(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)
(52) CPC특허분류
G06Q 40/00 (2013.01)
G06F 17/30 (2013.01)
(21) 출원번호 10-2015-0165763
(22) 출원일자 2015년11월25일
심사청구일자 2015년11월25일

전체 청구항 수 : 총 11 항

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
임희석
경기도 수원시 영통구 영통로 460, 304동 1704호 (영통동, 대우아파트)
(74) 대리인
특허법인충현

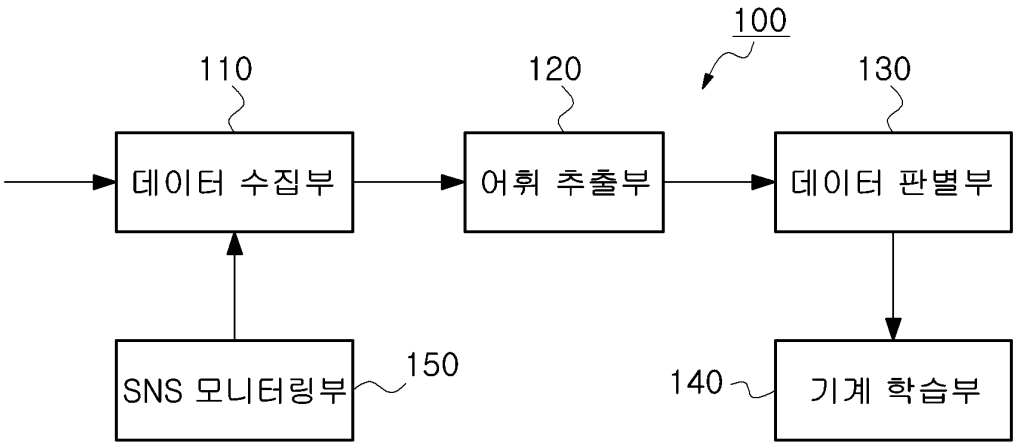
(54) 발명의 명칭 **금융 사기 방지 방법 및 시스템**

(57) 요 약

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.

대 표 도 - 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 확산 서비스 기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2015.05.01 ~ 2016.02.29

명 세 서

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 기설정된 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 기설정된 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 기설정된 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

기 술 분 야

[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.

배 경 기 술

[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.

선행기술문헌

특허문헌

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

발명의 내용

해결하려는 과제

[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.

과제의 해결 수단

[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 데이터의 띄어쓰기를 수행하는 과정을 포함하는 것을 특징으로 한다.

[0014] 본 발명에 따른 금융 사기 방지 방법에 있어서, 상기 품사별로 클러스터링된 상기 문장 단위 데이터와 유사한 어휘를 갖는 어휘 데이터를 기설정된 금융 사기 관련 데이터가 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 데이터와 유사한 어휘를 갖는 어휘 데이터를 기설정된 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 한다.

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

[0017] 본 발명에 따른 금융 사기 방지 방법에 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 한다.

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

[0019] 또한, 본 발명은 금융 사기 의심 데이터를 수집하는 데이터수집부와, 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 데이터판별부를 포함하여 구성한다.

발명의 효과

[0020] 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.

[0021] 또한, 본 발명의 금융 사기 방지 방법 및 시스템은 소셜 네트워크를 기반으로 단말간에 송수신되는 데이터가 금융 사기 관련 데이터에 해당하는지 여부를 기설정된 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.

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 데이터의 수집과정을 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 띄어쓰기를 수행한다.

[0035] 이처럼, 불용어를 제거하고, 띄어쓰기도 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] $$d_j=(\omega_{1,j},\omega_{2,j},\cdots,\omega_{t,j}),\quad q=(\omega_{1,q},\omega_{2,q},\cdots,\omega_{t,q})$$

[0041] 수학식 1에서 d_j는 문서 벡터를, q는 질의 벡터를 의마하며, 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] $$\cos\theta=\frac{d_2\cdot q}{\|d_2\|\cdot\|q\|}$$

[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_2의 노름, ||q||는 벡터 q의 노름을 의미한다. 벡터의 노름은 수학식 3과 같이 계산된다.

수학식 3

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

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

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

[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 설명할 수 있는 새로운 축을 찾아내고 정보가 적은 축들을 걸러냄으로써 데이터에 내포되어 있는 구조를 밝히는 기법이다.

[0061] LSA를 위해서 Singular Value Decomposition(SVD)이라는 선형대 수학 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×d 벡터 X는 수학식 6과 같이 분해된다.

수학식 6

[0065] $$X = T_0 S_0 D_0$$

[0066] 수학식 6에서 T_0, D_0은 직교정규(orthonormal) 열로 이루어지며 각각의 벡터들로 이루어져 있고, T_0는 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

[0068] $$X \approx X' = TSD'$$

[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 i와 단어 j의 유사성, 두번째로 문서 i와 문서 j의 유사성, 마지막으로 단어 i와 문서 j의 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

[0073] $$\frac{S \cdot S'}{\|S\|\|S'\|} = \frac{5.8 \times 5.8}{\sqrt{6^2} \times \sqrt{6^2}} = 0.93$$

[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. 이때, 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 방법은 지도 학습에서 사용되는 방법으로서, 주어진 자료에 대해서 그 자료들을 분리하는 초평면 중에서 자료들과 가장 거리가 먼 초평면을 찾는 방법을 말한다.

[0079] 더불어, 랜던 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), 펫처(Fetcher)로 시스템을 구성할 수 있다. 여기서 리프레셔는 수집 스케줄링을 제어하고, 업데이터는 데이터베이스 트랙잭션(Transaction)을 담당하며, 펫처에서는 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 사용하며 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 기설정된 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

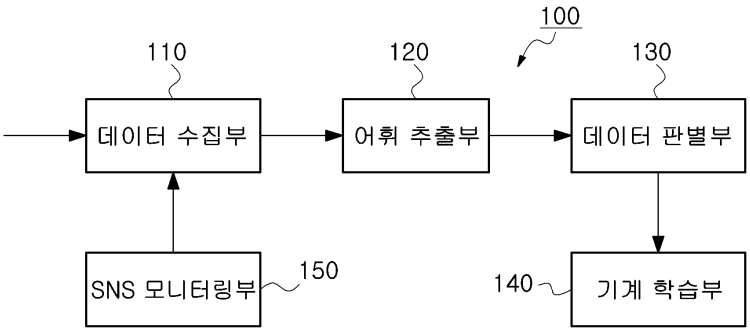
130: 데이터판별부

140: 기계학습부

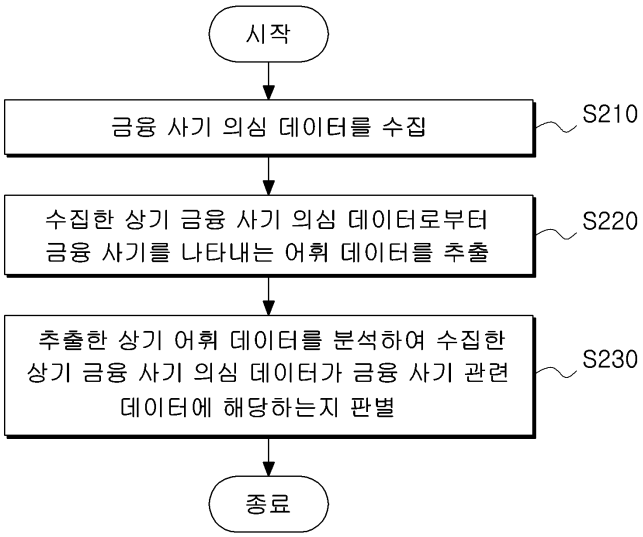
150: SNS모니터링부

도면

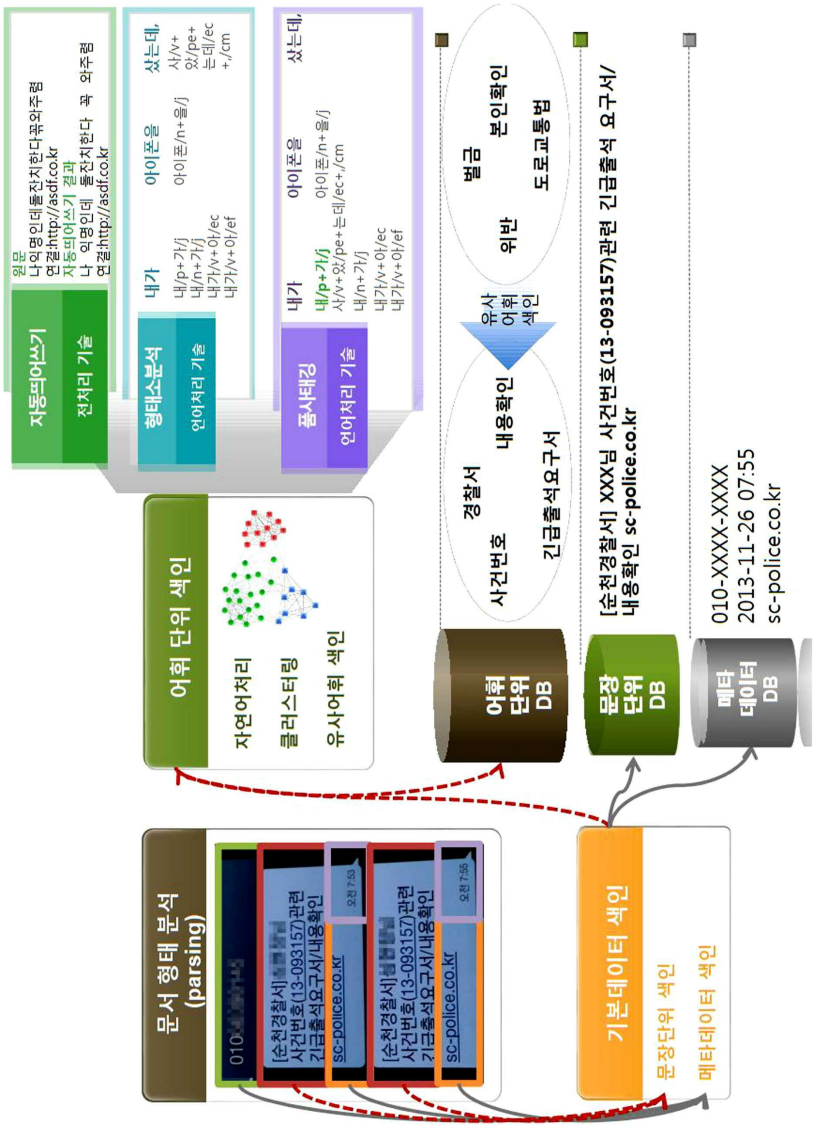
도면1


100
110
120
130
데이터 수집부
어휘 추출부
데이터 판별부
SNS 모니터링부
150
140
기계 학습부

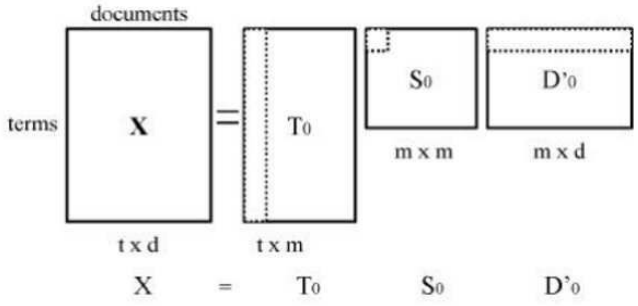
도면2


시작
금융 사기 의심 데이터를 수집
S210
수집한 상기 금융 사기 의심 데이터로부터
금융 사기를 나타내는 어휘 데이터를 추출
S220
추출한 상기 어휘 데이터를 분석하여 수집한
상기 금융 사기 의심 데이터가 금융 사기 관련
데이터에 해당하는지 판별
S230
종료

도면3


원문
나잉명인데 돌찬지한다 꼭 외주렴
연결http://asdf.co.kr
자동띄어쓰기 결과
나 잉명인데 돌찬지한다 꼭 외주렴
연결http://asdf.co.kr
자동띄어쓰기
전처리 기술
형태소분석
언어처리 기술
품사태깅
언어처리 기술
내가 아이폰을 샀는데,
내/p+가/j 아이폰/n+을/j 사/v+았/pe+는데/ec+,/cm
내/n+가/j
내가/v+아/ec
내가/v+아/ef
어휘 단위 색인
자연어처리
클러스터링
유사어휘 색인
문서 형태 분석 (parsing)
[순천경찰서] 사건번호(13-093157)관련 긴급출석요구서/내용확인
sc-police.co.kr
기본데이터 색인
문장단위 색인
메타데이터 색인
어휘 단위 DB
문장 단위 DB
메타 데이터 DB
경찰서
사건번호
내용확인
긴급출석요구서
유사 어휘 색인
벌금
본인확인
위반
도로교통법
[순천경찰서] XXX님 사건번호(13-093157)관련 긴급출석 요구서/ 내용확인 sc-police.co.kr
010-XXXX-XXXX
2013-11-26 07:55
sc-police.co.kr

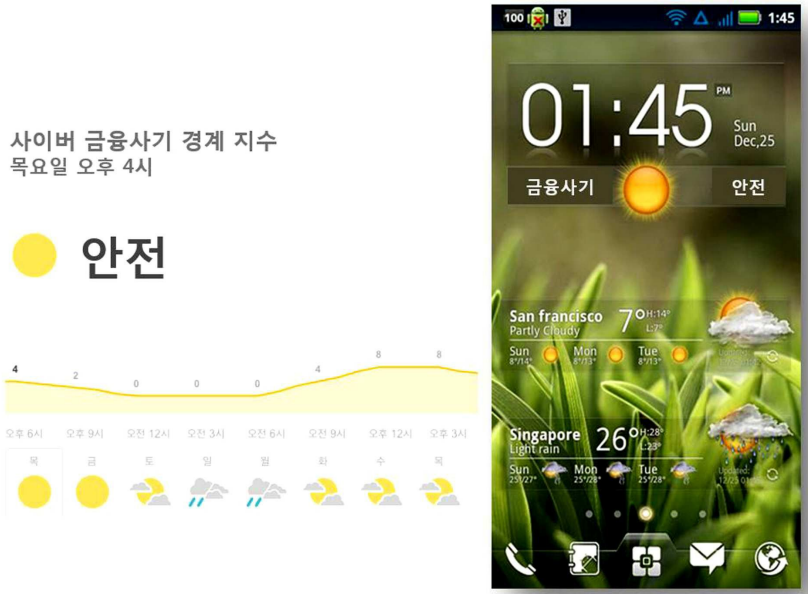
도면4


documents
terms
X
=
T0
S0
D'0
t x d
t x m
m x m
m x d
X = T0 S0 D'0

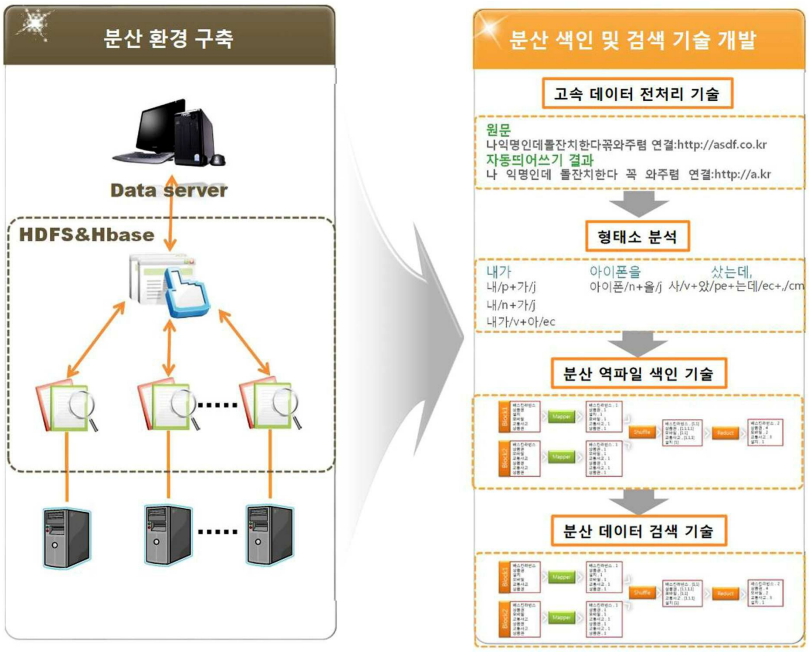
도면5


블로그
수집제어
수집
후처리
스케줄러
RSS 다운로더
Blog 다운로더
Post 다운로더
Post Parser
트위터
유저
펫처
문서
user
Refresher
Fetcher
Fetcher
Fetcher
Updater
document

도면6


사이버 금융사기 경계 지수
목요일 오후 4시
안전
01:45
Sun
Dec,25
금융사기
안전
San francisco
Partly Cloudy
Singapore
Light rain

도면7


분산 환경 구축
Data server
HDFS&Hbase
분산 색인 및 검색 기술 개발
고속 데이터 전처리 기술
원문
나익명인데롤잔치한다꾜와주렴 연결:http://asdf.co.kr
자동띄어쓰기 결과
나 익명인데 롤잔치한다 꼭 와주렴 연결:http://a.kr
형태소 분석
분산 역파일 색인 기술
분산 데이터 검색 기술