuru No:
2017/21525Başvuru Tarihi:
24/12/2017(İlk) Rüçhan Tarihi
-Patent Sınıfı (IPC⁸):**G06Q 30/02, G06N 20/00 (2009.01)****GENEL GÖZLEMLER****Buluş Bütünlüğü** Var (başvuru sadece bir buluş konusunu içermektedir) ... (başvuru birden çok buluş konusunu içermektedir) (Bakınız: Bölüm III)**Tarifname Takımı** Rapor aşağıda belirtilen tarifname takımı esas alınarak düzenlenmiştir.

Tarifname 6 sayfa (Orijinal)

İstem 12 adet (Orijinal)

Resim 2 sayfa (Orijinal)

Açıklık ... Tüm istemler araştırılabilir niteliktedir. ... nolu istemler araştırılabilir nitelikte değildir. (Bakınız: Bölüm IV) Başvuruyla ilgili diğer görüşler (Bakınız: Bölüm II)Raporun Tamamlandığı Tarih: **10/09/2020**

Türk Patent ve Marka Kurumu - Patent Dairesi
Başkanlığı
Hipodrom Cad. No:115 06330
Yenimahalle/ANKARA
Tel: (312) 303 1182
Faks: (312) 303 1220

Araştırmayı Yapan Uzman:

Zülal YAVUZ

Başvuru Numarası:

2017/21525

A. BULUŞUN PATENT SINIFI (IPC⁸)
G06Q 30/02,G06N 20/00 (2009.01)

B. ARAŞTIRILAN ALANLAR
G06Q,G06N

Araştırma esnasında kullanılan elektronik veritabanları ve -uygun olduğu durumlarda- kullanılan bazı anahtar kelimeler

EPODOC, WPI, EPOQUE İngilizce ve Almanca Tüm-metin Veritabanları (TXTE, TXTDE), Türk Patent Veritabanı, Espacenet, DEPATISnet, KIPRIS, PAJ, IPDL, AIPN, C-PAT

“service provider, database, analyze, query, inquiry, decision, judgment, check, determination, data, acquisition, collection, processing, unit, fraud, cheat, forgery, fishing, screening, visualization, machine learning, score, evaluate, categorize, segment, cluster, subscriber, customer” ve bunların uygun kombinasyonları

C. İLGİLİ DOKÜMANLAR

Kategori	Dokümanlar	İlgili Olduğu İstem
X	KR20170006158A (KT CORP [KR]) 17 Ocak 2017 (17.01.2017) Tarifname: özellikle Paragraf 12,13,23,27,28,37,40 -----	1,2,4-12
X	US2017193514A1 (E SUN COMMERCIAL BANK LTD [TW]) 6 Temmuz 2017 (06.07.2017) Tarifname: özellikle Paragraf 8-19,25,28,31,32,33 ----- -/-	1,2,4-12

İlgili Dokümanlar sonraki sayfadan devam etmektedir. Patent Ailesi Üyeleri ekine bakınız.

Kategorilerin Açıklaması:

- “X” Buluşun yeni olmadığını veya buluş basamağı “E” Başvuru tarihinde veya başvuru tarihinden içermediğini tek başına gösteren doküman
- “Y” Buluşun buluş basamağı içermediğini başka bir “T” Buluşun altında yatan ilke veya teoriyi dokümanla bir araya getirildiğinde gösteren anlamak için belirtilen doküman
- “A” Tekniğin bilinen durumunu belirten ama buluşla “L” Başka nedenlerle belirtilen doküman tam olarak ilgili olmayan doküman
- “O” Yazılı olmayan açıklama “D” Başvuruda belirtilen doküman
- “P” Başvuru tarihi ile rüçhan tarihi arasında “&” Aynı patent ailesinin dokümanı yayımlanan doküman

Türk Patent ve Marka Kurumu - Patent Dairesi Başkanlığı
Hipodrom Cad. No:115 06330 Yenimahalle/ANKARA
Tel: (312) 303 1182
Faks: (312) 303 1220

Araştırmayı Yapan Uzman:

Zülal YAVUZ

Başvuru Numarası:

2017/21525

C. İLGİLİ DOKÜMANLAR

Kategori	Dokümanlar	İlgili Olduğu İstem
X	KR20130095548A (KOREA PRIME TECHNOLOGY CO LTD [KR]) 28 Ağustos 2013 (28.08.2013) Tarifname: özellikle Paragraf 1,17,20-43,66,70 ----- WO2016065307A1 (INSURANCE SERVICES OFFICE INC [US]) 28 Nisan 2016 (28.04.2016) Tarifname: özellikle Sayfa 3, Satır 1-17; Sayfa 5, Satır 5-20,27-30; Sayfa 6, Satır 8-33; Sayfa 7, Satır 12-16 ----- KR20170060958A (UNIV KOREA RES) 2 Haziran 2017 (02.06.2017) Tarifname: özellikle Paragraf 10,16,26,29,76,80,84 -----	1,2,4-12
X		1-12
X		1,2,4-12

Başvuru Numarası:

2017/21525

II. GÖRÜŞLER

5-8,10,11 numaralı istemlerin koruma kapsamı belirsizlik yaratmaktadır zira korunmak istenenin bir cihaza ait unsurlar mı olduğu yoksa bir yöntem mi olduğu belirsizdir. Buluşun çalışma prensibi şeklinde yazılan istemler doğası gereği istemin kategorisini belirsizleştirdiği için açıklık sorunu yaratmaktadır. İstem ya cihazın yapısal unsurlarını anlatan bir aparat (ya da sistem) istemi olarak yazılmalı ya da bir yönteme ait işlem adımları şeklinde anlatılmalıdır. Rapor istemler ile korunmak istenenin bir sistem olduğu varsayılarak ve tarifnamede bahsedilen yapısal unsurlar dikkate alınarak düzenlenmiştir.



Europäisches
Patentamt
European
Patent Office
Office européen
des brevets

Espacenet my patents list on 10-09-2020 15:19

5 items in my patents list

Displaying selected publications

Publication	Title	Page
KR20170006158 (A)	SYSTEM AND METHOD FOR DETECTING FRAUD...	2
KR20170060958 (A)	METHOD AND SYSTEM FOR PREVENTING BANK...	19
KR20130095548 (A)	FINANCIAL FRAUD WARNING SYSTEM USING ...	34
WO2016065307 (A1)	SYSTEMS AND METHODS FOR COMPUTERIZED ...	52
US2017193514 (A1)	Method for Performing Machine Detecti...	86



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0006158
(43) 공개일자 2017년01월17일

(51) 국제특허분류(Int. Cl.)
H04M 3/42 (2006.01)
(52) CPC특허분류
H04M 3/42 (2013.01)
(21) 출원번호 10-2015-0096671
(22) 출원일자 2015년07월07일
심사청구일자 없음

(71) 출원인
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
백승화
경기도 하남시 덕풍서로 65, 505동 602호 (덕풍동, 아이파크5단지아파트)
안태진
대전광역시 유성구 엑스포로 448, 506동 701호(전민동, 엑스포아파트)
(74) 대리인
특허법인필엔온지

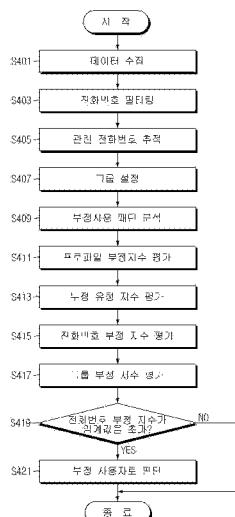
전체 청구항 수 : 총 24 항

(54) 발명의 명칭 문자 메시지 부정 사용 탐지 방법 및 시스템

(57) 요약

본 발명은 비정상적인 문자 메시지를 발송하는 부정 사용자를 탐지하는 방법 및 시스템에 관한 것이다. 본 발명에 따른, 부정 사용 탐지 시스템에서 문자 메시지를 비정상적으로 발송하는 부정 사용자를 탐지하는 방법은, 부정 사용자로 의심되는 전화번호를 수집하여 분석대상 전화번호로서 분석대상 목록에 등록하는 단계; 프로파일별 부정 사용 패턴이 기록된 룰셋을 참조하여, 분석대상 목록에 기록된 분석대상 전화번호를 이용한 문자 사용 패턴이 상기 룰셋에 기록된 각 부정 사용 패턴과 일치하는지 여부를 확인하여, 프로파일별 점수를 평가하는 단계; 평가된 각 프로파일 점수를 기초로 상기 분석대상 전화번호의 부정지수를 평가하는 단계; 및 평가된 상기 분석대상 전화번호의 부정지수가 사전에 설정된 부정 임계값을 초과하는지 여부를 판별하여 초과하면, 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자로서 판단하는 단계를 포함한다.

제 35 조 - 도4



영세서

청구범위

청구항 1

부정 사용 탐지 시스템에서 문자 메시지를 비정상적으로 발송하는 부정 사용자를 탐지하는 방법으로서,

부정 사용자로 의심되는 전화번호를 수집하여 분석대상 전화번호로서 분석대상 목록에 등록하는 단계;

프로파일별 부정 사용 패턴이 기록된 룰셋을 참조하여, 분석대상 목록에 기록된 분석대상 전화번호를 이용한 문자 사용 패턴이 상기 룰셋에 기록된 각 부정 사용 패턴과 일치하는지 여부를 확인하여, 프로파일별 점수를 평가하는 단계;

평가된 각 프로파일 점수를 기초로 상기 분석대상 전화번호의 부정지수를 평가하는 단계; 및

평가된 상기 분석대상 전화번호의 부정지수가 사전에 설정된 부정 임계값을 초과하는지 여부를 판별하여 초과하면, 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자로서 판단하는 단계;를 포함하는 문자 메시지 부정 사용 탐지 방법.

청구항 2

제 1 항에 있어서,

상기 룰셋에는 부정 유형에 따라 구분되는 프로파일별 부정 사용 패턴이 기록되고,

상기 부정지수를 평가하는 단계는,

부정 유형에 해당하는 프로파일 점수끼리 가산하여, 부정 유형별로 가산된 프로파일 점수를 토대로 각 부정 유형의 지수를 산출하고, 이 부정 유형의 지수 중에서 가장 높은 지수를 상기 전화번호의 부정 지수로서 평가하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 3

제 2 항에 있어서,

상기 부정 유형으로서 블랙 리스트 유형이 상기 룰셋에 기록되고, 상기 블랙 리스트의 프로파일에는 재인입 프로파일이 상기 룰셋에 기록되고, 상기 재인입에 대한 부정 사용 패턴으로서 하나 이상의 부정 사용 패턴이 상기 룰셋에 기록되는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 4

제 2 항에 있어서,

상기 부정 유형으로서, 명의도용자 유형이 상기 룰셋에 기록되고, 상기 명의도용자의 프로파일에는 명의도용 프로파일이 상기 룰셋에 기록되고, 상기 명의도용 프로파일에 대한 부정 사용 패턴으로서, 하나 이상의 부정 사용 패턴이 상기 룰셋에 기록되는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 5

제 2 항에 있어서,

상기 부정 유형으로서, 스파머 유형이 상기 룰셋에 기록되고, 상기 스파머의 프로파일에는 발번조작 프로파일, 스팸문구 프로파일, 신고건수 프로파일, 발신량 프로파일, 발신시각 프로파일, 발송대행 프로파일 중 하나 이상이 기록되고, 각각의 프로파일과 대응되어 하나 이상의 부정 사용 패턴이 상기 룰셋에 기록되는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 6

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 등록하는 단계 이후에,

상기 분석대상 목록에 기록된 분석대상 전화번호 중에서 분석이 불필요한 전화번호를 필터링하는 단계;를 더 포함하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 7

제 6 항에 있어서,

상기 필터링하는 단계는,

상기 분석대상 목록에 기록된 분석대상 전화번호 중에서 010으로 시작되지 않은 전화번호를 상기 분석대상 목록에서 제거하는 단계;

상기 분석대상 목록에 기록된 분석대상 전화번호 중에서 문자 메시지의 발신이 허용된 전화번호를 상기 분석대상 목록에서 제거하는 단계;

타 통신사에서 관리되는 전화번호를 상기 분석대상 목록에서 제거하는 단계; 및

문자 발송량 평균이 사전에 설정된 허용량을 초과하지 않은 전화번호를 상기 분석대상 목록에서 제거하는 단계;를 포함하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 8

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 등록하는 단계 이후에,

분석대상 목록에 기록된 분석대상 전화번호와 연관되는 전화번호를 추적하여 상기 분석대상 목록에 추가적으로 등록하는 단계;를 더 포함하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 9

제 8 항에 있어서,

상기 추가적으로 등록하는 단계는,

상기 분석대상 목록에 기록된 분석대상 전화번호와 동일한 명의를 가지는 전화번호, 상기 분석대상 전화번호와 동일한 단말기를 사용한 이력이 있는 전화번호, 상기 분석대상 전화번호를 가지는 가입자가 이전에 사용한 전화번호, 상기 분석대상 전화번호가 착신전환되는 전화번호 중 하나 이상을 추적하여 상기 분석대상 목록에 추가적으로 등록하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 10

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 등록하는 단계 이후에,

상기 분석대상 목록에 기록된 분석대상 전화번호와 각 그룹간의 상관관계를 분석하여, 상관관계가 가장 높은 그룹에 상기 분석대상 전화번호를 등록하는 단계;를 더 포함하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 11

제 10 항에 있어서,

상기 그룹에 상기 분석대상 전화번호를 등록하는 단계는,

상기 분석대상 전화번호의 데이터와 각 그룹의 대표 전화번호의 데이터를 비교하여, 상기 분석대상 전화번호와 동일한 명의를 사용하는 대표 전화번호, 상기 분석대상 전화번호와 동일한 문구의 문자 메시지를 발송한 이력이 대표 전화번호, 상기 분석대상 전화번호와 동일한 단말기를 사용한 이력이 있는 대표 전화번호, 상기 분석대상 전화번호와 동일한 결제정보를 가지는 대표 전화번호 또는 상기 분석대상 전화번호와 동일한 착신전환 전화번호가 설정된 대표 전화번호가 존재하는지 여부를 확인하는 단계; 및

상기 확인 결과, 대표 전화번호가 존재하면 이 대표 전화번호가 소속된 그룹에 상기 분석대상 전화번호를 등록하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 12

제 11 항에 있어서,

상기 확인 결과, 대표 전화번호가 존재하지 않으면, 사전에 설정된 그룹 설정을 위한 2차 조건 항목에 근거하여 분석대상 전화번호와 각 그룹의 대표 전화번호와의 상관점수를 산출하고, 이 중에서 가장 높은 상관점수를 가지는 대표 전화번호가 소속된 그룹에 상기 분석대상 전화번호를 등록하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 13

제 10 항에 있어서,

상기 부정지수를 평가하는 단계는,

상기 평가된 분석대상 전화번호의 부정지수를 토대로, 이 분석대상 전화번호가 소속된 그룹의 부정지수를 평가하는 단계;를 포함하는 것을 특징으로 하는 문자 메시지 부정 사용 탐지 방법.

청구항 14

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 등록하는 단계는,

외부의 서버 또는 센터로부터 스팸 신고 정보를 수신하여, 이 스팸 신고 정보에 기록된 전화번호를 상기 분석대상 목록에 등록하는 단계; 및

문자 메시지 발송 건수가 임계값을 초과한 전화번호를 확인하여, 상기 분석대상 목록에 등록하는 단계;를 포함하는 것을 특징으로 하는 부정 사용 탐지 방법.

청구항 15

프로파일별 부정 사용 패턴이 기록된 룰셋을 저장하는 데이터베이스;

부정 사용자로 의심되는 전화번호를 수집하여 분석대상 전화번호로서 분석대상 목록에 등록하는 데이터 수집부;

상기 룰셋을 참조하여, 분석대상 목록에 기록된 분석대상 전화번호를 이용한 문자 사용 패턴이 상기 룰셋에 기록된 각 부정 사용 패턴과 일치하는지 여부를 확인하여 프로파일별 점수를 평가하고, 이 평가된 각 프로파일 점수를 기초로 상기 분석대상 전화번호의 부정지수를 평가하는 부정지수 평가부; 및

상기 분석대상 전화번호의 부정지수가 사전에 설정된 부정 임계값을 초과하는지 여부를 판별하여 초과하면, 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자로서 판단하는 부정사용 판단부;를 포함하는 부정 사용 탐지 시스템.

청구항 16

제 15 항에 있어서,

상기 룰셋에는 부정 유형에 따라 구분되는 프로파일별 부정 사용 패턴이 기록되고,

상기 부정지수 평가부는, 부정 유형에 해당하는 프로파일 점수끼리 가산하여, 부정 유형별로 가산된 프로파일 점수를 토대로 각 부정 유형의 지수를 산출하고, 이 부정 유형의 지수 중에서 가장 높은 지수를 상기 전화번호의 부정 지수로서 평가하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 17

제 15 항 또는 제 16항에 있어서,

상기 분석대상 목록에 기록된 분석대상 전화번호 중에서 분석이 불필요한 전화번호를 필터링하는 전화번호 필터링부;를 더 포함하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 18

제 17 항에 있어서,

상기 전화번호 필터링부는,

상기 분석대상 목록에 기록된 분석대상 전화번호 중에서 010으로 시작되지 않은 전화번호, 문자 메시지의 발신이 허용된 전화번호, 타 통신사에서 관리되는 전화번호 및 문자 발송량 평균이 사전에 설정된 허용량을 초과하지 않은 전화번호를 상기 분석대상 목록에서 제거하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 19

제 15 항 또는 제 16 항에 있어서,

분석대상 목록에 기록된 분석대상 전화번호와 연관되는 전화번호를 추적하여 상기 분석대상 목록에 추가적으로 등록하는 번호 추적부;를 더 포함하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 20

제 19 항에 있어서,

상기 번호 추적부는,

상기 분석대상 목록에 기록된 분석대상 전화번호와 동일한 명의를 가지는 전화번호, 상기 분석대상 전화번호와 동일한 단말기를 사용한 이력이 있는 전화번호, 상기 분석대상 전화번호를 가지는 가입자가 이전에 사용한 전화번호, 상기 분석대상 전화번호가 착신전환되는 전화번호 중 하나 이상을 추적하여 상기 분석대상 목록에 추가적으로 등록하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 21

제 15 항 또는 제 16 항에 있어서,

상기 분석대상 목록에 기록된 분석대상 전화번호와 각 그룹간의 상관관계를 분석하여, 상관관계가 가장 높은 그룹에 상기 분석대상 전화번호를 등록하는 그룹 설정부;를 더 포함하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 22

제 21 항에 있어서,

상기 그룹 설정부는,

상기 분석대상 전화번호의 데이터와 각 그룹의 대표 전화번호의 데이터를 비교하여, 상기 분석대상 전화번호와 동일한 명의를 사용하는 대표 전화번호, 상기 분석대상 전화번호와 동일한 문구의 문자 메시지를 발송한 이력이 대표 전화번호, 상기 분석대상 전화번호와 동일한 단말기를 사용한 이력이 있는 대표 전화번호, 상기 분석대상 전화번호와 동일한 결제정보를 가지는 대표 전화번호 또는 상기 분석대상 전화번호와 동일한 착신전환 전화번호가 설정된 대표 전화번호가 존재하는지 여부를 1차 확인하여 대표 전화번호가 존재하면 이 대표 전화번호가 소속된 그룹에 상기 분석대상 전화번호를 등록하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 23

제 22 항에 있어서,

상기 그룹 설정부는,

상기 1차 확인 결과 대표 전화번호가 존재하지 않으면, 사전에 설정된 그룹 설정을 위한 2차 조건 항목에 근거하여 분석대상 전화번호와 각 그룹의 대표 전화번호와의 상관점수를 산출하고, 이 중에서 가장 높은 상관점수를 가지는 대표 전화번호가 소속된 그룹에 상기 분석대상 전화번호를 등록하는 것을 특징으로 하는 부정 사용 탐지 시스템.

청구항 24

제 21 항에 있어서,

상기 부정지수 평가부는,

상기 평가된 분석대상 전화번호의 부정지수를 토대로, 이 분석대상 전화번호가 소속된 그룹의 부정지수를 평가하는 것을 특징으로 하는 부정 사용 탐지 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 문자 메시지의 부정 사용을 탐지하기 위한 방법에 관한 것으로서, 더욱 상세하게는 비정상적인 문자 메시지를 발송하는 부정 사용자를 탐지하는 방법 및 시스템에 관한 것이다.

본 발명

[0002] 오늘날 이동통신망과 이동통신 기기의 비약적인 발전으로 인하여, 문자 메시지를 이용한 광고가 성행하고 있다. 아래의 특허문헌은 기지국 위치를 이용한 위치 기반 문자 메시지 광고 방법에 대해서 개시한다. 그런데 이러한 문자 메시지를 이용한 광고가 악용되어, 악성 스팸 메시지, 즉 음란물, 도박, 약물 및 대출과 관련된 스팸 메시지도 발송되고 있다.

[0003] 이동통신 가입자가 수신한 스팸 문자 메시지를 지정된 기관(예컨대, 한국인터넷진흥원)에 신고하면, 해당 기관은 이동통신사로 스팸 문자를 발송한 발신번호에 대한 문자 발신 차단을 요청하고, 이동통신사는 문자 메시지의 내용을 검토한 후 상기 발신번호에 대한 이용정지나 직권해제를 실행하여 스파머의 문자 발신을 차단한다.

[0004] 그런데 이러한 수신자 신고방식은, 기관 및 이동통신사가 신고된 스팸 문자의 내용을 직접 검토하고, 해당 문자가 스팸 문자인지 여부를 최종적으로 판단하기 때문에, 투입되는 인력도 많고 사후대응만 가능한 형태이다.

[0005] 한편, 과거에는 스파머들이 스팸 문자 발송 서버를 구축하여, 이 서버를 통해 이동통신사보다 저렴한 비용으로 스팸 문자 발송 대행 사업을 하였으나, 발신량 기반의 스팸 탐지 시스템이 이동통신사에서 도입되고 문자 발송 대행 서비스와 관련된 행위를 불법으로 간주하는 약관과 제도가 신설됨으로 인하여, 문자 대행 서버 기반의 스팸 발송 방식은 그 사용빈도가 많이 감소하고 있다.

[0006] 그러나 최근에는 스파머들이 다량의 저가폰을 개통한 후, 불법 문자 발송 애플리케이션을 저가폰에 설치하고, 이 애플리케이션과 연동되는 서버가 구비된 불법 문자 발송 시스템을 구축하고 있다. 이러한 불법 문자 발송 시스템은, 스파머가 서버에 접속하여 스팸 문자 메시지를 작성하면, 이 스팸 문자 메시지가 불법 문자 발송 애플리케이션이 설치된 저가폰을 통해서 발송되는 구조이다.

[0007] 이러한 불법 문자 발송 시스템을 통해서 계속적으로 스팸 문자가 발송되면, 이동통신사의 수익구조에도 악영향을 미칠 수 있으며, 또한 사용자의 서비스 만족도를 저하시키는 문제점으로 작용할 수도 있다.

설명기술분야

특허분야

[0008] (특허문헌 0001) 한국공개특허 10-2006-0107729

발명의 내용

본 발명의 과제

[0009] 본 발명은 이러한 종래의 문제점을 해결하기 위하여 제안된 것으로, 수집된 데이터를 분석하여 스파머를 실시간으로 감시하고 탐지하는 문자 메시지 부정 사용 탐지 방법 및 시스템을 제공하는데 그 목적이 있다.

[0010] 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특히 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

파제의 해설 수단

[0011]

상기 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 부정 사용 탐지 시스템에서 문자 메시지를 비정상적으로 발송하는 부정 사용자를 탐지하는 방법은, 부정 사용자로 의심되는 전화번호를 수집하여 분석대상 전화번호로서 분석대상 목록에 등록하는 단계; 프로파일별 부정 사용 패턴이 기록된 룰셋을 참조하여, 분석대상 목록에 기록된 분석대상 전화번호를 이용한 문자 사용 패턴이 상기 룰셋에 기록된 각 부정 사용 패턴과 일치하는지 여부를 확인하여, 프로파일별 점수를 평가하는 단계; 평가된 각 프로파일 점수를 기초로 상기 분석대상 전화번호의 부정지수를 평가하는 단계; 및 평가된 상기 분석대상 전화번호의 부정지수가 사전에 설정된 부정 임계값을 초과하는지 여부를 판별하여 초과하면, 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자로서 판단하는 단계를 포함하는 것을 특징으로 한다.

[0012]

상기 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 부정 사용 탐지 시스템은, 프로파일별 부정 사용 패턴이 기록된 룰셋을 저장하는 데이터베이스; 부정 사용자로 의심되는 전화번호를 수집하여 분석대상 전화번호로서 분석대상 목록에 등록하는 데이터 수집부; 상기 룰셋을 참조하여, 분석대상 목록에 기록된 분석대상 전화번호를 이용한 문자 사용 패턴이 상기 룰셋에 기록된 각 부정 사용 패턴과 일치하는지 여부를 확인하여 프로파일별 점수를 평가하고, 이 평가된 각 프로파일 점수를 기초로 상기 분석대상 전화번호의 부정지수를 평가하는 부정지수 평가부; 및 상기 분석대상 전화번호의 부정지수가 사전에 설정된 부정 임계값을 초과하는지 여부를 판별하여 초과하면, 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자로서 판단하는 부정사용 판단부를 포함하는 것을 특징으로 한다.

발명의 효과

[0013]

본 발명은 부정 사용자의 문자 발송 패턴을 분석하여 부정 사용자를 자동적으로 탐지하고, 이 부정 사용자에게 이용정지, 서비스 해제 등과 같은 제재를 가함으로써, 이동통신망에서 발생되는 스팸 문자 메시지를 줄일 수 있는 장점이 있다.

[0014]

또한, 본 발명은 사전에 정의된 부정 사용 패턴 정보와 문자 발송자의 문자 발송 패턴을 비교하고, 이 비교결과에 근거하여 부정 사용자로서 의심되는 전화번호의 부정지수를 평가하는 매우 빠르고 가벼운 알고리즘을 통해서 부정 사용자를 탐지하기 때문에, 부정 사용자 판별에 필요한 자원(즉, CPU, 메모리)을 절약할 수 있을 뿐만 아니라, 빠른 속도로 부정 사용자를 탐지할 수 있는 장점이 있다.

[0015]

또한, 본 발명은 전화번호가 스패머로서 신고되면, 이 전화번호와 연관된 다른 전화번호를 추적하여 그룹에 등록하고 동일 그룹에 속하는 전화번호를 통해 발송되는 문자 메시지를 지속적으로 모니터링함으로써, 복수의 전화번호를 이용하여 스팸 메시지를 발송하는 부정 사용자를 색출할 수 있는 효과도 있다.

[0016]

또한, 본 발명은 수집된 데이터를 분석하여 부정 사용자를 자동으로 탐지함으로써, 스팸 문자 메시지 발송에 따라 발생되는 이동통신사의 비용을 감소할 수 있으며, 스팸 문자 메시지를 판별하기 위해서 투입되는 노동력도 절감할 수 있는 장점이 있다.

도면의 간단한 설명

[0017]

본 명세서에 첨부되는 다음의 도면들은 본 발명의 바람직한 실시예를 예시하는 것이며, 발명을 실시하기 위한 구체적인 내용과 함께 본 발명의 기술사상을 더욱 이해시키는 역할을 하는 것이므로, 본 발명은 그러한 도면에 기재된 사항에만 한정되어 해석되어서는 아니 된다.

도 1은 본 발명의 일 실시예에 따른, 부정 사용 탐지 시스템이 적용되는 통신환경을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른, 부정 사용 탐지 시스템의 구성을 나타내는 도면이다.

도 3은 부정 사용 패턴 항목이 기록된 룰셋을 예시하는 도면이다.

도 4는 본 발명의 일 실시예에 따른, 부정 사용 탐지 시스템에서 스팸 문자 메시지를 발송하는데 이용되는 전화 번호의 부정 사용을 탐지하는 방법을 설명하는 흐름도이다.

도 5는 본 발명의 일 실시예에 따른, 부정지수가 평가된 그룹과 전화번호를 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0018] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명하기로 한다.

[0020] 도 1은 본 발명의 일 실시예에 따른, 부정 사용 탐지 시스템이 적용되는 통신환경을 나타내는 도면이다.

[0021] 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 부정 사용 탐지 시스템(200)은 네트워크(300)를 통하여 스팸 접수 센터(110)와 스팸 알림 서비스 서버(120)와 통신한다. 여기서, 네트워크(300)는 이동통신망과 광대역 유선 통신망을 포함하는 것으로서 본 발명의 있어서 주지의 관용기술에 해당하므로 자세한 설명은 생략한다.

[0022] 스팸 접수 센터(110)는 지정된 스팸 처리 기관(예컨대, 한국인터넷진흥원)에서 관리하는 시스템으로서, 스팸 문자 신고를 접수받아, 스팸 문자 메시지와 발신번호를 저장한다. 또한, 스팸 접수 센터(110)는 스팸으로 신고된 스팸 문자 메시지와 발신번호를 부정 사용 탐지 시스템(200)으로 실시간 또는 일정 주기 간격으로 제공한다.

[0023] 스팸 알림 서비스 서버(120)는 이동통신사 서버에서 구축한 서버(예컨대, KT사의 후후 서버)로서, 이동단말에 설치된 스팸 탐지 애플리케이션과 연동하여, 스팸 신고(즉, 전화번호와 문자 메시지)를 가입자로부터 접수받을 수 있다. 또한, 스팸 알림 서비스 서버(120)는 이동단말에 설치된 스팸 탐지 애플리케이션과 연동하여, 이동단말로부터 착신호가 수신되거나 문자 메시지가 수신되면, 착신호 또는 문자 메시지의 발신번호를 이동단말로부터 수신하고, 이 발신번호가 스팸 관련 전화번호인지 여부를 데이터베이스에 확인하여 그 결과를 이동단말로 실시간 제공한다. 상기 스팸 알림 서비스 서버(120)는 스팸으로 신고된 전화번호와 문자 메시지를 일정 간격 또는 실시간으로 부정 사용 탐지 시스템(200)으로 전송한다.

[0024] 부정 사용 탐지 시스템(200)은 스패머로서 의심되는 전화번호가 스팸 전화번호에 해당하는지 여부를 판별하는 일련의 동작을 수행한다. 즉, 부정 사용 탐지 시스템(200)은 스패머로서 의심되는 전화번호를 수집한 후, 이 수집한 전화번호를 일정 기준에 따라 필터링한다. 아울러, 부정 사용 탐지 시스템(200)은 필터링 전화번호와 일정한 조건을 만족하는 전화번호를 추적한 후, 이렇게 추적된 각각의 전화번호를 그룹에 등록한다. 또한, 부정 사용 탐지 시스템(200)은 각각의 전화번호의 문자 발송 패턴을 분석하여 프로파일에 대한 부정지수, 부정 유형에 대한 부정지수, 전화번호의 부정지수를 순차적으로 평가한 후에, 이 평가된 전화번호의 부정지수를 토대로 해당 전화번호가 부정 사용된 전화번호인지 여부를 판단한다.

[0026] 도 2는 본 발명의 일 실시예에 따른, 부정 사용 탐지 시스템의 구성을 나타내는 도면이다.

[0027] 도 2에 도시된 바와 같이, 본 발명의 일 실시예에 따른 부정 사용 탐지 시스템(200)은 데이터 수집부(210), 전화번호 필터링부(220), 번호 추적부(230), 그룹 설정부(240), 부정지수 평가부(250), 부정사용 판단부(260) 및 데이터베이스(270)를 포함하며, 이러한 구성요소는 하드웨어에 구현되거나, 소프트웨어로서 구현되거나 하드웨어와 소프트웨어의 조합에 의해 구현될 수 있다.

[0028] 데이터베이스(270)는 문자 발송 관련 전산 데이터, 가입자 정보, 부정 사용 패턴 항목이 기록된 룰셋(rule set), 분석대상 목록, 차단 목록, 불가 목록, 그룹 정보, 스패머 신고 이력 등과 같은 각종 데이터를 저장한다. 상기 룰셋(도 3 참조)은 블랙 리스트, 스패머, 명의 도용자와 같은 부정유형에 따라 구분되는 하나 이상의 프로파일이 정의되어 기록되고, 각 프로파일에는 하나 이상의 부정 사용 패턴과 그 패턴에 따른 점수가 정의되어 기록된다. 상기 분석대상 목록에는 부정 사용자로서 의심되는 하나 이상의 전화번호(이하, '분석대상 전화번호'와 혼용하여 지칭함)가 기록된다. 상기 차단 목록에는 과거 및 현재에 서비스 일시 정지된 전화번호가 기록되고, 불가 목록에는 과거 및 현재에 전화번호 재사용이 불가능한 전화번호(즉, 가입자에게 부여할 수 없는 전화번호)가 기록된다. 또한, 그룹 정보에는 해당 그룹에 소속된 하나 이상의 전화번호와 그룹을 대표하는 대표 전화번호가 기록된다. 상기 전산 데이터에는, 전화번호별 문자 발송량, 문자 발송 내용, 착신번호 등이 기록된다. 또한, 스팸 신고 이력에는 전화번호별 스패머 신고 횟수, 문자 메시지 내용, 착신번호 등이 기록된다. 상기 가입자 정보에는 이동통신 가입자의 명의 정보, 결제 정보(즉, 신용 카드 정보, 계좌 정보, 지로 청구지 주소), 개통점 정보, 이동단말기의 식별정보(예컨대, IMEI), 착신전환 서비스 가입 유무와 착신전환 전화번호, 개통일, 요금제 정보 등이 기록된다.

- [0029] 데이터 수집부(210)는 네트워크(300)를 통하여, 스팸 접수 센터(110), 스팸 알림 서비스 서버(120) 각각으로부터 스팸 신고 정보를 수신하면, 스팸 신고 정보에 기록된 전화번호를 데이터베이스(270)의 분석대상 목록에 기록한다. 상기 스팸 신고 정보에는 스패머로 신고된 전화번호와 문자 메시지가 포함된다. 또한, 데이터 수집부(210)는 특정기간(예컨대, 하루) 동안에 문자 메시지 발송 건수가 허용 임계값을 초과한 가입자의 전화번호를 확인하여, 상기 분석대상 목록에 기록할 수 있다.
- [0030] 전화번호 필터링부(220)는 데이터베이스(270)의 분석대상 목록에서 기록된 전화번호 중에서, 분석이 불필요한 전화번호를 제거하는 기능을 수행한다. 구체적으로, 전화번호 필터링부(220)는 '010'으로 시작되지 않는 전화번호, 발신 허용된 전화번호(예컨대, 카드사, 보험사 등과 같은 기업체 전화번호), 타 이동통신사에서 관리하는 전화번호를 분석대상 목록에서 제거한다. 또한, 전화번호 필터링부(220)는 데이터베이스(270)에 기록된 전산 데이터를 참조하여, 분석대상 목록에 기록된 각 전화번호의 전월과 전전월의 문자 발송량 평균을 전화번호별로 확인하고, 이렇게 확인된 문자 발송량 평균이 사전에 설정된 허용량(예컨대, 500건) 이하로 문자 메시지를 발송한 전화번호를 선별하여 상기 분석대상 목록에서 제거한다.
- [0031] 번호 추적부(230)는 데이터베이스(270)의 분석대상 목록에 기록된 전화번호를 확인하고, 데이터베이스(270)의 가입자 정보와 전산 데이터를 참조하여, 전화번호와 연관된 전화번호를 추적하여 분석대상 목록에 기록하는 기능을 수행한다. 상기 번호 추적부(230)는 분석대상 목록에 기록된 전화번호와 동일한 가입자 명의(즉, 개인명의 또는 법인명의)를 가지는 전화번호 및 동일한 단말기를 이용하는 전화번호를 추적하여, 분석대상 목록에 기록한다. 또한, 상기 번호 추적부(230)는 분석대상 목록에 기록된 전화번호를 가지는 가입자가 과거에 사용하였던 또 다른 전화번호를 추적하여 분석대상 목록에 기록한다. 게다가, 번호 추적부(230)는 분석대상 목록에 기록된 전화번호가 착신전환되는 전화번호를 추적하여 분석대상 목록에 기록한다.
- [0032] 그룹 설정부(240)는 사전에 정의된 그룹 규칙을 참조하여, 분석대상 목록에 저장된 각 전화번호를 그룹에 등록한다. 구체적으로, 그룹 설정부(240)는 분석대상 전화번호의 데이터(즉, 가입자 정보와 전산 데이터)와 각 그룹의 대표 전화번호의 데이터 비교하여, 분석대상 전화번호와 동일 명의 사용 여부, 동일 발송문구 전송 여부, 동일 단말을 이용한 이력이 있는지 여부, 동일한 결제정보를 가지는지 여부, 동일한 착신전환 전화번호가 설정되었는지 여부와 같은 그룹설정 1차 조건을 확인하여, 이 중에서 하나라도 부합되는 분석대상 전화번호와 그룹의 대표 전화번호가 존재하는 경우, 상기 분석대상 전화번호를 이 상기 그룹에 등록한다.
- [0033] 상기 그룹 설정부(240)는 그룹설정 1차 조건에 부합되는 그룹이 존재하지 않은 분석대상 전화번호에 대해서는, 아래의 표 1과 같은 2차 조건 항목에 근거하여 분석대상 전화번호와 각 그룹의 상관점수를 산출하고, 이 중에서 가장 높은 상관점수를 가지는 그룹에 해당 전화번호를 등록한다. 한편, 그룹 설정부(240)는 기존 그룹과의 상관점수가 전혀 나타나지 않은 분석대상 전화번호가 존재하면, 이 분석대상 전화번호를 별도의 신규 그룹으로 형성하여 데이터베이스(270)에 저장할 수 있다. 이 경우, 그룹 설정부(240)는 최초 그룹으로 설정된 전화번호를 대표 전화번호로 설정할 수 있다.
- [0034] 부정지수 평가부(250)는 데이터베이스(270)의 룰셋을 참조하여, 분석대상 전화번호를 이용한 문자 사용 패턴이 부정 사용 패턴에 해당하는 확인하는지 여부를 판별하고, 이 판별된 부정 사용 패턴에 근거하여 분석대상 전화번호의 프로파일의 지수, 부정유형의 지수를 순차적으로 평가한다. 또한, 부정지수 평가부(250)는 상기 평가한 부정유형의 지수 중에서 가장 높은 지수를 분석대상 전화번호의 부정지수로 평가한다. 분석대상 전화번호에 대한 부정지수 평가하는 구체적인 내용은 도 4를 참조한 설명을 통해 후술된다.
- [0035] 도 3은 부정 사용 패턴 항목이 기록된 룰셋을 예시하는 도면이다.
- [0036] 도 3을 참조하면, 상기 룰셋에는 대분류 구분자로서 부정 유형, 중분류 구분자로서 프로파일, 소분류 구분자로서 부정 사용 패턴이 기록된다. 상기 부정 유형으로서, 블랙 리스트, 스패머 및 명의 도용자가 상기 룰셋에 기록된다. 또한, 블랙 리스트 부정 유형에는 재인입 프로파일이 포함되고, 명의 도용자 부정유형에는 명의 도용 프로파일이 포함된다. 상기 스패머 부정 유형에는 발번조작 프로파일, 스팸문구 프로파일, 신고건수 프로파일, 발신량 프로파일, 발신시각 프로파일 및 발송대행 프로파일이 포함된다. 도 3에 도시된 바와 같이, 각각의 프로파일에는 부정 사용 패턴에 대한 정보와 해당 점수가 기록된다.
- [0037] 부정사용 판단부(260)는 분석대상 전화번호의 부정지수가 사전에 설정된 임계값(예컨대, 70%) 이상인지 여부를 판별하여 임계값 이상이면, 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자로서 판별한다. 이때, 부정 사용 판단부(260)는 부정 사용자로서 판별한 가입자에 대한 제재(예컨대, 서비스 직권 해제, 서비스 정지 등)를 운용자에게 요청할 수 있다.

- [0039] 도 4는 본 발명의 일 실시예에 따른, 부정 사용 탐지 시스템에서 스팸 문자 메시지를 발송하는데 이용되는 전화 번호의 부정 사용을 탐지하는 방법을 설명하는 흐름도이다.
- [0040] 도 4를 참조하면, 데이터 수집부(210)는 스패머로서 의심되는 전화번호를 수집하여, 데이터베이스(270)의 분석 대상 목록에 등록한다(S401). 상기 데이터 수집부(210)는 스팸 접수 센터(110), 스팸 알림 서비스 서버(120) 각각으로부터 스팸 전화번호와 스팸 문자 메시지를 수신하여 데이터베이스(270)의 분석대상 목록에 해당 스팸 전화번호를 기록한다.
- [0041] 또한, 데이터 수집부(210)는 특정기간(예컨대, 하루) 동안에 문자 메시지 발송 건수가 허용 임계값을 초과한 가입자의 전화번호를 확인하여, 데이터베이스(270)의 분석대상 목록에 기록할 수 있다. 선택적으로, 데이터 수집부(210)는 관리자로부터 스패머로 의심되는 전화번호를 입력받아, 데이터베이스(270)의 분석대상 목록에 기록할 수 있다.
- [0042] 다음으로, 이렇게 분석대상 목록에 전화번호가 기록되면, 전화번호 필터링부(220)는 일정 주기 간격 또는 실시간으로 분석대상 목록에 기록된 전화번호를 필터링하여 분석이 불필요한 전화번호를 분석대상 목록에서 제거한다(S403). 이때, 전화번호 필터링부(220)는 '010'으로 시작되지 않는 전화번호를 분석대상 목록에서 1차적으로 제거하고, 분석대상 목록에 전화번호 중에서 발신 허용 전화번호 목록에 등록된 전화번호(예컨대, 기업체 전화번호)를 분석대상 목록에서 2차적으로 제거한다. 그리고 전화번호 필터링부(220)는 분석대상 목록에 기록된 전화번호 중에서 타 이동통신사에서 관리하는 전화번호가 기록되는 여부를 확인하여, 타 이동통신사에서 관리하는 전화번호를 상기 분석 대상 리스트에서 3차 제거한다. 또한, 전화번호 필터링부(220)는 데이터베이스(270)의 전산 데이터를 참조하여, 분석대상 목록에 기록된 각 전화번호의 전월과 전전월의 문자 발송량 평균을 전화번호별로 확인하고, 이렇게 확인된 문자 발송량 평균이 사전에 설정된 허용량(예컨대, 500건) 이하인 전화번호를 선별하여 상기 분석대상 목록에서 제거한다.
- [0043] 분석대상 목록의 필터링이 완료되면, 번호 추적부(230)는 분석대상 목록에 기록된 전화번호와 연관되는 전화번호를 추적하여 분석대상 목록에 추가적으로 등록한다(S405). 구체적으로 번호 추적부(230)는 분석대상 목록에 기록된 전화번호와 동일한 가입자 명의(즉, 개인명의 또는 법인명의)를 가지는 전화번호를 데이터베이스(270)의 가입자 정보에서 추적하여 분석대상 목록에 기록한다. 또한, 번호 추적부(230)는 분석대상 목록에 기록된 전화번호를 이용하는 단말기의 식별정보(예컨대, IMEI : International Mobile Equipment Identity)를 가입자 정보에서 확인하고, 이 식별정보와 대응되는 또 다른 전화번호를 가입자 정보에서 추적하여, 분석대상 목록에 기록한다. 즉, 번호 추적부(230)는 분석대상 전화번호를 사용하는 단말기를 식별정보를 확인하고, 상기 식별정보를 가지는 단말기가 또 다른 전화번호를 이용하여 문자 메시지를 발송한 이력이 있는지 여부를 가입자 정보에서 확인하여 발송 이력이 있으면, 상기 또 다른 전화번호를 분석대상 목록에 기록한다.
- [0044] 또한, 번호 추적부(230)는 분석대상 목록에 기록된 전화번호를 가지는 가입자가 이전에 사용하였던 또 다른 전화번호를 가입자 정보에서 추적한다. 즉, 가입자가 전화번호 변동 이력이 존재하면, 번호 추적부(230)는 상기 가입자가 이전에 사용한 또 다른 번호변호를 가입자 정보에서 추적하여 분석대상 목록에 등록한다. 그리고 번호 추적부(230)는 분석대상 목록에 기록된 전화번호가 착신전환 서비스로 이용되었는지 여부를 가입자 정보에서 확인하고, 착신전화 서비스로 이용된 경우, 상기 전화번호와 함께 착신전환 서비스가 진행된 또 다른 전화번호를 가입자 정보에서 추적하여 분석대상 목록에 기록한다.
- [0045] 부연하면, 부정 사용자가 복수의 전화번호를 이용하여 스팸 문자 메시지를 발송하기 때문에, 번호 추적부(230)는 분석대상 전화번호와 연관되는 전화번호를 추적하여 분석대상 목록에 기록한다.
- [0046] 번호 추적부(230)에서 관련 전화번호의 추적이 완료되면, 그룹 설정부(240)는 사전에 정의된 그룹 규칙을 참조하여, 분석대상 목록에 저장된 각 전화번호를 그룹에 등록하여, 각 전화번호별로 그룹을 설정한다(S407). 이때, 그룹 설정부(240)는 분석대상 목록에 등록된 전화번호와 기존의 그룹과의 상관관계를 분석하여, 상관관계가 가장 높게 형성된 그룹에 해당 전화번호를 등록하여, 분석대상 전화번호를 그룹에 등록한다.
- [0047] 부연하면, 상기 그룹 설정부(240)는 분석대상 항목에 등록된 전화번호의 전산 데이터, 각 그룹의 대표 전화번호의 전산 데이터를 일대일 비교하여, 1차 상관관계, 즉, 동일 명의 사용 여부, 동일 발송문구 전송 여부, 동일 단말을 이용한 이력이 있는지 여부, 동일한 결제정보(결제정보로서 동일 은행계좌, 동일 신용카드 정보 또한 동일한 지로 청구지 주소)를 가지는지 여부, 동일한 착신전환 전화번호가 설정된 여부를 확인하여 이 중에서 어느 하나라도 부합되는 전화번호와 그룹의 대표 전화번호가 존재하는 경우, 상기 전화번호를 이 대표 전화번호를 가

지는 그룹에 등록한다. 즉, 그룹 설정부(240)는 동일 명의를 가지는 전화번호, 동일한 발송문구를 전송한 전화 번호, 동일 단말기를 사용한 이력정보가 가지는 전화번호 또는 동일한 결제정보를 가지는 전화번호 동일한 착신 전화번호가 설정된 전화번호를 동일한 그룹으로 형성시킨다.

[0048] 한편, 그룹 설정부(240)는 1차 조건에 부합되는 그룹이 존재하지 않은 분석대상 전화번호에 대해서는, 아래의 2 차 조건 항목에 근거하여 분석대상 전화번호와 각 그룹의 대표 전화번호와의 상관점수를 산출하고, 이 중에서 가장 높은 상관점수를 가지는 그룹에 해당 전화번호를 등록한다.

[0049] 아래의 표 1은 그룹을 형성하기 위한 2차 조건 항목을 예시한 표이다.

표 1

[0050]

2차 조건	상관점수
동일 회신 전화번호	3
동일 개통점	3
유사 개통일	1
유사한 문자사용량	1
동일한 전화번호 뒷 4자리	1
유사한 요금제	1
착신전환 부가서비스 가입	1

[0052] 표 1을 참조하면, 그룹 설정부(240)는 분석대상 전화번호의 전산 데이터와 그룹 대표 전화번호의 전산 데이터를 일대일 비교하여, 분석대상 전화번호와 그룹의 대표 전화번호가 동일 회신 전화번호를 사용하였는지 여부에 확인하여 동일하면, 분석대상 전화번호와 상기 그룹의 상관점수에 3점을 가산시킨다. 또한, 그룹 설정부(240)는 분석대상 전화번호와 상기 대표 전화번호가 동일 개통점에서 개통되었는지 여부를 확인하여, 동일 개통점에서 개통되었으면 분석대상 전화번호와 상기 그룹의 상관점수에 3점을 가산시킨다. 게다가, 그룹 설정부(240)는 분석대상 전화번호와 상기 대표 전화번호의 개통 간격이 사전에 설정된 기간(예컨대, 30) 이내이면, 분석대상 전화번호와 상기 그룹의 상관점수에 1점을 가산시킨다. 상기 그룹 설정부(240)는 분석대상 전화번호와 상기 대표 전화번호의 문자 사용량이 유사하면, 분석대상 전화번호와 상기 그룹의 상관점수에 1점을 가산시킨다. 이때, 상기 그룹 설정부(240)는 일정 기간 동안(예컨대, 3개월)에 발송된 분석대상 전화번호와 상기 대표 전화번호의 문자 사용량 평균값의 차이가 임계사용량 이하이면, 두 전화번호의 문자 사용량이 유사한 것으로 판단하여 분석대상 전화번호와 상기 그룹의 상관점수에 1점을 가산시킬 수 있다.

[0053] 또한, 상기 그룹 설정부(240)는 분석대상 전화번호와 상기 대표 전화번호가 전화번호 뒷 네자리가 동일하면, 분석대상 전화번호와 상기 그룹의 상관점수에 1점을 가산시킨다. 상기 그룹 설정부(240)는 분석대상 전화번호와 상기 대표 전화번호가 착신전환 서비스를 이용된 전화번호이면, 분석대상 전화번호와 상기 그룹의 상관점수에 1점을 가산시킨다.

[0054] 이렇게 그룹설정 2차 조건에 따라 분석대상 전화번호와 각 그룹의 상관점수가 산출이 완료되면, 그룹 설정부(240)는 이 중에서 가장 높은 상관점수를 가지는 그룹에 분석대상 전화번호를 등록한다.

[0055] 한편, 그룹 설정부(240)는 기존 그룹과의 상관점수가 전혀 나타나지 않은 전화번호가 존재하면, 이 전화번호를 별도의 신규 그룹으로 형성할 수 있다.

[0056] 그룹 설정부(240)에 의해 분석대상 전화번호의 그룹이 설정되면, 부정지수 평가부(250)는 데이터베이스(270)에 저장된 룰셋을 참조하여, 이 룰셋에 정의된 부정 사용 패턴과 전화번호별 전산 데이터를 비교 분석하여(S409), 분석대상 전화번호를 이용한 문자 사용 패턴이 부정 사용 패턴에 해당하는 확인하는지 여부를 판별한다. 즉, 부정지수 평가부(250)는 분석대상 전화번호를 이용한 문자 사용 패턴이 도 3과 같은 룰셋(rule set)에 기록된 각 부정 사용 패턴과 일치하는지 여부를 확인하여, 일치하면 프로파일의 점수에 부정 사용 패턴에 해당하는 점수를 가산시킨다.

[0057] 도 3을 참조하여 다시 설명하면, 부정지수 평가부(250)는 분석 대상 전화번호가 불가 목록에 기록된 경우에 해당 전화번호의 재인입 프로파일의 점수를 5점 가산시킨다. 또한, 부정지수 평가부(250)는 분석 대상 전화번호가 차단 목록에 기록된 전화번호인 경우에 분석대상 전화번호의 재인입 프로파일의 점수를 3점 가산시킨다.

- [0058] 부정지수 평가부(250)는 분석대상 전화번호의 전산 데이터를 분석하여, 분석대상 전화번호를 이용한 문자 메시지의 발신번호가 변경된 것으로 판별되면, 상기 분석대상 전화번호의 발신조작 프로파일 점수를 3점 가산시킨다. 이때, 부정지수 평가부(250)는 분석대상 전화번호의 전산 데이터를 토대로, 실제 발신번호와 문자 메시지 내에서의 회선번호가 상이한지 여부를 확인함으로써, 문자 메시지의 발신번호가 조작되었는지 여부를 판별할 수 있다. 게다가, 부정지수 평가부(250)는 일정 기간 동안(예컨대, 3개월 동안)에 분석대상 전화번호를 이용한 문자 발송량의 평균이 1000건 이상인지 여부를 확인하여, 1000건 이상이면, 상기 분석대상 전화번호의 발신조작 프로파일 점수를 3점 가산시킨다.
- [0059] 부정지수 평가부(250)는 분석대상 전화번호를 이용하여 발신된 문자 메시지를 분석하여, 메시지 내용에 악성 스팸 내용(즉 음란/성인, 약물, 대출, 도박)과 관련된 문구가 기록되어 있는지 여부를 판별하여, 기록된 경우에 분석대상 전화번호의 스팸문구 프로파일 점수를 3점 가산시킨다. 또한, 부정지수 평가부(250)는 분석대상 전화번호가 스패머로서 신고된 이력을 데이터베이스(270)에 확인하고, 신고된 이력이 존재하면 이 신고된 문자의 내용이 악성 스팸 내용이지 여부를 판별하여 악성 스팸 내용에 해당하면, 분석대상 전화번호의 스팸문구 프로파일 점수를 3점 가산시킨다.
- [0060] 부정지수 평가부(250)는 분석대상 전화번호가 스패머로서 신고스팸 접수 센터(110)로부터 신고된 횟수를 확인하고, 이 신고 횟수가 5회 이상이면, 분석대상 전화번호의 신고건수 프로파일 점수에 3을 가산시킨다. 부정지수 평가부(250)는 분석대상 전화번호가 스패머로서 스팸 알림 서비스 서버(120)로부터 신고된 횟수를 확인하고, 이 신고 횟수가 10회 이상이면, 분석대상 전화번호의 신고건수 프로파일 점수에 3을 가산시킨다.
- [0061] 부정지수 평가부(250)는 분석대상 전화번호의 문자 발신량을 데이터베이스(270)의 전산 데이터에서 확인하고, 일정기간 동안(예컨대, 3개월 동안)에 상기 분석대상 전화번호를 이용하여 발신된 문자 메시지의 착신번호 개수의 평균(예컨대, 월평균)이 1000개 이상이면, 분석대상 전화번호의 발신량 프로파일 점수에 3점을 가산시킨다. 부정지수 평가부(250)는 일정기간 동안에 상기 분석대상 전화번호가 이용되어 발신된 문자 메시지 발송 건수의 평균(예컨대, 월평균)이 1000건 이상이면, 분석대상 전화번호의 발신량 프로파일 점수에 3점을 가산시킨다. 부정지수 평가부(250)는 일정기간 동안에 분석대상 전화번호를 이용한 일별 문자 메시지의 발송 건수가 150건 이상인 횟수를 확인하고, 이 횟수가 10회 이상이면, 분석대상 전화번호의 발신량 프로파일 점수에 1점을 가산시킨다. 부정지수 평가부(250)는 분석대상 전화번호가 속하는 그룹을 확인하고, 이 그룹에 등록된 전화번호가 10개 이상인지 여부를 판별하여 10개 이상이면, 분석대상 전화번호의 발신량 프로파일 점수에 1점을 가산시킨다. 부정지수 평가부(250)는 분석대상 전화번호가 속하는 그룹에서, 일정기간(예컨대, 한달) 동안에 문자 메시지 착신자로 지정된 착신번호의 개수가 1000개 이상이면, 분석대상 전화번호의 발신량 프로파일 점수에 3점을 가산시킨다.
- [0062] 부정지수 평가부(250)는 분석대상 전화번호에서 발신한 문자 메시지의 일정량(예컨대, 50%) 이상이, 21시에서 8시에서 발신한 것으로 확인되면, 상기 분석대상 전화번호의 발신시각 프로파일 점수에 3점을 가산시킨다. 부정지수 평가부(250)는 분석대상 전화번호에서 발신한 문자 메시지의 내용을 분석하여, 악성(즉, 도박, 약물, 대출, 음란/성인) 스팸 문자 메시지와 관련된 문자 메시지가 존재하면, 상기 분석대상 전화번호의 발신시각 프로파일의 점수에 3점을 가산시킨다.
- [0063] 부정지수 평가부(250)는 분석대상 전화번호가 동일한 내용으로 발송한 문자 메시지를 전산 데이터에서, 이 발송한 문자 메시지에 기록된 문구 종류가 5종류 이상이면, 상기 분석대상 전화번호의 발송대행 프로파일 점수에 3점을 가산시킨다. 즉, 부정지수 평가부(250)는 동일한 문구를 가지는 문자 메시지의 종류가 5종류 이상이면, 해당 분석대상 전화번호가 발송대행에 이용되는 전화번호로서 의심하면, 이 분석대상 전화번호의 발송대행 프로파일 점수에 3점을 가산시킨다. 또한, 부정지수 평가부(250)는 분석대상 전화번호가 속하는 그룹에서 발송된 문자 메시지를 분석하여, 동일한 내용의 문자 메시지를 발송한 전화번호가 3개 이상 존재하면, 상기 분석대상 전화번호의 발송대행 프로파일 점수에 3점을 가산시킨다.
- [0064] 부정지수 평가부(250)는 분석대상 전화번호가 속하는 그룹에서 서로 다른 명의자의 수를 확인하고, 이 명의자의 수가 3개 이상이면, 상기 분석대상 전화번호의 명의도용 프로파일 점수에 3점을 가산시킨다. 또한, 부정지수 평가부(250)는 분석대상 전화번호가 속하는 그룹에서 발송된 문자 메시지를 분석하여, 동일한 내용의 문자 메시지를 발송한 전화번호가 3개 이상 존재하면, 상기 분석대상 전화번호의 명의도용 프로파일 점수에 3점을 가산시킨다.
- [0065] 상기 부정지수 평가부(250)는 각 프로파일의 점수가 5를 초과하지 않도록, 각 프로파일 점수를 조정할 수 있다. 즉, 부정지수 평가부(250)는 특정 프로파일 점수가 5를 초과하는 경우에, 이 프로파일 점수를 5로서 유지시킬

수 있다. 이에 따라, 프로파일 점수는 5 이하의 숫자를 가지게 된다.

[0066] 이렇게, 각각의 프로파일에 점수가 평가되면, 부정지수 평가부(250)는 상기 프로파일 점수를 토대로 프로파일의 지수(%)를 평가한다(S411). 즉, 부정지수 평가부(250)는 프로파일 점수를 5를 나누고 100%를 곱함으로써, 프로파일별 지수를 평가한다. 예컨대, 부정지수 평가부(250)는 발번조작 프로파일 점수가 3점인 경우, 이 발번조작 프로파일의 지수를 60%로 평가할 수 있다.

[0067] 부정지수 평가부(250)는 부정유형(즉, 블랙리스트, 스파머, 명의 도용자)에 포함되는 하나 이상의 프로파일을 각각 확인하고, 부정유형에 포함되는 각 프로파일의 지수 중에서 가장 큰 지수를 해당 부정유형의 지수로서 평가한다(S413). 예컨대, 발번조작 프로파일 지수가 60%, 스팸문구 프로파일 지수가 60%, 신고건수 프로파일 지수가 60%, 발신량 프로파일 지수가 100%, 발신시각 프로파일 지수가 60%, 발송대행 프로파일 지수가 0%인 경우, 부정지수 평가부(250)는 이 중에서 가장 높은 지수(즉, 100%)를 스파머 부정유형의 지수로서 평가할 수 있다.

[0068] 이어서, 부정지수 평가부(250)는 평가된 복수의 부정유형 중에서, 가장 큰 지수를 분석대상 전화번호의 부정지수로서 평가한다(S415). 예컨대, 블랙리스트의 부정유형 지수가 60%, 스파머의 부정유형 지수가 100%, 명의 도용자의 부정유형 지수가 0%인 경우, 부정지수 평가부(250)는, 이 중에서 가장 높은 지수(즉, 100%)를 분석대상 전화번호의 부정지수로서 평가할 수 있다.

[0069] 다음으로, 부정지수 평가부(250)는 그룹의 부정지수를 평가한다(S417). 이때, 부정지수 평가부(250)는 그룹에 소속된 전화번호 부정지수의 평균값을 해당 그룹의 부정지수로서 평가한다.

[0070] 도 5는 본 발명의 일 실시예에 따른, 부정지수가 평가된 그룹과 전화번호를 예시한 도면이다.

[0071] 도 5를 참조하면, 010-XXXX-1234는 각 프로파일 중에서 발신량 프로파일에 가장 높은 지수가 평가되었으며, 이에 따라, 스파머의 부정유형 지수도 90%로 평가되고, 또한 분석대상 전화번호인 010-XXXX-1234의 부정지수도 90%로 평가된다.

[0072] 게다가, 발신번호 010-XXXX-1234의 부정지수(90%)와 010-XXXX-3456의 부정지수(75%)의 평균값(82.5%)가 ID 201를 가지는 그룹의 부정지수로서 평가된다.

[0073] 부정지수 평가부(250)에 의해 분석대상 전화번호의 부정지수가 평가되면, 부정사용 판단부(260)는 분석대상 전화번호의 부정지수가 사전에 설정된 부정 임계값(예컨대, 70%)을 초과하는지 여부를 판별하여(S419), 부정 임계값을 초과하면 상기 분석대상 전화번호를 가지는 가입자를 부정 사용자(예컨대, 스파머)로서 판단한다(S421). 그리고 부정사용 판단부(260)는 상기 부정 사용자로서 판단한 가입자에 대한 제재(예컨대, 서비스 차단 해제, 서비스 정지 등)를 운용자에게 요청한다.

[0075] 상술한 도 4에 따른 프로세스는 한 사이클에 대한 설명으로서, 부정 사용 탐지 시스템(200)은 도 4에 따른 프로세스를 일정한 주기 간격으로 반복적으로 수행하거나, 분석대상 목록에 신규 전화번호가 기록된 경우에 반복적으로 수행한다.

[0076] 한편, 상술한 실시예에서 설명한 그룹 규칙, 룰셋에는 하나 이상의 항목이 생략되거나 새로운 항목이 추가될 수도 있음을 분명히 해 둔다.

[0078] 상술한 바와 같이, 본 발명의 실시예에 따른, 부정 사용 탐지 시스템(200)은 부정 사용자의 문자 발송 패턴을 분석하여 부정 사용자를 자동적으로 탐지하고, 상기 부정 사용자에게 이용정지, 서비스 차단 등과 같은 제재를 가함으로써, 이동통신망에서 발생되는 스팸 문자 메시지를 줄일 수 있다. 또한, 본 발명에 따른 부정 사용 탐지 시스템(200)은 사전에 정의된 부정 사용 패턴 정보와 문자 발송자의 문자 발송 패턴을 비교하고, 이 비교결과에 근거하여 부정 사용자로서 의심되는 전화번호의 부정 지수를 평가하는 매우 빠르고 가벼운 알고리즘을 통해서 부정 사용자를 탐지하기 때문에, 부정 사용자 판별에 필요한 자원(즉, CPU, 메모리)을 절약할 수 있을 뿐만 아니라, 빠른 속도로 부정 사용자를 탐지할 수 있다. 또한, 본 발명에 따른 부정 사용 탐지 시스템(200)은 전화번호가 스파머로서 신고되면, 이 전화번호와 연관된 다른 전화번호를 추적하여 그룹에 등록하고, 동일 그룹에 속하는 전화번호를 통해 발송되는 문자 메시지를 지속적으로 모니터링함으로써, 복수의 전화번호를 이용하여 스팸 메시지를 발송하는 부정 사용자를 색출할 수 있다.

[0079] 본 명세서는 많은 특징을 포함하는 반면, 그러한 특징은 본 발명의 범위 또는 특허청구범위를 제한하는 것으로

해석되어서는 안 된다. 또한, 본 명세서에서 개별적인 실시예에서 설명된 특징들은 단일 실시예에서 결합되어 구현될 수 있다. 반대로, 본 명세서에서 단일 실시예에서 설명된 다양한 특징들은 개별적으로 다양한 실시예에서 구현되거나, 적절히 결합되어 구현될 수 있다.

[0080] 도면에서 동작들이 특정한 순서로 설명되었으나, 그러한 동작들이 도시된 바와 같은 특정한 순서로 수행되는 것으로, 또는 일련의 연속된 순서, 또는 원하는 결과를 얻기 위해 모든 설명된 동작이 수행되는 것으로 이해되어서는 안 된다. 특정 환경에서 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 아울러, 상술한 실시예에서 다양한 시스템 구성요소의 구분은 모든 실시예에서 그러한 구분을 요구하지 않는 것으로 이해되어야 한다. 상술한 프로그램 구성요소 및 시스템은 일반적으로 단일 소프트웨어 제품 또는 멀티풀 소프트웨어 제품에 패키지로 구현될 수 있다.

[0081] 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(시디롬, 램, 톱, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

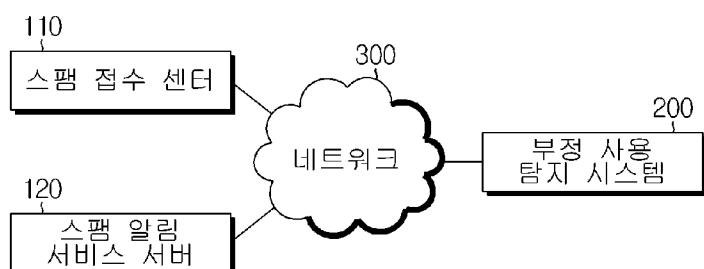
[0082] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

부호의 설명

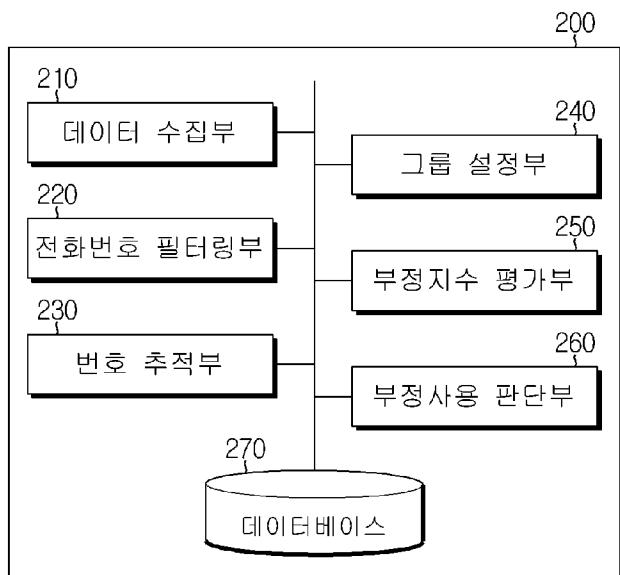
110 : 스팸 접수 센터	120 : 스팸 알림 서비스 서버
200 : 부정 사용 탐지 시스템	210 : 데이터 수집부
220 : 전화번호 필터링부	230 : 번호 추적부
240 : 그룹 설정부	250 : 부정지수 평가부
260 : 부정사용 판단부	270 : 데이터베이스
300 : 네트워크	

도면

도면 1



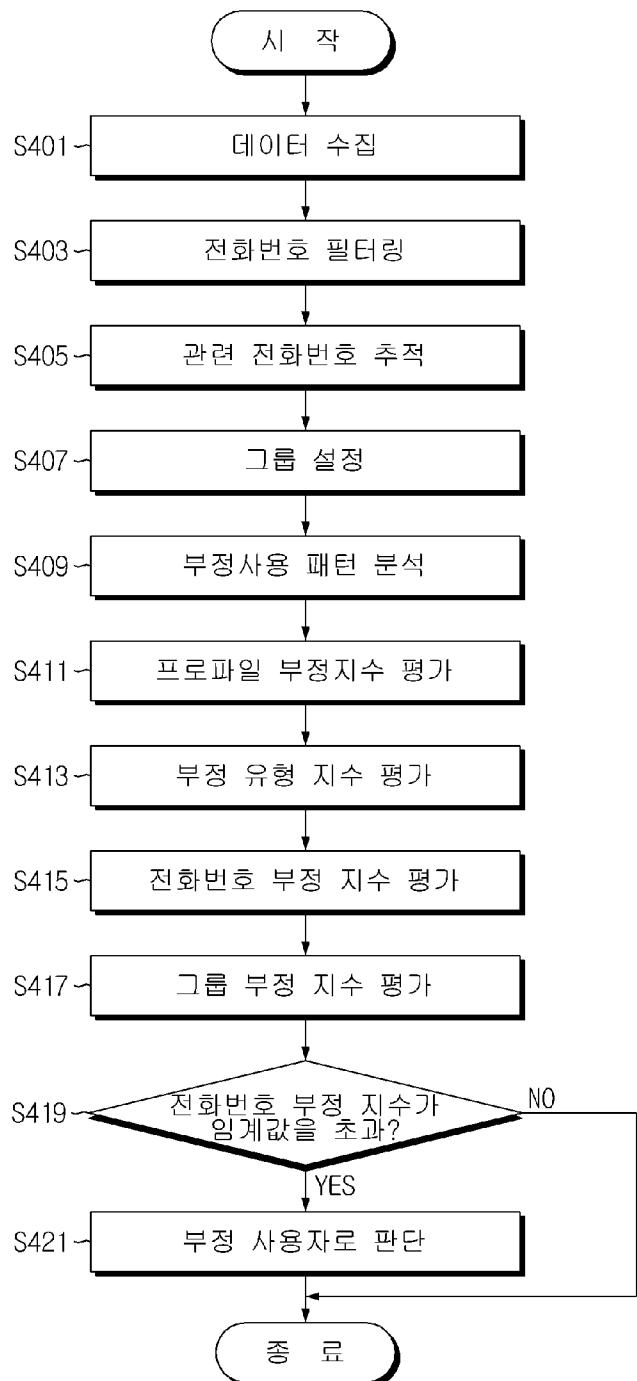
도면2



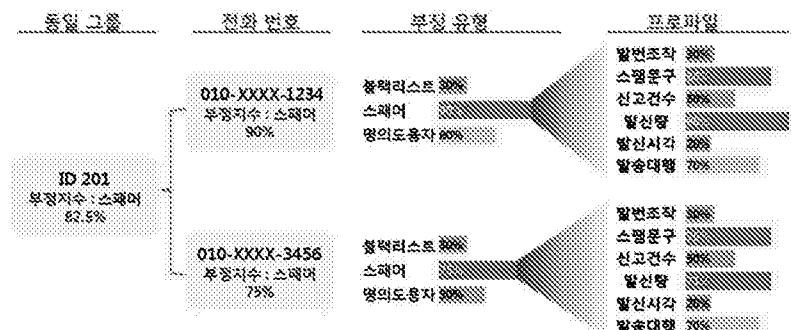
도면3

부정유형	프로파일	부정 사용 기준	점수
블랙리스트	재인입	불가 목록 번호 차단 목록 번호	5 3
스팸	발번조작	발신 번호 조작 문자발송 평균 건수가 1000건 이상	3 3
		문구 내용이 악성 스팸 문구 신고 유형이 악성 스팸 문구	3 3
	신고건수	스팸 접수 센터의 신고 건수가 5건 이상 스팸 알림 서비스 서버의 신고 건수가 10건 이상	3 3
		착신 번호 수가 1000개 이상 문자발송 건수가 1000건 이상	3 3
	발신량	150건 이상의 메시지를 발송한 일수가 10회 이상 동일 그룹에서의 발신번호 개수가 10개 이상 동일 그룹에서의 착신번호 개수가 1000개 이상	1 1 3
		문자 발신 시각이 21시~08시	3
		문구 유형이 악성 스팸 문구	3
		문구 종류가 5가지 이상 동일 그룹에서 동일문구로 발송한 전화번호가 3개 이상	3 3
명의도용자	명의도용	동일 그룹에서의 명의자 수가 3 이상 동일 그룹에서 동일문구로 발송한 전화번호가 3개 이상	3 3

도면4



도면 5





(19) 대한민국특허청(KR)
 (12) 공개특허공보(A)

(11) 공개번호 10-2017-0060958
 (43) 공개일자 2017년06월02일

(51) 국제특허분류(Int. Cl.)
G06Q 40/00 (2006.01) *G06F 17/30* (2006.01)
G06Q 50/10 (2012.01)

(71) 출원인
 고려대학교 산학협력단
 서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(52) CPC특허분류
G06Q 40/00 (2013.01)
G06F 17/30 (2013.01)

(72) 발명자
 임희석
 경기도 수원시 영통구 영통로 460, 304동 1704호
 (영통동, 대우아파트)

(21) 출원번호 10-2015-0165763
 (22) 출원일자 2015년11월25일
 심사청구일자 2015년11월25일

(74) 대리인
 특허법인충현

전체 청구항 수 : 총 11 항

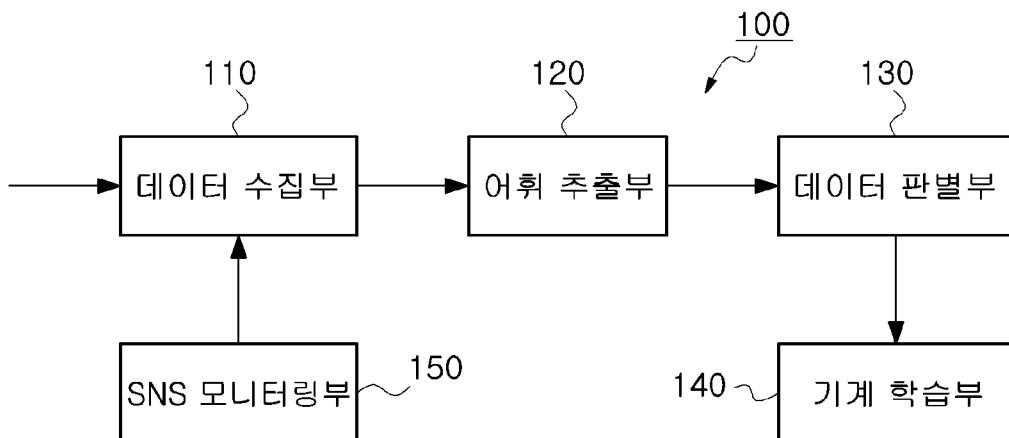
(54) 발명의 명칭 금융 사기 방지 방법 및 시스템

(57) 簡 説

본 발명은 금융 사기 방지 방법 및 시스템에 관한 것으로, 데이터수집부가 금융 사기 의심 데이터를 수집하는 단계와 어휘추출부가 수집한 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하는 단계 및 데이터판별부가 추출한 상기 어휘 데이터를 분석하여 수집한 상기 금융 사기 의심 데이터가 금융 사기 관련 데이터에 해당하는지 판별하는 단계를 포함한다.

이러한 구성에 의해, 본 발명의 금융 사기 방지 방법 및 시스템은 금융 사기가 의심되는 데이터를 수집하고, 수집된 데이터 내 금융 사기를 나타내거나 암시하는 어휘 데이터가 존재하는지 확인하여 수집한 데이터가 금융 사기 관련 데이터인지 여부를 판별함으로써, 불특정 다수의 사람들이 금융 사기 피해를 입는 것을 미연에 방지할 수 있는 효과가 있다.

☞ ☞ ☞ - 도1



(52) CPC특허분류

G06Q 40/02 (2013.01)

G06Q 50/10 (2015.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 R1415242

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 개인과 집단지성의 디지털콘텐츠화를 통한 유통 및 홍보 서비스 기술 개발

기여율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.05.01 ~ 2016.02.29

영세서

청구범위

청구항 1

데이터수집부가 금융 사기 의심 데이터를 수집하는 단계;

어휘추출부가 수집한 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하는 단계; 및

데이터판별부가 추출한 상기 어휘 데이터를 분석하여 수집한 상기 금융 사기 의심 데이터가 금융 사기 관련 데이터에 해당하는지 판별하는 단계;를 포함하는 금융 사기 방지 방법.

청구항 2

제 1 항에 있어서,

상기 데이터수집부가 금융 사기 의심 데이터를 수집하는 단계는

이동단말 데이터 수집 클라이언트 또는 이메일 데이터 수집 클라이언트로부터 문자열로 이루어지는 금융 사기 의심 데이터를 입력받는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 3

제 1 항에 있어서,

상기 어휘추출부가 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하는 단계는

수집한 상기 금융 사기 의심 데이터에 대하여 전처리를 수행하여 문장 단위 데이터를 획득하는 과정;

상기 문장 단위 데이터의 형태소를 분석하는 과정;

형태소가 분석된 상기 문장 단위 데이터에 해당하는 품사를 태깅하는 과정;

품사가 태깅된 상기 문장 단위 데이터에 대하여 품사별 클러스터링을 수행하는 과정; 및

품사별로 클러스터링된 상기 문장 단위 데이터와 유사한 어휘를 갖는 어휘 데이터를 기 설정된 금융 사기 관련 데이터가 기저장된 데이터베이스로부터 추출하는 과정;을 포함하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 4

제 3 항에 있어서,

상기 금융 사기 의심 데이터에 대하여 전처리를 수행하여 문장 단위 데이터를 획득하는 과정은

상기 금융 사기 의심 데이터 내 문자열의 형태를 분석하여, 문장 단위 데이터 또는 메타 데이터를 검출하는 과정; 및

검출된 상기 문장 단위 데이터 내 존재하는 불용어를 제거하거나, 또는 문장 단위 데이터의 띄어쓰기를 수행하는 과정;을 포함하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 5

제 3 항에 있어서,

상기 품사별로 클러스터링된 상기 문장 단위 데이터와 유사한 어휘를 갖는 어휘 데이터를 기 설정된 금융 사기 관련 데이터가 기저장된 데이터베이스로부터 추출하는 과정은

벡터 공간 모델을 이용하여 문서 연관도를 계산하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 6

제 3 항에 있어서,

상기 품사별로 클러스터링된 상기 문장 단위 데이터와 유사한 어휘를 갖는 어휘 데이터를 기 설정된 금융 사기 관련 데이터가 기저장된 데이터베이스로부터 추출하는 과정은

다변량 통계분석 방법(Latent Semantic Analysis, LSA)의 의미 검색 모델을 이용하여 의미적 유사성을 파악하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 7

제 1 항에 있어서,

기계학습부가 금융 사기 관련 데이터라고 판별한 의심 데이터에 대하여 기계학습을 수행하는 단계;를 더 포함하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 8

제 7 항에 있어서,

상기 기계학습부가 금융 사기 관련 데이터라고 판별한 의심 데이터에 대하여 기계학습을 수행하는 단계는

나이브 베이즈(Naive Bayes) 분류 방법, SVM(Support Vector Machine) 분류 방법, 랜덤포레스트(Random Forest) 분류 방법 중 적어도 하나의 분류방법을 이용하여 기계학습한 금융 사기 관련 데이터라고 판별한 의심 데이터를 분류하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 9

제 1 항에 있어서,

SNS모니터링부가 소셜 네트워크를 통해 복수 개의 단말간에 송수신되는 데이터에 대하여 데이터베이스에 기저장된 금융 사기 관련 데이터에 해당하는지 여부를 모니터링하는 단계;를 더 포함하는 것을 특징으로 하는 금융 사기 방지 방법.

청구항 10

제1항 내지 제9항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

청구항 11

금융 사기 의심 데이터를 수집하는 데이터수집부;

수집한 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하는 어휘추출부; 및

추출한 상기 어휘 데이터를 분석하여 수집한 상기 금융 사기 의심 데이터가 금융 사기 관련 데이터에 해당하는지 판별하는 데이터판별부;를 포함하는 금융 사기 방지 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 금융 사기 방지 방법 및 시스템에 관한 것으로, 특히 불특정 다수가 사용하는 이동 단말이 해킹을 당해 이로 인한 금융 사기가 발생하는 것을 미연에 방지하기 위한 금융 사기 방지 방법 및 시스템에 관한 것이다.

◆ 경기 ◆

[0002] IT 기술이 급속히 발전함에 따라, 발전된 IT 기술을 사용하는 사용자들의 삶이 편리해지는 장점이 발생하는 반면에, 이와 같이 발전된 IT 기술을 부정적인 목적으로 이용하여 불특정 다수의 사용자들에게 피해를 입히는 금융 사기의 발생 횟수 또한 급격히 증가하고 있다.

[0003] 이처럼 빈번히 발생하는 금융 사기는 금융 거래에서 사람을 속이거나 착각하게 하여 이득을 취하려는 불법적인 행동으로서, 다단계 피라미드 금융 사기, 보험 사기, 허위 투자 설명회를 통한 사기 등과 같이 그 종류도 다양

하다.

[0004] 특히, 지금까지는 적은 돈으로 많은 돈을 벌 수 있는 특별한 방법을 찾는 일부의 사람들이 금융 사기의 주요 피해 대상이 되는 경우가 많았지만, 최근에는 불특정 대다수의 사람들을 상대로 금융 사기를 시도하는 경우가 점차 늘어남에 따라, 일반 대중들도 금융 사기의 피해를 당하는 일이 많아지고 있다. 그 피해의 대표적인 예가 전화 금융 사기인 보이스 피싱(voice phishing)이다.

[0005] 보이스 피싱이란, 음성(Voice)과 개인정보(private information) 및 낚시(fishing)의 복합어로서, 전화로 하는 가장 오래된 사기 수법이지만 여전히 진화하고 있으며, 불특정 다수의 사람들에게 손쉽게 노출되는 금융 사기 유형이다.

[0006] 특히, 예전에는 전화번호가 추적되지 않는 해외에서 범죄자가 금융회사를 사칭하여 다수의 사람들에게 피해를 입혔지만, 최근에는 발신번호가 금융기관의 전화번호를 표시하는 전화 금융 사기 사례 또한 발생하고 있다. 이러한 전화 금융 사기 사례의 경우에는 범죄자가 공공기관의 전화번호와 직원을 사칭하고, 개인정보 유출로 인해 예금보호조치가 필요하다고 현금지급기로 유인하여 자금을 이체하도록 한다.

[0007] 이처럼, 이메일, 문자메시지, SNS 정보 등을 이용한 금융 사기 수법이 점차 고도화 됨에 따라, 불특정 다수의 사람들이 금융 사기의 피해자를 입는 문제점이 발생했다.

실행기술문항

특허문항

[0008] (특허문항 0001) 대한민국 공개특허공보 제10-2011-0048825호 (2011년 05월 12일)

발명의 내용

제1장 제1부 제1장

[0009] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 이메일, 문자 메시지, SNS 정보 등을 이용한 금융 사기가 의심되는 데이터를 수집하고, 수집된 데이터 내 금융 사기를 나타내거나 암시하는 어휘 데이터가 존재하는지 확인하여 수집한 데이터가 금융 사기 관련 데이터인지 여부를 판별함으로써, 불특정 다수의 사람들이 금융 사기 피해를 입는 것을 미연에 방지할 수 있는 금융 사기 방지 방법 및 시스템을 제공하고자 한다.

제2장 제1부 제2장

[0010] 상기 목적을 달성하기 위해 본 발명은 데이터수집부가 금융 사기 의심 데이터를 수집하는 단계와, 어휘추출부가 수집한 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하는 단계 및 데이터판별부가 추출한 상기 어휘 데이터를 분석하여 수집한 상기 금융 사기 의심 데이터가 금융 사기 관련 데이터에 해당하는지 판별하는 단계를 포함하여 구성한다.

[0011] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 데이터수집부가 금융 사기 의심 데이터를 수집하는 단계는 이동단말 데이터 수집 클라이언트 또는 이메일 데이터 수집 클라이언트로부터 문자열로 이루어지는 금융 사기 의심 데이터를 입력받는 것을 특징으로 한다.

[0012] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 어휘추출부가 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하는 단계는 수집한 상기 금융 사기 의심 데이터에 대하여 전처리를 수행하여 문장 단위 데이터를 획득하는 과정과, 상기 문장 단위 데이터의 형태소를 분석하는 과정과, 형태소가 분석된 상기 문장 단위 데이터에 해당하는 품사를 태깅하는 과정과, 품사가 태깅된 상기 문장 단위 데이터에 대하여 품사별 클러스터링을 수행하는 과정 및 품사별로 클러스터링된 상기 문장 단위 데이터와 유사한 어휘를 갖는 어휘 데이터를 기설정된 금융 사기 관련 데이터가 기저장된 데이터베이스로부터 추출하는 과정을 포함하는 것을 특징으로 한다.

[0013] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 금융 사기 의심 데이터에 대하여 전처리를 수행하여 문장 단위 데이터를 획득하는 과정은 상기 금융 사기 의심 데이터 내 문자열의 형태를 분석하여, 문장 단위 데이터 또는 메타 데이터를 검출하는 과정 및 검출된 상기 문장 단위 데이터 내 존재하는 불용어를 제거하거나, 또는

문장 단위 토큰화를 수행하는 과정을 포함하는 것을 특징으로 한다.

[0014] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 품사별로 클러스터링된 상기 문장 단위 토큰화와 유사한 어휘를 갖는 어휘 토큰화를 기 설정된 금융 사기 관련 토큰화가 기저장된 데이터베이스로부터 추출하는 과정은 벡터 공간 모델을 이용하여 문서 연관도를 계산하는 것을 특징으로 한다.

[0015] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 품사별로 클러스터링된 상기 문장 단위 토큰화와 유사한 어휘를 갖는 어휘 토큰화를 기 설정된 금융 사기 관련 토큰화가 기저장된 데이터베이스로부터 추출하는 과정은 다변량 통계분석 방법(Latent Semantic Analysis, LSA)의 의미 검색 모델을 이용하여 의미적 유사성을 파악하는 것을 특징으로 한다.

[0016] 본 발명에 따른 금융 사기 방지 방법에 있어서, 기계학습부가 금융 사기 관련 토큰화라고 판별한 의심 토큰화에 대하여 기계학습을 수행하는 단계를 더 포함하는 것을 특징으로 한다.

[0017] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 기계학습부가 금융 사기 관련 토큰화라고 판별한 의심 토큰화에 대하여 기계학습을 수행하는 단계는 나이브 베이즈(Naive Bayes) 분류 방법, SVM(Support Vector Machine) 분류 방법, 랜덤포레스트(Random Forest) 분류 방법 중 적어도 하나의 분류방법을 이용하여 기계학습한 금융 사기 관련 토큰화라고 판별한 의심 토큰화를 분류하는 것을 특징으로 한다.

[0018] 본 발명에 따른 금융 사기 방지 방법에 있어서, SNS모니터링부가 소셜 네트워크를 통해 복수 개의 단말간에 송수신되는 토큰화에 대하여 토큰화에 기저장된 금융 사기 관련 토큰화에 해당하는지 여부를 모니터링하는 단계를 더 포함하는 것을 특징으로 한다.

[0019] 또한, 본 발명은 금융 사기 의심 토큰화를 수집하는 토큰화수집부와, 수집한 상기 금융 사기 의심 토큰화로부터 금융 사기를 나타내는 어휘 토큰화를 추출하는 어휘추출부 및 추출한 상기 어휘 토큰화를 분석하여 수집한 상기 금융 사기 의심 토큰화가 금융 사기 관련 토큰화에 해당하는지 판별하는 토큰화판별부를 포함하여 구성한다.

발명의 효과

[0020] 본 발명의 금융 사기 방지 방법 및 시스템은 금융 사기가 의심되는 토큰화를 수집하고, 수집된 토큰화 내 금융 사기를 나타내거나 암시하는 어휘 토큰화가 존재하는지 확인하여 수집한 토큰화가 금융 사기 관련 토큰화인지 여부를 판별함으로써, 불특정 다수의 사람들이 금융 사기 피해를 입는 것을 미연에 방지할 수 있는 효과가 있다.

[0021] 또한, 본 발명의 금융 사기 방지 방법 및 시스템은 소셜 네트워크를 기반으로 단말간에 송수신되는 토큰화가 금융 사기 관련 토큰화에 해당하는지 여부를 기 설정된 시간마다 모니터링하고, 모니터링 결과를 금융 사기 경계 지수로 연산하여, 연산된 금융 사기 경계 지수를 수치, 텍스트, 그림 등의 여러 형태로 표시함으로써, 소셜 네트워크를 이용하는 불특정 다수에게 금융 사기 예방에 대한 안전성을 제공할 수 있는 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시 예에 따른 금융 사기 방지 시스템의 블록도이다.

도 2는 본 발명의 다른 실시 예에 따른 금융 사기 방지 방법의 순서도이다.

도 3은 금융 사기 의심 토큰화를 수집하는 과정을 나타낸 도면이다.

도 4는 본 발명의 일 실시 예에 따른 의미 검색 모델을 나타내는 도면이다.

도 5는 본 발명의 일 실시 예에 따른 언어자원 구축 방법을 나타내는 도면이다.

도 6은 소셜 네트워크 기반 금융 사기 경계 지수를 나타낸 도면이다.

도 7은 본 발명의 금융 사기 방지 방법을 분산 처리 시스템을 통해 구현하는 과정을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

- [0024] 이하, 도 1을 참조하여 본 발명의 일 실시 예에 따른 금융 사기 방지 시스템에 대하여 보다 자세히 살펴보도록 한다.
- [0025] 도 1은 본 발명의 일 실시 예에 따른 금융 사기 방지 시스템의 블록도이다.
- [0026] 도 1에 도시된 바와 같이, 본 발명의 금융 사기 방지 시스템(100)은 데이터수집부(110), 어휘추출부(120), 데이터판별부(130), 기계학습부(140), 및 SNS모니터링부(150)를 포함하며, 마이크로프로세서, 입출력 장치, 메모리를 통해 구현될 수 있다.
- [0027] 데이터수집부(110)는 이동 단말간 송수신되는 데이터를 수집하는 별도의 이동 단말 데이터 수집 클라이언트 또는 이메일로 송수신되는 데이터를 수집하는 별도의 이메일 데이터 수집 클라이언트로부터 문자열로 이루어지는 금융 사기 의심 데이터를 수집한다.
- [0028] 어휘추출부(120)는 수집한 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내는 어휘 데이터를 추출하고, 데이터판별부(130)는 추출한 상기 어휘 데이터의 형태 및 내용을 분석하여 수집한 상기 금융 사기 의심 데이터가 금융 사기 관련 데이터인지 여부를 판별한다.
- [0029] 기계학습부(140)는 금융 사기 관련 데이터라고 판별한 의심 데이터에 대하여 기계학습을 수행하고, SNS모니터링부(150)는 소셜 네트워크를 통해 복수 개의 단말간에 서로 송수신되는 데이터가 데이터베이스에 기저장된 금융 사기 관련 데이터에 해당하는지 여부를 모니터링한다.
- [0030] 이하, 도 2를 참조하여 본 발명의 다른 실시 예에 따른 금융 사기 방지 방법에 대하여 자세히 살펴보도록 한다.
- [0031] 도 2는 본 발명의 다른 실시 예에 따른 금융 사기 방지 방법의 순서도이다. 도 2에 도시된 바와 같이, 본 발명의 금융 사기 방지 방법은 먼저 데이터수집부(110)가 이동단말 데이터 수집 클라이언트 또는 이메일 데이터 수집 클라이언트로부터 문자열로 이루어지는 금융 사기 의심 데이터를 입력받아 수집한다(S210). 예를 들면, 도 3에 도시된 바와 같이, “[순천경찰서]홍길동님사건번호(13-093157)관련긴급출석요구서/내용확인sc-police.co.kr”와 같은 문자열로 이루어진 금융 사기 의심 데이터를 수집할 수 있다.
- [0032] 어휘추출부(120)가 앞서 수집한 상기 금융 사기 의심 데이터로부터 금융 사기를 나타내거나, 암시하는 어휘 데이터를 추출한다(S220). 이러한 어휘 데이터의 추출과정을 보다 자세히 살펴보면, 앞서 수집한 상기 금융 사기 의심 데이터에 대하여 전처리를 수행하여 문장 단위 데이터를 획득한다. 이때, 상기 금융 사기 의심 데이터에 수행되는 전처리 과정은 앞서 수집한 상기 금융 사기 의심 데이터를 이루는 문자열의 형태를 분석하여, 금융 사기 관련 내용을 나타내는 문장 단위 데이터 또는 상기 금융 사기 의심 데이터를 발송한 이동 단말의 메타 데이터를 검출한다.
- [0033] 이에 따라, “[순천경찰서] 홍길동님 사건번호(13-093157)관련 긴급 출석요구서/내용확인 sc-police.co.kr”이라는 문장 단위 데이터를 획득하고, 상기 금융 사기 의심 데이터를 발송한 휴대폰 번호, 날짜, 시간, 웹사이트 주소를 나타내는 메타 데이터 또한 획득할 수 있다.
- [0034] 이어서, 검출된 상기 문장 단위 데이터 내 존재하는 욕설, 비속어와 같은 불용어를 제거하거나, 또는 상기 문장 단위 데이터의 띠어쓰기를 수행한다.
- [0035] 이처럼, 불용어를 제거하고, 띠어쓰기도 수행된 상기 문장 단위 데이터에 대하여 형태소를 분석한다. 상기 문장 단위 데이터의 형태소를 분석하여, 상기 문장 단위 데이터를 주어, 명사, 동사, 목적어, 조사, 부사 등으로 각각 나눈다.
- [0036] 이후, 형태소를 분석한 상기 문장 단위 데이터 별로 각각 해당하는 품사를 태깅한다. 예를 들면, “순천경찰서”에 ‘명사’라는 품사를 태깅하고, “긴급”에 ‘부사’라는 품사를 태깅할 수 있다.
- [0037] 이처럼 품사가 태깅된 상기 문장 단위 데이터에 대하여 각각의 품사별로 클러스터링을 수행한다.
- [0038] 이후, 품사별로 클러스터링된 상기 문장 단위 데이터에 대하여 데이터베이스에 기저장된 복수 개의 금융 사기 관련 데이터와 동일 어휘 또는 유사 어휘를 검색하여 어휘 데이터를 추출한다. 이를 위해, 벡터 공간 모델, 의미 검색 모델을 이용하여 상기 동일한 품사별로 클러스터링된 문장 단위 데이터와 동일하거나, 유사한 어휘를 갖는 어휘 데이터를 추출할 수 있다.
- [0039] 여기서 어휘 데이터 추출을 위한 벡터 공간 모델은 텍스트 문서를 단어 색인 등의 식별자로 구성된 벡터로 표현하는 대수적 모델을 의미하며, 정보 검색, 정보 필터링 및 검색 엔진의 색인이나 연관도 순위에 사용된다. 문서

와 질의는 수학식 1과 같이 벡터로 표현된다.

수학식 1

$$[0040] \quad d_j = (\omega_{1,j}, \omega_{2,j}, \dots, \omega_{t,j}), \quad q = (\omega_{1,q}, \omega_{2,q}, \dots, \omega_{t,q})$$

[0041] 수학식 1에서 d_j 는 문서 벡터를, q 는 질의 벡터를 의미하며, 각각의 차원은 개별 단어에 대응된다. 어떤 단어가 문서에 포함되면, 해당 단어는 0이 아닌 벡터값을 갖는다. 단어 가중치라고도 불리는 이 값을 산출하는 방법에는 여러가지가 있으며 가장 널리 알려진 방식은 TF-IDF(Term Frequency - Inverse Document Frequency) 방식이다.

[0042] 벡터 공간 모델에서 단어(term)의 의미는 그 적용 대상에 따라 달라지며, 일반적으로 하나의 단어(word)나 키워드, 또는 좀더 긴 구를 의미한단. 벡터의 차원의 크기는 말뭉치에 포함된 단어의 개수와 같다.

[0043] 상기와 설명한 벡터 공간 모델에 대해서 문서 유사도 이론을 이용하여 키워드 검색에서 사용되는 문서의 연관도를 계산할 수 있다. 문서 유사도 이론에서 문서 유사도는 문서 벡터간의 각도의 편차를 이용하여 산출한다. 실제 적용 시에는 문서 벡터간의 각도 자체보다는 수학식 2와 같이 산출하기 용이하다.

수학식 2

$$[0044] \quad \cos\theta = \frac{d_2 \cdot q}{\|d_2\| \cdot \|q\|}$$

[0045] 수학식 2에서 " $d_2 \cdot q$ "는 문서 벡터(d_2)와 질의 벡터(q)의 교차점(스칼라 곱)에 해당하며, $\|d_2\|$ 는 벡터 d_2 의 노름, $\|q\|$ 는 벡터 q 의 노름을 의미한다. 벡터의 노름은 수학식 3과 같이 계산된다.

수학식 3

$$[0046] \quad \|q\| = \sqrt{\sum_{i=1}^n q_i^2}$$

[0047] 벡터의 모든 요소는 음수가 아닌 값이므로, 코사인 값이 0인 경우 질의 벡터와 문서 벡터가 직교하며 겹치는 부분이 전혀 없음(서로 동일하게 포함하고 있는 단어가 하나도 없음)을 의미한다. 벡터간 각도의 코사인 값을 이용한 유사도 계산은 수학식 2에서 설명한 코사인 값을 사용하여 유사도를 계산한다.

[0048] 상기와 같이 어휘 데이터 추출 시 공간 벡터 모델을 사용하면 선형 대수에 기반한 단순한 모델로 문서와 질의간의 유사도를 연속적인 값으로 계산이 가능하고, 연관도에 의한 문서 순위 결정이 가능하며, 부분 일치 등에 대해서도 고려가 가능한 이점이 있다.

[0049] 이러한 공간 벡터 모델은 금융 메시지를 벡터 모델로 표현하고 이를 기반의 서로의 유사도를 계산하는데 사용할 수 있다. 일 예를 들어 "농협 귀하의 개인 정보가 노출되었습니다. 정보 확인 : nh-mbank.com"과 같은 스팸 메시지가 있다. 여기서 이와 비슷하게 "수협 귀하의 개인 정보가 노출되었습니다. 정보 확인 : sh-mbank.com"이라는 의심 메시지가 있다. 여기서 농협과 수협의 두 메시지를 벡터모델로 변환하게 되면 수학식 4와 같다.

수학식 4

[0050] $S(\text{스팸 메시지}) = \{\text{농협, 개인, 정보, 노출, 확인, nh-mbank.com}\}$

[0051] $S'(\text{의심 메시지}) = \{\text{수협, 개인, 정보, 노출, 확인, sh-mbank.com}\}$

[0052] 수학식 4와 같이 스팸 메시지와 의심 메시지를 벡터모델로 변환하고 수학식 5를 이용하여 유사도를 계산할 수 있다.

수학식 5

[0053]
$$\frac{S \cdot S'}{\|S\| \|S'\|} = \frac{4 \times 4}{\sqrt{6^2} \times \sqrt{6^2}} = 0.44$$

[0054] 수학식 5와 같이 간단하게 일치 여부만을 계산할 경우 서로 44%의 유사도를 가지고 있음을 확인할 수 있다. 이렇게 벡터 모델을 이용하여 유사도를 계산하는 과정은 계산이 간단하고 직관적인 결과값을 얻을 수 있다.

[0055] 다음으로 어휘 데이터 추출을 위한 본 발명의 의미 검색 모델에 대해서 설명하겠다. 의미 검색 모델은 벡터 모델에 한계점인 의미적 유사성 탐색을 위한 모델로 빠르게 메시지의 스팸 여부를 확인이 가능하다.

[0056] 이러한 의미 검색 모델에 대해서 상세하게 설명하면, 먼저 언어에서 의미를 이해하고 처리하기 위한 가장 대표적인 방법은 의미 정보들을 미리 사전에 구축하고 이를 비교하며 사용하는 방법이다. 사전 구축은 언어의 의미를 파악할 수 있는 사람이 직접 사전에 등록함으로 정확하게 구축이 가능하다.

[0057] 다만 이러한 방법은 구축 과정에서 많은 비용이 든다는 단점이 있다. 또한, 언어 환경은 지속적으로 변화함으로 구축된 사전 역시 지속적으로 관리 및 업데이트를 실시해야 한다.

[0058] 금융 상기 메시지의 경우에는 현재 사회적 이슈에 따라서 발생했다가 사라지는 경우가 대부분으로 상기와 같이 금융 사기 방지를 위한 사전을 등록하여도 새로운 금융 사기 메시지를 잘 방지할 수 있다는 보장이 없다.

[0059] 따라서 본 발명의 의미 검색 모델은 언어의 문맥 안에서 어떠한 단어와 어떠한 단어가 같은 문맥에서 함께 사용되는지에 대한 공기 정보(co-occurrence)를 이용하고 있다. 의미적 검색을 위한 의미 검색 모델에서는 LSA(Latent Semantic Analysis)를 적용하여 고차원의 개념 공간을 생성하고 이를 통한 의미 분석을 수행할 수 있다.

[0060] 여기서 LSA는 다변량 통계분석 방법으로 고차원의 데이터 공간에 대해 축을 변경하여 그 데이터를 가장 잘 설명 할 수 있는 새로운 축을 찾아내고 정보가 적은 축들을 걸러냄으로써 데이터에 내포되어 있는 구조를 밝히는 기법이다.

[0061] LSA를 위해서 Singular Value Decomposition(SVD)이라는 선형대수학 기법을 사용하는데 SVD를 거치면서 설명력이 높은 순서로 원하는 만큼의 고유 벡터를 획득할 수 있다. 이때, 정보가 적은 축을 잡음으로 간주하여 제거함으로써 계산을 위한 데이터의 차원을 줄이는 효과도 얻을 수 있다.

[0062] 이러한 SVD를 통하여 얻어진 고유 벡터는 본래 데이터 벡터에서 나타나지 않은 의미구조를 나타내게 되므로 보다 심층적인 차원에서 의미 분석이 가능하다.

[0063] 상기 설명한 바와 같이 LSA 기법을 이용한 의미 검색 모델의 기본적 형태는 벡터 공간 모델과 동일하게 데이터를 벡터 형태로 표현한다. 표현된 벡터를 LSA를 통하여 의미적 구조가 내포된 새로운 벡터를 획득한다. 의미 검색 모델은 도 4와 같다.

[0064] 도 4는 본 발명의 일 실시 예에 따른 의미 검색 모델을 나타내는 도면이다. 도 4를 참조하면 단어-문서 형태로 표현된 행렬을 SVD 변환을 통하여 오른쪽 형태로 분해한다. 즉, 여기서 단어의 수가 t이고 문서의 수가 d인 $t \times d$ 벡터 X는 수학식 6과 같이 분해된다.

수학식 6

$$X = T_0 S_0 D_0$$

[0065] [0066] 수학식 6에서 T_0 , D_0 은 직교정규(orthonormal) 열로 이루어지며 각각의 벡터들로 이루어져 있고, T_0 는 고유값(singular value)의 대각선(diagonal) 벡터로 값이 큰 순서로 정렬되어 있다. 여기서 k개 만큼의 벡터만을 사용하여 행렬을 만들면 본래 행렬 S의 근사치가 된다. 각 벡터에 대응하는 고유값이 클수록 그 벡터는 주어진 데이터를 잘 설명하는 것이다.

[0067] 따라서 의미적 유사성을 파악하기 위해서 일정한 수만큼의 벡터를 선정하여 행렬로 나타내면 노이즈가 제거되고 더 일반화된 정보를 가지는 행렬로 변화된다.

수학식 7

$$X \approx X' = TSD'$$

[0068] [0069] 수학식 7에서 X' 은 X의 행렬에서 k개의 차원으로 축소된 값을 의미한다. k의 값에 따라 얼마나 어휘간 유사한 값을 표현하는지가 결정된다. 수학식 7에 대한 결과를 통하여 3가지에 대해 분석할 수 있다. 첫번째로 단어 i 와 단어 j 의 유사성, 두번째로 문서 i 와 문서 j 의 유사성, 마지막으로 단어 i 와 문서 j 의 연관성을 분석할 수 있다.

[0070] 본 발명의 의미 검색 모델은 이를 통하여 단어와 단어간의 유사성을 통계적 방법으로 찾아냄으로써 의미사전을 구축하지 않고도 의미적 연관성을 찾아낼 수 있다.

[0071] 이러한 의미 검색 모델에 대해서도 일 예를 들면, "농협 귀하의 개인 정보가 노출되었습니다. 정보 확인 : nh-mbank.com"과 같은 스팸 메시지가 있다. 여기서 이와 비슷하게 "수협 귀하의 개인 정보가 노출되었습니다. 정보 확인 : sh-mbank.com"이라는 의심 메시지가 있다.

[0072] 이 두 메시지를 벡터 공간 모델로 변환하면 수학식 4와 동일하다. 이러한 벡터 공간 모델에서 의미 유사도를 계산 시 벡터공간 모델의 경우 농협과 수협, nh-mbank.com과 sh-mbank.com은 서로 다른 키워드로 인식하여 가중치를 0에 두지만, 본 발명의 의미 검색 모델은 LSA를 통하여 0이 아닌 유사성을 가지는 값으로 인식하여 수학식 8과 같이 가중치를 계산한다.

수학식 8

$$\frac{S \cdot S'}{\|S\| \|S'\|} = \frac{5.8 \times 5.8}{\sqrt{6^2} \times \sqrt{6^2}} = 0.93$$

[0073] [0074] 수학식 5와 같이 벡터 공간 모델에서는 의미적으로 유사함에도 불구하고 단어의 일치만으로 계산할 경우 44%라는 낮은 일치도에 의해서 금융사기 메시지를 검색할 수 없으나 본 발명의 의미 검색 모델은 수학식 8과 같이 의미적 유사성을 검사함으로써 93%라는 높은 일치도를 확인할 수 있다.

[0075] 다음으로 다시 도 2로 돌아가 어휘 데이터 추출 단계(S220) 이후에 대해서 설명하겠다. 어휘 데이터 추출후 데이터판별부(130)가 추출한 어휘 데이터를 각각 분석하여 수집한 금융 사기 의심 데이터가 금융 사기 관련 데이터인지 여부를 판별한다(S230).

[0076] 이후, 기계학습부(140)가 금융 사기 관련 데이터라고 판별한 의심 데이터에 대하여 기계학습을 수행한다. 이 때, 기계학습부(140)가 금융 사기 관련 데이터라고 판별한 의심 데이터에 대하여 기계학습을 수행한 후에는 금융 사기 관련 데이터라고 판별한 의심 데이터에 대하여 나이브 베이즈(Naive Bayes) 분류 방법, 서브 벡터 머신(SVM,

Support Vector Machine) 분류 방법, 랜덤포레스트(Random Forest) 분류 방법 중 적어도 하나의 방법을 이용하여 분류할 수 있다.

- [0077] 이때, 이용되는 데이터 분류 방법 중 나이브 베이즈 분류 방법은 단순한 확률적 분류법으로서, 확률 모델이 베이즈 정리(Bayes' s theorem)를 사용하여 유도될 수 있다.
- [0078] 또한, 서포트 벡터 머신 분류 방법은지도 학습에서 사용되는 방법으로서, 주어진 자료에 대해서 그 자료들을 분리하는 초평면 중에서 자료들과 가장 거리가 먼 초평면을 찾는 방법을 말한다.
- [0079] 더불어, 랜덤 포레스트 분류 방법은 여러 개의 트리가 하나의 숲(포레스트)을 이루는 형태로서, 데이터 부집합의 순차적 분할로 표현할 수 있으며, 분류와 회귀 예측에 사용할 수 있다.
- [0080] 상술한 바와 같이, 금융 사기 관련 데이터라고 판별된 금융 사기 의심 데이터는 데이터베이스에 추가 저장되어, 이후 데이터의 금융 사기 판단 여부를 위한 비교자료로서 사용될 수 있다.
- [0081] 특히, SNS모니터링부(150)가 소셜 네트워크를 통해 복수 개의 단말간에 송수신되는 데이터에 대하여 데이터베이스에 기저장된 금융 사기 관련 데이터에 해당하는지 여부를 모니터링하고, 모니터링한 결과를 금융 사기 경계지수로 연산하고, 그 연산결과를 수치, 텍스트, 그림 형태로 각각 표시할 수 있다.
- [0082] 구체적으로, SNS모니터링부(150)는 송수신되는 데이터가 금융 사기 관련 데이터인지 모니터링하기 위해서 언어자원을 구축한다. 언어자원 구축은 도 5와 같이 크게 블로그 형식에서 언어자원을 수집하는 경우와, SNS 형식에서 언어자원을 수집하는 경우로 나눌 수 있다. 본 명세서에서는 SNS 형식에서 언어자원을 수집하는 경우에 대해서는 트위터를 이용하여 설명하겠다.
- [0083] 먼저, 블로그 형식에서 언어 자원 구축을 위해서는 시드(Seed) 블로그 URL(Uniform Resource Locator)에서 방문자, 이웃 블로거를 추출하여 수집영역 확장한다. 다음으로 스케줄러는 URL 중복체크와 다운로더의 문서 수집 속도를 제어하며, 새로운 포스트를 얻기 위해 RSS(Really Simple Syndication)를 다운받고 주기적으로 재방문하여 하루 20만 건 이상 블로그 포스트를 수집한다.
- [0084] 다음으로 SNS 형식인 트위터에서의 언어자원 구축은 도 5와 같이 업데이터(Updater), 리프레셔(Refresher), 팻처(Fetcher)로 시스템을 구성할 수 있다. 여기서 리프레셔는 수집 스케줄링을 제어하고, 업데이터는 데이터베이스 트랙잭션(Transaction)을 담당하며, 팻처에서는 실제 트윗을 수집하고 하루 35만건 이상 트윗을 수집한다.
- [0085] 여기서 블로그 형식 및 SNS 형식인 트위터에서 웹 데이터 수집을 위해서는 크롤러(Crawler)를 사용하며, 크롤링 방법은 Coordinator의 크롤링 모듈과 Agent의 크롤링 모듈을 사용하여 각각의 모듈을 이용한 크롤링 방법은 다음과 같다.
- [0086] 먼저 Coordinator의 크롤링 모듈은 시드 URL에 포함된 사이트 URL들을 사이트 내에서 수집할 URL의 집합인 V_{cr} 에 추가하고, V_{cr} 에 포함된 사이트 URL을 Agent에 전달하며 Agent에 전달한 사이트 URL을 사이트 내에서 수집한 URL인 V_{co} 에 추가한다. 이후, Agent로부터 수신한 사이트 URL의 집합이 V_{co} 에 속하지 않는 사이트 URL들만 V_{cr} 에 추가한다.
- [0087] 다음으로 Agent의 크롤링 모듈은 Coordinator가 전송한 사이트 URL에 해당하는 웹페이지를 웹 서버로부터 다운로드 사이트 내에서 수집한 URL인 A_{co} 에 저장한다. 다음으로 웹페이지에서 URL을 추출한 뒤 추출된 URL이 사이트 내부에 있는 경우 사이트 내에서 수집할 URL인 A_{cr} 에 추가하고 사이트 외부에 있는 경우 Coordinator에 전달할 사이트 URL인 A_{new} 에 추가한다. 이후 A_{cr} 에 URL이 존재하는 동안 웹 페이지 수집 및 URL 추출 과정을 반복하고, A_{new} 를 Coordinator로 전송한다.
- [0088] 이상으로, 상기와 같이 SNS모니터링부(150)가 소셜미디어에서 수집된 언어자원을 기반으로 소셜 네트워크 기반 금융 사기 관련 기초 어휘집을 구축한다.
- [0089] 상기와 같이 구축된 수 천 내지 수 만 단위의 언어 표현 중 소셜 네트워크 기반 금융 사기와 연관된 단어를 발굴하여 단일어, 복합 어구 대상으로 형태소 분석, 품사 태깅, 개체명 인식, 패러프레이징, 구문 분석을 하고 이를 기반으로 의미를 분석한다.
- [0090] 다음으로, 소셜 미디어에서 수집된 내용을 의미기반 분석을 통해 메시지 내용의 실제 의미를 수치화하여 소셜 네트워크 기반 금융 사기 경계지수 모니터링 예측 변수로 활용한다. 상기 수치화된 소셜 네트워크 기반 금융 사

기 경계지수에 대해서는 도 6을 참조하여 설명하겠다.

[0091] 도 6은 소셜 네트워크 기반 금융 사기 경계 지수를 나타낸 도면이다. 도 6에 도시된 바와 같이, 금융 사기 경계 지수가 그림 형태로 표시되는 경우에는 그 수치가 평균보다 높아질수록 먹구름을 동반한 폭우 또는 번개 형태로 표시될 수 있고, 상기 금융 사기 경계 지수의 수치가 평균보다 낮아질수록 맑은 날씨를 나타내는 태양을 표시할 수 있다. 또한, 미리 설정된 각 시간대별로 금융 사기 경계 지수를 모니터링하여 표현할 수 있다. 이처럼, 연산한 금융 사기 경계 지수를 수치, 텍스트, 그림 등의 여러 형태로 표현함으로써, 소셜 네트워크를 이용하는 불특정 다수에게 금융 사기에 대한 경각심을 야기시킬 수 있다.

[0092] 특히, 이때 데이터의 대용량 처리는 도 7에 도시된 바와 같이, 하둡 분산 파일 시스템(HDFS, Hadoop Distributed File System), Hbase 등의 분산 파일 시스템을 통해 처리될 수 있다. 또한 이러한 분산 파일 시스템을 구현하는 컨트롤 서버는 각종 데이터 서버의 관리 및 모니터링을 수행하고, 파일 시스템의 메타 데이터 즉, 디렉토리 트리, Inodes, Chunk Locations를 관리하고, Ext3, xfs, MySQL 등에 상기 파일 시스템의 메타 데이터를 저장한다.

[0093] 특히, 문장 단위 데이터의 전처리 과정, 전처리된 문장 단위 데이터의 형태소를 분석, 분산 역파일을 검출, 분산 데이터를 검색을 수행하기 위해, 맵리듀스를 할 수 있는 플랫폼을 선택한다. 이처럼 본 발명은 대용량의 데이터 분석 및 처리를 위해 분산 처리 구조를 사용하기 때문에 대용량 처리에 있어서 빠르다는 장점을 가지고 있다. 또한 분산 데이터에 대해서 맵리듀스를 통해 인덱스가 생성되고, 인덱스 정보는 대용량의 데이터베이스에 저장되어 데이터 접근이 빠르다는 장점 또한 갖는다.

[0094] 또한, 이러한 금융 사기 방지 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD ±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0095] 본 발명의 금융 사기 방지 방법 및 시스템은 금융 사기가 의심되는 데이터를 수집하고, 수집된 데이터 내 금융 사기를 나타내거나 암시하는 어휘 데이터가 존재하는지 확인하여 수집한 데이터가 금융 사기 관련 데이터인지 여부를 판별함으로써, 불특정 다수의 사람들이 금융 사기 피해를 입는 것을 미연에 방지할 수 있는 효과가 있다.

[0096] 또한, 본 발명의 금융 사기 방지 방법 및 시스템은 소셜 네트워크를 기반으로 단말간에 송수신되는 데이터가 금융 사기 관련 데이터에 해당하는지 여부를 기 설정된 시간마다 모니터링하고, 모니터링 결과를 금융 사기 경계 지수로 연산하여, 연산된 금융 사기 경계 지수를 수치, 텍스트, 그림 등의 여러 형태로 표시함으로써, 소셜 네트워크를 이용하는 불특정 다수에게 금융 사기에 대한 안전성을 제공할 수 있는 효과가 있다.

[0097] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

[0098] 100: 금융 사기 방지 시스템

110: 데이터수집부

120: 어휘추출부

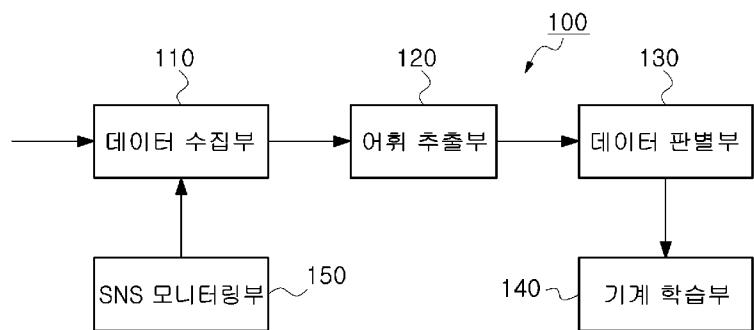
130: 데이터판별부

140: 기계학습부

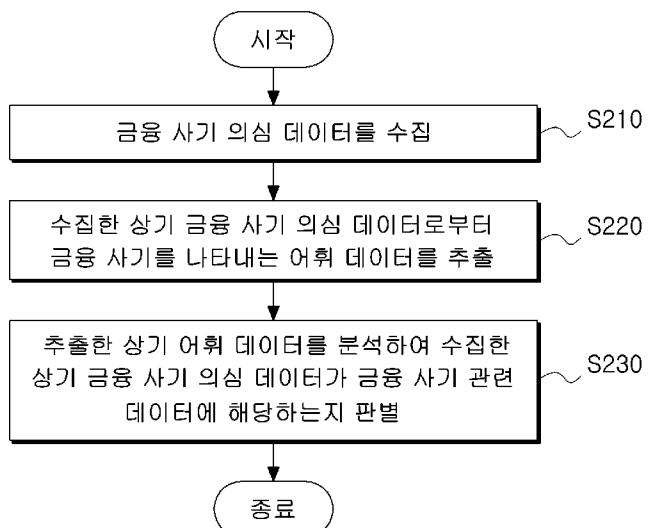
150: SNS모니터링부

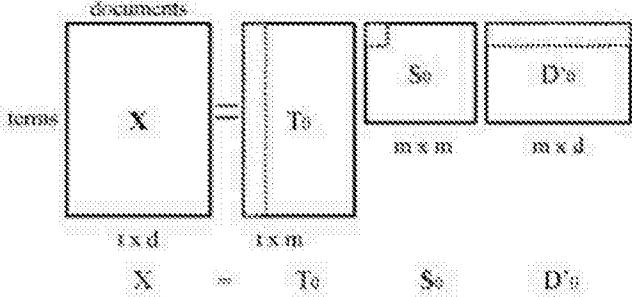
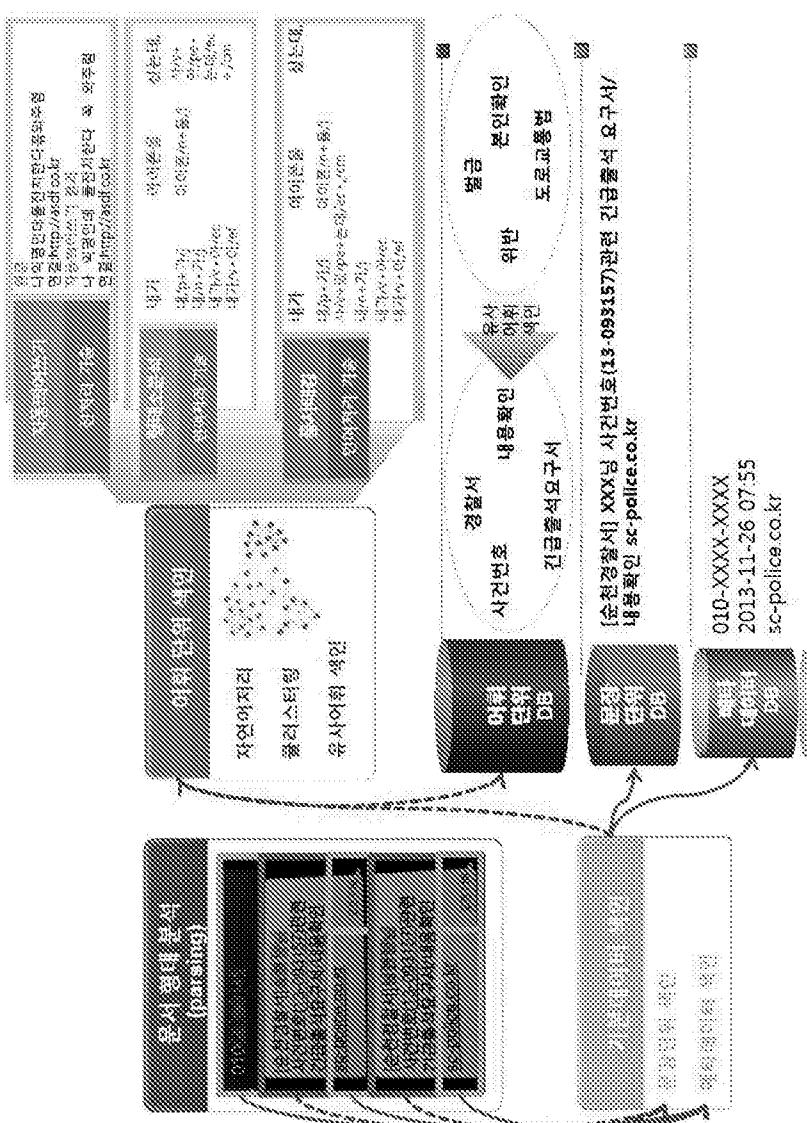
도면 1

도면 1

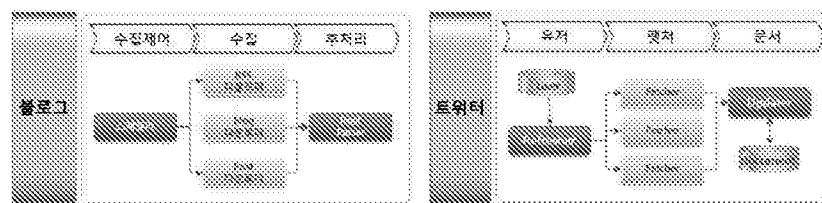


도면 2

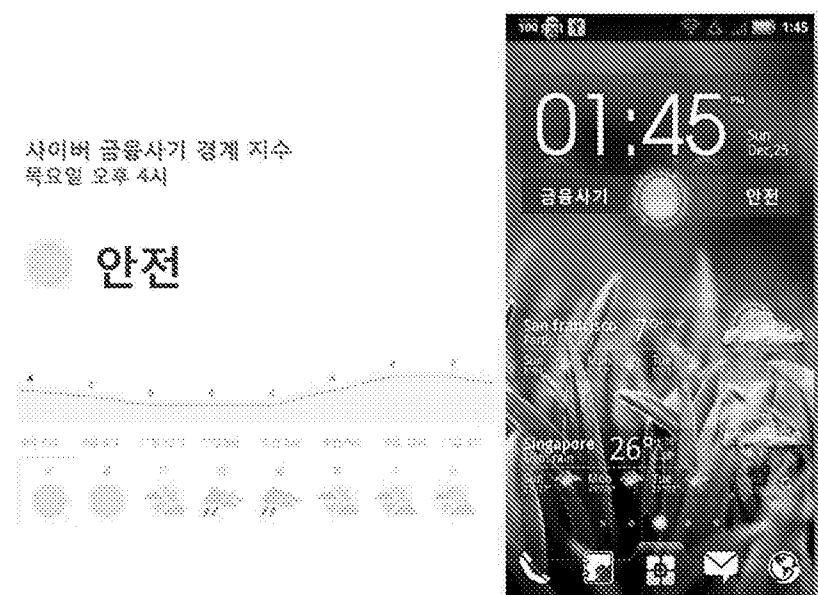




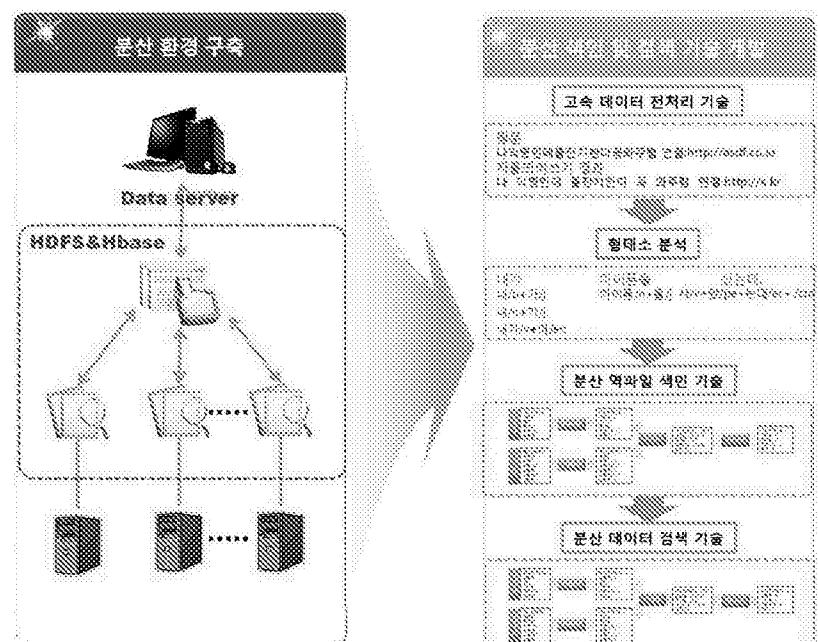
도면5



도면6



도면7





(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0095548
(43) 공개일자 2013년08월28일

(51) 국제특허분류(Int. Cl.)
G06Q 40/02 (2012.01) G06Q 20/42 (2012.01)
(21) 출원번호 10-2012-0017082
(22) 출원일자 2012년02월20일
심사청구일자 2012년02월20일

(71) 출원인
주식회사 한국프라임테크놀로지
서울특별시 강남구 논현로71길 17, 부영빌딩 2층
(역삼동)
(72) 발명자
장기윤
경기 수원시 팔달구 인계동 384 삼성래미안 노블
클래스 101동 2501호
(74) 대리인
유미특허법인

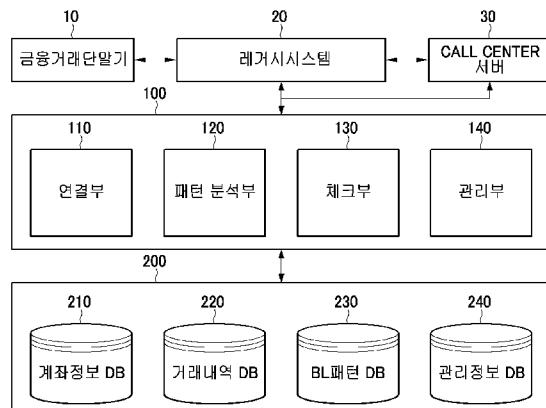
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 금융거래패턴분석을 이용한 금융사기 경보 시스템 및 방법

(57) 矽 說

본 발명은 금융기관에 있는 고객계좌의 입금 및 출금, 그리고 조회 등의 거래내역정보를 바탕으로 해당 거래패턴을 분석하여 해당 계좌의 금융거래위험도를 계산하여 관리하며, 금융거래고객이 금융거래단말기에서 계좌이체 거래를 수행 시에 입금계좌의 금융거래위험도를 체크하여 입금계좌의 금융거래위험도에 따라 금융거래 고객에게 적절한 메시지 처리를 수행하여 금융사기거래에 노출을 방지하며, 콜센터 또는 감사팀과 같은 모니터링부서에서 의심계좌의 거래패턴정보를 가지고 추가적인 조치를 할 수 있도록 콜센터 시스템으로 계좌의 금융거래위험도 및 거래패턴정보를 제공하는 금융사기경보시스템 및 방법에 관한 것이다.

- 도1



특허청구의 범위

청구항 1

적어도 하나의 금융거래 단말기로부터 금융거래 정보를 수신하여 금융 거래를 처리하는 금융사기 경보 시스템으로서,

고객의 계좌정보, 계좌거래내역정보 및 금융사기 패턴인 BL패턴 정보를 저장하는 데이터베이스부;

고객의 금융거래인 계좌이체 및 계좌조회를 포함한 금융온라인 거래의 처리를 수행하며, 계좌이체거래의 임금계좌 체크시에 상기 임금계좌의 금융 거래 위험성을 나타내는 금융거래 위험도 정보를 외부에 요청하고, 제공받은 상기 임금계좌의 금융거래위험도에 대응하여 상기 금융거래 단말기에 메시지를 송신하는 레거시 시스템;

상기 데이터베이스에 저장된 고객 계좌의 계좌거래내역정보와 레거시시스템으로부터 수신한 거래정보로부터 금융거래패턴을 도출하고, 도출된 거래패턴을 상기 BL패턴과 비교하여 해당계좌의 금융거래위험도를 산출하며, 계좌이체 거래시에 상기 레거시 시스템의 요청에 따라 상기 임금계좌의 금융거래위험도 정보를 상기 레거시시스템 및/또는 외부의 콜센터 시스템에 제공하는 서버를 포함하는 금융사기 경보 시스템.

청구항 2

제1항에 있어서,

상기 서버로부터 제공받은 상기 임금계좌의 금융거래패턴정보를 모니터링요원에게 알려서 금융계좌의 추가적인 안전조치를 지원하는 콜센터 시스템을 더 포함하는 금융사기 경보 시스템.

청구항 3

제1항 또는 제2항에 있어서,

상기 데이터베이스부는,

상기 고객의 계좌정보와 해당 계좌의 금융거래위험도 정보를 저장하는 계좌정보DB;

상기 고객의 계좌의 임금, 출금 및 조회에 대한 거래내역 정보 및 추출된 거래패턴정보를 저장하는 거래내역DB;

금융사기계좌의 특성으로부터 추출한 거래패턴정보 또는 금융사기가 예상되는 거래패턴 정보인 BL 패턴 정보를 저장하는 BL패턴DB,

금융사기 분석 케이스(CASE)정보, 스코어링(SCORING)을 위한 케이스별 가중치, 금융거래의 패턴분석을 위한 금융거래모형정보, 상기 레거시 시스템의 거래매핑정보를 저장하는 관리정보DB를 포함하고,

상기 서버는,

상기 레거시 시스템으로부터 상기 고객 계좌의 계좌거래내역 정보를 수신하고, 상기 레거시 시스템으로부터 상기 임금계좌의 금융거래위험도 정보의 체크를 요청받아 상기 임금계좌의 금융거래 위험도 정보를 전달하도록 연결하기 위한 연결부;

상기 연결부를 통해 상기 레거시 시스템으로부터 상기 고객 계좌의 계좌거래내역 정보를 받아 해당 거래의 거래패턴을 추출하여 BL거래패턴과 비교체크하고 체크결과에 따라 금융거래 위험도를 계산하는 패턴 분석부;

상기 레거시 시스템의 계좌이체 거래시에 상기 임금 계좌의 금융거래 위험도 또는 상기 거래패턴 정보를 제공하며, 상기 금융거래 위험도에 대응하여 상기 콜센터 시스템으로 상기 임금 계좌의 금융거래 위험도 또는 상기 거래패턴 정보를 제공하는 정보체크부;

금융사기 분석 케이스 정보, 스코어링을 위한 케이스별 가중치, 금융거래의 패턴분석을 위한 거래모형정보, 금융사기 거래의 BL패턴정보, 상기 레거시 시스템의 계좌 거래내역정보를 받기 위한 거래매핑정보를 상기 관리정보 DB에 등록하는 관리부를 포함하는 금융사기 경보 시스템.

청구항 4

제3항에 있어서,

상기 패턴 분석부는,

상기 연결부를 통해 수신한 고객 계좌의 계좌거래정보를 분석하여 상기 계좌정보DB 및 거래내역DB에 저장하는 거래정보 처리부;

상기 고객 계좌의 최종 거래정보를 기준으로 이전 거래정보와의 관계를 거래모형정의와 매핑하여 거래모형문자 의 문자열로 조립하는 거래패턴 구현부;

상기 거래패턴 구현부로부터 추출된 거래패턴이 BL거래패턴의 유형에 포함하는지를 체크하는 BL패턴 체크부;

상기 체크부에서 체크된 거래패턴을 정보를 가지고 각 케이스 및 거래유형에 스코어링 가중치를 반영하여 상기 고객 계좌의 금융거래 위험도를 계산하는 스코어링부를 포함하는 금융사기 경보 시스템.

청구항 5

적어도 하나의 금융거래 단말기로부터 레거시 시스템을 통해 금융거래 정보를 수신하여 금융 거래를 처리하는 금융사기 경보 방법으로서,

상기 레거시 시스템이 계좌이체거래의 입금계좌 체크과정에서 상기 서버로 입금계좌의 금융거래위험도 정보를 요청하고 수신하는 단계;

상기 레거시 시스템이 계좌이체거래의 입금계좌체크 과정에서 상기 서버로부터 받은 입금계좌의 금융거래위험도에 대응하여 상기 금융거래단말기로 계좌이체의 위험에 관한 고객대응 메시지를 출력하는 단계;

상기 서버가 상기 레거시 시스템의 금융계좌의 계좌거래내역 정보를 수신 하는 단계;

상기 서버가 수신한 계좌거래내역정보를 계좌정보 DB및 거래내역 DB에 저장하는 단계;

상기 서버가 거래모형정의단계 정보를 기반으로 상기 계좌거래내역 정보를 거래모형정의와 매핑하여 거래 모형을 결정하고 거래모형 문자의 문자열로 조립하여 거래패턴구현을 수행하는 단계;

상기 서버가 구현된 거래패턴으로 BL패턴과 비교하는 단계;

상기 서버가 BL패턴 비교 정보와 계좌정보, 그리고 금융사기분석 케이스별 스코어링 가중치를 참조하여 상기 고객계좌의 금융거래위험도를 계산하는 단계;

상기 서버가 상기 레거시 시스템으로부터 금융계좌의 금융거래위험도 정보요청을 받아 해당계좌의 금융거래위험도 정보를 제공하고, 금융거래위험도에 따라 콜센터 시스템으로 해당 계좌의 거래패턴 정보를 포함한 정보를 제공하는 단계를 포함하는 금융사기 경보 방법.

청구항 6

제5항에 있어서,

상기 서버가 고객 계좌의 거래패턴분석을 위하여 거래 요소(FACTOR)정의, 요소 세분화(FACTOR SEGMENTATION), 거래모델링 및 거래모형정의를 진행하여 거래모형 심볼라이징(SYMBOLIZING) 정보를 상기 관리정보 DB에 저장하는 거래모형정의단계;

상기 서버가 금융사기계좌의 거래패턴정보 및 금융사기가 예상되는 거래패턴 정보를 거래모형 심볼라이징 정보를 이용하여 상기 BL패턴DB에 등록하는 BL거래패턴등록단계를 더 포함하는 금융사기 경보 방법.

청구항 7

제5항 또는 제6항에 있어서.

상기 금융거래 단말기는 금융고객이 금융거래를 수행하는 금융자동화기기 또는 전자금융거래를 수행하는 인터넷 단말, 모바일 단말 또는 ARS 단말중 하나인 것을 특징으로 하는 금융사기 경보 방법.

명세서

기술 분야

- [0001] 본 발명은 금융기관의 금융사기 경보 시스템에 관한 것으로 특히, 금융기관에 있는 고객계좌의 입금 및 출금, 그리고 조회 등의 거래 수행패턴을 분석하여 해당 계좌의 금융거래위험도를 계산하고, 계좌이체거래에서 입금계좌의 금융거래위험도에 따라 금융거래고객에게 적절한 메시지 안내처리와 모니터링부서의 추가적인 조치를 할 수 있도록 정보를 제공하는 금융사기경보시스템 및 방법에 관한 것이다.

■ 경 기술

- [0002] 현재 금융기관의 금융시스템은 전자금융기술의 발전으로 고객의 편의성이 증진되는 반면에 개방형 정보기술의 특성으로 인한 3자의 해킹 및 각종 금융사기 사고 등 금융사고의 개연성 및 리스크가 증가하고 있다.
- [0003] 최근에는 특히 보이스피싱 등의 금융사기와 관련된 사고가 지속적이면서도 지능적으로 발생하고 있어서, 정부 또는 금융기관에서 이에 대한 대응을 위하여 제도적 및 시스템적인 많은 조치를 취하고 있지만 이러한 대부분의 대응조치는 사후조치에 그치고 있다.
- [0004] 그리고 대부분의 금융사기대응과 관련된 솔루션들이 IT기술요소를 이용한 대응기술로 IP의 추적이라든가, 해킹 방지 등 금융시스템의 핵심이 아닌, 주변 서브 시스템에 초점을 맞추고 있다. IT기술이 발달함에 따라 당연히 위와 같은 기술이 개발되어야 하지만 근본적으로 고객계좌의 입금 및 출금 등 온라인거래가 수행되는 금융시스템(이하 '레거시시스템'이라 한다)의 비즈니스 구조적인 차원의 대응은 한발 뒤로 물려서 있는 실정이다.
- [0005] 금융사기의 특성상 고객으로부터 계좌이체 등을 통하여 금전을 수취한 후에 해당계좌에서 수취한 금액을 즉시 인출을 하고 도주하며, 금융고객이 계좌이체 이후에 해당거래가 사기라는 것을 인지하여 해당계좌에 지급정지등 취하는 사후조치는 계좌이체를 수행한 금융고객에게는 별다른 효과가 없다.
- [0006] 금융기관의 고객이 금융자동화기기(Automated Teller Machine) 및 인터넷뱅킹 등으로 수행하는 계좌이체거래는 일반적으로 2단계의 절차로 계좌이체 거래가 수행되고 있는데, 첫째 단계는 입금계좌의 확인거래로 입력한 입금 계좌번호의 정확성 및 계좌소유주의 확인, 그리고 계좌의 상태 확인 등을 수행한다. 다음 단계로 수취계좌에 입금거래가 수행되는 둘째 단계의 절차로 출금계좌인 송금계좌에서 출금을 하고 수취계좌인 입금계좌로 입금처리를 수행하는 계좌입금 거래가 수행되고 있다.
- [0007] 이러한 단계에 걸쳐 계좌이체를 수행하는 과정에서 금융거래 고객에게 금융사기대응과 관련한 안내는 ATM기에서 계좌이체의 첫째 단계인 입금계좌의 확인거래를 수행하기 전에 나타나는 주의문구 정도이다.
- [0008] 금융고객이 인터넷뱅킹 및 ATM기 등에서 계좌이체거래를 수행하는 경우에 입금계좌의 확인 과정에서 해당 입금 계좌의 특성을 보다 지능적이고 다각적인 분석을 통하여 금융거래 고객이나 금융시스템으로 현재 수행하고 있는 금융거래의 위험도를 안내하여, 금융거래 고객은 한번 더 해당 거래의 수행을 고려할 수 있는 기회의 제공이 필요하며, 금융시스템은 금융거래의 위험도에 따라 수행되는 계좌이체거래의 시스템적인 조치를 취할 수 있도록 정보를 제공하는 금융사기 경보 시스템이 절실히 필요하다.
- [0009] 특히, 피라미드의 도굴 방지를 위해 피라미드 주변에 담장을 설치하는 것이 중요할 수 있지만 근본적으로 피라미드 자체에 도굴을 방지하기 위한 구조적인 설계가 필요 했던 것처럼 금융사기 즉 계좌이체를 통해 사기계좌에 입금되는 금액을 즉시 인출하여 도주하는 금융사기를 방지하기 위해서는 레거시시스템의 비즈니스 구조적인 보완을 통한 대책으로 사기계좌에 계좌이체거래가 수행되기 이전에 입금되는 계좌에 대한 특별하고 지능적인 분석으로 대처를 해야 하는 기술이 필요하다.
- [0010] 종래기술로 선 출원된 특허출원 2009-0105558호 '금융사기 방지시스템 및 방법'과 특허출원 2010-0074391호 '보이스 피싱 예방을 위한 보안성을 강화한 금융거래시스템 및 그 동작방법'은 이미 금융사기거래를 유발한 IP정보, MAC정보, 계좌정보 등을 데이터베이스(DATA BASE)화 하여 금융거래 수행 시 해당 DATA BASE를 조회하고 비교하여 등록되어 있는 정보와 같은 계좌나 채널에서의 금융거래인 경우 해당 금융거래의 차단과 금융사기 거래의 메시지를 처리하는 시스템 및 방법이다.
- [0011] 그리고 이외에도 고객계좌의 입금 및 출금정보를 다른 각도에서 뺏치(일괄처리) 방식으로 분석하여 CRM에서 이용하는 사례도 있으나, 이는 분석시점이 거래의 종료 후에 뺏치 방식으로 수행이 되며, 분석의 초점이 금융사기를 분석하기 위한 초점이 아니고, 고객의 입출패턴을 이용한 금융기관의 마케팅자료의 추출로 이용이 되고 있다.

발명의 내용

해결하려는 과제

[0012] 본 발명이 해결하고자 하는 기술적 과제는, 종래의 문제점을 해결하기 위한 것으로서, 금융계좌의 거래내역 즉 입금과 출금, 조회거래 등을 기반으로 금융거래패턴을 실시간 또는 지연처리(DEFERRED)방식으로 추출하고 추출된 거래패턴을 금융사기에 이용된 계좌의 거래패턴정보 또는 금융사기가 예상되는 거래패턴 정보 등 블랙리스트(Black List)거래 패턴(이하 'BL패턴"이라 한다)과 비교 및 분석을 통해 해당 계좌의 금융거래위험도를 계산하여 저장 및 관리하며 금융고객이 금융거래를 수행하기 전에 또는 금융거래를 수행하는 과정에서 입금계좌에 대한 금융거래위험도에 따라 금융고객이 적절한 조치를 할 수 있도록 메시지처리를 하며, 콜센터(CALL CENTER)와 같은 모니터링부서로 계좌이체와 관련된 입금계좌의 거래패턴정보를 제공하여 추가적인 고객안전조치를 수행할 수 있는 금융사기 경보 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

- [0013] 이러한 과제를 해결하기 위한 본 발명의 특징에 따른 금융사기 경보 시스템은,
- [0014] 적어도 하나의 금융거래 단말기로부터 금융거래 정보를 수신하여 금융 거래를 처리하는 금융사기 경보 시스템으로서,
- [0015] 고객의 계좌정보, 계좌거래내역정보 및 금융사기 패턴인 BL패턴 정보를 저장하는 데이터베이스부;
- [0016] 고객의 금융거래인 계좌이체 및 계좌조회를 포함한 금융온라인 거래의 처리를 수행하며, 계좌이체거래의 입금계좌 체크시에 상기 입금계좌의 금융 거래 위험성을 나타내는 금융거래 위험도 정보를 외부에 요청하고, 제공받은 상기 입금계좌의 금융거래위험도에 대응하여 상기 금융거래 단말기에 메시지를 송신하는 레거시시스템;
- [0017] 상기 데이터베이스에 저장된 고객 계좌의 계좌거래내역정보와 레거시시스템으로부터 수신한 거래정보로부터 금융거래패턴을 도출하고, 도출된 거래패턴을 상기 BL패턴과 비교하여 해당계좌의 금융거래위험도를 산출하며, 계좌이체 거래시에 상기 레거시 시스템의 요청에 따라 상기 입금계좌의 금융거래위험도 정보를 상기 레거시시스템 및/또는 외부의 콜 센터 시스템에 제공하는 서버를 포함한다.
- [0018] 상기 시스템은,
- [0019] 상기 서버로부터 제공받은 상기 입금계좌의 금융거래패턴정보를 모니터링요원에게 알려서 금융계좌의 추가적인 안전조치를 지원하는 콜 센터 시스템을 더 포함한다.
- [0020] 상기 데이터베이스부는,
- [0021] 상기 고객의 계좌정보와 해당 계좌의 금융거래위험도 정보를 저장하는 계좌정보DB;
- [0022] 상기 고객의 계좌의 입금, 출금 및 조회에 대한 거래내역 정보 및 추출된 거래패턴정보를 저장하는 거래내역DB;
- [0023] 금융사기계좌의 거래특성으로부터 추출한 거래패턴정보와 금융사기가 예상되는 BL패턴정보를 저장하는 BL패턴 DB,
- [0024] 금융사기 분석 케이스(CASE)정보, 스코어링(SCORING)을 위한 케이스별 가중치, 금융거래의 패턴분석을 위한 금융거래모형정보, 상기 레거시시스템의 거래매핑정보를 저장하는 관리정보DB를 포함한다.
- [0025] 상기 서버는,
- [0026] 상기 레거시 시스템으로부터 상기 고객 계좌의 계좌거래내역 정보를 수신 하고, 상기 레거시 시스템으로부터 상기 입금계좌의 금융거래위험도 정보의 체크를 요청받아 상기 입금계좌의 금융거래 위험도 정보를 전달하도록 연결하기 위한 연결부;
- [0027] 상기 연결부를 통해 상기 레거시 시스템으로부터 상기 고객 계좌의 계좌거래내역 정보를 받아 해당 거래의 거래패턴을 추출하여 BL거래패턴과 비교체크하고 체크결과에 따라 금융거래 위험도를 계산하는 패턴 분석부;
- [0028] 상기 레거시 시스템의 계좌이체 거래시에 상기 입금 계좌의 금융거래 위험도 또는 상기 거래패턴 정보를 제공하며, 상기 금융거래 위험도에 대응하여 상기 콜센터 시스템으로 상기 입금 계좌의 금융거래 위험도 또는 상기 거래패턴 정보를 제공하는 정보체크부;
- [0029] 금융사기 분석 케이스 정보, 스코어링을 위한 케이스별 가중치, 금융거래의 패턴분석을 위한 거래모형정보, 금융사기거래의 BL패턴정보, 상기 레거시 시스템의 계좌 거래내역정보를 받기 위한 거래매핑정보를 상기 관리정보

DB에 등록하는 관리부를 포함한다.

- [0030] 상기 패턴 분석부는,
- [0031] 상기 연결부를 통해 수신한 고객 계좌의 계좌거래정보를 분석하여 상기 계좌정보DB 및 거래내역DB에 저장하는 거래정보 처리부;
- [0032] 상기 고객 계좌의 최종 거래정보를 기준으로 이전 거래정보와의 관계를 거래모형정의와 매핑하여 거래모형문자 의 문자열로 조립하는 거래패턴 구현부;
- [0033] 상기 거래패턴 구현부로부터 추출된 거래패턴이 BL거래패턴의 유형에 포함하는지를 체크하는 BL패턴 체크부;
- [0034] 상기 BL패턴 체크부에서 체크된 거래패턴을 정보를 가지고 각 금융사기분석케이스별 스코어링 가중치를 반영하여 상기 고객 계좌의 금융거래 위험도를 계산하는 스코어링부를 포함한다.
- [0035] 이러한 과제를 해결하기 위한 본 발명의 특징에 따른 금융사기 경보 방법은
- [0036] 적어도 하나의 금융거래 단말기로부터 레거시 시스템을 통해 금융거래 정보를 수신하여 금융 거래를 처리하는 금융사기 경보 방법으로서,
- [0037] 상기 레거시 시스템이 계좌이체거래의 입금계좌 체크과정에서 상기 서버로 입금계좌의 금융거래위험도 정보를 요청하고 수신하는 단계;
- [0038] 상기 레거시시스템이 계좌이체거래의 입금계좌체크 과정에서 상기 서버로부터 받은 입금계좌의 금융거래위험도에 대응하여 상기 금융거래단말기로 계좌이체의 위험에 관한 고객대응 메시지를 출력하는 단계;
- [0039] 상기 서버가 상기 레거시 시스템의 금융계좌의 계좌거래내역 정보를 수신하는 단계;
- [0040] 상기 서버가 수신한 계좌거래내역정보를 계좌정보 DB및 거래내역 DB에 저장하는 단계;
- [0041] 상기 서버가 거래모형정의단계 정보를 기반으로 상기 계좌거래내역 정보를 거래모형정의와 매핑하여 거래 모형을 결정하고 거래모형문자의 문자열로 조립하여 거래패턴구현을 수행하는 단계;
- [0042] 상기 서버가 구현된 거래패턴으로 BL패턴과 비교하는 단계;
- [0043] 상기 서버가 BL패턴 비교 정보와 계좌정보, 그리고 금융사기분석케이스별 스코어링 가중치를 참조하여 상기 고객계좌의 금융거래위험도를 계산하는 단계;
- [0044] 상기 서버가 상기 레거시 시스템으로부터 금융계좌의 금융거래위험도 정보요청을 받아 해당계좌의 금융거래위험도 정보를 제공하고, 금융거래위험도에 따라 콜센터 시스템으로 해당 계좌의 거래패턴 정보를 포함한 정보를 제공하는 단계를 포함한다.
- [0045] 상기 방법은,
- [0046] 상기 서버가 고객 계좌의 거래패턴분석을 위하여 거래 요소(FACTOR)정의, 요소세그멘테이션(FACTOR SEGMENTATION), 거래모델링 및 거래모형정의를 진행하여 거래모형 심볼라이징(SYMBOLIZING) 정보를 상기 관리정보 DB에 저장하는 거래모형정의단계;
- [0047] 상기 서버가 금융사기계좌의 거래패턴정보 및 금융사기가 예상되는 거래패턴정보를 거래모형 심볼라이징 정보를 이용하여 상기 BL패턴DB에 등록하는 BL거래패턴등록단계를 더 포함한다.
- [0048] 상기 금융거래 단말기는 금융고객이 금융거래를 수행하는 금융자동화기기 또는 전자금융거래를 수행하는 인터넷 단말 또는 모바일 단말, ARS단말 중 하나인 것을 특징으로 한다.

5.2.3. 결론

- [0049] 본 발명의 실시예에서는 레거시 시스템의 고객계좌 거래내역을 바탕으로 거래패턴을 분석하여 해당계좌의 금융거래 위험도를 관리함으로써 금융사기 의심계좌를 추출하여 모니터링 할 수 있으며, 발생하는 금융사기계좌의 거래패턴을 추가 등록관리를 함으로써 금융사기 의심계좌추출을 효율화 할 수 있으며, 계좌이체거래의 첫째 단계인 입금계좌 확인단계에서 입금계좌의 금융거래위험도를 맞는 고객의 대응조치 메시지 출력으로 금융고객은 수행하는 금융거래의 위험도에 대한 생각을 다시 한번 할 수 있으며, 입금계좌의 금융거래위험도의 경증에 따라 콜센터(CALL CENTER)와 같은 모니터링 시스템으로 정보를 제공하여 모니터링요원의 적극적인 개입으로 금융고객의 금융사기피해를 적극적으로 예방함으로써 금융고객의 재산을 보호하는 금융기관으로써의 믿음과 신뢰를 확보

할 수 있다.

도면의 간단한 설명

- [0050] 도 1은 본 발명의 실시 예에 따른 금융사기경보시스템의 블록구성도이다.
 도 2는 도 1의 패턴추출부의 상세도이다.
 도 3은 계좌이체거래의 처리흐름도이다.
 도 4는 서버 처리흐름도이다.
 도 5는 거래패턴 분석 방법에 대한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0051] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0052] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.
- [0053] 도 1은 본 발명의 실시 예에 따른 금융사기경보시스템의 블록구성도이다.
- [0054] 도 1을 참조하면, 본 발명의 실시 예에 따른 금융사기 경보 시스템은,
- [0055] 금융고객이 금융거래를 수행하는 특히 계좌이체거래를 수행하는 금융자동화기기, 또는 전자금융거래를 수행하는 인터넷단말 또는 모바일단말 등을 포함한 금융거래단말기(10);
- [0056] 고객의 금융거래인 계좌이체 및 계좌조회 등의 금융온라인 거래의 처리를 수행하며, 계좌이체거래의 입금계좌체크 시 입금계좌의 금융거래위험도 정보를 서버(100)에 요청하여 제공받은 입금계좌의 금융거래위험도에 따라 금융거래고객에게 메시지를 송신 처리하는 레거시시스템(20);
- [0057] 상기 레거시시스템(20)으로부터 계좌정보 및 거래정보를 받아 거래패턴을 추출하고, 추출된 거래 패턴 정보와 BL패턴을 비교하여 금융거래위험도를 계산하여 거래내역 DB(220)에 저장해두고, 계좌이체 거래 시 입금계좌의 금융거래위험도 체크요청을 받아 해당 계좌의 금융거래위험도 및 관련정보 등을 레거시시스템(20)과 콜센터 시스템(30)에 제공하는 서버(100);
- [0058] 서버(100)로부터 제공받은 입금계좌의 거래패턴정보를 콜센터 또는 모니터링 요원에게 알려서 건전한 금융고객의 금융거래에 추가적인 안전조치를 수행하게 지원하는 콜센터 시스템(30);
- [0059] 계좌정보 및 거래내역정보를 저장 및 관리하며, BL패턴정보와 관리정보를 저장 및 관리하는 데이터베이스부(200)로 구성된다.
- [0060] 상기 데이터베이스부(200)는,
- [0061] 계좌의 정보와 해당계좌의 스코어링된 금융거래위험도를 저장하는 계좌정보DB(210); 레거시 시스템(20)으로부터 실시간 또는 지연(DEFERRED)방식, 기타방식으로 수신하는 계좌의 입금거래, 출금거래, 조회거래 등의 거래내역 정보 및 거래패턴구현을 통해 추출된 각 거래의 거래패턴 정보를 저장 및 관리하는 거래내역DB(220); 금융사기 계좌의 거래특성으로부터 추출한 거래패턴정보 및 금융사기가 예상되는 거래패턴 유형정보를 저장하는 BL패턴 DB(230);
- [0062] 상기 서버(100)의 효율적인 운용 및 관리를 위한 기초정보와 금융사기분석케이스 정보, 스코어링을 위한 케이스 별 가중치정보, 거래패턴 추출 시 기준이 거래모형정보, 레거시 시스템(20)과의 연계를 위한 거래매핑정보 등을 저장하는 관리정보DB(240)을 포함한다.

- [0063] 상기 서버(100)는,
- [0064] 레거시 시스템(20)과 연계를 위한 연결부(110); 연결부(110)를 통하여 수신한 금융거래 내역으로부터 거래 패턴을 추출하고, BL 패턴을 체크하여 금융거래위험도를 계산하는 패턴분석부(120); 레거시 시스템(20)으로부터 특정계좌의 금융거래 위험도 체크요청을 받아 처리하는 정보 체크부(130); 금융사기 경보 시스템의 효율적인 운용 관리를 위해 관련정보를 조정 및 관리하는 관리부(140)를 포함한다.
- [0065] 연결부(110)는 레거시시스템(20)과 연계를 수행하는 것으로 금융계좌의 거래내역정보를 실시간 또는 지연처리(DEFERRED)방식, 기타방식 등으로 연계를 수행하며, 상기 서버(100)에서 필요한 금융거래종류 및 필요 데이터의 매팽 정보를 관리정보DB(240)에서 참조하여 레거시 시스템(20)으로부터 받은 거래 데이터를 선택적으로 추출할 수 있으며, 매팽 정보에 의해 상기 서버(100)에서 필요한 데이터형식으로 변환하여 패턴분석부(120)로 거래내역 데이터를 전송 처리한다.
- [0066] 패턴 분석부(120)는 연결부(110)를 통하여 전달받은 거래내역 데이터를 데이터베이스에 저장하는 거래정보 처리부(121); 전달받은 거래내역을 기준으로 해당 계좌의 거래패턴을 추출하는 거래패턴 구현부(122); 추출된 거래 패턴을 BL거래패턴과 비교 및 체크하는 BL패턴 체크부(123); BL패턴 체크 정보를 가지고 금융거래 위험도를 계산하는 스코어링부(124)를 포함한다.
- [0067] 도 2를 참조하면, 거래정보 처리부(121)는 연결부(110)로부터 전달받은 거래내역 데이터를 분석하여 거래코드에 따라 거래와 관련된 정보를 계좌정보DB(210)나 거래내역DB(220)에 저장한다.
- [0068] 거래패턴 구현부(122)는 관리정보DB(240)에 관리되는 금융사기분석 항목을 정의한 CASE정보에 따라 거래의 패턴 구현을 수행한다. 특히 입금 및 출금거래, 그리고 조회거래를 중심으로 거래패턴구현이 처리되며, 거래패턴구현도 금융사기 분석항목을 정의한 케이스 정보에 따라 입출거래패턴 케이스 또는 테스트거래패턴 케이스 등과 같이 중복으로 거래패턴구현을 수행하기도 한다. 거래패턴의 구현은 현재 전달받은 거래정보를 기준으로 과거 거래데이터와의 시간관계 및 입출거래의 형태, 잔액의 상태 등과 같은 관리정보DB(240)에 정의되어 있는 거래 요소(factor)의 정보를 기준으로 비교하여 개별거래모형을 결정하며, 결정된 개별거래모형을 거래패턴문자열로 조립을 수행하여 거래패턴을 구현한다.
- [0069] BL패턴 체크부(123)는 거래패턴 구현부(122)로부터 추출된 거래패턴문자열로 BL패턴DB(230)에 등록되어 있는 BL 거래패턴 중에 같은 거래패턴이 등록되어 있는지를 체크하여 그 결과를 스코어링부로 넘긴다.
- [0070] 스코어링부(124)는 BL패턴체크부(123)로부터 BL체크결과를 받아 관리정보DB(240)에 관리되는 SCORING관련 가중치를 참조하여 해당 계좌의 금융거래위험도를 계산한 후에 계좌정보DB(210)의 자동금융거래위험도와 최종금융거래위험도에 정보를 갱신한다. 이때 해당 계좌가 수기판리 계좌인 경우에는 자동금융거래위험도 정보만 갱신하고 최종금융거래위험도 정보에는 갱신하지 않고 수기판리정보를 유지한다. 특히 스코어링을 하는데 있어 거래패턴 정보와 기타 계좌정보 및 계좌소유주의 신용정보나 계좌간 거래정보 등과 같은 다른 정보를 같이 연계하여 평가를 효율적으로 할 수도 있다.
- [0071] 정보 체크부(130)는 레거시 시스템(20)으로부터 또는 이와 유사한 금융거래를 하는 타 시스템(도면 미도시)으로부터 특정계좌의 금융거래위험도를 조회요청 받을 때 해당계좌의 금융거래위험도를 체크하여 정보를 넘겨준다. 그리고 금융거래위험도의 경중에 따라 콜센터 시스템(30)등의 모니터링 시스템 등으로 입금계좌의 거래패턴정보를 제공하여 모니터링요원으로 하여금 금융거래고객에게 추가적인 안전조치를 수행할 수 있게 한다.
- [0072] 관리부(140)는 서버(100)의 효율적인 운용과 관리를 위하여 금융사기 분석 케이스 정보 및 사용여부 정보의 등록, 관리 및 스코어링을 하기 위한 각 금융사기 분석 케이스별 가중치정보의 등록 및 관리한다.
- [0073] 또한, 금융거래패턴 추출을 위한 거래모형정보의 정의 및 관리, 금융사기거래유형의 BL패턴정보의 등록 및 관리 등을 수행한다.
- [0074] 또한, 레거시 시스템(20)으로부터 거래내역을 받을 거래정보와 서버(100)에서 요구되는 거래종류 및 데이터형식 등에 관한 정보의 등록 및 관리하고 상기 서버(100)의 기초정보 등을 관리정보DB(240)에 등록하고 관리한다.
- [0075] 이러한 등록 및 관리를 위해 운영자가 별도의 단말기나 입력부(도면 미도시)를 이용하여 원하는 정보를 입력, 수정, 삭제 할 수 있다.
- [0076] 그러면, 이러한 구성을 가진 본 발명의 실시예에 따른 금융사기 경보 시스템의 동작에 대해 상세히 설명하기로 한다.

- [0077] 도 3은 계좌이체거래의 처리흐름도이다.
- [0078] 도 3을 참조하면, 금융거래 고객이 금융거래 단말기(10)를 이용하여 계좌이체거래선택(S11)을 하고 화면에 이체 금액과 입금계좌번호입력(S12) 등 필요한 데이터를 입력한 후에 실행버튼을 누르면 입금계좌확인(S13)단계로 관련 거래전문이 레거시 시스템(20)으로 전송된다.
- [0079] 그러면, 레거시 시스템(20)은 금융거래단말기(10)로부터 입금계좌확인전문접수(S21)를 하여 입금계좌의 상태를 확인하며 계좌금융거래위험도체크요청(S22)을 서버(100)로 보낸다.
- [0080] 서버(100)는 계좌금융거래위험도 체크요청전문(S131)을 접수하여 금융거래위험도 체크단계(S132)에서 계좌정보 DB(210)에 있는 해당 계좌의 금융거래위험도 및 거래내역DB(220)에 있는 거래패턴정보를 읽는다.
- [0081] 다음, 해당 계좌의 금융거래위험도가 높으면(S133) 콜센터 서버(30)에 거래패턴 정보 전송단계(S134)로 분기를 하며, 금융거래위험도가 높지 않으면 응답 전송단계(S135)로 분기한다. 그리고 콜 센터 서버(30)에 거래패턴 정보 전송단계(S134)는 금융거래위험도 정보를 요청한 시스템이 계좌이체를 수행하던 레거시 시스템(20)인 경우에는 금융거래위험도의 경중에 따라 해당 계좌의 금융거래패턴정보를 콜 센터 시스템의 콜센터 서버(30)와 같은 모니터링시스템으로 제공하여 모니터링 요원으로 하여금 금융거래고객에게 전화 등을 이용한 추가적인 안전조치를 수행 할 수 있다.
- [0082] 다음, 응답전송단계(S135)에서는 서버(130)의 체크부(130)가 응답전문을 작성하여 응답전문을 금융거래위험도를 요청한 레거시 시스템(20)으로 전송처리 한다.
- [0083] 레거시 시스템(20)의 응답전문수신단계(S23)에서는 계좌금융거래 위험도 체크요청(S22) 단계에서 서버(100)에 요청한 응답을 받아 금융거래단말기(10)로 위험도에 따른 메시지조립전송(S24)을 수행한다.
- [0084] 금융거래단말기(10)에서는 입금계좌확인단계(S13)의 거래응답을 받아 계좌확인메시지출력(S14)을 수행한다.
- [0085] 금융거래단말기(10)에서 금융거래 고객은 메시지에 따른 고객이체거래 결정단계(S15)에서 출력된 입금계좌 확인 결과메시지의 내용을 확인하여 계좌이체를 수행할 것인지 아니면 계좌이체거래를 중단할 것인지를 판단을 한다. 계좌이체거래를 중단하면 고객의 계좌이체는 수행되지 않고 거래는 종료된다. 이 때 고객메시지는 고객이 수행하고 있는 금융거래의 위험도를 이해하기 쉽고 보기 쉽게 출력을 해야 한다. 일반적으로 금융거래를 수행하면서 ATM기나 인터넷뱅킹 등의 거래를 수행하면서 나오는 메시지에 고객은 크게 신경을 쓰지 않는 경향이 있다. 특히, 금융거래위험도가 높은 거래는 메시지의 출력방법을 기존방식과는 다르게 출력하여 고객이 반드시 읽고 판단을 할 수 있어야 한다.
- [0086] 금융거래 단말기(10)에서 메시지에 따른 고객이체거래결정단계(S15)의 계좌이체를 계속할 것을 선택하면 이체처리단계(S16)에서 레거시 시스템(20)으로 이체처리전문을 발송한다.
- [0087] 레거시 시스템(20)에서는 이체처리전문접수(S25)단계를 수행하고 해당 전문의 계좌이체처리(S26)단계에서 출금 계좌에서 출금처리를 하고 입금계좌에 입금처리를 수행한다.
- [0088] 다음, 레거시 시스템(20)이 LOG생성단계(S27)에서 계좌이체처리를 수행한 LOG를 조립하여 기록하고, 계좌이체처리결과를 조립하여 금융거래단말기(10)로 전송하는 계좌이체처리결과 전송단계(S28)를 수행한다.
- [0089] 금융거래단말기(10)는 이체처리(S16)를 선택하여 수행한 계좌이체처리결과를 레거시 시스템(20)으로부터 수신하여 계좌이체결과출력(S17)함으로써 거래가 종료된다.
- [0090] 여기서, 서버(100)의 동작에 대해 이하에서 상세히 설명한다.
- [0091] 도 4는 서버의 처리흐름도이다.
- [0092] 도4를 참조하면 서버(100)의 관리부(140)에서 시스템의 효율적인 운영과 관리를 위한 기초정보를 먼저 등록하여야 한다.
- [0093] BL 케이스 정보 단계(S141)는 서버(100)에서 관리할 금융사기 분석을 위한 각종 케이스 정보 등을 등록 관리한다. 케이스 정보는 해당 케이스의 사용여부 정보 및 해당 케이스 분석을 수행할 매서드의 종류 등의 정보를 관리한다. 이러한 등록 및 관리는 운영자 또는 담당자가 별도의 단말기나 입력부(도면 미도시)를 이용하여 원하는 정보를 입력, 수정, 삭제하는 동작에 의해 수행된다. 예를 들면, 금융계좌의 입금과 출금의 거래패턴을 가지고 의심계좌를 추출하는 입출패턴케이스, 대포계좌를 받아 해당계좌의 정상여부 또는 출금기능등을 확인하기 위하여 수행하는 테스트용 거래를 추출하는 테스트패턴케이스, 그리고 수취계좌가 해당계좌에 입금되는 상황을

모니터링하기 위한 조회패턴 케이스 등과 같이 금융사기 분석을 위한 각종 케이스 정보를 관리한다.

- [0094] 스코어링 가중치 단계(S142)는 계좌의 금융거래 위험도를 계산하는 과정에서 BL 케이스에 따른 위험도 계산 가중치 및 각 케이스의 스코어링 계산 방법에 대한 정보를 등록 관리한다. 예를 들면, 테스트 패턴 케이스는 위험도가 높은 등급, 조회패턴 케이스는 위험도가 낮은 등급으로 스코어링을 할 수 있는 정보를 관리한다.
- [0095] 거래모형 정의단계(S143)는 금융거래패턴추출을 위한 기초정보로 금융계좌의 거래패턴분석을 위하여 거래 요소(FACTOR)정의, 요소 세분화(FACTOR SEGMENTATION), 거래모델링, 그리고 거래모형정의를 진행하고 거래모형 심볼라이징 정보를 관리정보DB(240)에 저장 관리한다. 예를 들면, 입출패턴을 분석하기 위한 요소(FACTOR)로 시간, 잔액, 현금대체등과 같은 요소(FACTOR)를 정의하고 잔액 요소(FACTOR)의 경우 잔액유무로 세분화(Segmentation)하여 출금거래를 접목하여 모델링을 하면 잔액이 없는 '전액출금', 잔액이 남아 있는 '일부출금'으로 구분할 수 있다. 그리고 이렇게 모델링 된 정보를 거래모형으로 정의하여 전액출금은 'A' 일부출금은 'P'로 각 모형을 심볼라이징(Symbolizing)하여 정보를 등록할 수 있다.
- [0096] 그리고 거래매핑정보단계(S144)는 래거시 시스템(20)에서 받을 거래종류에 대한 거래코드정보와 서버(100)에서 필요로 하는 데이터형식, 그리고 어떤 케이스 정보에 따라 처리를 할 것인지에 대한 정보를 저장 관리한다.
- [0097] BL거래패턴 등록단계(S145)는 서버(100)에서 패턴체크에 필요한 금융사기계좌의 거래특성으로부터 추출한 거래패턴정보와 금융사기가 예상되는 거래패턴을 등록하고 관리하여 BL패턴 체크의 정보로 활용이 가능하게 된다.
- [0098] 관리부(140)의 필요한 정보가 모두 등록된 서버(100)는 정상적인 동작을 수행할 수 있는 것이다.
- [0099] 래거시 거래내역 수신(RECV)단계(S111)에서 금융 계좌의 거래정보를 래거시시스템(20)으로부터 또는 래거시 시스템(20)의 거래로그로부터 받아 읽은 후에, 거래매핑DATA존재단계(S112)에서는 읽은 거래정보가 금융사기경보시스템(10)에서 필요한 거래인지를 판단하기 위해 관리정보DB(240)에서 확인하여 존재하지 않은 거래는 필요하지 않은 거래로 해당 데이터를 버리고 다음의 거래내역 데이터를 읽기 위해 다시 래거시 거래내역 수신(RECV)단계(S111)로 분기를 하며, 거래매핑 데이터(DATA)가 존재하는 경우에는 필요한 거래인 경우로 매핑 데이터 변환단계(S113)에서 서버(100)에서 필요한 데이터형식으로 변환을 하여 해당 데이터전문을 데이터 송신(DATA SEND)단계(S114)에서 패턴분석부(120)로 전달한다.
- [0100] 다음, 데이터 수신(DATA RECV)단계(S1211)에서는 연결부(110)로부터 거래패턴분석을 위한 계좌의 거래정보 데이터를 받거나, 래거시 시스템(20) 또는 타 시스템으로부터 계좌 금융거래 위험도 체크요청(S131) 전문을 받는다.
- [0101] 다음, 분석거래 여부단계(S1212)는 접수한 거래가 거래패턴 분석거래인지 계좌의 금융거래 위험도 체크거래인지를 판단하여 거래패턴 분석거래인 경우에는 거래원장생성 및 갱신단계(S1213)로 분기를 하고, 금융거래위험도 체크거래인 경우에는 체크부(130)의 금융거래 위험도 체크단계(S132)로 분기를 한다.
- [0102] 접수한 거래가 거래패턴 분석거래인 경우에는 거래원장생성 및 갱신단계(S1213)에서 해당 거래정보를 계좌정보 DB(210)이나 거래정보DB(220)에 기록 및 갱신을 한다.
- [0103] 다음, 케이스 정보 체크단계(S1214)는 후속 패턴체크거래를 결정하기 위해 거래 매핑정보를 참조하여 관리정보 DB(240)에 정의되어 있는 금융사기 분석 케이스(CASE)의 매서드 정보를 읽어온다. 예를 들면, 계좌신규거래는 입출패턴, 테스트패턴, 조회패턴 등의 분석은 필요가 없기에 거래매핑 정보에는 필요한 패턴분석정보가 등록되지 않아서 패턴분석을 하지 않고 생략(SKIP)하며, 조회거래는 조회패턴의 분석이 필요한 거래이므로 조회거래의 매핑정보에 필요한 조회패턴 분석정보가 있고 이를 참조하여 조회패턴분석 케이스(CASE) 정보에는 해당되는 분석 매서드 정보를 관리하여 이를 참조하여 패턴분석을 수행하게 된다.
- [0104] 그 다음, 케이스(CASE) 정보에 따라 패턴체크 필요여부 단계(S1215)에서 패턴분석이 필요한 경우에는 거래모형정보 세트(SET)단계(S1221)로 로직을 분기하여 패턴분석을 진행하며, 패턴분석이 필요 없는 경우에는 스코어링(SCORING)을 위한 스코어링(SCORING)변수 읽기(READ)단계(S1241)로 분기를 한다.
- [0105] 패턴분석이 필요하여 거래모형정보 세트(SET) 단계(S1221)로 분기를 하면 현재거래를 기준으로 각 거래의 거래모형을 추출하기 위해 기준시각 등이 현재거래의 정보로 세팅(SETTING)되며, 관리정보DB(240)로부터 거래패턴추출을 위한 거래모형정보를 참조하여 세팅(SETTING)한다.
- [0106] 그리고 다음 단계인 개별거래모형결정단계(S1222)에서 읽혀진 거래정보를 거래모형정보와 비교하여 해당 거래의 거래모형을 결정하며, 결정된 거래모형을 심볼라이징(SYMBOLIZING)한다. 이렇게 심볼라이징(SYMBOLIZING)된 개별거래모형은 거래패턴문자열 조립단계(S1223)에서 먼저 처리한 거래정보의 거래모형과 연속된 문자열로 조립을

한다.

- [0107] 다음, 이전거래읽기(READ)단계(S1224)에서는 현재 처리한 거래내역의 바로 이전거래를 거래내역DB(220)로부터 읽는다. 읽은 거래내역을 가지고 패턴추출의 엔드(END)조건체크단계(S1225)에서 패턴추출을 종료하기 위한 조건이 만족되지 못하면 읽은 거래내역의 데이터를 가지고 개별거래모형결정단계(S1222)로 분기를 하여 엔드(END)조건체크단계(S1225) 까지를 반복 수행하며, 패턴추출을 종료하기 위한 조건이 만족되면 패턴추출을 종료하고 다음단계인 BL패턴 읽기(READ)단계(S1231)로 분기를 한다.
- [0108] 예를 들면, 상기 거래모형정의단계(S143)에서의 예시처럼 입금거래도 시간요소(FACTOR)를 가지고 기준거래와 10분이내 또는 10분이외 거래로 정의를 하여 시간내입금 또는 시간외입금으로 거래모형을 정의하고 시간내입금을 '1'로, 그리고 시간외입금을 '3'으로 심볼라이징(Symbolizing)한 정보를 등록 하였다면, 어떤 계좌에 잔액이 없는 상태에서 입금거래 후 즉시 5분이내에 전액출금이 발생한 출금거래의 거래패턴을 분석하면 출금거래를 기준으로 하여 개별거래 모형결정단계(S1222)에서 최종출금거래는 '전액출금'이기에 거래모형이 'A'로 결정이 되며, 이전거래는 입금거래로 출금거래와의 시간관계가 10분이내로 '시간내입금'이기에 거래모형이 '1'로 결정되며, 거래패턴문자열조립단계(S1223)를 수행하면 'A1'의 문자열로 조립이 되어 최종출금거래의 거래패턴은 시간 순으로 조립된 거래모형문자열인 '1A'가 추출되는 것이다.
- [0109] 다음 단계인 BL패턴 읽기(READ)단계(S1231)는 현재 추출한 거래패턴문자열이 BL패턴인지를 체크하기 위해 BL패턴DB(230)에 등록되어 있는 해당 체크패턴을 모두 읽어서 BL패턴체크를 위한 변수에 저장한다. 그리고 BL패턴체크단계(S1232)에서는 현재 추출한 거래패턴문자열과 BL패턴 읽기(READ)단계(S1231)에서 만든 BL패턴을 비교하여 추출된 패턴이 BL패턴인지를 판단하게 된다. 이렇게 판단된 거래패턴문자열과 BL거래패턴 여부정보가 스코어링(SCORING) 관련 단계로 전달된다.
- [0110] 다음, 스코어링(SCORING) 변수 읽기(READ) 단계(S1241)에서는 해당 거래의 계좌에 대한 금융거래위험도를 다시 평가하기 위해 사전에 등록된 각종변수 및 가중치를 읽어서 금융거래 위험도 계산을 위한 변수에 저장한다. 앞의 패턴체크 필요 여부단계(S1215)에서 패턴체크가 필요 없는 거래인 경우에도 스코어링(SCORING)을 위해 본 스코어링(SCORING)변수 READ단계(S1241)로 분기를 하는 것은 해당 계좌의 금융거래가 발생되면 거래가 있을 때마다 금융거래위험도를 다시 평가하여 항상 최신의 정보를 유지하기 위함이다.
- [0111] 다음, 스코어링(SCORING) 단계(S1242)는 스코어링(SCORING)을 위한 변수를 읽어서 해당 계좌의 금융거래 위험도를 다시 계산하는 단계로 각 스코어링(SCORING) 변수의 세팅(SETTING)을 어떻게 하느냐에 따라 다양한 스코어링(SCORING)을 할 수 있다. 예를 들면, 상기의 예시에서 추출한 입출패턴 '1A'가 BL패턴 DB(230)에 등록이 되어 있으면 해당계좌는 입출패턴에서 BL패턴이 추출되었으며, 스코어링(SCORING) 가중치정보에 입출패턴케이스는 높은 위험등급으로 등록이 되었을 경우 해당 계좌는 금융거래위험도가 높은 등급으로 결정된다.
- [0112] 다음, 금융거래 위험도 쟁신단계(S1243)는 금융계좌의 거래패턴분석을 통한 금융거래 위험도를 지수화 하기 위한 단계로 스코어링(SCORING)된 금융거래 위험도와 이미 추출된 거래의 패턴정보를 계좌원장DB(210)와 거래내역DB(220)에 기록 및 쟁신을 수행한다.
- [0113] 다음, 입금거래인가(S1244)단계에서는 현재 거래패턴분석을 수행한 기준거래가 입금거래가 아닌 경우에는 패턴분석을 종료하며, 입금거래인 경우에는 다음 단계인 콜센타전송단계(S1245)에서 현재 분석한 계좌의 금융거래패턴정보 또는 금융거래위험도 정보를 콜센타로 전송하여 모니터링 요원의 추가적인 관리를 진행하도록 한다.
- [0114] 그리고 금융계좌의 금융거래위험도 체크를 위해 타 시스템 또는 레거시 시스템(20)에서 계좌금융거래 위험도 체크요청전문(S131)으로 계좌의 금융위험도 체크를 요청하면 서버(100)의 패턴분석부(121)의 데이터 수신(DATA RECV)단계(S1211)에서 해당 전문을 접수한다.
- [0115] 다음, 분석거래여부단계(S1212)에서 분석거래가 아닌 체크거래로 금융거래위험도체크단계(S132)로 분기를 한다. 이 단계(S132)에서는 계좌정보DB(210)에 있는 해당 계좌의 금융거래위험도 및 거래내역DB(220)에 있는 거래패턴정보를 읽는다.
- [0116] 다음, 금융거래위험도수준체크단계(S133)에서 계좌의 금융거래위험도가 높으면 콜센터 서버(300)에 거래패턴정보전송단계(S134)로 분기를 하며, 금융거래위험도가 높지 않으면 응답전송단계(S135)로 분기한다.
- [0117] 그리고 콜센터(CALL CENTER)에 거래패턴정보전송단계(S134)는 금융거래위험도 정보를 요청한 시스템이 계좌이체를 수행하던 레거시 시스템(20)인 경우에는 금융거래 위험도의 경중에 따라 해당 계좌의 금융거래패턴정보를

콜센터 서버(30)와 같은 모니터링 시스템으로 제공하여 모니터링 요원으로 하여금 금융거래고객에게 전화 등을 이용한 추가적인 안전조치를 수행 할 수 있다.

- [0118] 다음, 응답전송단계(S135)에서는 응답전문을 작성하여 응답전문을 금융거래위험도를 요청한 시스템으로 전송처리 한다.
- [0119] 상기 과정에서 거래패턴 분석 방법에 관하여 상세히 설명하면 다음과 같다.
- [0120] 도 5는 거래패턴분석방법에 대한 순서도이다.
- [0121] 거래패턴분석은 거래모형정의와 거래패턴구현, 두 부분으로 구분하며, 거래모형정의는 관리부에서 정의를 수행하고, 거래패턴구현은 관리부의 정보를 가지고 패턴분석부에서 구현을 수행한다. 이런 거래패턴분석방법에 있어서
- [0122] 첫째 단계인 관심요소(Factor)정의(S1) 단계는 금융거래에 대해 관심을 가지는 Factor에 따라 분석을 하기 위해 잔액의 유무, 시간관계, 거래의 자금형태, 연속거래, 채널구분, 자행 또는 타행구분 등과 같은 금융거래에 대한 관심 요소(factor)를 도출한다.
- [0123] 관심 요소를 도출하고 정의하기 위해서는 해당 요소가 거래정보에 존재하는 항목이거나 또는 존재하는 항목으로 비교 및 연산하여 구분이 가능해야 한다.
- [0124] 둘째 단계인 요소 세분화(Factor segmentation) (S2) 단계는 도출된 각 관심요소를 어떤 기준으로 세분화를 할 것인지에 대한 기준을 정의하고 그에 따라 관심요소를 거래중심으로 세분화하는 요소세분화 단계이며, 이렇게 세분화가 수행된 관심요소(Factor)를 거래모형정의요소라 한다. 예를 들면 아래 표1과 같다.

표 1

관심요소	정의	세분화
잔액의 유무	거래처 계좌의 잔액에 따른 거래의 구분으로 전액출금, 일부출금으로 나누며, 잔액은 ATM 기 단위출금액을 기준으로 한다. 즉 10,000 원을 기준으로 하여 10,000 원미만의 잔액이 남아 있으면 전액출금으로 구분한다.	전액출금 일부출금
시간관계	기준거래와의 시간 간격을 기준으로 일정시간범위 안의 거래와 일정시간범위 밖의 거래로 구분하며, 일정시간을 정하여 처리한다.	시간내거래 시간외거래
연속거래	동일거래가 연속으로 발생하는가에 따라 구분하여, 연속거래와 단독거래로 구분한다. 연속거래도 시간관계를 고려하여 앞거래와의 시간간격이 일정시간 이내일 때 연속거래로 정의한다.	연속거래 단독거래
자금거래	현금거래와 대체거래로 구분한다.	현금거래 대체거래

- [0125]
- [0126] 셋째 단계인 거래 모델링(S3) 단계에서 모델링은 거래모형을 도출하기 전 단계로 요소 세분화(Factor segmentation) 정보를 바탕으로 금융거래를 매핑하여 금융거래의 여러 가지 기본 유형을 만들어 내는 것이다. 이로써 향후에 거래패턴을 분석하기 용이한 거래를 정의하게 된다.
- [0127] 예를 들면 아래 표2와 같다.

※ 2

관심요소	세분화	대상금융거래	모델링
잔액의 유무	전액	출금	전액출금
	일부	출금	일부출금
시간관계	시간내	입금	시간내입금
	시간외	입금	시간외입금
시간내		출금	시간내출금
	시간외	출금	시간외출금
연속거래	단독거래	조회	단독조회
	연속거래	조회	연속조회
	단독거래	출금	단독출금
	연속	출금	연속출금

[0128]

[0129] 상기 표 2와 같이 각 금융거래를 세분화한 요소정보와 조합하여 금융거래를 모델링을 한다.

[0130] 넷째 단계인 거래모형 정의(S4) 단계에서, 거래모형은 거래의 모델링 정보를 가지고 각각의 경우에 대해 또는 모델링 정보의 조합을 통하여 더욱 다양한 거래모형을 정의할 수 있다. 거래모형은 다음의 framework를 기반으로 도출한다.

[0131] 예를 들면, 입금거래의 경우 시간관계 요소에 따른 세분화 모델을 그대로 거래모형으로 정의할 수 있다. 이를 아래 표3에 나타내었다.

※ 3

금융거래	Factor 1(시간관계)	거래모형
입금	시간내	시간내입금
입금	시간외	시간외입금

[0132]

[0133] 또한, 출금거래의 경우 관심요소인 잔액유무와 시간관계에 따라 다음과 같이 복수개의 factor 조합으로 거래모형을 정의할 수 있으며, 아래 표 4와 같다.

※ 4

금융거래	관심요소 1 (시간관계)	관심요소 2 (잔액유무)	거래모형
출금	시간내	전액	시간내전액출금
	시간내	일부	시간내일부출금
시간외	전액	시간외전액출금	
	일부	시간외일부출금	

[0134]

[0135] 다섯째 단계인 Symbolizing(S5) 단계에서 상기와 같은 거래모형 정의방법에 의해 도출된 각각의 거래모형은 이를 거래패턴 분석에서 사용을 쉽게 하기 위하여 심볼라이징(symbolizing)이 필요하다. 심볼라이징(Symbolizing)은 형태나 의미가 없는 것에 정확한 개념과 의미를 부여하는 작업으로 금융계좌의 거래패턴추출이 용이하게 문자화를 이용하여 작업을 수행한다. 문자화로 정의를 할 때는 각각의 거래모형에 중복되지 않게 문자를 매핑하며, 문자는 사용하기 편하게 1개 또는 복수개의 문자로 정의할 수 있다.

[0136] 상기에서 도출된 거래모형을 다음 표5와 같이 1개의 문자화로 정의를 하여 거래모형문자를 만든다.

※ 5

금융거래	거래모형	Symbolizing(거래모형문자)
입금거래	시간내입금	1
	시간외입금	2
출금거래	시간내전액출금	A
	시간내일부출금	B
	시간외전액출금	C
	시간외일부출금	D

[0137]

[0138] 여섯째 단계인 거래모형결정(S6) 단계에서 금융계좌의 거래내역정보를 바탕으로 거래패턴의 추출은 특정거래를 기준으로 전. 후 거래와의 관계를 거래모형정의요소에 따라 비교 분석하여 각 거래의 거래모형을 도출하는 것이다. 즉, 각 거래에 대해 기준거래와의 관계를 거래모형정의요소 기준별로 비교하여 해당하는 거래모형을 찾아 결정한다.

[0139] 결정된 거래모형은 심볼라이징(SYMBOLIZING)한 거래모형문자로 변환하여 거래패턴문자열에 조립을 한다.

[0140] 이와 같이 거래모형결정과 거래패턴문자열조립을 반복적으로 수행하여 거래패턴의 도출이 수행된다.

[0141] 일곱째 단계인 거래패턴 도출(S7) 단계에서는 상기과정에서 예시로 정의한 거래모형과 심볼라이징(SYMBOLIZING)문자를 기준으로 하여 거래패턴을 도출한다.

[0142] 예를 들면, 어떤 금융계좌의 거래가 다음 표 6과 같다고 하면,

※ 6

거래구분	신규입금	입금 2	출금 1	출금 2	출금 3
현금대체구분	대체	대체	현금	현금	현금
거래시각 HHMMSS	10:21:40	13:22:40	13:23:40	13:24:40	13:24:40
거래금액	1,000	1,500,000	700,000	700,000	100,000
거래시잔액	1,000	1,501,000	801,000	101,000	1,000

[0143]

[0144] 마지막 출금거래(출금3)의 거래패턴을 추출하기 위해서는 출금3을 기준으로 거래패턴을 추출하며, 마지막 거래부터 거래모형을 결정한다. 마지막 거래의 거래모형을 결정하기 위해서는 거래모형정의 요소(factor)가 시간 관계와 잔액유무이므로 그 기준은 요소 세분화(factor segmentation)에 있는 것으로 하여 시간관계는 기준거래와 시간차이가 10분이내는 '시간내거래'이며, 10분이상은 '시간외거래'이다. 따라서 본 거래는 기준거래도 출금3이므로 시간차가 0이 되어 '시간내'이며 잔액유무는 남아있는 잔액이 10,000원미만이면 '전액출금'이고, 10,000원 이상이면 '일부출금'이다. 따라서 본 거래는 전액출금이 되어 두 개의 요소(factor)를 기준으로 분석한 것은 "시간내전액출금"의 거래모형이 된다.

[0145] 상기와 같이 이전 거래들도 분석을 하면 다음과 같이

[0146] 출금3(시간내전액출금=A)->출금2(시간내일부출금=B)->출금1(시간내일부출금=B) ->입금2(시간내입금=1)->신규입금(시간외입금=2)

[0147] 거래패턴문자열이 추출된다.

[0148] 그리고 추출된 거래패턴문자열은 시간순서로 나열하여 "21BBA"의 거래패턴이 추출되는 것이다.

[0149] 그리고 마지막인 여덟째 단계인 거래패턴의 해석(S8) 단계는

[0150] 상기 '일곱째 단계'에서 추출된 거래패턴을 해석하면

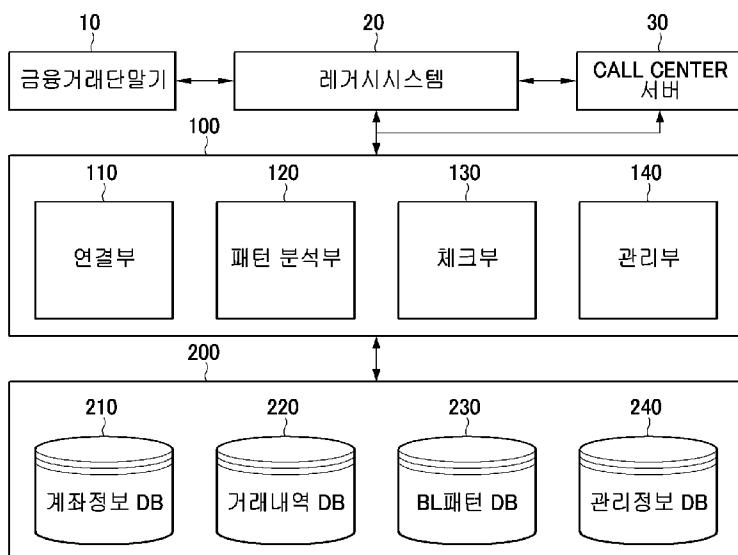
[0151] 최종출금거래(출금3)가 전액출금 거래인데 그 앞의 거래(출금2)는 시간내 일부출금 거래로 최종출금거래의 몇 분전 즉 10분을 초과하지 않는 시간의 범위 내에서 일부출금을 한 것이며, 그 앞의 거래(출금1)역시 최종출금거

래의 10분을 초과하지 않는 시간의 범위 내에서 일부출금을 한 것이다. 그리고 출금1 거래의 앞 거래인 입금2도 최종출금거래가 수행되기 전 10분을 초과하지 않는 시간의 범위 내에서 입금을 한 것이다. 신규입금거래는 최종 출금거래가 수행되기 오래 전 즉 10분이 넘는 시간 전에 계좌를 개설한 것으로 해석이 된다.

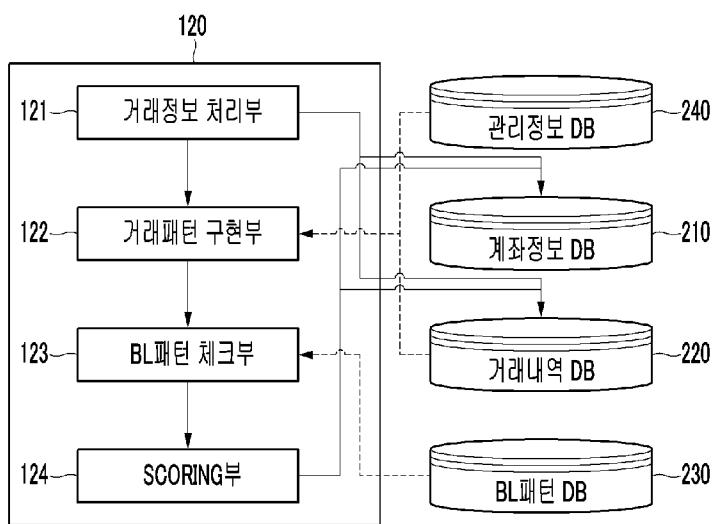
- [0152] 상기의 거래패턴을 또 다른 각도에서 해석을 하면, 계좌를 개설한 후에 해당 계좌에 입금이 되는 즉시 금액을 나누어 현금으로 모든 금액을 출금한 거래패턴이 된다.
- [0153] 이러한 거래 패턴에 관하여는 다양하게 변형이 가능하며, 필요에 따라 추가 삭제나 수정이 가능하다.
- [0154] 이상에서 설명한 본 발명의 실시 예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술 분야의 전문가라면 쉽게 구현할 수 있는 것이다.
- [0155] 이상에서 본 발명의 실시 예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

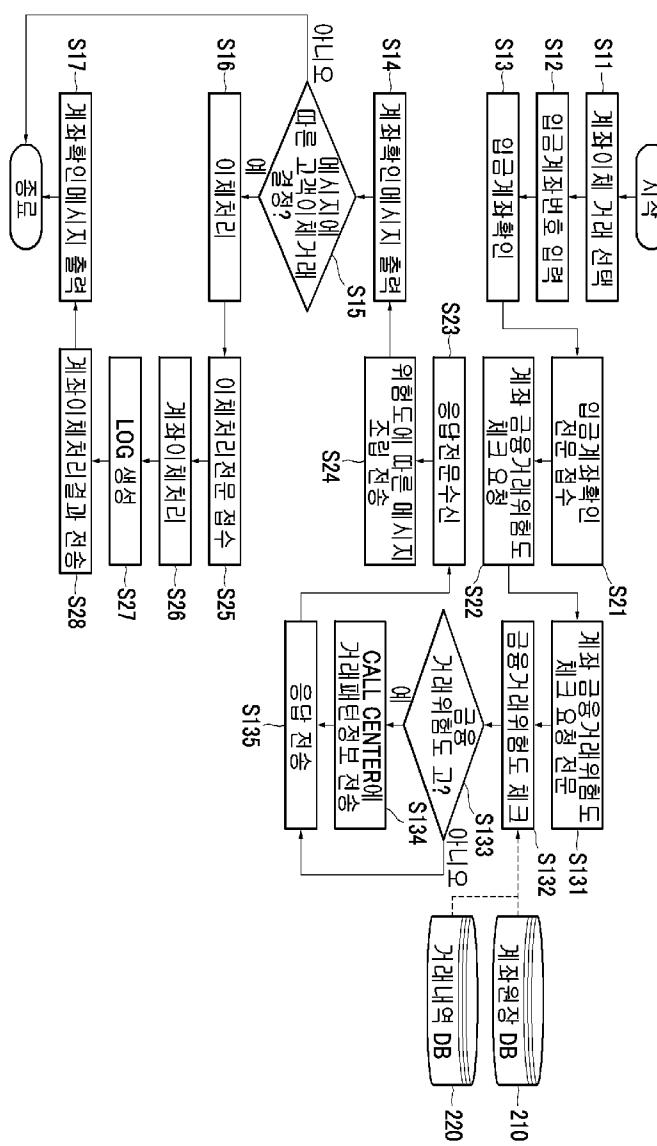
도면 1



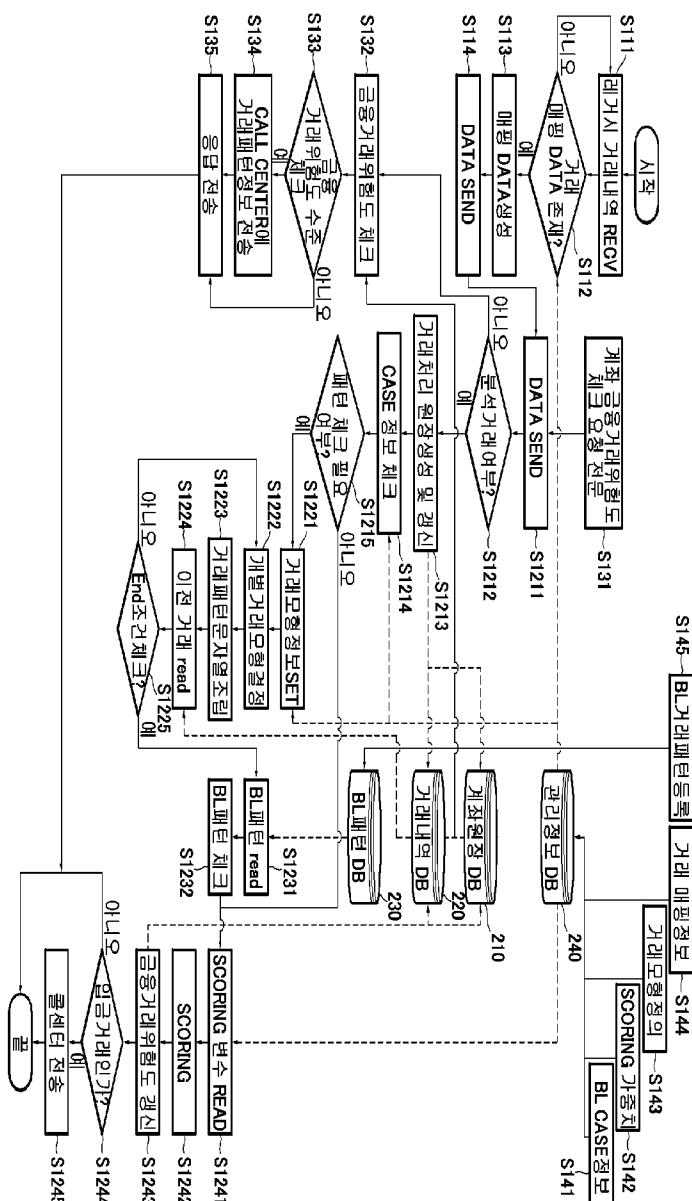
도면 2



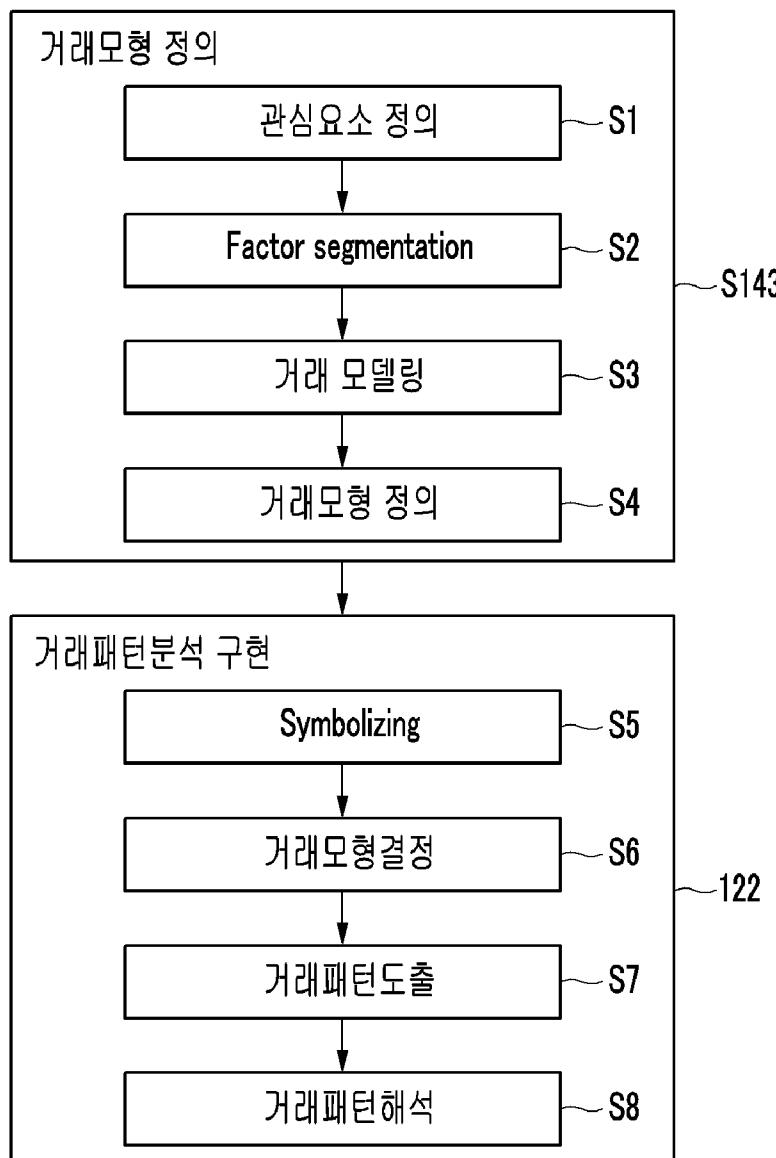
도면 3



제작



도 55



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization

International Bureau



(10) International Publication Number

WO 2016/065307 A1

(43) International Publication Date
28 April 2016 (28.04.2016)

(51) International Patent Classification:
G06Q 99/00 (2006.01)

(21) International Application Number:
PCT/US2015/057195

(22) International Filing Date:
23 October 2015 (23.10.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/067,792 23 October 2014 (23.10.2014) US

(71) Applicant: INSURANCE SERVICES OFFICE, INC.
[US/US]; 545 Washington Boulevard, Jersey City, NJ
07310-1686 (US).

(72) Inventors: COSTELLO, Tamara; 2127 Hanover Avenue,
Richmond, VA 23220 (US). IANAKIEV, Krassimir;
1550 Bay Street, San Francisco, CA 94123 (US). JOHN-
SON, Janine; 21852 Ada Street, Castro Valley, CA 94546
(US).

(74) Agents: FRISCIA, Michael, R. et al.; McCarter & Eng-
lish, LLP, Four Gateway Center, 100 Mulberry Street, Ne-
wark, NJ 07102 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

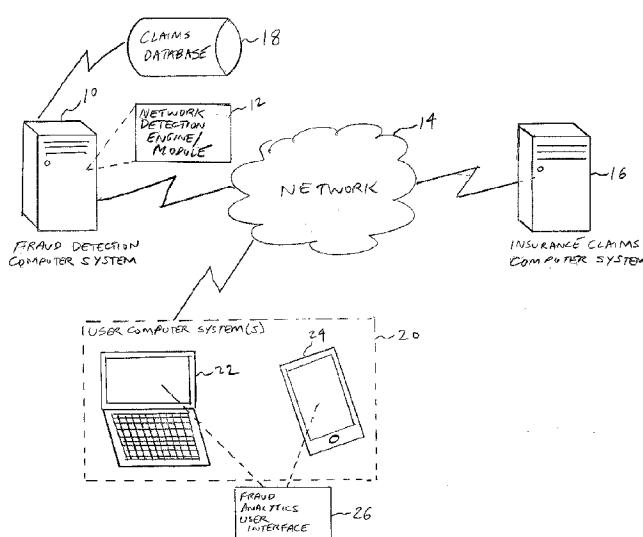
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SYSTEMS AND METHODS FOR COMPUTERIZED FRAUD DETECTION USING MACHINE LEARNING AND NETWORK ANALYSIS

FIG. 1



(57) Abstract: Systems and methods for computerized fraud detection using machine learning and network analysis are provided. The system includes a fraud detection computer system that executes a machine learning, network detection engine/module for detecting and visualizing insurance fraud using network analysis techniques. The system electronically obtains raw insurance claims data from a data source such as an insurance claims database, resolves entities and events that exist in the raw claims data, and automatically detects and identify relationships between such entities and events using machine learning and network analysis, thereby creating one or more networks for visualization. The networks are then scored, and the entire network visualization, including associated scores, are displayed to the user in a convenient, easy-to-navigate fraud analytics user interface on the user's local computer system.

SYSTEMS AND METHODS FOR COMPUTERIZED FRAUD DETECTION
USING MACHINE LEARNING AND NETWORK ANALYSIS

SPECIFICATION

5

BACKGROUND

RELATED APPLICATIONS

This application claims priority to U.S. Provisional Application Serial No. 62/067,792 filed October 23, 2014, which is expressly incorporated herein by reference in 10 its entirety.

FIELD OF THE INVENTION

The present invention relates to improvements in computing systems utilized in the insurance- and risk-related industries. More specifically, the present invention relates to 15 systems and methods for computerized fraud detection using machine learning and network analysis.

RELATED ART

In the insurance industry, detection of fraudulent activities is an extremely 20 important issue. Fraudulent insurance practices, particularly organized insurance fraud occurring across different geographic locations (e.g., in multiple states) are not only severe crimes, but they also represent undue burden and expense to insurers. Organized insurance fraud has a greater risk of repeat fraudulent activity, and also results in significantly greater financial exposure to insurers than opportunistic fraud. Also, perpetrators of organized 25 insurance fraud often employ sophisticated techniques for eluding traditional methods of detecting fraud. As such, there is a significant need to detect wide-spread fraud in the insurance industry, particularly organized insurance fraud.

In the fields of mathematics and computer science, graph theory is an important technique for studying the relationships between entities (nodes), as well as networks 30 formed by such entities and relationships. Typically, a graph is a network of nodes and lines called “edges” which connect the nodes. A graph can be undirected, in that there is no distinction between two nodes associated with an edge, or directed, in that nodes are connected by edges in specific directions. Graphs (networks) can be used to model many

types of relationships and processes in the physical world, in biology, and other fields of endeavor such as social and information systems.

Of particular interest to those in the insurance and risk-related industries, and as discussed in detail herein, graph theory and network analysis can be powerful tools for 5 detecting and analyzing fraudulent insurance activity, particularly organized insurance fraud. Accordingly, the present disclosure addresses these and other needs.

SUMMARY

The present disclosure relates to systems and methods for computerized fraud detection using machine learning and network analysis. The system includes a fraud detection computer system that executes a machine learning, network detection engine/module for detecting and visualizing insurance fraud using network analysis techniques. The system electronically obtains raw insurance claims data from a data source such as an insurance claims database. The raw insurance claims data is processed by the network detection engine/module to resolve entities and events that exist in the raw claims data. Once the entities and events have been resolved, the system electronically processes the resolved entities and events using network analysis techniques to detect and identify relationships between such entities and events, thereby creating one or more networks for visualization. The networks are then scored by the engine using one or more models, and the entire network visualization, including associated scores, are displayed to the user in a convenient, easy-to-navigate fraud analytics user interface on the user's local computer system. The system provides a significant advance in computing technology by allowing existing computers to perform sophisticated fraud detection techniques which such computers would not ordinarily be able to perform.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing features of the invention will be apparent from the following Detailed Description, taken in connection with the accompanying drawings, in which:

FIG. 1 is a diagram illustrating a system in accordance with the present disclosure
5 for fraud detection using network analysis;

FIG. 2 is diagram illustrating software modules of the network detection engine/module of FIG. 1;

FIG. 3 is a high-level flowchart illustrating processing steps carried out by the network detection engine/module of FIG. 1;

10 FIG. 4 is a flowchart illustrating step 44 of FIG. 3 in greater detail;

FIG. 5 is a flowchart illustrating step 72 of FIG. 4 in greater detail;

FIG. 6 is flowchart illustrating step 44 of FIG. 3 in greater detail;

FIG. 7 is a flowchart illustrating step 46 of FIG. 3 in greater detail;

FIG. 8 is a flowchart illustrating step 134 of FIG. 7 in greater detail;

15 FIG. 9 is a flowchart illustrating step 48 of FIG. 3 in greater detail;

FIG. 10 is a table illustrating event resolution processing performed by the system;

FIG. 11 is a diagram illustrating a network visualization generated by the system for detecting and visualizing fraud; and

FIGS. 12-13 are screenshots illustrating the user interface generated by the system,
20 including a network visualization generated by the system.

DETAILED DESCRIPTION

The present disclosure relates to a system and method for computerized fraud detection using machine learning and network analysis, as described in detail below in connection with FIGS. 1-13.

5 FIG. 1 is a diagram illustrating a system in accordance with the present disclosure for fraud detection using network analysis. The system includes a fraud detection computer system 10 which is a specially-programmed computer system that stores and executes a machine learning, artificially intelligent, network detection engine/module 12. The fraud detection computer system 10 could include a computer system such as a server, 10 a network of servers (e.g., a server farm, server cluster, etc.), or any other desired computer system having one or more microprocessors (e.g., one or more microprocessors manufactured by INTEL, Inc.) and executing a suitable operating system such as UNIX, LINUX, etc. Importantly, the network detection engine/module 12 comprises specially-programmed software code which, when executed by the computer system 10, causes the 15 computer system to perform fraud detection and visualization functions described in detail below, using machine learning techniques. As described in detail below, such functions allow for precise and rapid automatic detection and visualization of potentially fraudulent activities such as organized insurance fraud, etc., but it is noted that the system could also be used to detect other activities across large data sets, such as underwriting fraud and 20 other activities. The network detection engine/module 12 could be programmed in one or more suitable high-level computer programming languages such as C, C++, C#, Java, Python, Ruby, Go, etc. Of course, it is noted that any other suitable programming language could be utilized without departing from the spirit or scope of the present invention.

25 The network detection engine/module 12 can optionally communicate over a network 14 with one or more insurance claims computer systems 16 to obtain and process digital information relating to insurance claims. Alternatively, or additionally, such information could be stored in an insurance claims database 18 which could be stored on the fraud detection computer system 10 and hosted using a suitable relational database 30 management system (DBMS) such as that manufactured by ORACLE, Inc. or any other equivalent DBMS. The insurance claims database 18 could also include other relevant information such as payments made by insurers on claims, etc. Of course, the database 18 could be stored on another computer system in communication with the computer system

10, if desired. The network 14 could include any suitable digital communications network such as the Internet, an intranet, a wide area network (WAN), a local area network (LAN), a wireless network, cellular data network(s), or any other suitable type of communications network. As can be appreciated by one of ordinary skill in the art, suitable network
5 security equipment and/or software could be provided to secure both the fraud detection computer system 10 and the insurance claims computer system 16, such as routers, firewalls, etc.

One or more user computer systems 20, such as a laptop 22, a smart cellular telephone (such as an IPHONE, an ANDROID phone, etc.), a personal computer, a tablet computer, etc., could communicate with the fraud detection computer system 10 via the network 14. The fraud detection computer system 10 generates a web-based fraud analytics user interface 26 which is displayed by the computer system(s) 20 and which allows a user of the computer system(s) 20 to conduct detailed analysis, detection, and visualization of fraud that may exist in the claims database 18 utilizing the user interface
10 26. Advantageously, as discussed in detail below, the engine/module 12 conducts network analysis on data in the claims database 18 to detect potential fraud, and quickly and conveniently illustrates such potential fraud using one or more network visualizations that are displayed in the user interface 26 and can be quickly and conveniently accessed by a user of the computer system(s) 20.
15

FIG. 2 is diagram illustrating various software modules of the network detection engine/module 12 of FIG. 1. The network detection engine/module 12 is a machine learning module that includes a plurality of software modules 30-38 which perform various functions. It includes a claims data processing module 30, an entity and event resolution module 32, a network analysis module 34, a network scoring module 36, and a user interface module 38. Together, these customized modules, when executed by the computer system 10, cause the computer system to automatically learn relationships (using machine learning techniques) between potentially massive quantities of insurance data, and to automatically identify potentially fraudulent activities and to visualize the identified relationships and identities using a customized visualization user interface. With use, the
20 module 12 automatically improves its own performance through machine learning techniques, including, but not limited to, the network detection and scoring features discussed herein. The modules thus significantly improve the functioning of the computer system 10 by allowing the system 10 to rapidly and dynamically detect and visualize
30

potential insurance fraud for users of the system, in a way that computer systems could heretofore not perform such functions.

Turning to the specific modules, the claims data processing module 30 electronically receives and processes raw claims data from, for example, the claims database 18 of FIG. 1. Functions performed by the module 30 include, but are not limited to, optionally removing (cleansing) personal information from the data, formatting the data into a common data storage (table) format, etc. The entity and event resolution module 32 processes output data from the claims processing module 30 to resolve both entities within the data (e.g., the identities of individuals, claimants, policy holders, insurers, service providers (e.g., healthcare service providers, etc.), employers, etc.) as well as events (e.g., insurance claim events, medical claims/procedures, legal actions, etc.).

The network analysis module 34 processes output from the entity and event resolution module 32 to automatically generate one or more networks linking entities and events identified by the entity and event resolution module 32. The network scoring module 36 scores each network generated by the network detection module 34, so as to provide an indication of the degree of fraud occurring within the network. Importantly, the modules 34 and 36, by automatically generating networks from the ingested data and scoring those networks, cause the computer system 10 to automatically learn relationships between insurance data and to automatically detect and visualize potentially fraudulent activities. They therefore constitute significant machine learning (artificial intelligence) modules that cause the computer system to perform functions that it could not perform before, thereby significantly improving the functioning of the computer system 10. As such, the computer system 10, when programmed to execute the modules discussed herein, becomes a particular machine capable of performing advanced, automated fraud detection and visualization techniques not heretofore provided. Indeed, as discussed below, the processes executed by the network detection and scoring modules 34 and 36 improve their own functionality and ability to detect fraudulent activity through feedback techniques (e.g., by automatically adjusting and improving the scoring functions performed by the system, with subsequent use of the system).

The user interface module 38 generates a computer user interface, discussed below, which displays a visualization of the network(s) generated by the network detection module 34 and provides other useful information. As will be discussed in greater detail

below, the network visualization generated by the system allows a user of the system to quickly and conveniently detect potentially fraudulent insurance-related activities.

FIG. 3 is a flowchart showing processing steps, indicated generally at 40, carried out by the network detection engine/module 12 of FIG. 1. Beginning in step 42, the system electronically collects insurance claims data from a data source, such as from the claims database 18 of FIG. 1. In step 44, the system performs entity and event resolution processes on the claims data in order to resolve entities (e.g., persons, legal entities, insurance claimants, healthcare providers, legal service providers, etc.) and events (e.g., insurance claims, medical claims, legal actions, etc.) from the raw claims data. Then, in step 46, the system performs network analysis on the revolved entities and events. Importantly, as will be discussed in greater detail below, such network analysis permits a user of the system to identify connections (links) between events and entities, and to discover potentially fraudulent activities. In step 48, the system performs network scoring by scoring the links established between the entities and events by the network analysis performed in step 46. As discussed in greater detail below, the network scoring performed in step 48 could be carried out using one or more predictive computer models (supervised and/or unsupervised) which are applied by the system to the networks identified by the system, and specifically, to variables which are associated with the networks and automatically identified by the system. These network variables are scored by the predictive computer models to provide indications of fraud-related risk, which can be visualized by the system as discussed below. Then, in step 50, the system generates a graphical network visualization for display in the user's interface, as illustrated in FIGS. 13-14 and described in greater detail below. Then, in step 52, the visualization is displayed on a visual display 54 of the user's computer device (e.g., on the computing device(s) 20 of FIG. 1). The user can then view and interact with the visualization to discover potential network fraud and to conduct various analytics, as desired. It is noted that the network visualizations generated by the system can be generated upon request from the user of the system ("pull" delivery) or, they could be programmed to happen automatically ("push" delivery).

FIG. 4 is a flowchart showing step 44 of FIG. 3 in greater detail. The steps shown in FIG. 4 illustrate how the system resolves entities from the raw claims data using "keys." In step 60, the system populates a "keys" database table 42 with network keys. By the term "keys" it is meant data which represents individuals (e.g., individual insureds) and

which facilitates searching and matching functions performed by the system. Examples of such keys include, but are not limited to, primary keys (keys which are used to perform database/table queries), range keys (keys which represent ranges of values, such as ranges of names, etc.), and/or alternate keys (keys which represent other types of information).

5 Then, in step 64, the system populates a network entity table 66 with primary keys for all identities, including business keys, address keys, primary key ranges, and other metadata. In step 68, alternate key ranges are generated by the system using a systematic process that performs a lookup against the primary key ranges (e.g., on a state-wide or a nationwide basis) to find a range in which the alternate key fits. This then becomes the alternate key

10 range for that alternate key (one range for each alternate key). The alternate key ranges are stored in an alternate key range database table 70. In step 72, the system resolves entities using the network entity table 66 and the alternate key range table 70. Prior to performing this step, it is noted that the system could perform name “cleansing” (e.g., scrubbing and/or normalization of data), if desired. In step 74, a determination is made as

15 to whether all entities have been resolved. If a negative determination is made, step 72 occurs, wherein further resolution processing occurs. Otherwise, processing ends.

FIG. 5 is a flowchart showing step 72 of FIG. 4 in greater detail. The entity resolution step 72 processes keys to resolve entities using a variety of approaches, including, but not limited to, resolution using keys by state designation, resolution without state designation, and resolution based on ranges. Of course, other types of resolution (e.g., processing keys on a nation-wide basis) could be performed, if desired. Ranges could be provided by one or more suitable third-party data providers, such as, but not limited to, Search Software of America (SSA)/Informatica, Experian (QAS Name Search product), Lexis, IBM, etc. In step 80, the system first resolves entities using state designations. This can be accomplished, for example, by processing name ranges and address ranges, by processing exact names with exact addresses, by processing driver license numbers with Social Security numbers, by processing name ranges with driver license numbers, by processing driver license numbers with dates of birth, by processing medical license and name ranges, by processing address ranges with first names and Social

20 Security numbers, and/or by processing address ranges with first names and driver license numbers. Of course, other types of resolution using state designations are possible.

25

30

In step 82, the system resolves entities without use of state designations. This can be accomplished by, for example, processing Social Security numbers with dates of birth, by processing name ranges with Social Security numbers, and/or by processing name ranges with claim numbers. Of course, other types of resolution are possible.

5 In step 84, the system resolves entities based on ranges. This can be accomplished, for example, by processing alternate name ranges with address ranges, by processing alternate name ranges with exact addresses, by processing alternate name ranges with Social Security numbers, and/or by processing alternate name ranges with driver license numbers. Of course, other types of resolution are possible. In step 90, a
10 determination is made as to whether all claims have been resolved based on ranges. If not, control returns back to step 80; otherwise, processing ends.

FIG. 6 is a flowchart illustrating additional processing steps carried out by step 44 of FIG. 3. Importantly, in addition to resolving entities (as discussed above in connection with FIGS. 3-5), the system also resolves insurance-related events from raw claims data.
15 In step 100, the system populates an events database table 102 with events obtained from the raw claims data. This data could include scrubbed event data (e.g., event data without any personally-identifiable information) that has been processed by the system and obtained from the raw claims data. In step 104, the system creates a candidate event set for resolution from the event table 102. This could be accomplished by selecting events based
20 on event types and/or by role types. Then, in step 106, the system resolves events using the candidate event set. This could be accomplished, for example, by: grouping events by a carrier main affiliate number, a date of loss (associated with an insurance claim), and/or by an entity identifier; grouping events by carrier main affiliate number, date of loss, location of loss street/city and state; grouping events based on carrier main affiliate
25 number, date of loss, and policy number; and/or by grouping events based on carrier main affiliate number, date of loss and claim number (based on claim pattern cleansing applied during event extraction/cleansing). In step 108, the system combines grouped results using a transitive property, which functions as a “wrapper” that finds all parties in an event to ensure that the reported relationships are maintained. In step 110, the resolved events are
30 stored in the event table 102. In step 112, a determination is made as to whether all events have been resolved. If not, control passes back to step 104; otherwise, processing ends.

FIG. 7 is a flowchart showing step 46 of FIG. 3 in greater detail. Importantly, step 46 conducts network analysis on the entity and event data in order to detect and indicate

relationships between entities and events, using machine learning (artificial intelligence) techniques. In step 120, the system generates a candidate set for generating nodes in a network graph, using the network entity table 66 and the event table 102. Then, in step 122, the system identifies nodes that will be utilized for visualization. Service providers
5 that are identified by the system could be linked to their associated entities. In step 124, a determination is made as to whether more nodes should be identified. If so, control passes back to step 120; otherwise, in step 126, the system filters the events and entities, and in step 128, the system identifies edges between the previously-identified nodes and stores the edges in an edge table 130. In step 132, a determination is made as to whether more
10 edges require processing. If so, control passes back to step 126; otherwise, step 134 occurs. In step 134, the system identifies networks, whereby nodes and edges are grouped into discrete networks. Once the networks are identified, they are stored in the edge table 130. In step 136, a determination is made as to whether additional networks require identification. If so, step 134 is repeated; otherwise, processing ends.

15 FIG. 8 is a flowchart showing step 134 of FIG. 7 in greater detail. The system automatically identifies networks using machine learning algorithms as follows. First, in step 140, the system looks up the lowest party entity identifier in the candidate set (represented by a node). Then, in step 142, the system seeks all of the node's connections through the edges. The process then continues across the depth of the candidate set, until
20 all connections are found. If, in step 144, more parties must be processed, processing returns back to step 140. The network identifier is designated as the minimum entity identifier of the step. These processes can be repeated for each involved party (entity) associated with an event, until all entities are processed. This machine learning approach automatically improves the system's ability to automatically identify networks and
25 associated nodes and edges, with subsequent use.

FIG. 9 is a flowchart showing processing step 48 of FIG. 3 in greater detail. In step 150, the system pre-processes data from the network entity table 66, the event table 102, the edge table 130, and other tables 152 (which could include tables containing data extracts, line-of-business (LOB) information, vehicle identifier numbers, injury descriptions, etc.). Such pre-processing involves, for example, the system automatically selecting only networks where there are a pre-defined number of events, populating key tables that will later be used by the system, determining LOB information (e.g., for claims based on loss type, coverage types, etc.), counting event injuries, etc. In step 154, the

system automatically determines which model(s) will be used to score a network, as well as generates and populates series of interim tables to calculate and store all variables and corresponding measures. In step 160, the system generates variables that will be used by the system, and stores the variables in a supervised model variable table 156 and an unsupervised model variable table 158. Such variables include graph theory variables, claim-related variables, and variables relating to service providers. Importantly, the values assigned to these values by the scoring models/modules of the system influence the machine learning behavior of the system, as well as automatically improving subsequent machine learning behavior of the system through automatic adjustment of such variables with future use.

In step 162, the system scores the networks using one or more models, and stores the output in a supervised score table 164, an unsupervised score table 166, and a contributing variables table 168. Each scorable network is preferably analyzed using a supervised model and an unsupervised model, both of which are embodied as machine learning (artificial intelligence) computer algorithms. Specifically, with the supervised model, the system automatically infers an outcome using training data, while with the unsupervised model, the system automatically attempts to find hidden structure/relationships in data. The top contributing variables for the supervised model (e.g., scores that pass a pre-set threshold) are stored in ranked order. For the unsupervised model, the top 50 variables could be ranked in order and stored. The supervised score table 164 includes a network identifier, a supervised model region, and raw and normalized scores for all scorable networks. The unsupervised score table 166 includes a network identifier as well as raw and normalized scores for all scorable networks. The contributing variables table 168 includes all top variables in ranked order for all scorable networks. The supervised score table 164, the unsupervised score table 166, and any interim tables are processed in step 170, and the system generates and stores a final score for the network and stores the final score in a final score table 172. The final score for a scorable network is the higher of the normalized supervised score and the normalized unsupervised score. Data elements such as counts of entities, events, and counts of involved parties and service providers are collected along with model scores and are stored in the table 172, which includes the final score, region, the model which yielded the maximum score, counts of entities and events, counts of involved parties and service providers for each scorable network, etc. Finally, in step 174, the system generates and stores a custom score, if

desired, and stores the score in a custom score table 176. The custom score could be determined using any desired parameters. For example, any scorable networks that have a score of 750 or higher could be designated as a network of special interest (NSI), and for each NSI, a custom score could be calculated based on core events for each insurer group 5 that makes up the NSI. The custom score for the NSI could be company-specific, if desired. The custom score table 176 could include company-specific scores for each insurer group for each NSI, if desired. Importantly, with subsequent use, the machine learning components executed by the system (including the supervised and unsupervised models) automatically improve speed and accuracy in identifying and scoring network 10 nodes and edges, thus improving the system's ability to automatically detect and visualize potentially fraudulent activity.

FIG. 10 is a table illustrating event resolution processing carried out by the system. As mentioned above, the system can process raw claims data to resolve entities. Advantageously, this permits the system to compensate for inconsistencies in claim data, 15 including missing data, skewed data, incorrectly formatted data, etc. For example, as shown in FIG. 10, a table 180 of raw claims data could include a column 182 identifying claim references. As can be seen, each entry in the column is not consistent, and there are different claim references. While these references are different, they all relate to the same loss event occurring at the same location, and involving the same carrier. The system can 20 thus compensate for different claim references by resolving them with the same entity.

FIG. 11 is a diagram illustrating network analysis performed by the system. Entities could be graphically represented as nodes 232a-232g in a network graph 230, and events linking those entities could be represented as edges 234a-234h. Such a representation allows a user of the system to quickly see relationships between entities and 25 events, and to detect potentially fraudulent activity (e.g., organized fraudulent activity, etc.).

FIGS. 12-13 are screenshots illustrating an interactive graphical user interface 250 generated by the system and displayed on a user's computer system, such as the computer system(s) 20 of FIG. 1. As can be seen, the interface 250 includes an interactive network 30 visualization area 252 that graphically depicts the network and related analysis generated by the system (including networks, entities, links between entities, etc.). A detailed network information region 254 is also provided and lists the network ID, the geographic region covered by the network, the dominant state within the region, the network score,

total number of loss events in the network, total insurer groups, number of insured and claimants, and other information. A “reason” pane 256 displays detailed reasons in support of the network score, and an expandable pane 258 allows the user to access permitted third-party information, if desired. Additionally, a “hot spots” pane 260 allows
5 the user to access detailed information about the network. Another pane 270 (see FIG. 13) allows the user to access information about significant entities, such as prominent medical providers, prominent legal providers, etc. Also, as shown in FIG. 13, different icons can be used to indicate different nodes. For example, the icon 272 could represent an individual claimant, while the icon 274 could represent a legal service provider and the
10 icon 276 could represent a healthcare provider. As can be appreciated, the network visualization provided by the system allows a user to visually see relationships between entities and associated events, thereby facilitating detection of insurance-related fraud. By clicking on one of the icons 272-276, the user can access detailed information about the particular entity, as well as information about events (edges) linking that entity to other
15 entities.

It is noted that the network visualizations generated by the system could be further analyzed/interrogated using any desired visualization tools, such as the NETMAP visualization tool. Further, the intelligence developed by the system of the present disclosure (e.g., through the assembly and scoring of the networks) is stored and can be represented or conveyed in a downloadable format which captures key elements of the network (such as the data shown in elements 252-260 of FIG. 12), and the network-embedded set of data which defines the network. Such information could include data relating to events and entities which exist in that data set and which may be reported at a later point in time. Such features allow a user to work with the network visualizations from various perspectives (e.g., an “aerial view” provided by the web and a “ground view” provided in NETMAP). Further, it is noted that the visualization information (and embedded network intelligence) generated by the system could be conveyed digitally using hypertext markup language (HTML) and transported to a separate software-based analytics tool (such as NETMAP), if desired.
25

Having thus described the system and method in detail, it is to be understood that the foregoing description is not intended to limit the spirit or scope thereof. It will be understood that the embodiments of the present disclosure described herein are merely exemplary and that a person skilled in the art may make any variations and modification
30

without departing from the spirit and scope of the disclosure. All such variations and modifications, including those discussed above, are intended to be included within the scope of the disclosure. What is desired to be protected by letters patent is set forth in the appended claims.

CLAIMS

What is claimed is:

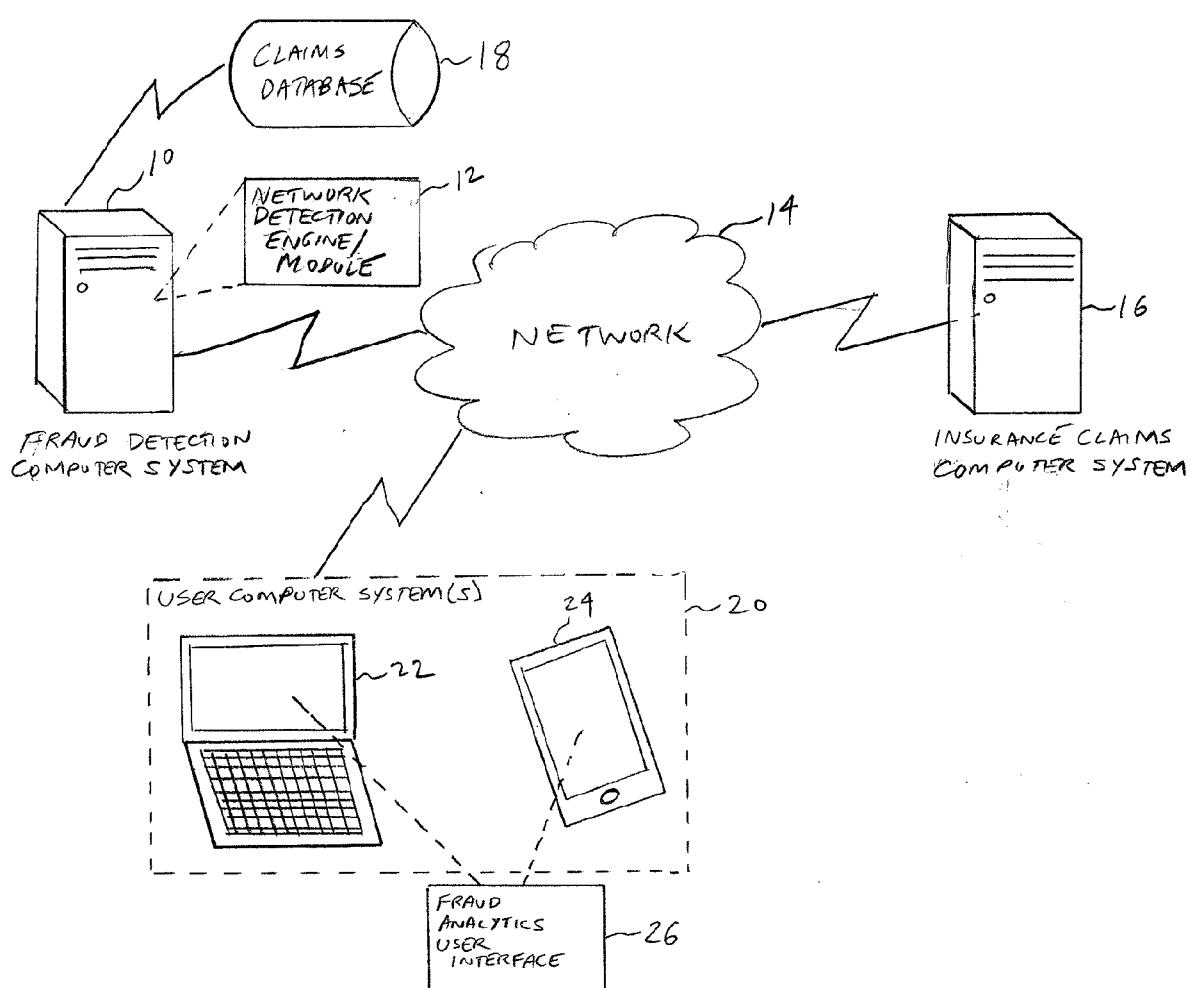
1. A system for computerized fraud detection using machine learning and network analysis, comprising:
 - 5 a first computer system in electronic communication with a second computer system via a communications network, the first computer electronically obtaining insurance claims data from the second computer system, wherein:
 - the first computer system executes a network detection module that processes the insurance claims data received from the second computer system using at least one machine learning algorithm which automatically identifies network nodes, edges, and relationships based on the processed insurance claims data, the identified network nodes, edges, and relationships indicative of potential insurance fraud; and
 - 10 a third computer system in electronic communication with the first computer system via the communications network, wherein:
 - 15 the third computer system generates and displays an interactive visualization user interface to a user of the third computer system, the interactive visualization user interface including an interactive graphical representation of the identified network nodes, edges, and relationships indicative of potential insurance fraud.
 2. The system of Claim 1, further comprising a claims database stored on the first computer system, the claims database locally storing the insurance claims data received from the second computer system.
 3. The system of Claim 1, wherein the network detection module further comprises a claims data processing module, an entity and event resolution module, a network analysis module, a network scoring module, and a user interface module.
 4. The system of Claim 3, wherein the claims data processing module electronically receives and processes raw claims data.
 5. The system of Claim 4, wherein the claims data processing module removes personal information from the raw claims data.
 6. The system of Claim 5, wherein the claims data processing module formats the raw data into a common data storage format.
 7. The system of Claim 3, wherein the entity and event resolution module processes output data from the claims processing module to resolve entities and events within the output data.

8. The system of Claim 3, wherein the network analysis module processes output from the entity and event resolution module to automatically generate one or more networks linking entities and events identified by the entity and event resolution module, the one or more networks including the nodes, edges, and relationships.
- 5 9. The system of Claim 3, wherein the network scoring module scores each network generated by the network detection module to provide an indication of a degree of fraud occurring within the network.
10. The system of Claim 3, wherein at least one of the network analysis module or the network scoring module executes a supervised machine learning algorithm.
- 10 11. The system of Claim 3, wherein at least one of the network analysis module or the network scoring module executes an unsupervised machine learning algorithm.
12. The system of Claim 3, wherein the user interface module generates the interactive graphical representation of the identified network nodes, edges, and relationships indicative of potential insurance fraud, and transmits the graphical representation to the interactive visualization interface for display to the user.
- 15 13. A method for computerized fraud detection using machine learning and network analysis, comprising the steps of:
 - electronically obtaining insurance claims data at a first computer system from a second computer system in electronic communication with the first computer system via a communication network;
 - executing a network detection module at the first computer system, the network detection module processing the insurance claims data received from the second computer system using at least one machine learning algorithm which automatically identifies network nodes, edges, and relationships based on the processed insurance claims data, the identified network nodes, edges, and relationships indicative of potential insurance fraud;
 - 25 and
 - generating and displaying at a third computer system in communication with the first computer system via the communication network an interactive visualization user interface to a user of the third computer system, the interactive visualization user interface including an interactive graphical representation of the identified network nodes, edges, and relationships indicative of potential insurance fraud.
- 30

14. The method of Claim 1, further comprising storing a claims database on the first computer system, the claims database locally storing the insurance claims data received from the second computer system.
15. The method of Claim 1, wherein the step of executing the network detection module further comprises executing a claims data processing module, an entity and event resolution module, a network analysis module, a network scoring module, and a user interface module.
16. The method of Claim 15, further comprising electronically receiving and processing raw claims data using the claims data processing module.
17. The method of Claim 16, further comprising removing personal information from the raw claims data using the claims data processing module.
18. The method of Claim 17, further comprising formatting the raw data into a common data storage format using the claims data processing module.
19. The method of Claim 15, further comprising processing output data from the claims processing module to resolve entities and events within the output data using the entity and event resolution module.
20. The method of Claim 15, further comprising processing output from the entity and event resolution module using the network analysis module to automatically generate one or more networks linking entities and events identified by the entity and event resolution module, the one or more networks including the nodes, edges, and relationships.
21. The method of Claim 15, further comprising scoring each network generated by the network detection module using the network scoring module to provide an indication of a degree of fraud occurring within the network.
22. The method of Claim 15, wherein the step of executing the network analysis module or the network scoring module further comprises executing a supervised machine learning algorithm.
23. The method of Claim 15, wherein step of executing the network analysis module or the network scoring module further comprises executing an unsupervised machine learning algorithm.
24. The method of Claim 15, wherein the step of executing the user interface module further comprises generating the interactive graphical representation of the identified network nodes, edges, and relationships indicative of potential insurance fraud using the

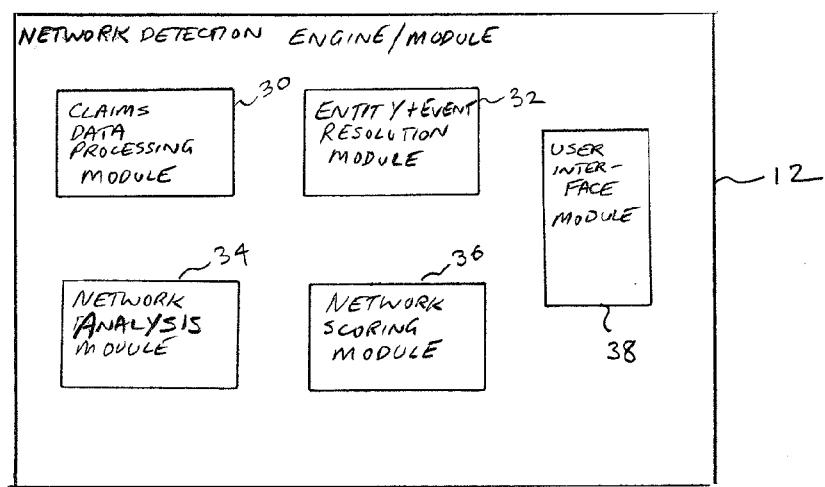
user interface module, and transmitting the graphical representation to the interactive visualization interface for display to the user.

FIG. 1



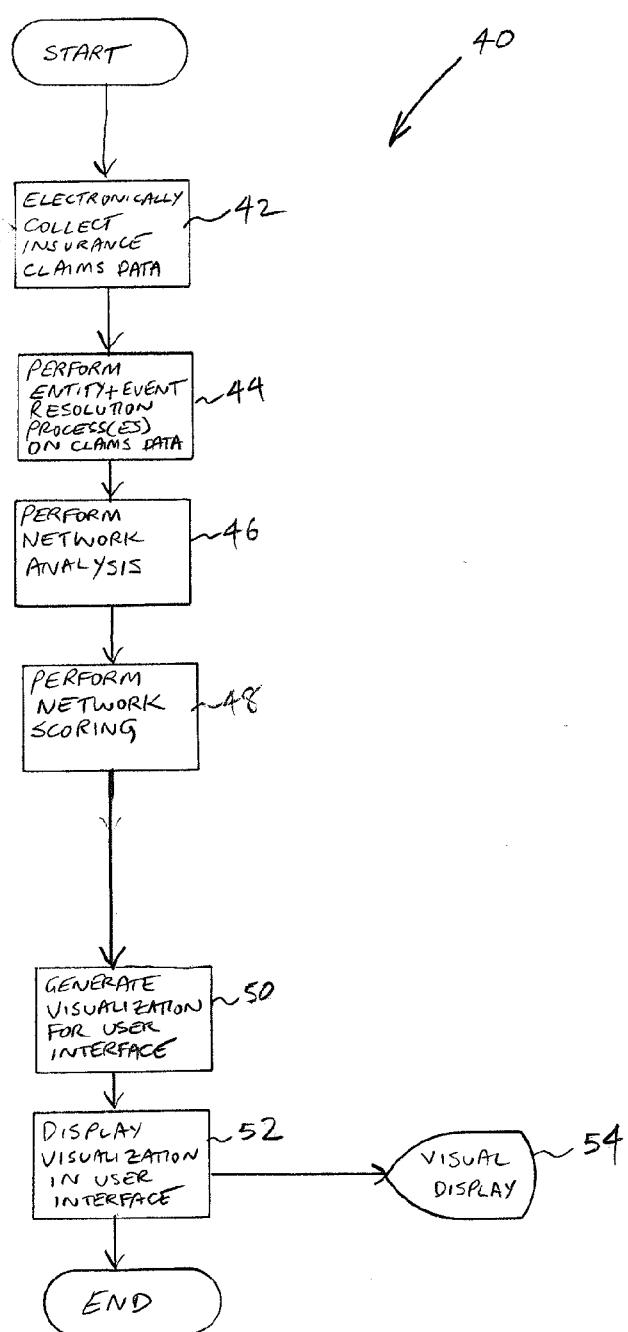
2/13

FIG. 2



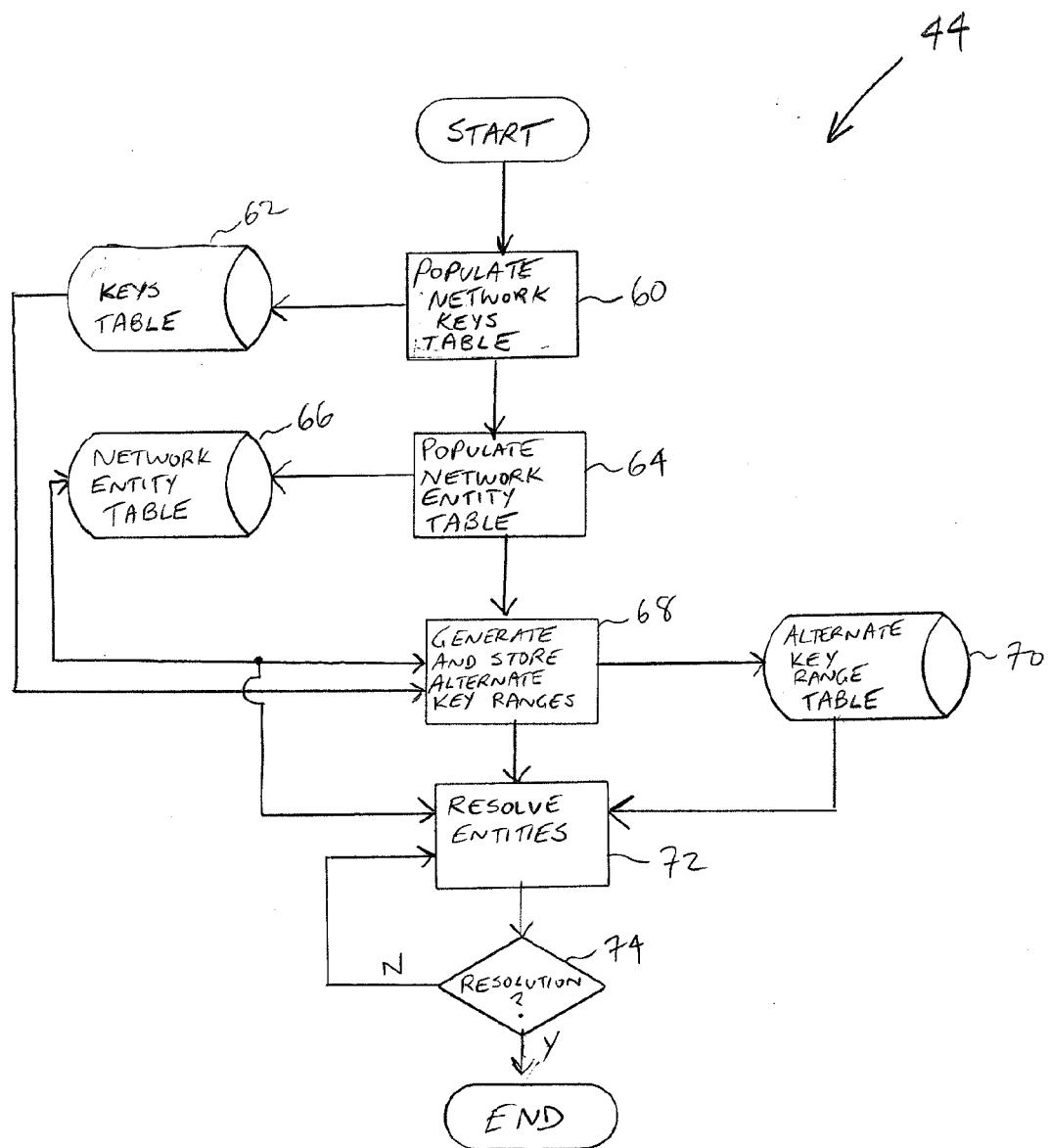
3/13

FIG. 3



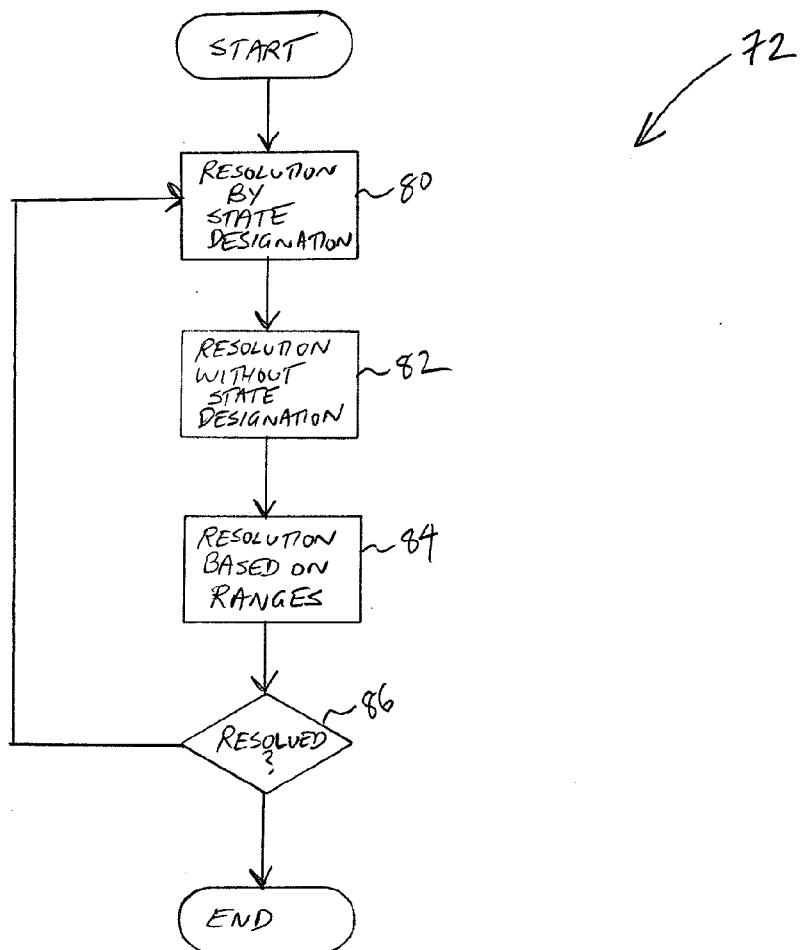
4/13

FIG. 4



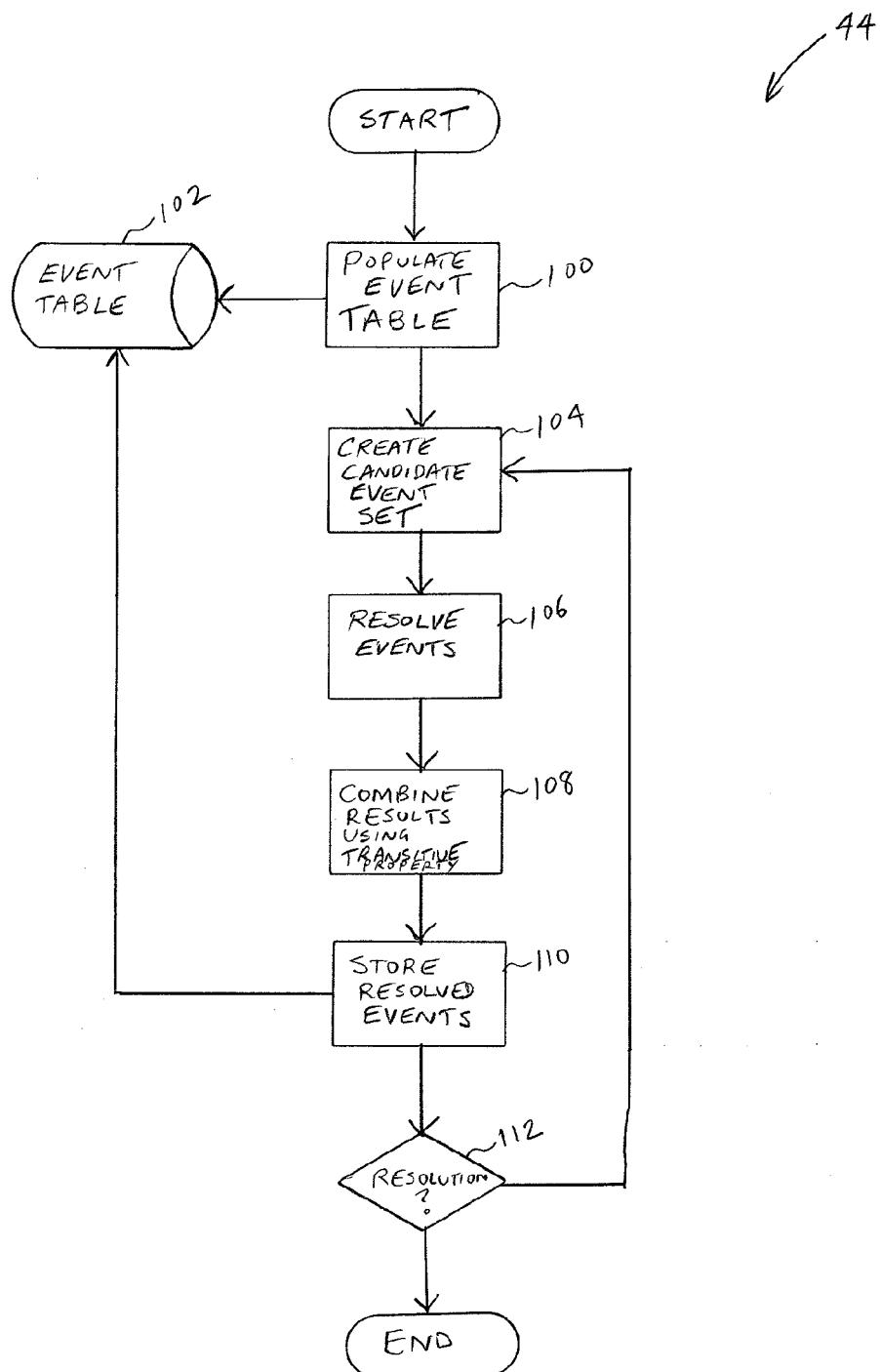
5/13

FIG. 5



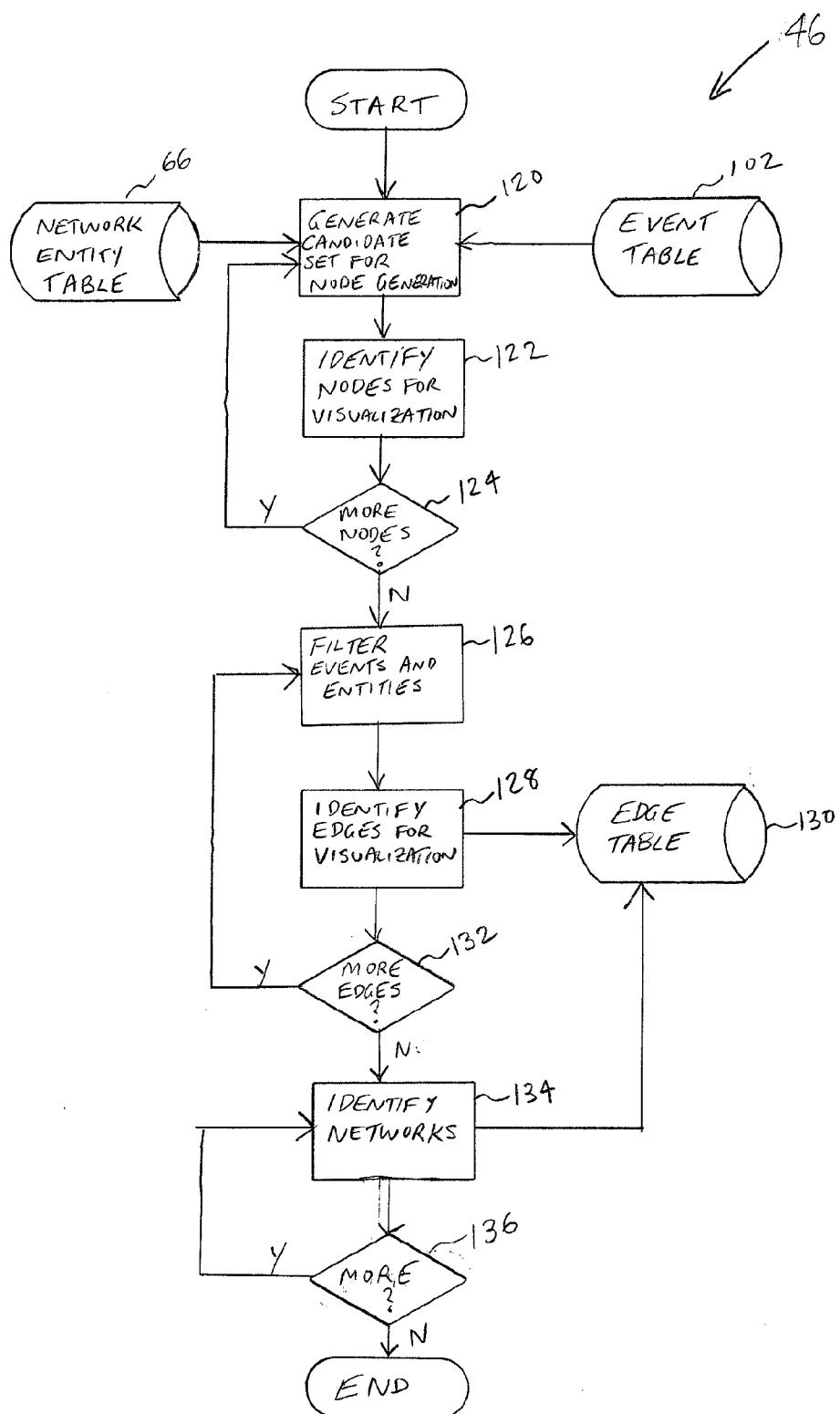
6/13

FIG. 6



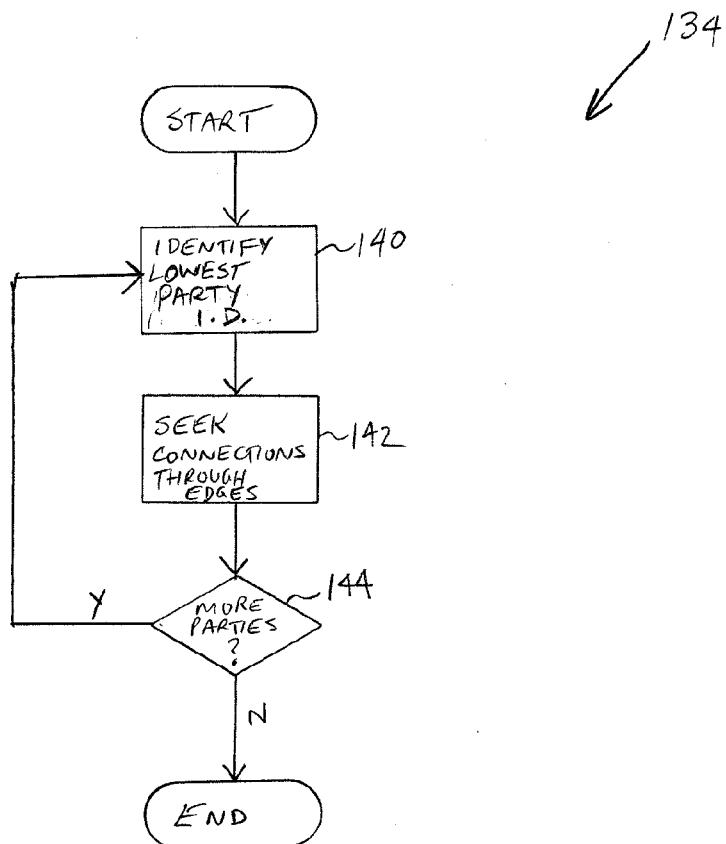
7/13

FIG. 7



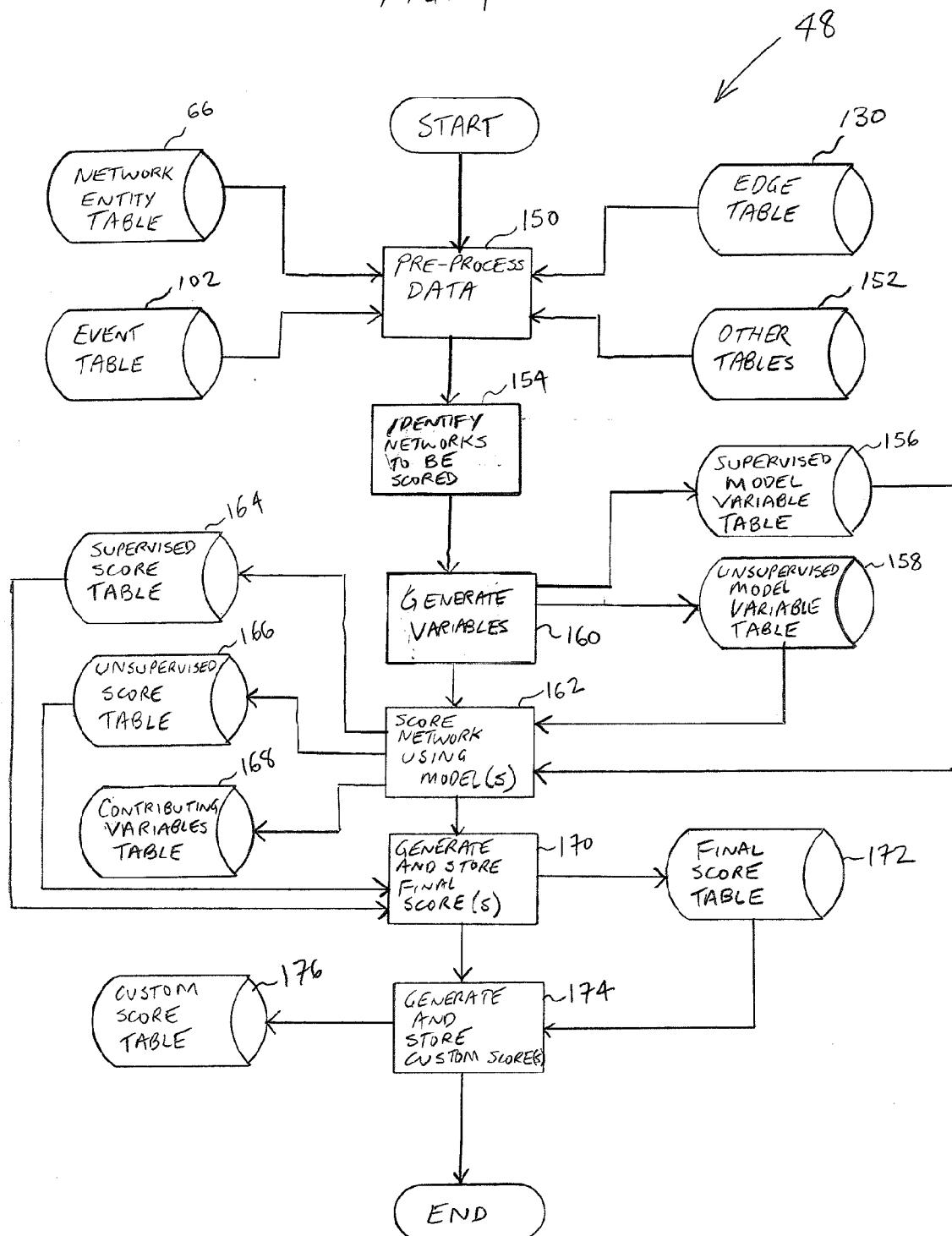
8/13

FIG. 8



9/13

FIG. 9



10/13

FIG. 10

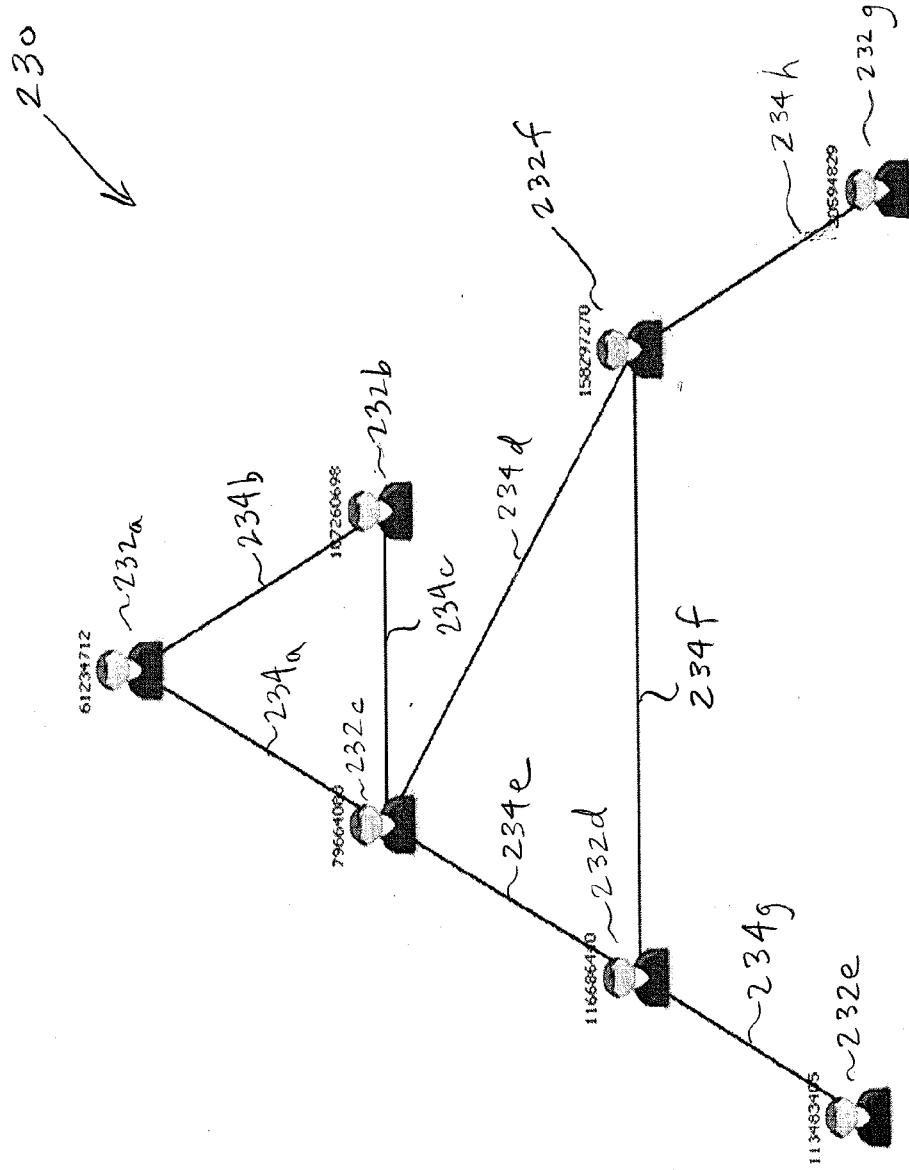
182

180

Reference number	Carrier	Office	Claim Reference	Pol reference	Date of Loss	Location of loss Street address	City	State	Entity_ID
0A1234567	ABC Company	45678	123456789		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	93676
0A1234567	ABC Company	45678	123456789		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	95400
0A1234568	ABC Company	45679	123456788		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	93676
0A1234568	ABC Company	45679	123456788		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	89400
0A1234569	ABC Company	45680	123456788		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	93640
0A1234569	ABC Company	45680	123456788		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	89400
0A1234570	ABC Company	45681	123456786	123456789	3/31/2000		Anytown		94228
0A1234571	ABC Company	45682	123456785		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	94228
0A1234571	ABC Company	45682	123456785		3/31/2000	W. JOHN ST/ ALFA PLACE	Anytown	NY	89400

11/13

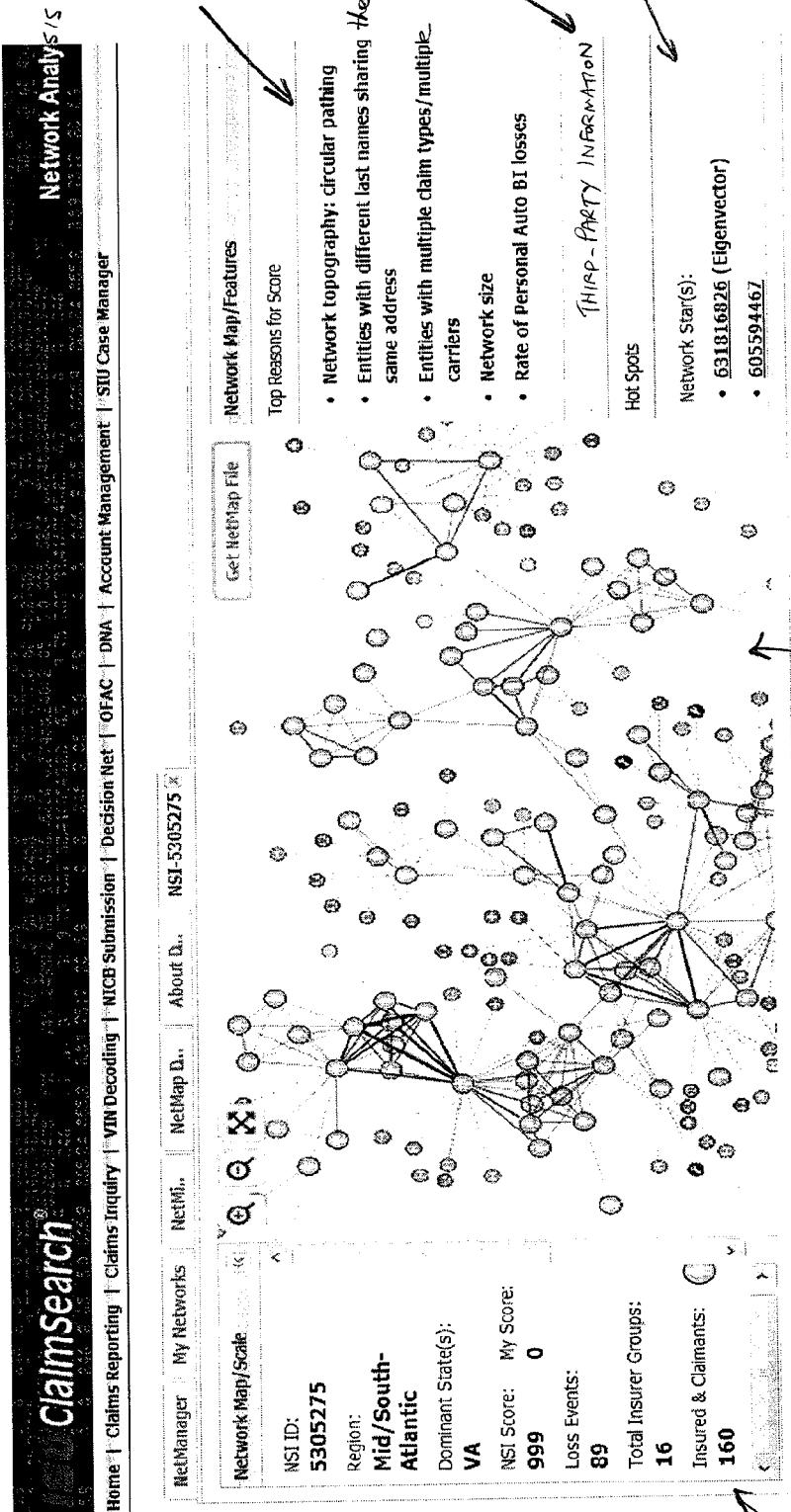
FIG. 11.



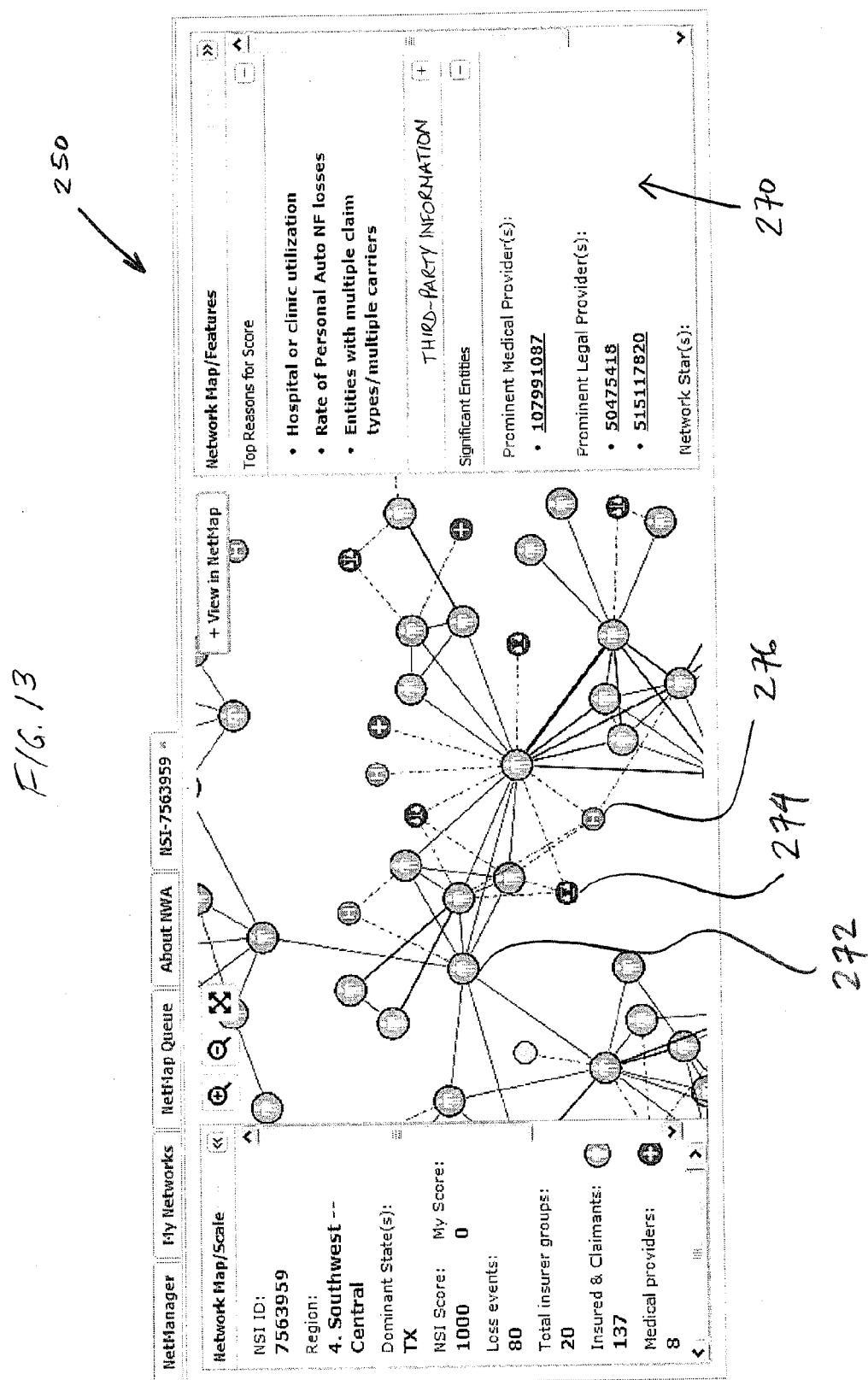
12/13

F16. 12

250



13/13



INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 15/57195

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 99/00 (2015.01)

CPC - G06Q 30/0185, G06Q 40/025, G06Q 50/265

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - G06Q 99/00 (2015.01)

CPC - G06Q 30/0185, G06Q 40/025, G06Q 50/265

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
IPC(8) - G06Q 99/00 (2015.01) (text search); USPC - 705/318, 706/12, 706/925 (text search)

CPC - G06Q 30/0185, G06Q 40/025, H04M 15/00, H04M 15/47 (text search)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, Google Scholar; Search terms used: fraud machine learning network analysis insurance claim user interface database data information raw format common score supervised unsupervised

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/0058763 A1 (ZIZZAMIA et al.) 27 February 2014 (27.02.2014), entire document, especially Fig. 1, 2, 5, 10, 12a, 12b; para [0064], [0087], [0106], [0112], [0159], [0166], [0204], [0316], [0319], [0352], [0359], [0553]	1-4, 7-16, 19-24
Y	US 2010/0174813 A1 (HILDRETH et al.) 08 July 2010 (08.07.2010), entire document, especially Fig. 3; para [0076]	5, 6, 17, 18
Y	US 2013/0085769 A1 (JOST et al.) 04 April 2013 (04.04.2013), entire document, especially para [0126]	5, 6, 17, 18
A	US 2012/0109821 A1 (BARBOUR et al.) 03 May 2012 (03.05.2012), entire document	6, 18
		1-24

 Further documents are listed in the continuation of Box C.

* Special categories of cited documents:	
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier application or patent but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search 17 December 2015 (17.12.2015)	Date of mailing of the international search report 12 JAN 2016
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774



US 20170193514A1

(19) **United States**

(12) **Patent Application Publication**
Chen

(10) **Pub. No.: US 2017/0193514 A1**
(43) **Pub. Date:** **Jul. 6, 2017**

(54) **METHOD FOR PERFORMING MACHINE DETECTION OF A SUSPICIOUS TRANSACTION**

(52) **U.S. Cl.**

CPC **G06Q 20/4016** (2013.01); **G06Q 20/108** (2013.01)

(71) Applicant: **E. Sun Commercial Bank, Ltd.**, Taipei City (TW)

(57)

ABSTRACT

(72) Inventor: **Hung-Yao Chen**, Taipei City (TW)

(21) Appl. No.: **15/393,320**

A method for detection of a suspicious transaction includes: retrieving a data set of client data associated with a client account and a client; assigning respective risk values to items of the data set of client data; calculating a weighted score based on the risk values and a weight list; assigning a risk level to the client based on the weighted score; retrieving transaction details of the client account for calculating a transaction parameter set; and when it is determined that the client account is involved in at least one transaction, determining whether the transaction is a suspicious transaction based on the risk level, the transaction parameter set and a pre-stored rule set.

(22) Filed: **Dec. 29, 2016**

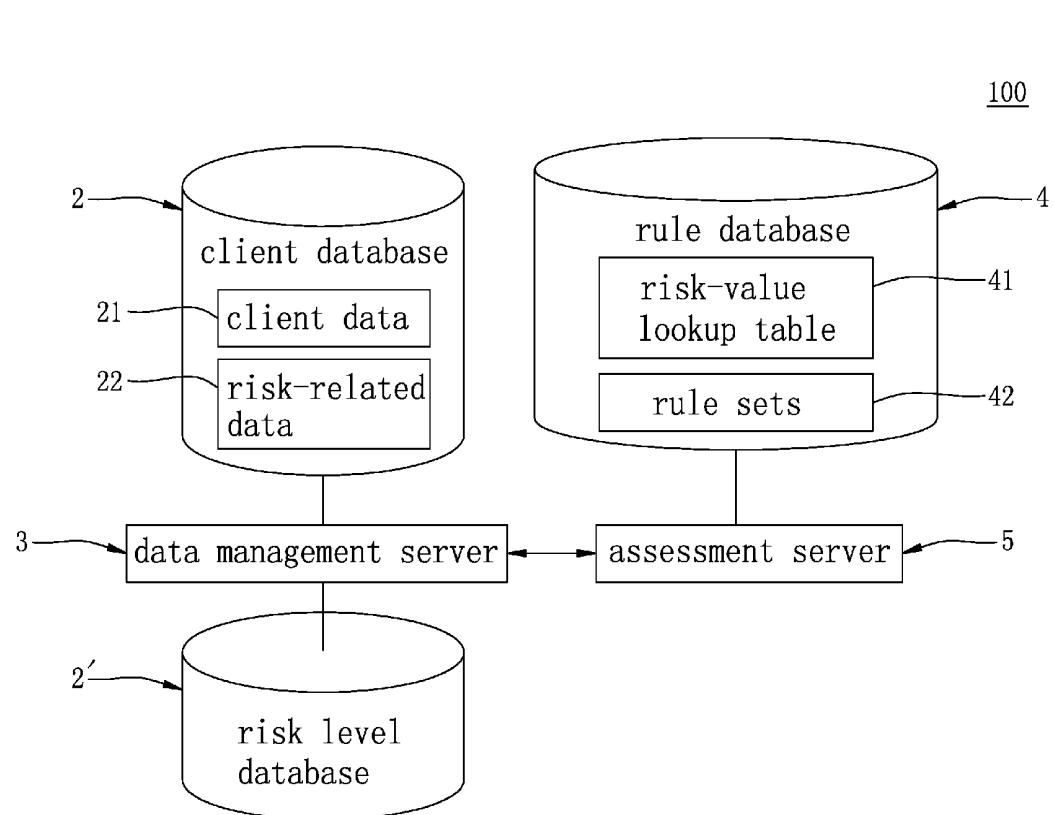
(30) Foreign Application Priority Data

Dec. 31, 2015 (TW) 104144745

Publication Classification

(51) **Int. Cl.**

G06Q 20/40 (2006.01)
G06Q 20/10 (2006.01)



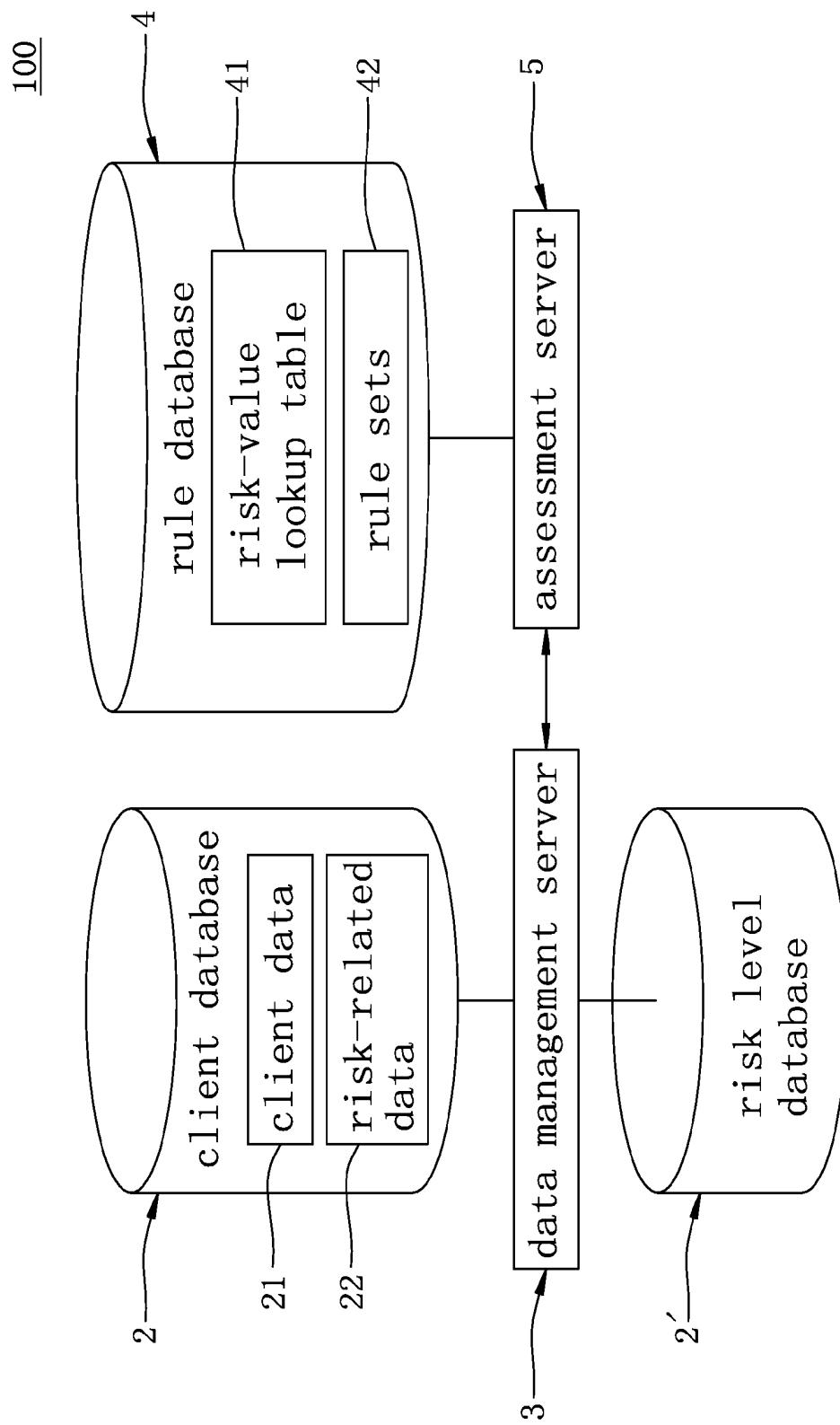


FIG.1

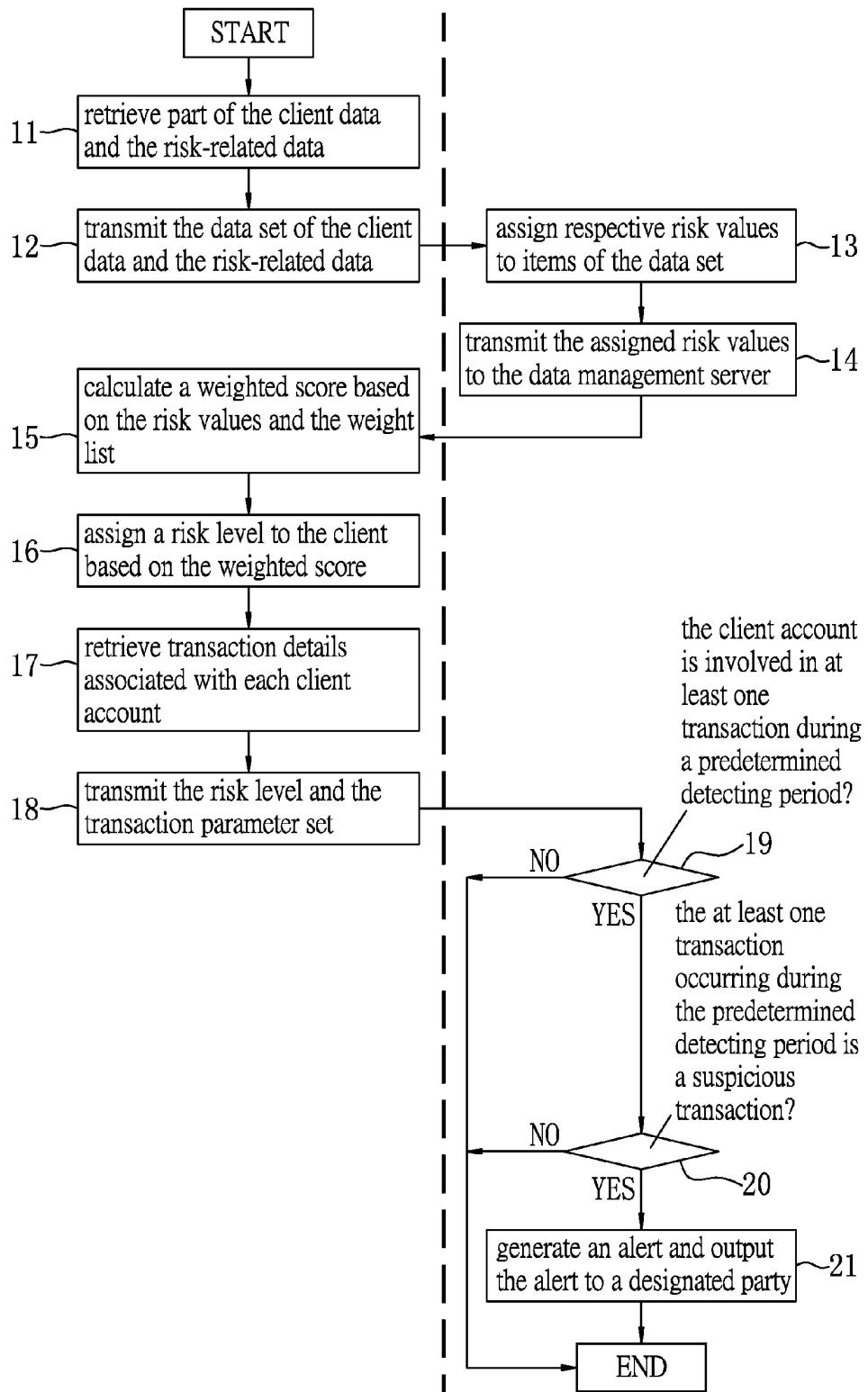


FIG.2

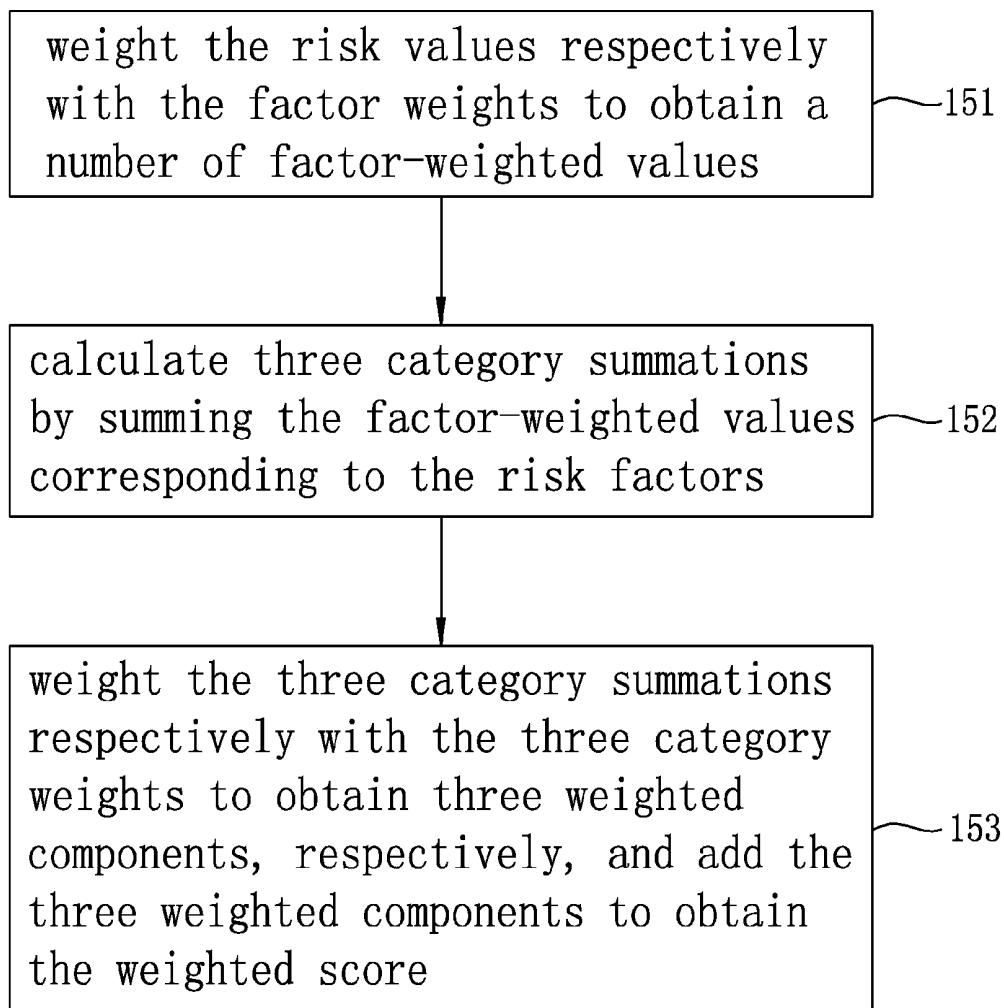
data management server

FIG.3

METHOD FOR PERFORMING MACHINE DETECTION OF A SUSPICIOUS TRANSACTION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority of Taiwanese Patent Application No. 104144745, filed on Dec. 31, 2015.

FIELD

[0002] The disclosure relates to a method for performing machine detection of a suspicious transaction on at least one client account that is associated with a client.

BACKGROUND

[0003] Typically, for a money services business (MSB), a considerable amount of transaction activities (e.g., transfer, deposit, withdrawal and conversion) may be processed in any business day. It is then desirable for a financial institution to monitor the transaction activities in order to identify one or more suspicious transactions, which may be actions of money laundering conducted in an attempt to be buried in the sea of transaction activities and remain undetected.

[0004] It is known that suspicious transactions may be conducted using dummy accounts with fake identifications and/or shell corporations.

[0005] As a result, in order to achieve the desired effect of anti-money laundering (AML), most countries have provided regulations for financial institutions to monitor the transactions. For example, Taiwanese government provides regulations regarding AML for reference by both banks and securities brokers. Under such regulations, a client may be required to present his/her identification for allowing process of domestic transfers. Note that the regulations regarding AML may vary from time to time, and from country to country.

[0006] It is noted that due to the large amount of transactions being processed, higher efficiency and accuracy may be desired for simultaneously monitoring as much transaction activities as possible.

SUMMARY

[0007] One object of the disclosure is to provide a method for detecting a suspicious transaction with a high efficiency and accuracy, and allows for simple adjustments for accommodating changes of regulations regarding anti-money laundering.

[0008] According to one embodiment of the disclosure, the method is for performing machine detection of a suspicious transaction on at least one client account that is associated with a client. The method may be implemented by a system that includes a client database, a rule database, a data management server and an assessment server. The data management server stores data regarding the client account. The method includes the steps of:

[0009] a) retrieving, by the data management server, a data set of client data from the client database, the data set of client data being associated with the client account and the client, and including a number of items respectively directed to a number of risk factors;

[0010] b) transmitting, by the data management server, the data set of client data to the assessment server;

[0011] c) assigning, by the assessment server, respective risk values to the items of the data set of client data based on a risk-value lookup table that is pre-stored in the rule database;

[0012] d) transmitting, by the assessment server, the risk values to the data management server;

[0013] e) calculating, by the data management server, a weighted score based on the risk values and a weight list that is pre-stored in the client database and that is associated with the risk factors;

[0014] f) assigning, by the data management server, a risk level to the client based on the weighted score;

[0015] g) retrieving, by the data management server, from the client database transaction details associated with the client account within a predetermined previous period that is immediately prior to a current business day, the transaction details including information associated with at least one transaction that has occurred on the client account;

[0016] h) calculating, by the data management server, a transaction parameter set based on the transaction details;

[0017] i) transmitting, by the data management server, the risk level and the transaction parameter set to the assessment server;

[0018] j) determining, by the assessment server, whether the client account is involved in at least one transaction during a predetermined detecting period that includes the current business day and at least one previous business day immediately prior to the current business day; and

[0019] k) when the determination of step j) is affirmative, determining, by the assessment server, whether the transaction is a suspicious transaction based on the risk level, the transaction parameter set and a rule set pre-stored in the rule database.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] Other features and advantages of the disclosure will become apparent in the following detailed description of the embodiments with reference to the accompanying drawings, of which:

[0021] FIG. 1 is a block diagram illustrating a system according to one embodiment of the disclosure;

[0022] FIG. 2 is a flow chart illustrating steps of a method for performing machine detection of a suspicious transaction on at least one client account, according to one embodiment of the disclosure; and

[0023] FIG. 3 is a flow chart illustrating sub-steps performed by a data management server for calculating a weighted score.

DETAILED DESCRIPTION

[0024] FIG. 1 is a block diagram illustrating a system 100 according to one embodiment of the disclosure.

[0025] The system 100 includes a client database 2, a data management server 3, a rule database 4 and an assessment server 5. The system 100 is capable of performing machine detection of a suspicious transaction on at least one client account that is associated with a client.

[0026] The client database 2 stores therein client data 21 associated with a number of clients, and risk-related data 22. The client data 21 includes a number of data sets each associated with a respective one of the clients. Each of the data sets includes basic information regarding the respective client, account information regarding any client account that

is associated with the respective client, and transaction details regarding all transactions involving the client account (s) associated with the respective client. In particular, each data set has a number of items, each directed to a corresponding one of risk factors. The items may constitute part or one or more of the basic information, the account information and the transaction details. The transaction details may include information on transactions processed within a predetermined time period, including a current business day.

[0027] The risk-related data 22 includes a risk-related data list that includes item options for each of the risk factors. Each item in each data set is one of the item options corresponding to the respective risk factor.

[0028] Specifically, in this embodiment, the risk factors are categorized into one or more of a client-related category, an account-related category and a geographical category.

[0029] The client-related category includes, but is not limited to, risk factors of a client type, a client identification type or a client occupation type. The account-related category includes, but is not limited to, risk factors of an account type, a manner in which the client account is opened, a source of fund used to open the client account, a service that is associated with the client account, or an activity frequency of the client account. The geographical category includes, but is not limited to, risk factors of an address of the client, or a location (e.g., country or region) in which a financial activity has occurred on the client account.

[0030] The following Table 1 includes exemplary information that may be used to further describe the item options included in the risk-related data list.

TABLE 1

Category	Risk Factor	Item Options
Client-related category	Client type	Natural person; Juridical person (Medium/Large (M/L)); Juridical person (Medium/Small (M/S)); Juridical person (Global Finance); Juridical person(SB)
	Client identification type	ID Card; Business Registration Certificate; Residence Permit; Passport; Offshore Banking Unit (OBU) ID number
	Client occupation type	Distinct codes associated with the occupation of the client, as announced by the Directorate General of Budget, Accounting and Statistics (DGBAS)
Account-related category	Account type	Time deposit; Composite deposit; Checking deposit; Gold account; Foreign Exchange (FOREX) time deposit; FOREX composite deposit; FOREX checking deposit;
	Account open manner	At-the-Counter; Online
	Source of fund	Cash; Check; Transfer; Domestic remittance; Foreign remittance
Geographical category	Service associated	Loan
	Activity frequency	Dormant; Active
	Address of the client	Names of possible countries/regions in which the address may be located
	Location of activity	Names of possible countries/regions in which a financial activity may occur on an account

[0031] For example, in Taiwan, a juridical person is categorized as medium/large (M/L) when an annual revenue thereof is larger than 1 billion NTD, as medium/small (M/S) when the annual revenue thereof is between 30 million and 1 billion NTD, and as SB when the annual revenue thereof is less than 30 million NTD. A juridical person that operates across Taiwan, Hong Kong and China with an offshore banking unit (OBU) is categorized as a Global Finance.

[0032] Based on the activity frequency of the client account, the client account may be categorized as a dormant account when the transaction details indicate that the client account is involved in no more than one transaction during a given period (e.g., 6 months) that precedes a predetermined detecting period (e.g., three consecutive business days including the current business day). On the other hand, when the client account is involved in more than one transaction during the 6-month period, the client account may be categorized as an active account.

[0033] The risk-related data 22 further includes a weight list having a number of factor weights corresponding respectively with the risk factors, and three category weights corresponding respectively with the client-related category, the account-related category and the geographical category.

[0034] The following Table 2 includes exemplary factor weights and category weights that may be used to define a risk level associated with a client.

TABLE 2

Category	Category Weight (%)	Risk Factor	Factor Weight (%)
Client-related category	30	Client type	30
		Client identification type	30
		Client occupation type	40
Account-related category	35	Account type	25
		Account open manner	5
		Source of fund	5
Geographical category	35	Service associated	40
		Activity frequency	25
		Address of the client	10
		Location of activity	90

[0035] The rule database 4 stores therein a risk-value lookup table 41 and a number of rule sets 42.

[0036] The risk-value lookup table 41 includes a number of risk values assigned respectively to the item options of the risk-related data list.

[0037] The following Tables 3A to 3C each include exemplary risk values assigned to the item options of the risk-related data list, for a respective one of the client-related category, the account-related category and the geographical category.

TABLE 3A

(client-related category)		
Risk Factor	Item Option(s)	Risk Value
Client type	Natural person or Juridical person	100
Client	ID Card	40

TABLE 3A-continued

(client-related category)		
Risk Factor	Item Option(s)	Risk Value
identification type	Business Registration Certificate Residence Permit, Passport, OBU ID number	100 140
Client occupation/ Occupational type	Public Sector, Education, Water & Gas, Wholesale & Retail, Accommodation & Catering Services, Transport, Storage & Communication, Finance & Insurance, Real Estate & Leasing, Professional Services, Technical Services/ Agriculture, Forestry, Fishery, Animal Husbandry, Manufacturing, Spinning, Weaving, Transportation, Warehousing, Publishing, Television Broadcasting and Pay Broadcasting, Telecommunications, Services, Financial Institutions, Insurance, Securities, Futures, Market Research and Opinion Polls, Leasing, Personal and Household Maintenance Manufacturing, Wholesale and Retail Trade, Accommodation and Catering/ Construction, Civil Engineering, Construction Industry, Commodity Brokerage, Watches and Eyewear Wholesale, Watches and Eyewear Retail, Building Materials Wholesale, Building Materials Retail, Secondhand Commodity Retailing, Fuel Retailing, Direct Selling, Catering, Financial Assistance, Real Estate, Corporation Management Agencies, Private Detective Services, Laundry, Hairdressing, Beauty Industry, Funeral Services Industrial and Commercial Services, Agriculture, Forestry, Fisheries and Animal Husbandry, Ore, Earth and Stone Mining Industry, Construction Industry/ Waste Removal, Treatment and Recycling, Pollution Remediation, Jewelry and Precious Metal Production, Jewelry & Precious Metal Products Wholesale, Jewelry & Precious Metals Retail, Real Estate Brokerage, Legal & Accounting Services, Management Consultancy, Gaming Industry, Ballroom, Electronic Arcade Industry, Pawnbroking, Private Financing	40 100 140

TABLE 3B

(account-related category)		
Risk Factor	Item Option(s)	Risk Value
Account type	Time deposit; Composite deposit; FOREX time deposit; FOREX composite deposit	40
	Checking deposit; Gold account; FOREX checking deposit	100
Account open manner	At-the-Counter	40
Source of fund	Online	140
	Cash; Check	40
Service associated	Domestic remittance	100
Activity frequency	Foreign remittance; Transfer	140
	Loan; Deposit	40
Dormant		200
Active		40

TABLE 3C

(geographical category)		
Risk Factor	Item Option(s)	Risk Value
Address of the client/ Locations of activity	Aland Islands, American Samoa Andorra, British Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin (Dahomey), Bermuda, Bhutan, Bolivia, Bonaire, Sint Eustatius and Saba, Bosnia and Herzegovina, Botswana, Bouvet Island, Brazil, British Indian Ocean Territory, Brunei, Bulgaria, Ethiopia, Faroe Islands, Falkland Islands, Fiji, Finland, France, French Guiana, French Polynesia, French Southern Territories, Gabon, Gambia, Georgia, Germany, Ghana, Gibraltar, Greece, Greenland, Grenada, Guadeloupe Island, Guam, Guatemala, Guernsey, Guinea, Guinea-Bissau, Guyana, Haiti, Heard and McDonald Islands, Holy See, Honduras, Hong Kong, Hungary, Iceland, India, Mauritania, Mauritius, Mayotte, Mexico, Micronesia, Moldova, Monaco, Mongolia, Montenegro, Montserrat, Morocco, Mozambique, Nauru, Nepal, the Netherlands, New Caledonia, New Zealand, Niger, Nigeria, Niue, Norfolk Islands, Northern Mariana Islands, Norway, Oman, Palau, Panama Canal Zone, Paraguay, South Georgia and the South Sandwich Islands, South Sudan, Spain, Sri Lanka, Suriname, Svalbard and Jan Mayen Islands, Swaziland, Sweden, Switzerland, Taiwan, Taiwan (OBU), Tajikistan, Tanzania, Thailand, East Timor, Togo, Tokelau, Tonga, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Turks and Caicos Islands, Tuvalu, Uganda, Ukraine, Republic of Upper Volta (Burkina Faso), Burundi, Cameroon, Canada, Cape Verde and the Cayman Islands, Central African Republic, Chad, Chile, mainland China, Christmas Island, Cocos Islands, Colombia, Comoros, Congo (Zaire), Cook Islands, Costa Rica, Ivory Coast, Croatia, Cuba, Curacao, Cyprus, the Czech Republic, Denmark, Djibouti, Dominica, Dominican Republic, Egypt, El Salvador, Equatorial Guinea, Eritrea, Estonia, Iraq, Ireland, Isle of Man, Israel, Italy, Jamaica, Japan, Jersey, Jordan, Kazakhstan, Kenya, Kiribati, Republic of Korea, Kyrgyzstan, Latvia, Lebanon, Lesotho, Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Madagascar, Malawi, Malaysia, Maldives, Mali, Malta, Marshall Islands, French Martinique, Peru, Philippines, Pitcairn Island, Poland, Portugal, Puerto Rico, Qatar, Réunion, Romania, the Russian Federation, Rwanda, Saint Barthelemy, St. Helena, Saint Kitts and Nevis, St. Lucia, St. Martin (French), Saint Pierre and Miquelon Islands, Saint Vincent and the Grenadines, Samoa Islands, San Marino, Sao Tome and Principe, Saudi Arabia, Senegal, Serbia, Seychelles, Sierra Leone, Singapore, St. Martin (Netherlands), Slovakia, Slovenia, Solomon Islands, Somalia, Republic of South Africa, United Arab Emirates, United Kingdom, United States, United States Minor Outlying Islands, Uruguay, Uzbekistan, Vanuatu, Venezuela, Vietnam,	40

TABLE 3C-continued

(geographical category)		Risk Value
Risk Factor	Item Option(s)	
	British Virgin Islands, United States Virgin Islands, Wallis and Futuna, Western Sahara, Zambia, Automated Teller Machine (ATM) cash withdraw*, International airport settlement*	
	Afghanistan, Albania, Angola, Namibia, Nicaragua, Pakistan, Panama, Papua New Guinea, Sudan, Syria, Khmer, Kuwait, Laos, North Yemen, Zimbabwe (Rhodesia)	100
	Algeria, Indonesia, Myanmar, Ecuador Iran, North Korea	140 200

*only applies to location of activity

[0038] FIG. 2 is a flow chart illustrating steps of a method for performing machine detection of a suspicious transaction on at least one client account that is associated with a client. The method may be implemented by the system 100 as depicted in FIG. 1.

[0039] It is noted that each of the data management server 3 and the assessment server 5 includes a processor for executing instructions of an application program in order to implement corresponding steps of the method, and includes a communication component for supporting wired and/or wireless communication with each other.

[0040] In step 11, the data management server 3 retrieves part of the client data 21 and the risk-related data 22 from the client database 2. Specifically, aside from the risk-related data 22, the data management server 3 retrieves the data set of the client data 21 that corresponds to the client.

[0041] Afterward, in step 12, the data management server 3 transmits the data set of the client data 21 and the risk-related data 22 to the assessment server 5.

[0042] In response to receipt of the data set of the client data 21 and the risk-related data 22, in step 13, the assessment server 5 assigns respective risk values to the items of the data set associated with the client, based on the risk-related data list and the weight list included in the risk-related data 22 and the risk-value lookup table 41 pre-stored in the rule database 4.

[0043] The following Table 4 includes an exemplary part of the data set associated with a particular client, and the corresponding assigned risk values based on the risk-value lookup table 41 as exemplified by Table 3.

TABLE 4

Category	Risk Factor	Item in the data set	Risk Value	Value assigned
Client-related category	Client type	Natural person	100	
	Client identification type	ID Card	40	
	Client occupation/ Occupational type	Financial assistance	100	
Account-related category	Account type	Time deposit	40	
	Account open manner	Online	140	
	Source of fund associated	Transfer	140	
	Service frequency	Deposit	40	

TABLE 4-continued

Category	Risk Factor	Item in the data set	Risk Value assigned
Geographical category	Activity frequency	Active	40
	Address of the client/	Taiwan	40
	Countries of activity	Taiwan	40

[0044] In step 14, the assessment server 5 transmits the assigned risk values to the data management server 3.

[0045] In step 15, the data management server 3 calculates a weighted score based on the risk values and the weight list (see Table 2).

[0046] Specifically, FIG. 3 is a flow chart illustrating sub-steps performed by the data management server 3 for calculating the weighted score. The sub-steps may be implemented by the data management server 3 executing an application program.

[0047] In sub-step 151, in response to receipt of the risk values, the data management server 3 weights the risk values respectively with the factor weights to obtain a number of factor-weighted values, respectively.

[0048] The following Tables 5A to 5C illustrate exemplary factor-weighted values, taking the factor weights set in Table 2 and the risk values assigned in Table 4 as an example.

TABLE 5A

(client-related category)				
Risk Factor	Information	Risk Value	Factor Weight (%)	Factor-weighted values
Client type	Natural person	100	30	30
Client identification type	ID Card	40	30	12
Client occupation/ Occupational type	Financial assistance	100	40	40

TABLE 5B

(account-related category)				
Risk Factor	Information	Risk Value	Factor Weight (%)	Factor-weighted values
Account type	Time deposit	40	25	10
Account open manner	Online	140	5	7
Source of fund	Transfer	140	5	7
Service associated	Deposit	40	25	10
Activity frequency	Active	40	40	16

TABLE 5C

(geographical category)				
Risk Factor	Information	Risk Value	Factor Weight (%)	Factor-weighted values
Address of the client/	Taiwan	40	10	4
Location of activity	Taiwan	40	90	36

[0049] In sub-step 152, the data management server 3 calculates three category summations by summing the factor-weighted values corresponding to the risk factor(s) categorized in a respective one of the client-related category, the account-related category and the geographical category in order to obtain each category summation.

[0050] Taking the data included in Tables 5A to 5C as an example, the three category summations may be calculated as 82 (30+12+40), 50 (10+7+7+10+16), and 40 (4+36), respectively.

[0051] In sub-step 153, the data management server 3 weights the three category summations respectively with the three category weights to obtain three weighted components, respectively. Afterward, the data management server 3 adds the three weighted components to obtain the weighted score.

[0052] The following Table 6 includes the three weighted components and the weighted score using the data from Tables 2 and 5A to 5C.

TABLE 6

Category	Category summations	Category Weight (%)	Weighted component	Weighted score
Client-related	82	30	24.6	56.1
Account-related	50	35	17.5	
Geographical	40	35	14	

[0053] In step 16, the data management server 3 assigns a risk level to the client based on the weighted score. In particular, the data management server 3 assigns a high risk level when the weighted score is above a first threshold, assigns a medium risk level when the weighted score is between the first threshold and a second threshold that is smaller than the first threshold, and assigns a low risk level when the weighted score is below the second threshold. In this embodiment, the first threshold is 80 and the second threshold is 60. As a result, the client whose weight score is 56.1 as shown in Table 6 is assigned the low risk level.

[0054] In one embodiment, the risk level assigned may be separately stored in a risk level database 2' that is coupled to or accessible by the data management server 3 (see FIG. 1).

[0055] In step 17, the data management server 3 retrieves, from the client database 2, transaction details associated with each client account corresponding to the client within a predetermined previous period that is immediately prior to the current business day. The transaction details include information associated with transactions that have occurred on the client account. In this embodiment, the predetermined previous period is set at three months.

[0056] Afterwards, the data management server 3 calculates a transaction parameter set based on the transaction details for each client account. In this embodiment, the transaction parameter set includes an average dollar amount

(can be any currency as desired) of multiple transactions within the predetermined previous period, and a standard deviation associated with the dollar amounts of the transactions within the predetermined previous period.

[0057] In step 18, the data management server 3 transmits the risk level and the transaction parameter set to the assessment server 5.

[0058] In step 19, the assessment server 5 determines whether the client account is involved in at least one transaction during a predetermined detecting period. Specifically, the predetermined detecting period includes the current business day and a number (N) of previous business days immediately prior to the current business day. When the determination is affirmative, the flow proceeds to step 20. Otherwise, the method is terminated.

[0059] In step 20, the assessment server 5 determines whether each transaction occurring during the predetermined detecting period is a suspicious transaction. The determination may be made based on the risk level associated with the client (as assigned in step 16), the transaction parameter set and the rule sets 42 pre-stored in the rule database 4.

[0060] A number of examples regarding the implementation of step 20 using various rule sets 42 (first to sixth rule sets) will now be described in the following paragraphs.

[0061] In a first example, the first rule set includes a daily transaction threshold (i.e., a threshold set for the number of transactions within one business day), and a daily dollar amount threshold for a client type and the risk level of the client (i.e., a threshold set for the total dollar amount involved in the transaction(s) within one business day).

[0062] With such a rule set, in step 20, when a number of transactions involving the client account within the current business day is no smaller than the daily transaction threshold, and when at least one of a total cash withdrawal amount from the client account and a total cash deposit amount into the client account within the current business day exceeds the daily dollar amount threshold, any cash withdrawal/deposit transaction that contributes to the at least one of the total cash withdrawal amount and the total cash deposit amount is determined as a suspicious transaction.

[0063] In this example, the daily transaction threshold and/or the daily dollar amount threshold may be set differently for different clients. The following Table 7 lists exemplary daily dollar amount thresholds set based on the client type and the risk level.

TABLE 7

Client type	Daily dollar amount threshold (unit: 10K NTD)			Daily transaction threshold (number of times)
	High Risk Level	Medium Risk Level	Low Risk Level	
Natural person	50	80	90	2
Juridical person	100	100	100	2

[0064] When it is detected that a client account, which is associated with a natural person assigned a high risk level, receives three cash deposit transactions of 100,000, 300,000 and 180,000 NTD, respectively, the assessment server 5 determines that the a number of transactions (i.e., 3) exceeds

the daily transaction threshold (i.e., 2), and the total cash deposit amount into the client account within the current business day (580,000) exceeds the daily dollar amount threshold (500,000). As such, all three cash deposit transactions are determined to be suspicious transactions.

[0065] It is noted that the first rule set is created to detect withdrawal or deposit activities in the client account that is deemed abnormal based on the risk factors of the client.

[0066] In a second example, the second rule set includes a daily transaction threshold (i.e., a threshold set for the number of transactions within one business day), and a dollar amount threshold for the client type and the risk level of the client (i.e., a threshold set for the dollar amount involved in an individual transaction).

[0067] With such a rule set, in step 20, a transaction occurring in the current business day having an amount larger than the dollar amount threshold is defined as an abnormal transaction. When a number of abnormal transactions each having an amount larger than the dollar amount threshold is no smaller than the daily transaction threshold, the abnormal transactions are determined as suspicious transactions.

[0068] In this example, the dollar amount threshold may be calculated by

$$T_d = \text{Avg} + (\text{Stdev} * M)$$

where T_d represents dollar amount threshold, Avg represents the average dollar amount, Stdev represents the standard deviation, and M represents a multiplier associated with the risk level of the client.

[0069] The following Table 8 lists exemplary multipliers and daily transaction thresholds set based on clients with different risk levels.

TABLE 8

Client type	Multiplier			Daily transaction threshold		
	High Risk Level	Medium Risk Level	Low Risk Level	High Risk Level	Medium Risk Level	Low Risk Level
Natural person	3	10	10	2	5	5
Juridical person	3	10	10	2	5	5

[0070] For example, a dollar amount threshold for a client account associated with a natural person assigned a high risk level and having an average dollar amount of 500,000 NTD and a standard deviation associated with the transactions of 50,000 NTD is calculated by $500,000 + (50,000 * 3) = 650,000$.

[0071] In such a case, when the client account receives three deposit transactions of 1,000,000, 1,200,000 and 3,000,000 NTD in the current business day, the assessment server 5 first determines that since each time the amount of deposit into the client account exceeds the dollar amount threshold (i.e., 650,000 NTD), all three deposit transactions are determined to be abnormal transactions. Then, the assessment server 5 determines that the number of transactions (i.e., 3) exceeds the daily transaction threshold (i.e., 2). As such, all three deposit transactions are determined to be suspicious transactions.

[0072] It is noted that the second rule set is created to detect sudden large-amount withdrawal or deposit activities

in the client account within the current business day based on the risk factors of the client.

[0073] In a third example, the third rule set includes a cash transaction threshold (i.e., a threshold set for the number of cash transactions within the predetermined detecting period), a dollar amount threshold for a client type with a specific risk level (i.e., a threshold set for the dollar amount), and a predetermined withdrawal/deposit ratio range.

[0074] With such a rule set, in step 20, when the client account is determined as a dormant account, and when a number of cash transactions involving the client account within the predetermined detecting period is no smaller than the cash transaction threshold, and when an accumulated cash dollar amount within the predetermined detecting period is larger than the dollar amount threshold, and when a withdrawal/deposit ratio of the cash transactions is within the predetermined withdrawal/deposit ratio range, each of the cash transactions occurred during the predetermined detecting period is determined as a suspicious transaction.

[0075] Specifically, the client account is determined as a dormant account when the transaction details indicate that the client account is involved in no more than one transaction during a 6-month period that precedes the predetermined detecting period. Moreover, the predetermined detecting period is three business days including the current business day.

[0076] The following Table 9 lists exemplary withdrawal/deposit ratio ranges (which are defined by an upper bound and a lower bound), dollar amount thresholds, and daily transaction thresholds set based on attributes of the client.

TABLE 9

Client type	Withdrawal/deposit ratio range (%)		Dollar amount threshold (Unit: 10K NTD)			Cash transaction threshold (number of times)
	Lower bound	Upper bound	High Risk Level	Medium Risk Level	Low Risk Level	
Natural person	90	110	80	80	90	2
Juridical person	90	110	100	100	100	2

[0077] A client account associated with a judicial person and determined to be a dormant account may be then monitored for suspicious transactions.

[0078] In such a case, when in the predetermined detecting period, the client account receives one cash deposit transaction in the amount of 2,000,000 NTD, and is involved in one cash withdrawal transaction in the amount of 1,900,000 NTD, the assessment server 5 first determines that the accumulated cash dollar amount within the predetermined detecting period (3,900,000 NTD) is larger than the dollar amount threshold (1,000,000 NTD), and the withdrawal/deposit ratio of the cash transactions (95%) is within the predetermined withdrawal/deposit ratio range. Then, the assessment server 5 determines that the number of cash transactions (i.e., 2) is no smaller than the cash transaction threshold (i.e., 2). As such, all two transactions are determined to be suspicious transactions.

[0079] It is noted that the third rule set is created to detect suspicious activities in a client account that is considered dormant.

[0080] In a fourth example, the fourth rule set includes a deposit amount threshold (i.e., a threshold set for an accumulated deposit amount of all deposit transactions related to the client account within the predetermined detecting period) and a predetermined withdrawal/deposit ratio range.

[0081] With such a rule set, in step 20, when the client account is determined as a recently opened account, and when an accumulated deposit amount into the client account during the predetermined detecting period is larger than the deposit amount threshold, and when a withdrawal/deposit ratio of transactions that involve the client account during the predetermined detecting period is within the predetermined withdrawal/deposit ratio range, each of the transactions that occurred is determined as a suspicious transaction.

[0082] Specifically, the client account is determined as a recently opened account if the client account was opened within a predetermined period immediately prior to the current business day. In this example, the predetermined period is 90 days. Moreover, the predetermined detecting period is three business days including the current business day. The deposit amount threshold is 900,000 NTD, and the predetermined withdrawal/deposit ratio range is [90%, 110%].

[0083] In such a case, when the recently opened account has one cash deposit transaction in the amount of 1,000,000 NTD and one cash withdrawal transaction in the amount of 990,000 NTD in the predetermined detecting period, the assessment server 5 determines that the accumulated deposit amount within the predetermined detecting period (1,000,000 NTD) is larger than the deposit amount threshold (900,000 NTD), and the withdrawal/deposit ratio of the transactions (99%) is within the predetermined withdrawal/deposit ratio range. As such, both cash transactions are determined to be suspicious transactions.

[0084] It is noted that the fourth rule set is created to detect suspicious activities in the client account that is considered recently opened.

[0085] In a fifth example, the fifth rule set includes a predetermined withdrawal/deposit ratio range.

[0086] With such a rule set, in step 20, when a cash withdrawal transaction occurs in one of the client accounts and a cash deposit transaction occurs in another one of the client accounts during the predetermined detecting period, both client accounts belonging to the same client, and when a withdrawal/deposit ratio of a withdrawal amount of the cash withdrawal transaction to a deposit amount of the cash deposit transaction is within the predetermined withdrawal/deposit ratio range, each of the cash withdrawal transaction and the cash deposit transaction is determined as a suspicious transaction. Specifically, the predetermined withdrawal/deposit ratio range may be [85%, 110%].

[0087] It is noted that the fifth rule set is created to detect suspicious activities in client accounts that are commonly owned by the client.

[0088] In a sixth example, the sixth rule set includes a predetermined deposit/debit ratio.

[0089] With such a rule set, in step 20, when the client account is associated with a loan, and when a deposit/debit ratio of an accumulated deposit amount into the client account for paying the loan within the current business day to a debit of the loan is larger than the predetermined deposit/debit ratio, the transaction contributed to the accumulated deposit amount within the current business day is

determined as a suspicious transaction. Specifically, the predetermined deposit/payment ratio may be 50%.

[0090] When at least one of the transactions is determined as a suspicious transaction in step 20, in step 21, the assessment server 5 may generate an alert, and output the alert to a designated party (e.g., a related party).

[0091] It should be noted that the above-mentioned standards of each of the rule sets 42 may be flexibly adjusted and updated by the assessment server 5 according to actual conditions.

[0092] In sum, embodiments of the disclosure provide a method that employs the system 100 to assign a risk level to the client based on certain information regarding the client, and to determine whether a transaction involving any client account of the client is a suspicious transaction, based on the risk level and the rule sets 42. The method implemented by the system 100 may be capable of covering a large number of daily transactions during each business day, thereby reducing the possibility of money-laundering related transactions being processed undetected. Additionally, since the rule sets 42 are stored in the rule database 4, they may be readily adjusted to accommodate changes in regulations.

[0093] In the description above, for the purposes of explanation, numerous specific details have been set forth in order to provide a thorough understanding of the embodiments. It will be apparent, however, to one skilled in the art, that one or more other embodiments may be practiced without some of these specific details. It should also be appreciated that reference throughout this specification to "one embodiment," "an embodiment," an embodiment with an indication of an ordinal number and so forth means that a particular feature, structure, or characteristic may be included in the practice of the disclosure. It should be further appreciated that in the description, various features are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding various inventive aspects.

[0094] While the disclosure has been described in connection with what are considered the exemplary embodiments, it is understood that this disclosure is not limited to the disclosed embodiment(s) but is intended to cover various arrangements included within the spirit and scope of the broadest interpretation so as to encompass all such modifications and equivalent arrangements.

What is claimed is:

1. A method for performing machine detection of a suspicious transaction on at least one client account that is associated with a client, the method being implemented by a system that includes a client database, a rule database, a data management server and an assessment server, the data management server storing data regarding the client account, the method comprising the steps of:

- a) retrieving, by the data management server, a data set of client data from the client database, the data set of client data being associated with the client account and the client, and including a number of items respectively directed to a number of risk factors;
- b) transmitting, by the data management server, the data set of client data to the assessment server;
- c) assigning, by the assessment server, respective risk values to the items of the data set of client data based on a risk-value lookup table that is pre-stored in the rule database;

- d) transmitting, by the assessment server, the risk values to the data management server;
 - e) calculating, by the data management server, a weighted score based on the risk values and a weight list that is pre-stored in the client database and that is associated with the risk factors;
 - f) assigning, by the data management server, a risk level to the client based on the weighted score;
 - g) retrieving, by the data management server, from the client database transaction details associated with the client account within a predetermined previous period that is immediately prior to a current business day, the transaction details including information associated with at least one transaction that has occurred on the client account;
 - h) calculating, by the data management server, a transaction parameter set based on the transaction details;
 - i) transmitting, by the data management server, the risk level and the transaction parameter set to the assessment server;
 - j) determining, by the assessment server, whether the client account is involved in at least one transaction during a predetermined detecting period that includes the current business day and at least one previous business day immediately prior to the current business day; and
 - k) when the determination of step j) is affirmative, determining, by the assessment server, whether the transaction is a suspicious transaction based on the risk level, the transaction parameter set and a rule set pre-stored in the rule database.
2. The method of claim 1, wherein the risk factors are categorized into one or more of:
- a client-related category including risk factors of one or more of a client type, a client identification type and a client occupation type;
 - an account-related category including risk factors of one or more of an account type, a manner in which the client account is opened, a source of fund used to open the client account, a service that is associated with the client account, and an activity frequency of the client account; and
 - a geographical category including risk factors of one of more of an address of the client and a location in which a financial activity has occurred on the client account.
3. The method of claim 2, the weight list having a number of factor weights corresponding respectively with the risk factors, and three category weights corresponding respectively with the client-related category, the account-related category and the geographical category, wherein step e) includes:
- in response to the risk values, weighting the risk values respectively with the factor weights to obtain a number of factor-weighted values, respectively;
 - calculating three category summations each by summing the factor-weighted values categorized in a respective one of the client-related category, the account-related category and the geographical category;
 - weighting the three category summations respectively with the three category weights to obtain three weighted components, respectively; and
 - adding the three weighted components to obtain the weighted score.

4. The method of claim 1, wherein step f) includes: assigning a high risk level to the client when the weighted score is above a first threshold;

assigning a medium risk level to the client when the weighted score is between the first threshold and a second threshold that is smaller than the first threshold; and

assigning a low risk level to the client when the weighted score is below the second threshold.

5. The method of claim 1, wherein the rule set includes a daily transaction threshold, and a daily dollar amount threshold for a client type and the risk level of the client,

wherein, in step k), when a number of transactions involving the client account within the current business day is no smaller than the daily transaction threshold, and when at least one of a total cash withdrawal amount from the client account and a total cash deposit amount into the client account within the current business day exceeds the daily dollar amount threshold, at least one of the transactions that contributes to the at least one of the total cash withdrawal amount and the total cash deposit amount is determined as a suspicious transaction.

6. The method of claim 1, wherein the transaction parameter set includes an average dollar amount of multiple transactions within the predetermined previous period, and a standard deviation associated with the dollar amounts of the transactions within the predetermined previous period.

7. The method of claim 6, wherein the rule set includes a daily transaction threshold and a dollar amount threshold for the client type and the risk level of the client,

wherein, in step k), when a number of abnormal transactions each involving an amount larger than the dollar amount threshold is no smaller than the daily transaction threshold, the abnormal transactions are determined as suspicious transactions.

8. The method of claim 7, wherein the dollar amount threshold is calculated by

$$T_d = \text{Avg} + (\text{Stdev} * M),$$

where T_d represents the dollar amount threshold, Avg represents the average dollar amount, Stdev represents the standard deviation, and M represents a multiplier associated with the risk level of the client.

9. The method of claim 1, wherein the rule set includes a cash transaction threshold, a dollar amount threshold for a client type with a specific risk level, and a predetermined withdrawal/deposit ratio range,

wherein, in step k), when the client account is determined as a dormant account, and when a number of cash transactions that involve the client account is no smaller than the cash transaction threshold within the predetermined detecting period, when an accumulated cash dollar amount of the cash transactions involving the client account within the predetermined detecting period is larger than the dollar amount threshold, and when a withdrawal/deposit ratio of the cash transactions is within the predetermined withdrawal/deposit ratio range, each of the cash transactions that occurred during the predetermined detecting period is determined as a suspicious transaction.

10. The method of claim 9, wherein the client account is determined as a dormant account when the transaction details indicate that the client account is involved in no more

than one transaction during a 6-month period that precedes the predetermined detecting period.

11. The method of claim 1, wherein the rule set includes a deposit amount threshold and a predetermined withdrawal/deposit ratio range,

wherein, in step k), when the client account is a recently opened account, and when an accumulated deposit amount into the client account during the predetermined detecting period is larger than the deposit amount threshold, and when a withdrawal/deposit ratio of transactions that involve the client account during the predetermined detecting period is within the predetermined withdrawal/deposit ratio range, each of the transactions that occurred is determined as a suspicious transaction.

12. The method of claim 11, wherein the client account is determined as a recently opened account when the client account was opened within a predetermined period immediately prior to the current business day.

13. The method of claim 1, wherein the rule set includes a predetermined withdrawal/deposit ratio range,

wherein, in step k), when the client owns an additional account, and when a cash withdrawal transaction

occurs in one of the client account and the additional account and a cash deposit transaction occurs in the other one of the client account and the additional account during the predetermined detecting period, and when a withdrawal/deposit ratio of a withdrawal amount of the cash withdrawal transaction to a deposit amount of the cash deposit transaction is within the predetermined withdrawal/deposit ratio range, each of the cash withdrawal transaction and the cash deposit transaction is determined as a suspicious transaction.

14. The method of claim 1, wherein the rule set includes a predetermined deposit/payment ratio,

wherein, in step k), when the client account is associated with a loan, and when a deposit/debit ratio of an accumulated deposit amount into the client account for paying the loan within the current business day to a debit of the loan is larger than the predetermined deposit/debit ratio, at least one transaction contributing to the accumulated deposit amount within the current business day is determined as a suspicious transaction.

* * * * *