(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020 년 9 월 24 일 (24.09.2020)

WIPO | PCT

(10) 국제공개번호
WO 2020/189846 A1

(51) 국제특허분류:
G06F 16/2452 (2019.01) *G06F 21/62* (2013.01)
G06F 15/16 (2006.01) *H04L 29/08* (2006.01)
G06F 16/2453 (2019.01)

(21) 국제출원번호: PCT/KR2019/006498

(22) 국제출원일: 2019 년 5 월 30 일 (30.05.2019)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2019-0032442 2019 년 3 월 21 일 (21.03.2019) KR

(71) 출원인: 공주대학교 산학협력단 (**KONGJU NATIONAL UNIVERSITY INDUSTRY-UNIVERSITY COOPERATION FOUNDATION**) [KR/KR]; 32588 충청남도 공주시 공주대학로 56 (신관동, 공주대학교), Chungcheongnam-do (KR).

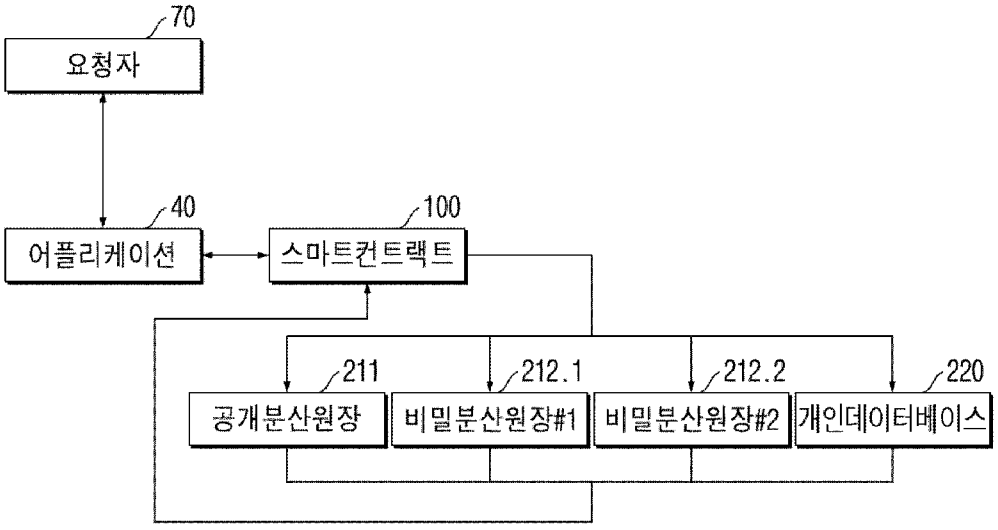
(72) 발명자: **서창호 (SEO, Changho)**; 34191 대전시 유성구 봉명로 48 803동 2403호., Daejeon (KR). **김현일 (KIM, Hyunil)**; 30064 세종시 도움1로 145 105동 1405호., Sejong (KR). **성열욱 (SUNG, Yeoulouk)**; 30063 세종시 마음로 67 105동 704호., Sejong (KR).

(74) 대리인: **강정빈 등 (KANG, Jeongvin** et al.); 06748 서울시 서초구 양재천로21길 9 화암빌딩 3층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK,

(54) **Title:** METHOD FOR PRIVACY-PRESERVING DATA ANALYSIS IN PERMISSIONED BLOCKCHAIN SYSTEM

(54) **발명의 명칭:** 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법



40 ... Application
70 ... Requester
100 ... Smart contract
211 ... Public distributed ledger
212.1 ... Secret distributed ledger#1
212.2 ... Secret distributed ledger#2
220 ... Personal database

(57) **Abstract:** The present invention relates to a method for privacy-preserving data analysis in a permissioned blockchain system and, more specifically, to a method for privacy-preserving data analysis in a permissioned blockchain system, wherein when specific data analysis is performed in a blockchain-based system, a value, which is obtained by adding noise to a response of a secret distributed ledger with respect to a query, is returned so as to enable data analysis to be performed while preserving personal privacy.

(57) **요약서:** 본 발명은 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법에 관한 것으로서, 더욱 상세하게는 블록체인 기반 시스템에서 특정 데이터 분석을 수행할 때 질의에 대한 비밀분산원장의 응답에 노이즈가 추가 된 값을 반환하여 개인 프라이버시가 보존된 상태로 데이터 분석을 수행 할 수 있도록 하는 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법에 관한 것이다.

WO 2020/189846 A1

[다음 쪽 계속]

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) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (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).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법

기술분야

[1] 본 발명은 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법에 관한 것으로서, 더욱 상세하게는 블록체인 기반 시스템에서 특정 데이터 분석을 수행할 때 질의에 대한 비밀분산원장의 응답에 노이즈가 추가 된 값을 반환하여 개인 프라이버시가 보존된 상태로 데이터 분석을 수행 할 수 있도록 하는 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법에 관한 것이다.

배경기술

[2] 블록체인 기술은 암호화폐(Cryptocurrency)로 인해 널리 알려진 기술로써, 기존의 중앙 집중형 데이터베이스가 아닌 해당 네트워크에 참여 중인 참여자들이 모두 공유된 데이터베이스를 갖는 분산 데이터베이스 기반 시스템에서 안전하고 효율적인 데이터 공유를 수행하기 위한 기법이다.

[3]

[4] 비특허문헌 1에 의해 제안된 암호화폐 기술 및 이를 기반으로 하는 블록체인 시스템들은 해당 네트워크에 누구든지 참여할 수 있고, 참여된 모든 구성원(노드)들이 데이터베이스에 해당하는 분산 원장을 보유하고 있다. 이를 보통 무 허가형 블록체인(Permissionless blockchain) 시스템 이라고 하며 이는 보통 퍼블릭 블록체인(Public blockchain)이라고 불리기도 한다. 이와는 달리 특정 동일 목적을 가진 기관들의 집합 또는 특정 단체만이 해당 네트워크에 참여할 수 있는 시스템을 허가형 블록체인(Permissioned blockchain)이라고 하며 이는 중앙집중화의 정도에 따라 프라이빗 블록체인(Private blockchain) 또는 컨소시엄 블록체인(Consortium Blockchain)이라고 불리기도 한다.

[5] 비특허문헌 1에 의해 제안된 무 허가형 블록체인은 대개 네트워크에서 이루어지는 트랜잭션 및 이에 대한 안전한 분산 원장에 대한 처리 및 저장에 대한 효율성 보다는 완전한 탈 중앙화를 통해 누구든지 참여할 수 있는 규모의 확장성을 가짐을 목적으로 한다.

[6] 이에 비해 허가형 블록체인은 누구든지 참여할 수 있는 무 허가형 블록체인에 비해 규모의 확장성이 떨어지나, 무 허가형 블록체인에 비해 트랜잭션 실행 및 이에 대한 안전한 분산 원장에 대한 처리와 저장에 대해 매우 빠른 시스템 성능과 함께 금융거래, 제조사 간 공급망, 제조사와 소비자 간 유통망, 의료 분야에서의 병원 및 기타 관련사 간의 질병 이력 공유 및 정부 주도의 공공 분야에서의 정보 공유 등에 적용할 수 있는 시스템이다. 허가형 블록체인은 Linux Foundation에 의해 설립된 허가형 블록체인 오픈 소스 프로젝트인

하이퍼레저에 의해 관련 연구가 집중적으로 시작되었으며 현재 대표적인 허가형 블록체인 기술로는 하이퍼레저(Hyperledger Indy, Hyperledger Sawtooth, Hyperledger Fabric) 등이 있으며 국내에서는 삼성SDS의 넥스레저(Nexledger) 등이 있다.

[7]

[8] 또한 다수의 기업 혹은 단체는 각자의 목적을 위해 데이터로부터 유용한 정보를 얻어내는 데이터 마이닝(Data Mining) alc 기계학습(Machine Learning) 등의 데이터 분석 기술을 사용한다. 특정 예로 금융 및 보험 관련계열에서는 고객에 대한 특정 이력 여부를 분석해 보험 사기 등을 방지할 수 있으며, 상업 관련계열에서는 물품 판매자가 물품의 특성에 대한 소비자들의 선호도를 분석하여 향후 판매에 유용한 정보를 얻을 수 있고 또한 의료 관련계열에서는 희귀 질병 등에 대처할 수 있는 치료 기술의 성공률을 분석하여 환자의 치료율을 더욱 높일 수 있게 된다. 따라서 이 때 단체 또는 기업들은 각각 보유하고 있는 데이터를 상호간에 공유한다면 더욱 더 의미 있는 유용한 정보들을 얻어낼 수 있겠지만, 비특허문헌 2에 의해 개인정보의 프라이버시 보존을 위해서는 데이터 공유 이전에 데이터 비 식별화(De-identification) 기술이 적용되어야만 하며, 따라서 이에 관련한 많은 연구가 지속적으로 관심을 받아오고 있다.

[9] 또한 최근에는 데이터의 크기 및 규모가 날이 갈수록 방대 해지며 이로 인해 분산 데이터 환경에서의 데이터 분석 기술이 활발하게 연구 중에 있다. 이는 데이터 중앙 집중화 후 데이터 분석을 수행하는 것이 아닌 분산 분석 후 이에 대한 결과값을 수집하고 합산하여 데이터 분석 결과를 도출해내는 기술이다. 이하 본 발명에서 분산 데이터 환경에서의 데이터 분석 기술을 분산 학습(Distributed Learning) 기술이라고 대체하여 후술한다. 상기 데이터 분석 기술에 사용되는 알고리즘은 여러 번의 반복 학습을 수행하며 이에 대한 최종 라운드의 결과값을 대개 학습 모델이라고 서술한다. 각 라운드의 결과 값이 하나만 존재하는 데이터 중앙 집중형 데이터 분석에 비해 각 라운드 마다 다수의 결과값이 존재하고 이를 올바르게 수집하고 합산하는 것이 분산 학습 기술의 핵심에 해당한다.

[10] 또한 이러한 분산 학습 기술 역시 프라이버시 보존을 위해 비 식별화 기술이 적용되어야만 한다.

[11]

[12] 데이터 비 식별화 기술 중 차분 프라이버시(Differential Privacy)라 함은 상기 비 식별화 기법 중 하나로써 데이터 분석가에 의해 수행되는 정보에 대한 질의에 응답 시 수학적 확률에 기반한 노이즈를 추가함으로써 분석가가 쉽게 개인정보를 유추할 수 없게 하는 기술이다.

[13] 차분 프라이버시는 특정 개인 데이터의 존재 유무에 따른 두 데이터베이스에 대하여 어떠한 질의에 대한 두 데이터베이스에서의 출력이 확률적으로 얼마만큼의 차분을 가지고 있는지를 기반으로 프라이버시의 정도를 수학적으로

정의한다. 여기에서 개인 데이터는 의료 데이터 상에서 환자에 대한 개인정보를 포함한 질병이력으로, 거래 데이터 상에서 특정 물품에 대한 개인정보와 물품의 특징 및 거래내역을 포함한 데이터를 예로 들 수 있다.

[14]

[15] 예를 들어 질병 이력에 관한 데이터가 있으며, 이는 모두 비밀 값이라 가정하자. 이 때 만일 악의적인 분석가가 '폐암 환자는 몇 명인가?'와 같은 특정 질의를 수행하여 해당 데이터베이스에 속한 특정 공격 대상자의 폐암 여부를 알아내려 한다고 가정하자. 이러한 경우 질의의 응답이 항상 같다면 악의적인 분석가는 '폐암 환자는 몇 명인가?'라는 질의와 '공격 대상자를 제외한 폐암 환자는 몇 명인가?' 라는 두 질의를 통해 공격 대상자의 폐암 여부를 쉽게 알아낼 수 있다.

[16] 하지만 차분 프라이버시가 적용된 데이터 분석 방법은 특정 공격 대상자가 실제로 폐암 환자라 할지라도 해당 질의를 기반으로 계산된 임의성을 갖는 노이즈를 응답 값에 추가함으로써 상기 질의와 같은 방식으로 여러 질의를 받게 되더라도 각 질의마다 다른 값을 응답하게 된다.

[17] 이는 근본적으로 데이터가 가지고 있는 확률적 분포도의 특성을 알려주되, 공격자의 입장에서 개인 데이터 값에 대한 정확한 추론은 어렵게 하는 데에 초점을 두고 있다.

[18] 따라서 상기 예에서의 차분 프라이버시는 악의적인 분석가가 피공격자에 대한 사전지식을 알고 있다고 하더라도 분석 이전과 분석 이후의 차이 값을 알 수 없기 때문에 쉽게 피공격자의 폐암 여부를 알 수 없게 된다.

[19] 이러한 차분 프라이버시 방법은 Randomized 알고리즘을 기반으로 설계된다. 이는 데이터베이스 내 각각의 데이터 열들이 가지고 있는 민감한 속성값에 임의성을 갖는 노이즈를 추가함을 의미한다. 다만, 데이터 분석가 입장에서 데이터 분석 수행 시 그에 대한 유용성을 해치지 않기 위해 민감한 정보의 속성을 드러내지 않을 정도의 적당한 노이즈를 추가하게 되며, 이에 대한 정도는 차분 프라이버시 정의 내의 측도에 의해 시스템 관리자 혹은 데이터 관리자 하에 정해질 수 있다.

[20]

[21]

[22] *현재 허가형 블록체인 시스템에서는 시스템 내의 모든 구성원이 공유하는 데이터가 있는가 하면 특정 구성원만이 공유하는 데이터도 존재한다. 따라서 데이터 분석 시 이러한 비밀 데이터의 정보가 누출되지 않은 상태에서 올바르게 분석될 수 있는 기술이 필요하다.

[23] 이와 같이 비밀 데이터의 정보가 누출되지 않은 상태에서 분석을 수행하는 기술로는 비특허문헌 3, 4, 5에 의해 제안된 기술이 존재한다. 상기 비특허문헌 3, 4, 5에 의해 제안된 기술들은 안전한 다자간 계산(Secure Multiparty Computation)을 통해 특정 구성원만이 공유하는 데이터에서 프라이버시를 노출시키지 않은 상태로 접근자가 원하는 값을 얻어낼 수 있다.

[24] 하지만 상기 비특허문헌 3, 4, 5에 의해 제안된 기술들은 계산 시 필요한 비밀 데이터가 많아질수록 경우 계산 복잡도가 매우 비효율적이며, 구매자들의 입찰가를 드러내지 않은 상태로 경매 등을 수행하는 특정 값 계산을 위한 기술에 주로 사용되므로 데이터의 확률적 분포를 파악하려는 데이터 분석 및 처리 기술에는 알맞지 않다.

[25] 또한 비밀 데이터의 정보가 누출되지 않은 상태에서 거래 수행이 가능한 기술로는 비특허문헌 6, 7, 8에 의해 제안된 기술이 존재한다. 상기 비특허문헌 6, 7, 8에 의해 제안된 기술들은 영지식 증명(Zero Knowledge Proof)을 통해 거래 당사자가 아닌 제 3자에게 거래정보를 보여주지 않는 상태로 올바른 거래를 입증할 수 있다.

[26] 하지만 상기 비특허문헌 6, 7, 8에 의해 제안된 기술들은 거래에 대한 기밀성을 보장하는 기술에 주로 사용되므로 데이터의 확률적 분포를 파악하려는 데이터 분석 및 처리 기술에는 알맞지 않다.

[27] 또한 프라이버시 보존형 분산 학습 기술로는 비특허문헌 9, 10에 의해 제안된 기술이 존재한다. 상기 비특허문헌 9, 10에 의해 제안된 기술들은 무허가형 블록체인(Permissionless blockchain) 기반의 탈중앙화 분산 분석 기법을 제안한다.

[28] 상기 비특허문헌 9, 10 에 의해 제안된 기술들은 분산 학습 시 각 라운드에서의 결과 값을 하나의 블록으로 생성하여 원장에 기록 후 이를 기반으로 다음 라운드를 진행하는 방식이다.

[29] 하지만 상기 비특허문헌 9, 10에 의해 제안된 기술들은 무 허가형 블록체인을 기반으로 한다. 무 허가형 블록체인과 허가형 블록체인은 서로 매우 다른 구조적 특성을 보인다. 보통의 무 허가형 블록체인은 분산 원장 내 안전하고 신뢰있는 하나의 블록을 생성하기 위해 약 10분 가량의 많은 시간을 필요로 한다. 대개 데이터 분석 기술은 시간이 많이 소모되는 큰 규모의 데이터에 대해 이루어지기는 하나 각 라운드 당 10분 가량의 소모는 매우 비 효율적 일 수 밖에 없다.

[30] 또한 상기 비특허문헌 9, 10에 의해 제안된 기술들은 기존의 허가형 블록체인을 사용 중인 금융 분야, 제조사 간 공급망, 제조사와 소비자 간 유통망, 의료 분야 등 수 많은 분야에 단순 적용할 수 없는 문제점을 지니고 있다.

[31] 이 외 안전하고 효율적인 데이터 비 식별화를 위해 블록체인 기술을 도입한 사례로는 특허문헌 1, 2에 의해 제안된 기술이 존재한다. 상기 특허문헌 1, 2에 의해 제안된 기술들은 다수의 데이터 소유자들로 이루어진 분산 데이터 환경에서 차분 프라이버시를 도입 할 때 적용되는 기술에 해당한다.

[32] 하지만 상기 특허문헌 1, 2에 의해 제안된 기술들은 분산 데이터 환경에서 차분 프라이버시가 도입될 때 차분 프라이버시 알고리즘의 안전성 및 효율성 측면에서 발생할 수 있는 요소들을 해결하기 위해 블록체인을 도입하는 기술로써 데이터의 확률적 분포를 파악하려는 데이터 분석 및 처리 기술에는

알맞지 않다.

[33]

[34] [선행기술문헌]

[35] [특허문헌]

[36] (특허문헌 1) US 2018-0307854 A1 "Tracking privacy budget with distributed ledger"

[37] (특허문헌 2) US 2018-0173894 A1 "Differential privacy and outlier detection within a non-interactive model"

[38]

[39] [비특허문헌]

[40] (비특허문헌 1) S.Nakamoto, "Bitcoin: A peer-to-peer electronic cash system"

[41] (비특허문헌 2) L.Sweeney, "k-anonymity: A model for protecting privacy" International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no.5, pp.557-570, 2002

[42] (비특허문헌 3) F.Benhamouda et al., "Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation" Cloud Engineering (IC2E), IEEE International Conference on, IEEE, pp.357-363, 2018

[43] (비특허문헌 4) G.Zyskind et al., "Decentralizing privacy: Using blockchain to protect personal data" IEEE Security and Privacy Workshops, IEEE, pp.180-184, 2015.

[44] (비특허문헌 5) G.Zyskind et al., "Enigma: Decentralized computation platform with guaranteed privacy" arXiv preprint arXiv:1506.03471, 2015.

[45] (비특허문헌 6) Zcash - all coins are created equal. https://z.cash/. Accesed Dec 2017.

[46] (비특허문헌 7) A. van Wirdum, ""Confidential assets" brings privacy to all blockchain assets: Blockstream" Bitcoin Magazine, April 2017, https://bitcoinmagazine.com/articles/confidential-assets-brings-privacy-all-blockchain-assets-blockstream/.

[47] (비특허문헌 8) E.Cecchetti et al., "Solidus: Confidential distributed ledger transactions via PVORM" Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2017.

[48] (비특허문헌 9) T. T. Kuo et al., "Modelchain: Decentralized Privacy-preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks" arXiv preprint arXiv:1802.01746, 2018.

[49] (비특허문헌 10) X.Chen et al., "Distributed Machine Learning Meets Blockchain: A Decentralized, Secure, and Privacy-preserving Realization" IEEE International Conference on Big Data (IEEE BigData'18), pp.1177-1186, 2018.

[50]

발명의 상세한 설명

기술적 과제

[51] 본 발명은 블록체인 기반 시스템에서 특정 데이터 분석을 수행할 때 질의에 대한 비밀분산원장의 응답에 노이즈가 추가 된 값을 반환하여 개인 프라이버시가 보존된 상태로 데이터 분석을 수행 할 수 있도록 하는 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법을 제공하는 것을 그 목적으로 한다.

과제 해결 수단

[52] 상기와 같은 과제를 해결하기 위하여 본 발명은, 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법으로서, 상기 허가형 블록체인 시스템은, 시스템 참여자인 노드가 상기 허가형 블록체인 시스템에 접근하기 위한 클라이언트 어플리케이션; 블록체인 네트워크상의 트랜잭션이 기록되는 분산원장; 상기 분산원장 및 노드 개인만이 보유하고 있는 개인 데이터베이스를 포함한 분산 데이터베이스; 및 상기 분산 데이터베이스에 대한 액세스를 제어하는 스마트컨트랙트; 를 포함하고, 상기 분산원장은, 상기 허가형 블록체인 시스템의 모든 구성원이 공유하는 공개분산원장; 상기 허가형 블록체인 시스템의 특정 구성원만이 공유하는 1 이상의 비밀분산원장을 포함하고, 상기 공개분산원장은, 상기 허가형 블록체인 시스템에서 이루어지는 트랜잭션을 저장하는 데이터 공개분산원장; 및 각 라운드 별 학습의 결과물 및 최종 분산 학습 모델을 저장하는 분산 학습 모델 공유원장을 포함하고, 상기 데이터 분석 방법은, 클라이언트 어플리케이션이 스마트컨트랙트에 데이터분석질의함수를 호출하는 질의호출단계; 상기 스마트컨트랙트가 상기 데이터분석질의함수에 기초하여 상기 분산 데이터베이스에 상기 데이터분석질의함수에 대한 응답 요청을 수행하는 질의응답요청단계; 상기 분산 데이터베이스가 차분 프라이버시를 적용하여 상기 데이터분석질의함수에 대한 응답 값을 반환하는 질의응답반환단계; 및 상기 스마트컨트랙트가 상기 응답 값을 분석하여 반환하는 분석결과반환단계; 상기 스마트컨트랙트가 상기 응답 값을 분석하여 계산된 분산학습모델을 저장하는 분산학습모델저장단계; 상기 스마트컨트랙트가 상기 응답 값을 분석하여 차후 오류기반감사를 위한 오류로그저장단계; 상기 스마트컨트랙트가 상기 응답 값을 분석하여 반환하는 분석결과반환단계; 상기 클라이언트가 향후 오류기반감사를 위해 저장된 오류로그값을 요청하는 오류로그요청단계; 상기 분산학습모델공개원장이 상기 오류로그요청에 대한 응답 값을 반환하는 오류로그반환단계; 및 상기 클라이언트가 상기 오류로그반환단계의 응답 값을 통해 오류기반감사를 수행하는 오류기반감사수행단계를 포함하는, 프라이버시 보존형 데이터 분석 방법을 제공한다.

[53] 본 발명에서는, 상기 스마트컨트랙트에는 상기 데이터분석질의함수가

저장되어 있고, 상기 데이터분석질의함수는, 상기 분산 데이터베이스가 차분 프라이버시를 적용하여 응답 값을 반환하도록 할 수 있다.

[54] 본 발명에서는, 상기 데이터 공개분산원장은, 상기 데이터분석질의함수에 대해 응답 값을 반환하고, 상기 비밀분산원장 및 상기 개인 데이터베이스는, 상기 데이터분석질의함수에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 반환할 수 있으며, 상기 분산학습모델 공유원장은 상기 분산학습모델저장단계에 대해 프라이버시 보존형 분산학습 모델을 저장하고 보유한다.

[55] 본 발명에서는, 상기 질의응답요청단계는, 상기 데이터 공개분산원장에 데이터분석질의함수에 대한 응답 값을 요청하는 공개분산데이터응답요청단계; 및 상기 비밀분산원장 및 상기 개인 데이터베이스에 차분 프라이버시를 적용한 데이터분석질의함수에 대한 응답 값을 요청하는 비밀분산데이터응답요청단계; 를 포함할 수 있다.

[56] 본 발명에서는, 상기 비밀분산원장이 2 이상 존재하는 경우, 2 이상의 상기 비밀분산원장은 독립적으로 상기 데이터분석질의함수에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 각각 반환할 수 있다.

[57] 본 발명에서는, 상기 분석결과반환단계는, 상기 데이터 공개분산원장 및 상기 비밀분산원장과 상기 개인 데이터베이스가 반환한 상기 응답 값을 통합하여 데이터분석질의함수에 기초한 분석을 수행하여 분석 결과를 반환할 수 있다.

[58] 본 발명에서는, 상기 분산학습모델 저장 및 오류기반감사를 위한 오류로그저장단계는, 상기 분산 데이터베이스가 반환한 상기 응답 값을 기반으로 계산되는 분산학습모델 및 오류로그를 저장할 수 있다.

[59] 본 발명에서는, 상기 오류기반감사수행을 위한 오류 로그값 요청 및 오류 로그값 반환 단계는, 데이터 분석을 수행할 수 있는 참여자 누구든지 클라이언트에 접근하여 언제든지 오류 로그값을 응답 받을 수 있으며, 상기 클라이언트는 이를 이용해 오류기반감사를 수행할 수 있다.

발명의 효과

[60] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 특정 구성원만이 소유하고 있는 비밀데이터의 값을 노출시키지 않은 상태로 데이터 분석을 수행하도록 하는 효과를 발휘할 수 있다.

[61] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 기존의 허가형 블록체인 시스템의 구조를 변형하지 않으면서도 비밀데이터를 보호하도록 하는 효과를 발휘할 수 있다.

[62] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 분산학습 기술 등의 데이터 분석 기술 사용 시 기존의 허가형 블록체인 시스템의 구조를 변형하지 않으면서도 안전하고 효율적으로 데이터를 분석하도록 하는 효과를 발휘할 수 있다.

[63] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 비밀데이터를 보호하기 위한 물리적 구성요소를 추가하지 않음으로써 네트워크 구성을 간이하게 유지하는 효과를 발휘할 수 있다.

[64] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에는 기존의 블록체인 시스템이 가지고 있는 속성과 마찬가지로 구성원 각각이 스마트컨트랙트와 분산 데이터베이스를 보유함으로써 단일 장애점(Single Point of Failure)을 방지하는 효과를 발휘할 수 있다.

[65]

도면의 간단한 설명

[66] 도 1은 본 발명의 일 실시예에 따른 허가형 블록체인 시스템의 구성을 개략적으로 도시하는 도면이다.

[67] 도 2는 본 발명의 일 실시예에 따른 스마트컨트랙트의 구성을 개략적으로 도시하는 도면이다.

[68] 도 3은 본 발명의 일 실시예에 따른 질의함수의 구성을 개략적으로 도시하는 도면이다.

[69] 도 4는 본 발명의 일 실시예에 따른 분산데이터베이스의 구성을 개략적으로 도시하는 도면이다.

[70] 도 5는 본 발명의 일 실시예에 따른 분산원장의 구성을 개략적으로 도시하는 도면이다.

[71] 도 6는 본 발명의 일 실시예에 따른 공개분산원장의 구성을 개략적으로 도시하는 도면이다.

[72] 도 7는 본 발명의 일 실시예에 따른 두 노드의 구성을 개략적으로 도시하는 도면이다.

[73] 도 8은 허가형 블록체인 시스템의 데이터 처리 과정의 흐름도이다.

[74] 도 9은 프라이버시가드가 적용된 데이터베이스가 차분 프라이버시를 적용하여 응답을 수행하는 분석 방법의 요청 및 응답 흐름도이다.

[75] 도 10은 본 발명의 일 실시예에 따른 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법의 요청 및 응답 흐름도이다.

[76] 도 11는 본 발명의 일 실시예에 따른 차분 프라이버시가 적용된 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법의 동작을 예시한 흐름도이다.

[77] 도 12는 본 발명의 일 실시예에 따른 차분 프라이버시가 적용된 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법의 동작을 예시한 흐름도이다.

[78]

발명의 실시를 위한 형태

[79] 이하에서는, 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여

개시된다. 하기 설명에서는 설명을 목적으로, 하나이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 발명의 기술 분야에서 통상의 지식을 가진 자에게 인식될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다.

[80]

[81] 또한, 다양한 양상들 및 특징들이 다수의 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있는 시스템에 의하여 제시될 것이다. 다양한 시스템들이, 추가적인 장치들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있다는 점 그리고/또는 도면들과 관련하여 논의된 장치들, 컴포넌트들, 모듈들 등 전부를 포함하지 않을 수도 있다는 점 또한 이해되고 인식되어야 한다.

[82] 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다. 아래에서 사용되는 용어들 '~부', '컴포넌트', '모듈', '시스템', '인터페이스' 등은 일반적으로 컴퓨터 관련 엔티티(computer-related entity)를 의미하며, 예를 들어, 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어를 의미할 수 있다.

[83] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다.

[84] 또한, 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[85] 또한, 본 발명의 실시예들에서, 별도로 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 발명의 실시예에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[86]

[87] 도 1은 본 발명의 일 실시예에 따른 허가형 블록체인 시스템의 구성을 개략적으로 도시하는 도면이다.

[88]

[89] 이하 본 명세서에서 설명되는 허가형 블록체인 시스템은 하이퍼레저 패브릭(Hyperledger Fabric)을 기반으로 정의한다.

[90] 도 1을 참조하면 본 발명의 일 실시예에 따른 허가형 블록체인 시스템은 1 이상의 노드(10); 시스템 참여자인 노드가 상기 허가형 블록체인 시스템에 접근하기 위한 클라이언트 어플리케이션(40); 클라이언트의 자격증명을 제공하는 멤버십 서비스 프로바이더(50); 및 트랜잭션을 블록으로 정렬하는 오더러(60); 를 포함한다.

[91]

[92] 상기 노드(10)는 피어(peer)라고도 불리며 블록체인 네트워크를 구성한다. 상기 노드(10)는 거래 정보(트랜잭션)가 저장되는 블록체인 네트워크를 유지하는 역할을 수행한다. 도 1에는 하나의 노드(10)만이 도시되어 있지만, 상기 블록체인 네트워크에는 복수의 노드(10)가 존재하여 네트워크를 구성할 수 있다. 이 중 일부의 노드(10)는 보증피어(엔도저, endorser)의 역할을 수행할 수 있다. 상기 보증피어는 상기 어플리케이션(40)의 요청에 따라 체인코드를 실행하고 결과를 보증하는 역할을 수행한다. 이와 같은 보증피어의 보증은 상기 체인코드에 연계된 보증 정책에 기초하여 수행될 수 있다.

[93] 상기 어플리케이션(40)은 클라이언트에 의해 트랜잭션을 생성하여 상기 트랜잭션을 보증하는 보증피어에 제출함으로써 거래의 보증을 요청할 수 있다. 이와 같은 어플리케이션(40)은 특정 개인에 의해 관리되는 것이 아니라 해당 블록체인 네트워크의 관리자 혹은 기관에 의해 수행된다.

[94] 상기 멤버십 서비스 프로바이더(50)는 상기 어플리케이션(40)을 사용하는 클라이언트의 자격을 증명하여 피어가 블록체인 네트워크에 참여할 수 있도록 한다. 상기 클라이언트는 상기 멤버십 서비스 프로바이더(50)의 자격 증명을 이용하여 트랜잭션을 인증하고, 피어는 상기 자격 증명을 사용하여 상기 트랜잭션의 처리 결과를 인증한다. 이와 같은 멤버십 서비스 프로바이더(50)를 통해 허가된 클라이언트만이 상기 블록체인 네트워크에 참여하도록 할 수 있다.

[95] 상기 오더러(60)는 트랜잭션을 블록으로 정렬하는 노드의 집합이다. 상기 오더러(60)는 일반적인 노드(10)와는 독립적으로 존재하여 상기 어플리케이션(40)으로부터 제안 되는 트랜잭션을 합의 알고리즘에 따라 순서화시켜 정렬한다. 상기 오더러(60)는 이와 같이 정렬 된 트랜잭션을 블록으로 생성하여 상기 블록체인 네트워크 상의 노드(10)에 전달한다. 이와 같은 블록을 전달 받은 노드(10)는 확정피어(커미터, committer)로 동작하여 거래를 확정할 수 있다.

[96] 상기 노드(10)는 블록체인 네트워크상의 트랜잭션이 기록되고 개인만이

보유하고 있는 개인 데이터베이스를 포함한 분산데이터베이스(200); 및 상기 분산데이터베이스(200)에 대한 액세스를 제어하는 스마트컨트랙트(100); 를 포함할 수 있다.

[97] 상기 분산데이터베이스(200)는 블록체인으로서 트랜잭션이 기록된다. 본 발명의 일 실시예에서 상기 분산데이터베이스(200)는 블록체인 네트워크상의 트랜잭션이 기록되는 분산원장; 및 상기 노드(10) 개인만이 보유하고 있는 개인데이터베이스(220)를 포함할 수 있다. 상기 스마트컨트랙트(100)는 체인코드로 작성되어 상기 어플리케이션(40)이 상기 분산데이터베이스(200)와 상호작용해야 할 때 상기 어플리케이션(40)에 의해 호출된다. 상기 스마트컨트랙트(100)는 상기 분산데이터베이스(200)에 대한 접근을 위해 다양한 함수들이 저장되어, 상기 함수에 의해 상기 분산데이터베이스(200)의 데이터를 갱신하거나, 혹은 상기 데이터로부터 필요한 정보를 추출할 수 있다.

[98]

[99] 도 2는 본 발명의 일 실시예에 따른 스마트컨트랙트의 구성을 개략적으로 도시하는 도면이다.

[100] 도 2를 참조하면 본 발명의 일 실시예에 따른 상기 스마트컨트랙트(100)에는 질의함수(110) 및 배포함수(120)가 저장되어 있다. 상기 질의함수(110)는 상기 분산데이터베이스(200)의 데이터를 조회하기 위한 함수이고, 상기 배포함수(120)는 상기 분산데이터베이스(200)에 데이터를 기록하기 위한 함수이다.

[101] 상기 질의함수(110)는 상기 분산데이터베이스(200)의 데이터를 조회하기 위해 블록을 검색하거나, 상기 분산데이터베이스(200)의 데이터의 크기 등을 조회할 수 있고, 상기 질의함수(110)의 실행 결과는 상기 분산데이터베이스(200)에 기록되지 않는다.

[102] 상기 배포함수(120)는 상기 분산데이터베이스(200)에 데이터를 기록하기 위한 함수이고, 상기 배포함수(120)는 상기 스마트컨트랙트(100)의 체인코드를 실행하거나, 체인코드를 새로 등록하는 등의 동작이 실행될 수 있다. 이와 같은 배포함수(120)의 실행에 따라 상기 분산데이터베이스(200)에 데이터가 기록될 수 있다.

[103] 또한, 본 발명의 일 실시예에서 상기 스마트컨트랙트(100)에는 이 외에도 다양한 함수들이 저장되어 있을 수 있다.

[104]

[105] 도 3은 본 발명의 일 실시예에 따른 질의함수의 구성을 개략적으로 도시하는 도면이다.

[106]

[107] 상기 질의함수(110)는 일반질의함수(111) 및 데이터분석질의함수(112)를 포함할 수 있다. 상기 일반질의함수(111)는 상기 분산데이터베이스(200)에 저장된 데이터에서 개별 데이터 분석을 수행할 수 없는 일반적인 질의를

수행하는 함수이고, 상기 데이터분석질의함수(112)는 데이터 분석을 수행할 수 있는 질의를 수행하는 함수이다.

[108] 즉, 본 발명의 일 실시예에서 상기 스마트컨트랙트(100)에는 상기 데이터분석질의함수(112)가 저장되어 있어, 상기 분산데이터베이스(200)에 대한 데이터 분석을 수행할 수 있도록 할 수 있다. 이 때, 상기 데이터분석질의함수(112)는 상기 분산데이터베이스(200)의 프라이버시를 유지하기 위하여 상기 분산데이터베이스(200)가 차분 프라이버시를 적용하여 응답 값을 반환하도록 할 수 있다.

[109]

[110] 도 4는 본 발명의 일 실시예에 따른 분산데이터베이스의 구성을 개략적으로 도시하는 도면이다.

[111]

[112] 도 4를 참조하면 본 발명의 일 실시예에 따른 분산데이터베이스(200)는 상기 허가형 블록체인 시스템이 공유하는 분산원장(210); 및 상기 허가형 블록체인 시스템 내의 상기 노드들이 각자 보유하는 개인 데이터베이스(220); 를 포함할 수 있다.

[113]

[114] 도 5는 본 발명의 일 실시예에 따른 분산원장의 구성을 개략적으로 도시하는 도면이다.

[115]

[116] 도 5를 참조하면 본 발명의 일 실시예에 따른 분산원장(210)은 상기 허가형 블록체인 시스템의 모든 구성원이 공유하는 공개분산원장(211); 및 상기 허가형 블록체인 시스템의 특정 구성원만이 공유하는 1 이상의 비밀분산원장(212); 을 포함할 수 있다. 도 5에는 n개의 비밀분산원장(212)을 포함하는 분산원장(210)이 도시되어 있다. 이와 같은 비밀분산원장(212)의 수는 동일한 블록체인 시스템의 노드마다 서로 다를 수 있다.

[117]

[118] 도 6는 본 발명의 일 실시예에 따른 공개분산원장의 구성을 개략적으로 도시하는 도면이다.

[119]

[120] 도 6를 참조하면 본 발명의 일 실시예에 따른 공개분산원장(211)은 상기 허가형 블록체인 시스템에서 이루어지는 트랜잭션을 저장하는 데이터공개분산원장(211.1); 및 상기 허가형 블록체인 시스템에서 이루어지는 각 라운드 별 학습의 결과물 및 최종 분산 학습 모델을 저장하는 분산학습모델공유원장(211.2); 을 포함할 수 있다. 본 발명의 일 실시예에 따른 공개분산원장(211)은 상기 허가형 블록체인 시스템의 모든 구성원이 공유할 수 있다.

[121]

[122] 도 7는 본 발명의 일 실시예에 따른 두 노드의 구성을 개략적으로 도시하는 도면이다.

[123]

[124] 도 7에 도시된 노드A(10) 및 노드B(20)는 상기 블록체인 네트워크를 구성하는 노드이다. 상기 노드A(10) 및 노드B((20) 모두 스마트컨트랙트(100) 및 분산데이터베이스(200)를 포함하고 있다. 이 때 상기 분산데이터베이스(200)는 분산원장(210) 및 개인데이터베이스(220)를 포함하고 있으며, 상기 분산원장(210)은 공개분산원장(211) 및 비밀분산원장(212)을 포함하고 있다. 또한 상기 공개분산원장(211)은 데이터공개분산원장(211.1) 및 분산학습모델공유원장(211.2)을 포함하고 있다.

[125]

[126] 이 때, 상기 노드A(10) 및 상기 노드B(20) 모두 비밀분산원장#1(212.1)을 포함하고 있다. 상기 비밀분산원장#1(212.1)은 상기 블록체인 네트워크의 노드 중 상기 노드A(10) 및 상기 노드B(20)가 공유하는 비밀분산원장이다. 상기 비밀분산원장#1(212.1)은 상기 노드A(10) 및 상기 노드B(20) 외에도 다른 노드에도 포함되어 있을 수 있다.

[127] 비밀분산원장#2(212.2)는 상기 노드A(10)에는 포함되어 있으나, 상기 노드B(20)에는 포함되어 있지 않다. 상기 비밀분산원장#2(212.2)은 상기 노드A(10)외에 다른 노드에도 포함되어 있을 수 있다. 다만 상기 노드B(20)에는 포함되어 있지 않아, 상기 노드B(20)의 스마트컨트랙트(100)는 상기 비밀분산원장#2(212.2)에 저장되어 있는 데이터에는 접근할 수 없다.

[128] 반면, 비밀분산원장#3(212.3)는 상기 노드B(20)에는 포함되어 있으나, 상기 노드A(10)에는 포함되어 있지 않다. 상기 비밀분산원장#3(212.3)은 상기 노드B(20)외에 다른 노드에도 포함되어 있을 수 있다. 다만 상기 노드A(10)에는 포함되어 있지 않아, 상기 노드A(10)의 스마트컨트랙트(100)는 상기 비밀분산원장#3(212.3)에 저장되어 있는 데이터에는 접근할 수 없다.

[129]

[130] 도 8은 허가형 블록체인 시스템의 데이터 처리 과정의 흐름도이다.

[131]

[132] 도 8에서 요청자(70)는 상기 분산데이터베이스(200)에 저장된 데이터를 분석하려 하는 블록체인 네트워크의 노드이다. 상기 요청자(70)는 상기 어플리케이션(40)을 통해 스마트컨트랙트(100)에 접근할 수 있다. 도 8의 실시예에서 상기 스마트컨트랙트(100)는 하나의 공개분산원장(211), 두 개의 비밀분산원장(212) 및 하나의 개인데이터베이스(220)에 접근할 수 있다.

[133]

[134] 본 발명의 일 실시예에 따른 상기 데이터 분석 방법은, 클라이언트 어플리케이션(40)이 스마트컨트랙트(100)에 데이터분석질의함수(112)를 호출하는 질의호출단계(S100); 상기 스마트컨트랙트(100)가 상기

데이터분석질의함수(112)에 기초하여 상기 분산데이터베이스(200)에 상기 데이터분석질의함수(112)에 대한 응답 요청을 수행하는 질의응답요청단계(S200); 상기 분산데이터베이스(200)가 차분 프라이버시를 적용하여 상기 데이터분석질의함수(112)에 대한 응답 값을 반환하는 질의응답반환단계(S300); 상기 스마트컨트랙트(100)가 상기 응답 값을 분석하여 반환하는 분석결과반환단계(S400); 및 오류로그에 기초하여 악의적인 공격자의 공격 행동을 사전 방지하는 오류기반감사수행단계(S500); 를 포함한다.

[135]

[136] 도 9은 프라이버시가드가 적용된 데이터베이스가 차분 프라이버시를 적용하여 응답을 수행하는 분석 방법의 요청 및 응답 흐름도이다.

[137]

[138] 도 9에서는 차분 프라이버시를 이용하여 노이즈를 추가하는 방법이 도시되어 있다. 도 9을 참조하면, 데이터 분석을 하려는 요청자(70)와 분산데이터베이스(90) 사이에 분석에 관한 질의함수를 관리하고 노이즈가 추가된 응답 값을 계산해주는 프라이버시가드(80)가 존재한다. 도 9에는 분산데이터베이스(90)가 도시되어 있지만 이와 같은 프라이버시가드(80)는 일반적인 데이터베이스에서도 동일하게 동작할 수 있다.

[139] 이와 같이 프라이버시가드(80)가 적용된 분산데이터베이스(90)에 있어서 차분 프라이버시를 적용하기 위해서 우선 상기 요청자(70)가 프라이버시가드(80)에 특정 정보를 획득하기 위한 질의를 요청하는 단계(S10)가 수행된다.

[140] 이 후, 상기 프라이버시가드(80)가 기설정된 정책에 의해 요청된 질의를 분석하는 단계(S20)가 수행된다. 상기 프라이버시가드(80)는 기설정된 정책에 의해 상기 질의의 프라이버시 영향 정도를 평가할 수 있다.

[141] 이 후, 상기 프라이버시가드(80)가 상기 분산데이터베이스(90)로 질의를 전송하는 단계(S30)가 수행된다. 이와 같은 질의에 따라 상기 분산데이터베이스(90)가 상기 프라이버시가드(80)로 왜곡되지 않은 데이터에 기반한 응답 값을 반환하는 단계(S40)가 수행된다.

[142] 이 후, 상기 프라이버시가드(80)가 상기 S20단계에서 평가한 상기 질의의 프라이버시 영향 정도에 기초하여 적절한 양의 노이즈를 추가하는 단계(S50)가 수행된다. 이와 같이 상기 프라이버시가드(80)는 상기 분산데이터베이스(90)에 있는 정보의 기밀성을 보호하기 위하여 상기 응답 값에 노이즈가 추가된 결과 값을 생성하고, 상기 요청자(70)에게 노이즈가 추가된 결과 값을 반환하는 단계(S60)를 수행한다.

[143] 이와 같은 과정을 통해 상기 요청자(70)는 요청한 질의에 대한 정보를 전달 받으면서도, 구체적인 데이터에 대해서는 노이즈에 의해 알 수 없게 되어 상기 분산데이터베이스(90)의 프라이버시를 유지할 수 있게 된다.

[144]

[145] 도 10은 본 발명의 일 실시예에 따른 허가형 블록체인 시스템의 프라이버시

보존형 데이터 분석 방법의 요청 및 응답 흐름도이다.

[146]

[147] 도 10을 참조하면 도 9에서의 프라이버시가드(80)와 같은 역할을 데이터분석질의함수를 포함하는 스마트컨트랙트(100)가 수행하게 된다. 본 발명의 일 실시예에서는 이와 같이 차분 프라이버시를 구현하는 방법이 상기 도 9의 프라이버시가드(80)처럼 물리적, 단일적으로 나뉘어져 있는 형태가 아니라 스마트컨트랙트(100)의 내부에 추가 된 자동함수의 형태를 취하게 된다. 즉, 물리적인 개체가 추가되는 것이 아니라 블록체인 네트워크 상에 논리적으로 추가구성 됨으로써 네트워크 구성에 대한 부담감을 줄일 수 있으며, 구성원 모두가 공개분산원장(211)을 동일하게 공유하고, 각각 개인데이터베이스(220)를 포함하고 있으며, 비밀분산원장(212)에 기반한 일부의 구성원들이 동일한 데이터분석질의함수(112)를 포함하는 스마트컨트랙트(100)를 보유하게 되므로 기존 프라이버시가드(80) 기반 차분 프라이버시 구현 방법에 비해 단일실패점(Single Point of Failure)을 방지할 수 있는 효과를 발휘할 수 있다.

[148]

[149] 도 10을 참조하면 우선 요청자(70)가 어플리케이션(40)을 통해 스마트컨트랙트(100)에 데이터분석질의함수(112)를 호출하는 질의호출단계(S100)를 수행한다.

[150] 이 후, 상기 스마트컨트랙트(100)가 상기 데이터분석질의함수(112)에 기초하여 상기 분산데이터베이스(200)에 상기 데이터분석질의함수(112)에 대한 응답 요청을 수행하는 질의응답요청단계(S200)가 수행된다. 본 발명의 일 실시예에서 상기 질의응답요청단계(S200)는, 상기 데이터공개분산원장(211.1)에 데이터분석질의함수(112)에 대한 응답 값을 요청하는 공개분산데이터응답요청단계(S210); 및 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)에 차분 프라이버시를 적용한 데이터분석질의함수(112)에 대한 응답 값을 요청하는 비밀데이터응답요청단계(S220); 를 포함할 수 있다. 도 10에는 상기 공개분산데이터응답요청단계(S210) 수행 후에 상기 비밀데이터응답요청단계(S220)가 수행되는 것으로 도시되어 있으나, 본 발명에서 상기 공개분산데이터응답요청단계(S210) 및 상기 비밀데이터응답요청단계(S220)는 동시에 수행될 수도 있고, 혹은 상기 비밀데이터응답요청단계(S220)가 먼저 수행될 수도 있다. 즉, 상기 공개분산데이터응답요청단계(S210) 및 상기 비밀데이터응답요청단계(S220)는 독립적으로 수행됨이 바람직하다.

[151] 이 후, 상기 데이터공개분산원장(211.1)은, 상기 데이터분석질의함수(112)에 대해 응답 값을 반환하고(S310), 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)는, 상기 데이터분석질의함수(112)에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 반환한다(S320). 이와 같이 상기

비밀분산원장(212) 및 상기 개인데이터베이스(220)는 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 반환함으로써, 상기 요청자(70)가 상기 분산원장(210)의 확률적 분포 특성은 알아낼 수 있으나, 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)에 저장된 개별적인 정보는 알아낼 수 없어 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)의 데이터에 대한 프라이버시를 보호할 수 있게 된다.

[152] 본 발명의 일 실시예에서 상기 비밀분산원장(212) 또는 상기 개인데이터베이스(220)가 2 이상 존재하는 경우, 2 이상의 상기 비밀분산원장(212) 또는 상기 개인데이터베이스(220)는 독립적으로 상기 데이터분석질의함수(112)에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 각각 반환할 수 있다.

[153] 이 후, 상기 스마트컨트랙트(100)가 상기 응답 값을 분석하여 반환하는 분석결과반환단계(S400)가 수행된다. 이 때, 상기 분석결과반환단계(S400)는, 상기 공개분산원장, 상기 비밀분산원장 및 상기 개인데이터베이스(220)가 반환한 상기 응답 값을 통합하여 데이터분석질의함수에 기초한 분석을 수행하여 분석 결과를 반환할 수 있다.

[154] 이를 위해 상기 분석결과반환단계(S400)에서는 상기 스마트컨트랙트가 상기 공개분산원장(211), 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)의 응답 값을 통합하여 분석을 수행하는 단계(S410)를 수행하고, 상기 분석 결과를 상기 어플리케이션(40)을 통해 상기 요청자(70)에게 반환하는 단계(S420)를 수행할 수 있다.

[155] 또한 도 10을 참조하면 본 발명의 일 실시예에 따른 오류기반감사수행단계(S500)가 올바르지 않은 응답 값을 반환하는 악의적인 공격자의 공격 행동을 사전 방지하기 위해 수행될 수 있다. 도 10에는 상기 요청자(70)의 어플리케이션(40)이 상기 스마트컨트랙트(100)를 통해 단독적으로 수행하는 것으로 도시되어 있으나, 본 발명에서 상기 스마트컨트랙트(100)는 자동함수의 형태를 취하는 논리적인 개체이며 본 발명의 일 실시예에 따른 오류기반감사수행단계(S500)는 허가형 블록체인 내에 속한 어떠한 참여자이든지 어플리케이션(40)을 통해 스마트컨트랙트(100)에 접근하여 언제든지 오류기반감사수행단계(S500)을 실행할 수 있다.

[156] 이와 같은 오류기반감사수행단계(S500)를 수행하기 위해 본 발명의 일 실시예에 따른 상기 분석결과반환단계(S400)는 상기 스마트컨트랙트(100)가 상기 응답 값을 분석하여 계산된 분산학습모델을 저장하는 분산학습모델저장단계(S430); 및 상기 스마트컨트랙트(100)가 상기 응답 값을 분석하여 차후 오류기반감사를 위한 오류로그를 저장하는 오류로그저장단계(S440); 를 더 포함할 수 있다.

[157] 본 발명의 일 실시예에 따른 상기 분산학습모델저장단계(S430)에서는 상기 스마트컨트랙트(1000)가 상기 분산학습모델공유원장(211.2)에 분석을 수행하여

도출된 분산학습모델을 저장하고, 상기 오류로그저장단계(S440)에서는 오류기반감사를 위한 오류로그를 저장할 수 있다.

[158] 이후 수행되는 상기 오류기반감사수행단계(S500)는, 상기 클라이언트가 향후 오류기반감사를 위해 저장된 상기 오류로그를 요청하는 오류로그요청단계(S510); 상기 분산학습모델공개원장이 상기 오류로그요청에 대한 응답 값을 반환하는 오류로그반환단계(S520); 및 상기 클라이언트가 상기 오류로그반환단계의 응답 값에 기초하여 오류기반감사를 수행하는 감사수행단계(S530); 를 포함할 수 있다,

[159]

[160] 도 11는 본 발명의 일 실시예에 따른 차분 프라이버시가 적용된 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법의 동작을 예시한 흐름도이다.

[161]

[162] 도 11는 상기 오류기반감사수행단계(S500)의 보다 쉬운 이해를 위해 도 10에서 이루어지는 본 발명의 일 실시예에 따른 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법의 요청 및 흐름도에 대한 물리적 흐름도를 나타낸다. 도 11를 참조하면, 특정 데이터에 대한 데이터 분석이 수행될 시 분산데이터베이스(200)를 소유한 모든 노드들은 각 라운드 때마다 계산된 모델 및 그에 대한 오류값을 저장한다. 도 11에서는 이에 대한 예시를 나타내기 위해, 노드 A(10)와 노드B(20)만이 포함된 실시예가 도시되어 있으며, 이는 네트워크의 규모에 따라 소수에서 다수가 될 수 있다. 도 11를 참조하면, 노드A(10) 및 노드B(20)는 데이터 분석 수행 시 총 n(i는 1 이상 n 이하)번의 라운드를 진행하게 된다. 이때 각 라운드마다 노드A(10)와 노드B(20)는 _라운드결과값에 대한 저장요청(S441)을 하여 상기 분산학습모델공개원장(211.2)에 저장(S442)하게 된다. 구체적으로 상기 노드A는 1라운드에서 1라운드결과값에 대한 저장요청(S441.1A)을 하고, 상기 분산학습모델공개원장(211.2)는 이를 저장(S442.1A)한다. 또한, 상기 노드B는 1라운드에서 1라운드결과값에 대한 저장요청(S441.1B)을 하고, 상기 분산학습모델공개원장(211.2)는 이를 저장(S442.1B)한다. 이와 같은 단계가 반복되어 분산학습모델저장단계(S430) 및 오류로그저장단계(S440)가 수행될 수 있다.

[163] 이 후, 오류기반감사수행단계(S500)에서는 오류기반감사의 수행을 원하는 특정 노드에 의해 구동되는 요청자(70)가 상기 오류기반감사를 위한 저장된 오류로그값을 요청 하는 오류로그값요청단계(S510) 및 오류기반감사를 위한 저장된 오류로그값을 반환 하는 오류로그값반환단계(S520)을 통해 기존에 저장되어 있는 노드A(10)와 노드B(20)에 대한 모델의 오류 값을 반환 받는다. 이후 요청자(70)는 오류기반감사를 수행하여(S530) 높은 오류를 가지는 노드를 쉽게 파악할 수 있다.

[164] 또한 도 11를 참조하면 상기 오류기반감사수행단계(S500)는 상기와 같은 과정을 통해 높은 오류 값들을 가지는 특정 노드들을 선별할 수 있다. 본 발명의 일 실시예에 따른 차분 프라이버시가 적용된 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법에서의 상기 오류기반감사수행단계(S500)는 해당 오류 수치를 통해 향후 감사의 대상으로 노드를 관리할 수 있으며, 이는 네트워크의 정책에 따라 유동적으로 설정될 수 있다. 예를 들어 오류 값을 0부터 1까지의 수치로 나타내는 네트워크에서 0.7 이상의 평균적 오류를 갖는 노드에 대한 감사 및 관리를 수행하도록 할 수 있다.

[165]

[166] 도 12는 본 발명의 일 실시예에 따른 차분 프라이버시가 적용된 허가형 블록체인 시스템의 프라이버시 보존형 데이터 분석 방법의 동작을 예시한 흐름도이다.

[167]

[168] 도 12에 도시된 블록체인 네트워크에는 차량에 대한 데이터가 저장되어 있다. 상기 블록체인 네트워크에 저장된 데이터 형태는 {키 값; 제조사; 모델; 색상; 차주; 구입비용; 할부여부(개월)}와 같고, 각각 공개분산원장(211), 1 이상의 비밀분산원장(212) 및 개인데이터베이스(220)에 각각에 저장되어 있다.

[169] 또한, 상기 스마트컨트랙트(100)는 상기 분산원장(210)에 대해 쓰기, 수정, 삭제 등의 연산을 수행할 수 있는 배포함수(120), 상기 분산데이터베이스(200)의 기본적인 정보를 읽어올 수 있는 일반질의함수(111) 및 데이터 분석을 수행하기 위한 데이터분석질의함수(112)를 포함하고 있다. 이와 같은 함수들은 상기 블록체인 네트워크가 구동되기 전에 미리 설계되어 포함되어 있다.

[170]

[171] 도 12를 참조하면 우선 요청자(70)가 어플리케이션(40)을 통해 스마트컨트랙트(100)에 데이터분석질의함수(112)를 호출하는 질의호출단계(S100)를 수행한다.

[172] 이 후, 상기 스마트컨트랙트(100)가 상기 데이터분석질의함수(112)에 기초하여 상기 분산데이터베이스(200)에 상기 데이터분석질의함수(112)에 대한 응답 요청을 수행하는 질의응답요청단계(S200)가 수행된다. 상기 데이터분석질의함수(112)는 상기 분산데이터베이스(200)의 상위 제조사 혹은 상위 모델을 조회하거나, 저장된 차량 데이터의 색상 분포 조회 또는 향후 유행 모델에 대한 예측 및 분석 등의 함수를 포함할 수 있다.

[173] 이 때, 상기 질의응답요청단계(S200)는 상기 공개분산원장(211)에 데이터분석질의함수에 대한 응답 값을 요청하는 공개분산데이터응답요청단계(S210); 및 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)에 차분 프라이버시를 적용한 데이터분석질의함수에 대한 응답 값을 요청하는 비밀데이터응답요청단계(S220)의 단계로 나뉘어져 수행될 수 있다. 이를 통해 상기 공개분산원장(211)에는 상기

데이터분석질의함수(112)에 대한 응답 값을 요청하고, 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)에는 차분 프라이버시를 적용한 응답 값을 요청하여, 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)의 데이터에 대한 프라이버시를 보호할 수 있게 된다.

[174] 이 후, 상기 공개분산원장(211)은 상기 데이터분석질의함수(112)에 대해 응답 값을 반환하고(S310), 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)는, 상기 데이터분석질의함수(112)에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 반환한다(S320).

[175] 이 후, 상기 스마트컨트랙트(100)는 상기 공개분산원장(211), 상기 비밀분산원장(212) 및 상기 개인데이터베이스(220)가 반환한 상기 응답 값을 통합하여 데이터분석질의함수에 기초한 분석을 수행하여 분석 결과를 상기 어플리케이션(40)을 통해 상기 요청자(70)에게 반환하는 분석결과반환단계(S400)를 수행한다.

[176]

[177] 전술한 바와 같이 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 특정 구성원만이 소유하고 있는 비밀데이터의 값을 노출시키지 않은 상태로 데이터 분석을 수행하도록 하는 효과를 발휘할 수 있다.

[178] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 기존의 허가형 블록체인 시스템의 구조를 변형하지 않으면서도 비밀데이터를 보호하도록 하는 효과를 발휘할 수 있다.

[179] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 비밀데이터를 보호하기 위한 물리적 구성요소를 추가하지 않음으로써 네트워크 구성을 간이하게 유지하는 효과를 발휘할 수 있다.

[180] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에서는 오류기반감사수행단계(S500)를 통해 올바르지 않은 응답 값을 반환하는 악의적인 공격자의 공격 행동을 사전에 방지하기 위해 수행할 수 있다. 이는 허가형 블록체인 네트워크 내에 참여한 참여자 누구든지 어느 때나 수행할 수 있으며, 특정 참여자가 이전까지 올바른 값을 반환하였는지 혹은 올바르지 않은 값을 반환하였는지의 여부를 쉽게 쉽게 파악할 수 있다.

[181] 본 발명의 일 실시예에 따른 프라이버시 보존형 데이터 분석 방법에는 기존의 블록체인 시스템이 가지고 있는 속성과 마찬가지로 구성원 각각이 스마트컨트랙트와 분산 데이터베이스를 보유함으로써 단일 장애점(Single Point of Failure)을 방지하는 효과를 발휘할 수 있다.

[182]

[183] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨팅 장치를 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 특히, 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다. 본 발명이 적용되는

애플리케이션은 파일 배포 시스템이 제공하는 파일을 통해 이용자 단말에 설치될 수 있다. 일 예로, 파일 배포 시스템은 이용자 단말이기의 요청에 따라 상기 파일을 전송하는 파일 전송부(미도시)를 포함할 수 있다.

[184] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[185] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로 (collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨팅 장치 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[186] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical

disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[187] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

청구범위

[청구항 1] 허가형 블록체인 시스템 상에서의 프라이버시 보존형 데이터 분석 방법으로서,
상기 허가형 블록체인 시스템은,
시스템 참여자인 노드가 상기 허가형 블록체인 시스템에 접근하기 위한 클라이언트 어플리케이션;
블록체인 네트워크상의 트랜잭션이 기록되는 분산원장; 및 상기 노드 개인만이 보유하고 있는 개인데이터베이스; 를 포함하는
분산데이터베이스; 및
상기 분산원장에 대한 액세스를 제어하는 스마트컨트랙트; 를 포함하고,
상기 분산원장은,
상기 허가형 블록체인 시스템의 모든 구성원이 공유하는 공개분산원장; 및
상기 허가형 블록체인 시스템의 특정 구성원만이 공유하는 1 이상의 비밀분산원장; 을 포함하고,
상기 데이터 분석 방법은,
클라이언트 어플리케이션이 스마트컨트랙트에 데이터분석질의함수를 호출하는 질의호출단계;
상기 스마트컨트랙트가 상기 데이터분석질의함수에 기초하여 상기 분산원장에 상기 데이터분석질의함수에 대한 응답 요청을 수행하는 질의응답요청단계;
상기 분산원장이 차분 프라이버시를 적용하여 상기 데이터분석질의함수에 대한 응답 값을 반환하는 질의응답반환단계; 및
상기 스마트컨트랙트가 상기 응답 값을 분석하여 반환하는 분석결과반환단계; 를 포함하는, 프라이버시 보존형 데이터 분석 방법.

[청구항 2] 청구항 1에 있어서,
상기 스마트컨트랙트에는 상기 데이터분석질의함수가 저장되어 있고,
상기 데이터분석질의함수는,
상기 분산데이터베이스가 차분 프라이버시를 적용하여 응답 값을 반환하도록 하는, 프라이버시 보존형 데이터 분석 방법.

[청구항 3] 청구항 1에 있어서,
상기 공개분산원장은,
상기 데이터분석질의함수에 대해 응답 값을 반환하고,
상기 비밀분산원장 및 상기 개인데이터베이스는,
상기 데이터분석질의함수에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 반환하는, 프라이버시 보존형 데이터 분석 방법.

[청구항 4] 청구항 3에 있어서,

상기 질의응답요청단계는,
상기 공개분산원장에 데이터분석질의함수에 대한 응답 값을 요청하는 공개분산데이터응답요청단계; 및
상기 비밀분산원장에 차분 프라이버시를 적용한 데이터분석질의함수에 대한 응답 값을 요청하는 비밀분산데이터응답요청단계; 를 포함하는,
프라이버시 보존형 데이터 분석 방법.

[청구항 5] 청구항 3에 있어서,
상기 비밀분산원장이 2 이상 존재하는 경우,
2 이상의 상기 비밀분산원장은 독립적으로 상기 데이터분석질의함수에 대해 차분 프라이버시 기반의 노이즈가 추가된 응답 값을 각각 반환하는,
프라이버시 보존형 데이터 분석 방법.

[청구항 6] 청구항 3에 있어서,
상기 분석결과반환단계는,
상기 공개분산원장 상기 비밀분산원장 및 상기 개인데이터베이스가 반환한 상기 응답 값을 통합하여 데이터분석질의함수에 기초한 분석을 수행하여 분석 결과를 반환하는, 프라이버시 보존형 데이터 분석 방법.

[청구항 7] 청구항 1에 있어서,
상기 공개분산원장은,
상기 허가형 블록체인 시스템에서 이루어지는 트랜잭션을 저장하는 데이터공개분산원장; 및
상기 허가형 블록체인 시스템에서 이루어지는 각 라운드 별 학습의 결과물 및 최종 분산 학습 모델을 저장하는 분산학습모델공유원장; 을 포함하는, 프라이버시 보존형 데이터 분석 방법.

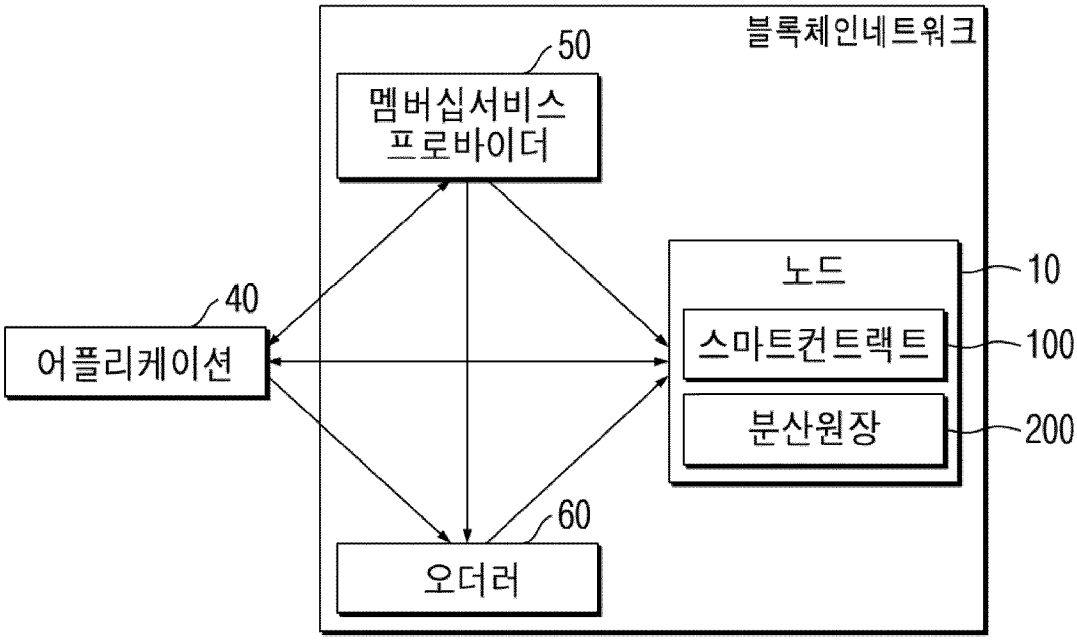
[청구항 8] 청구항 7에 있어서,
상기 데이터 분석 방법은,
오류로그에 기초하여 악의적인 공격자의 공격 행동을 사전 방지하는 오류기반감사수행단계를 더 포함하고,
상기 분석결과반환단계는,
상기 스마트컨트랙트가 상기 응답 값을 분석하여 계산된 분산학습모델을 저장하는 분산학습모델저장단계; 및
상기 스마트컨트랙트가 상기 응답 값을 분석하여 차후 오류기반감사를 위한 오류로그를 저장하는 오류로그저장단계; 를 더 포함하는,
프라이버시 보존형 데이터 분석 방법.

[청구항 9] 청구항 8에 있어서,
상기 분산학습모델공유원장에는,
상기 분산학습모델저장단계에서 프라이버시 보존형 분산학습 모델이 저장될 수 있는, 프라이버시 보존형 데이터 분석 방법.

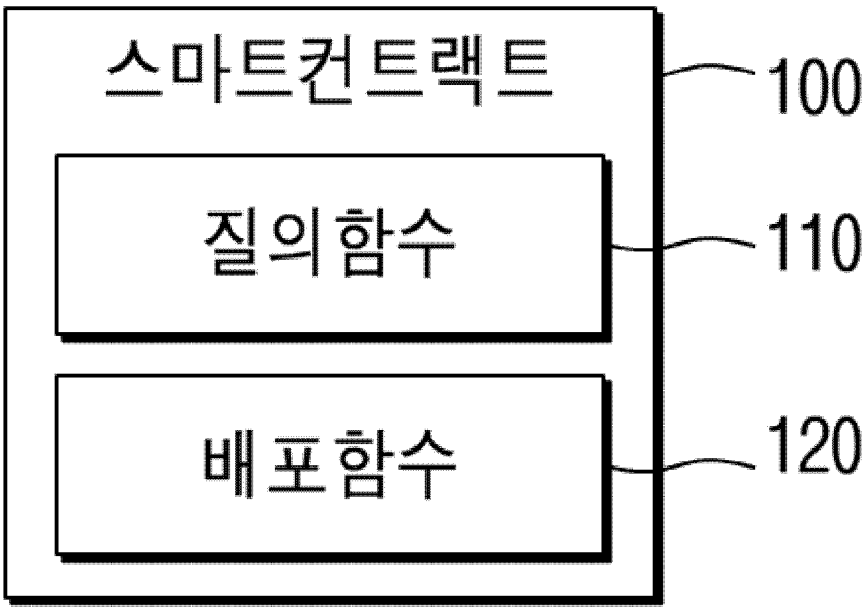
[청구항 10] 청구항 8에 있어서,

상기 오류기반감사수행단계는,
상기 클라이언트가 향후 오류기반감사를 위해 저장된 상기 오류로그를 요청하는 오류로그요청단계;
상기 분산학습모델공유원장이 상기 오류로그요청에 대한 응답 값을 반환하는 오류로그반환단계; 및
상기 클라이언트가 상기 오류로그반환단계의 응답 값에 기초하여 오류기반감사를 수행하는 감사수행단계; 를 포함하는, 프라이버시 보존형 데이터 분석 방법.

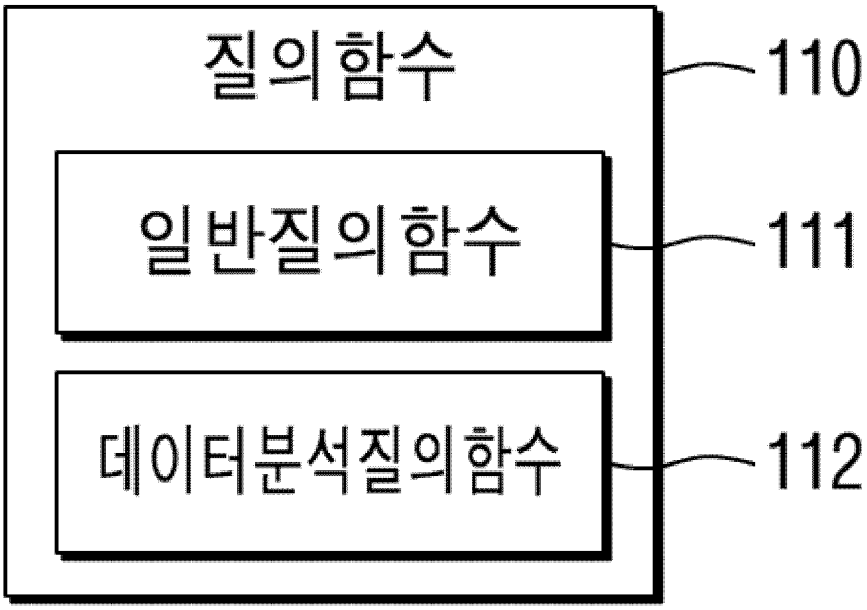
[도1]


블록체인네트워크
50
멤버십서비스 프로바이더
노드
10
스마트컨트랙트
100
분산원장
200
40
어플리케이션
60
오더러

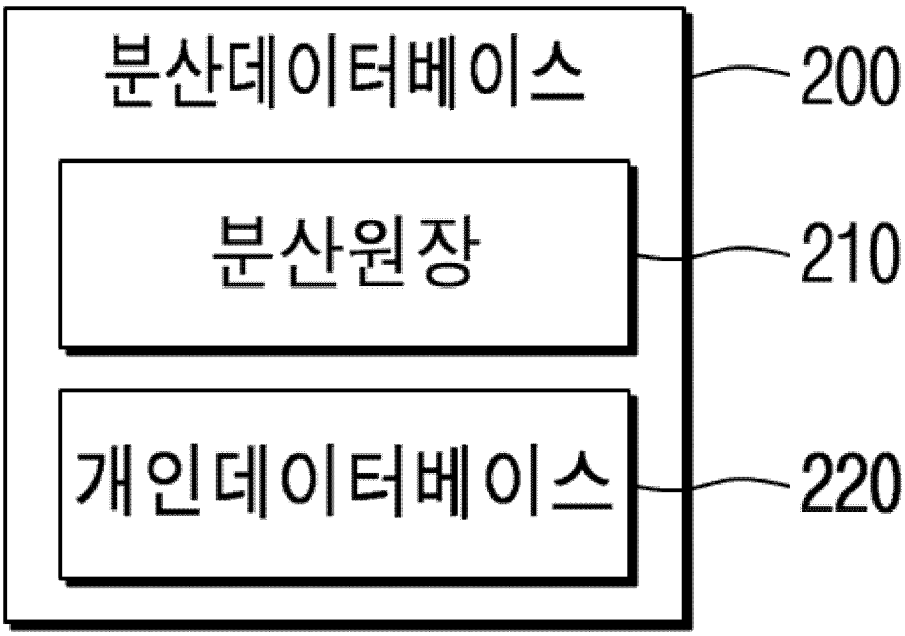
[도2]


스마트컨트랙트
100
질의함수
110
배포함수
120

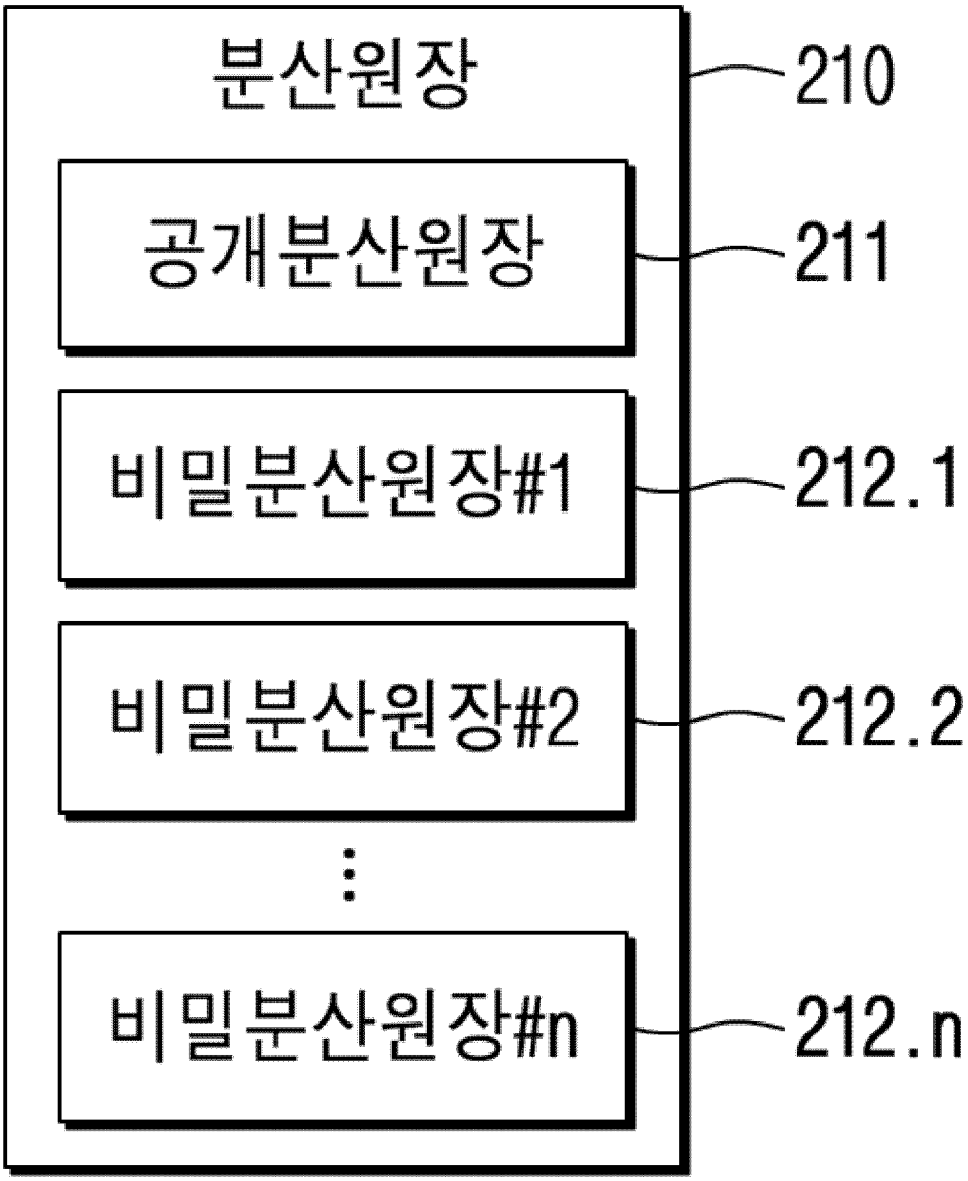
[도3]


질의함수
110
일반질의함수
111
데이터분석질의함수
112

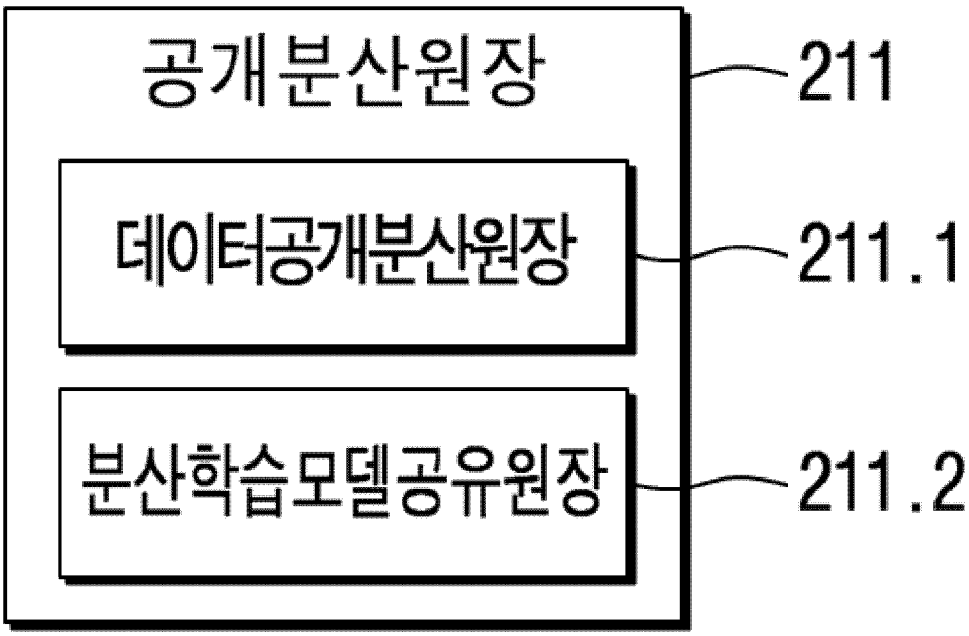
[도4]


분산데이터베이스
200
분산원장
210
개인데이터베이스
220

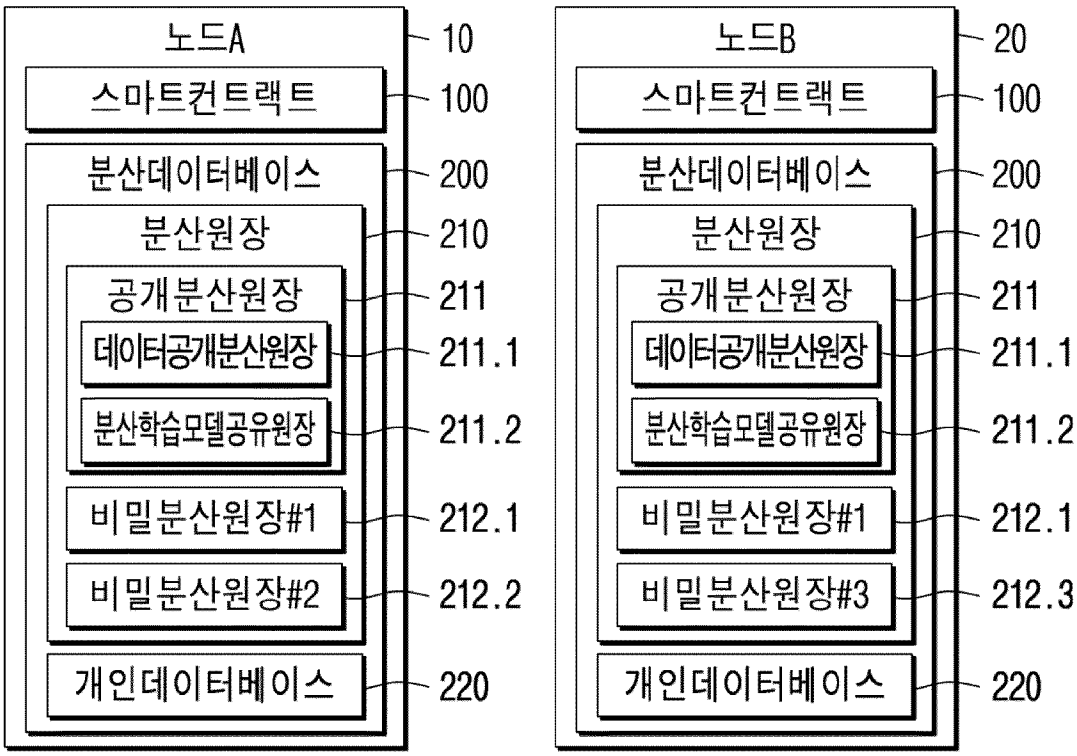
[도5]


분산원장
210
공개분산원장
211
비밀분산원장#1
212.1
비밀분산원장#2
212.2
비밀분산원장#n
212.n

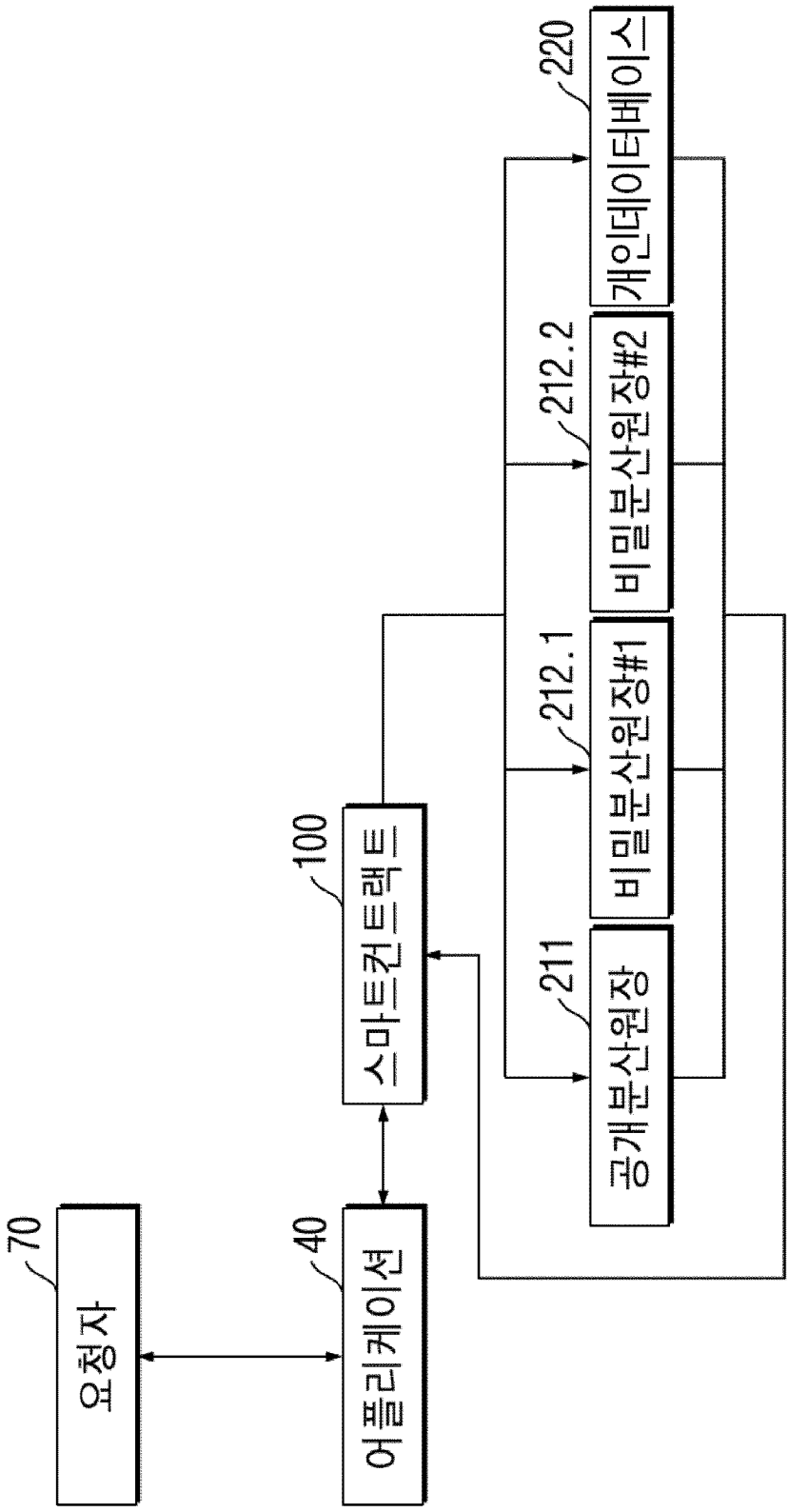
[도6]


공개분산원장
211
데이터공개분산원장
211.1
분산학습모델공유원장
211.2

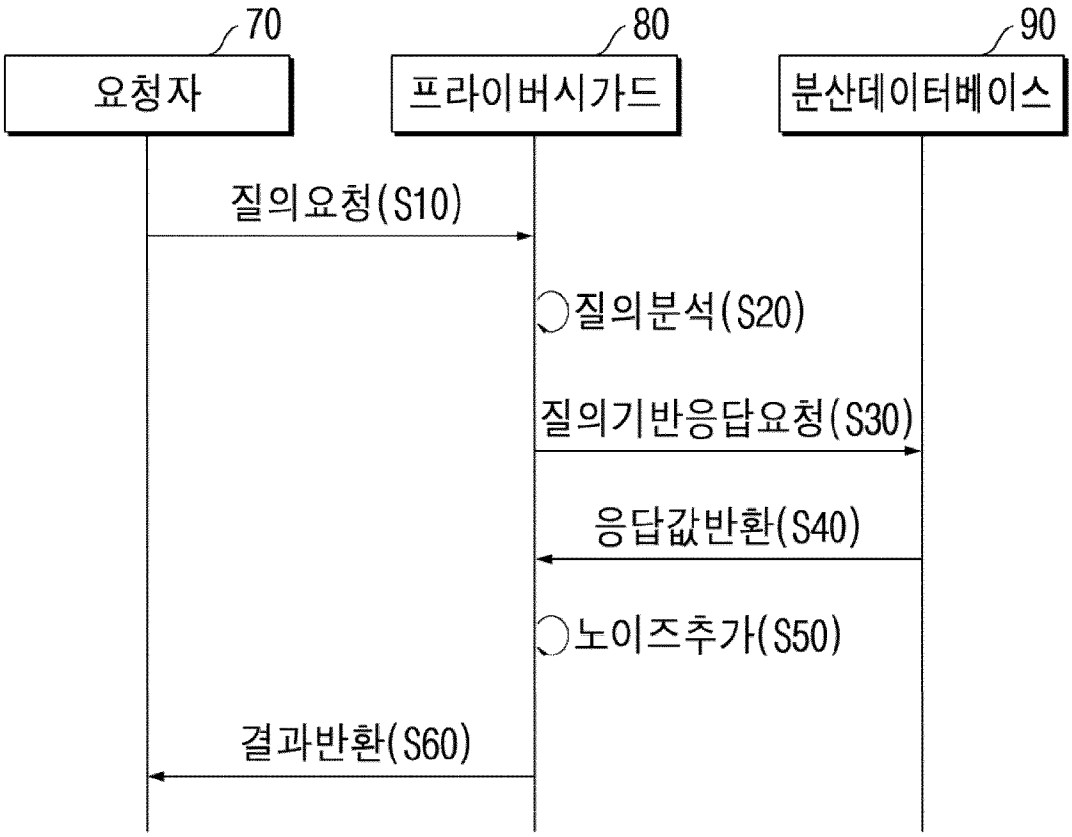
[도7]


노드A
10
스마트컨트랙트
100
분산데이터베이스
200
분산원장
210
공개분산원장
211
데이터공개분산원장
211.1
분산학습모델공유원장
211.2
비밀분산원장#1
212.1
비밀분산원장#2
212.2
개인데이터베이스
220
노드B
20
스마트컨트랙트
100
분산데이터베이스
200
분산원장
210
공개분산원장
211
데이터공개분산원장
211.1
분산학습모델공유원장
211.2
비밀분산원장#1
212.1
비밀분산원장#3
212.3
개인데이터베이스
220

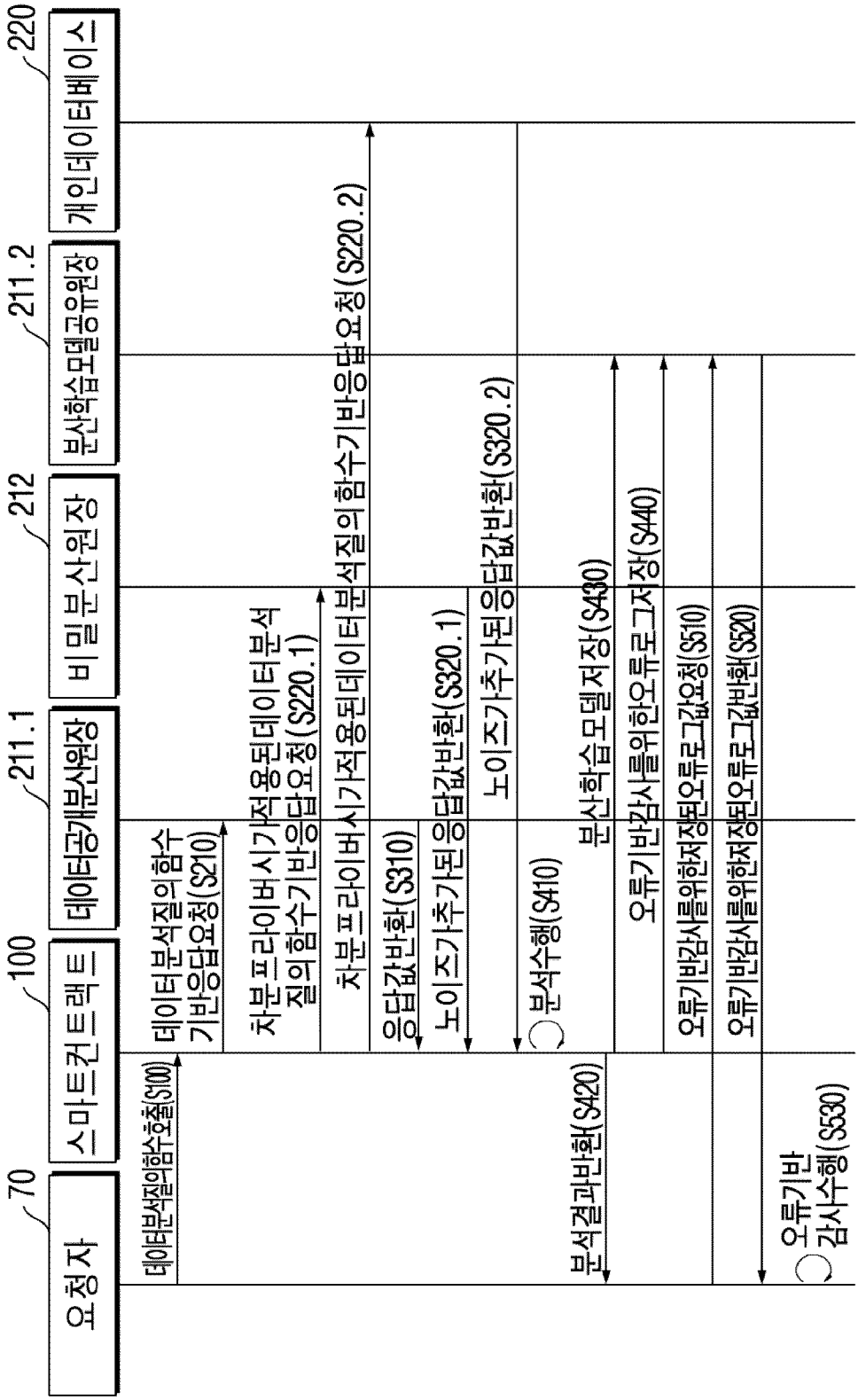
[도8]


70
요청자
40
어플리케이션
100
스마트컨트랙트
211
공개분산원장
212.1
비밀분산원장#1
212.2
비밀분산원장#2
220
개인데이터베이스

[도9]


70
80
90
요청자
프라이버시가드
분산데이터베이스
질의요청(S10)
질의분석(S20)
질의기반응답요청(S30)
응답값반환(S40)
노이즈추가(S50)
결과반환(S60)

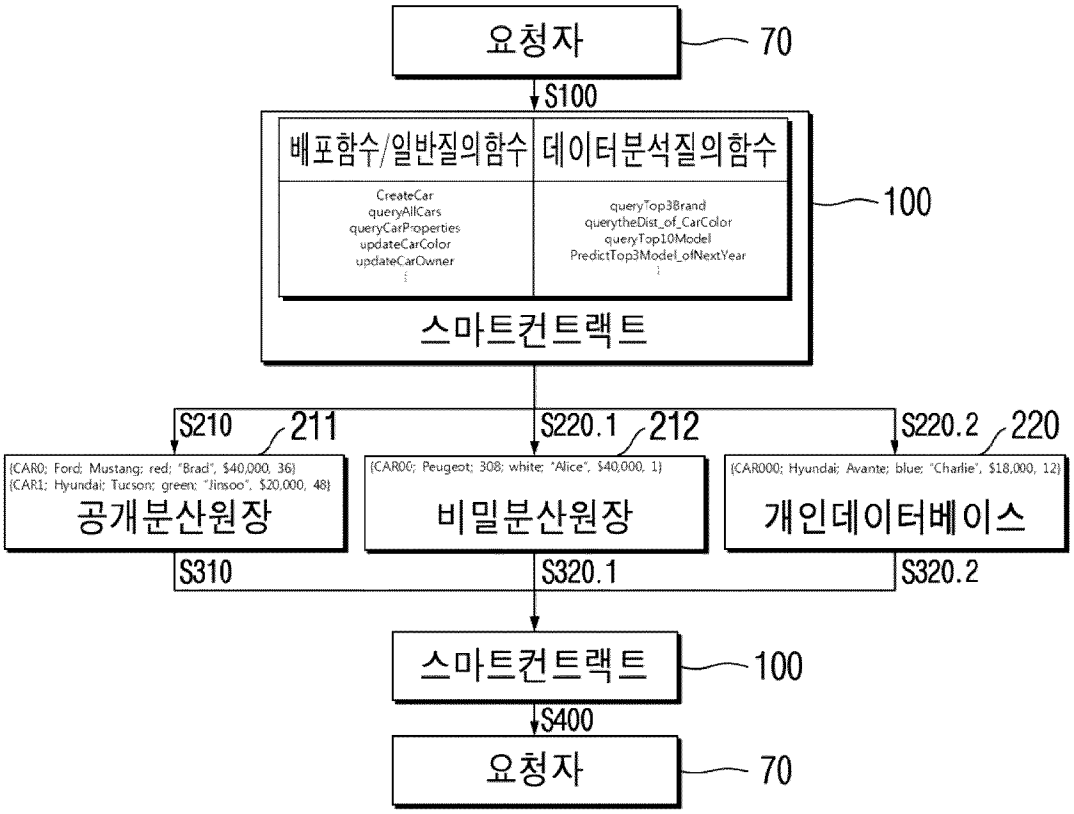
[도10]


70
요청자
100
스마트컨트랙트
211.1
데이터공개분산원장
212
비밀분산원장
211.2
분산학습모델공유원장
220
개인데이터베이스
데이터분석질의함수호출(S100)
데이터분석질의함수 기반응답요청(S210)
차분프라이버시가적용된데이터분석 질의함수기반응답요청(S220.1)
차분프라이버시가적용된데이터분석질의함수기반응답요청(S220.2)
응답값반환(S310)
노이즈가추가된응답값반환(S320.1)
노이즈가추가된응답값반환(S320.2)
분석수행(S410)
분산학습모델저장(S430)
분석결과반환(S420)
오류기반감사를위한오류로그저장(S440)
오류기반감사를위한저장된오류로그값요청(S510)
오류기반감사를위한저장된오류로그값반환(S520)
오류기반 감사수행(S530)

[도11]


70
10
20
211.2
요청자
노드A
노드B
분산학습모델공유원장
1라운드결과값저장요청(S441.1A)
1라운드모델및 오류값저장(S442.1A)
1라운드결과값 저장요청(S441.1B)
1라운드모델및 오류값저장(S442.1B)
i라운드결과값저장요청(S441.iA)
i라운드모델및 오류값저장(S442.iA)
i라운드결과값 저장요청(S441.iB)
i라운드모델및 오류값저장(S442.iB)
오류기반감사를위한저장된오류로그값요청(S510)
오류기반감사를위한저장된오류로그값반환(S520)
오류기반 감사수행(S530)

[도12]


요청자
70
S100
배포함수/일반질의함수
데이터분석질의함수
CreateCar
queryAllCars
queryCarProperties
updateCarColor
updateCarOwner
queryTop3Brand
querytheDist_of_CarColor
queryTop10Model
PredictTop3Model_ofNextYear
100
스마트컨트랙트
S210
211
S220.1
212
S220.2
220
{CAR0; Ford; Mustang; red; "Brad", $40,000, 36}
{CAR1; Hyundai; Tucson; green; "Jinsoo", $20,000, 48}
공개분산원장
{CAR00; Peugeot; 308; white; "Alice", $40,000, 1}
비밀분산원장
{CAR000; Hyundai; Avante; blue; "Charlie", $18,000, 12}
개인데이터베이스
S310
S320.1
S320.2
스마트컨트랙트
100
S400
요청자
70

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2019/006498

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/2452(2019.01)i, G06F 15/16(2006.01)i, G06F 16/2453(2019.01)i, G06F 21/62(2013.01)i, H04L 29/08(2006.01)i

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)

G06F 16/2452; G06F 16/00; G06F 17/30; G06F 21/30; G06F 21/60; G06F 21/62; G06F 15/16; G06F 16/2453; H04L 29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: blockchain, distributed ledger, smart contract, differential private, query

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-1946196 B1 (GRAPH BLOCKCHAIN LIMITED) 08 February 2019 See paragraphs [0047]-[0065] and figure 1.	1-10
A	금융보안원. 전자금융과 금융보안 (Financial Security Institute. E-Finance and Financial Security). no. 8, ISSN 2671-7093. 26 April 2017, Retrieved from the Internet: <URL: http://www.fsec.or.kr/user/bbs/fsec/146/313/bbsDataView/792.do?pag> See pages 10-30.	1-10
A	KR 10-2018-0095896 A (SONY CORPORATION) 28 August 2018 See paragraphs [0030]-[0049] and figures 1, 2.	1-10
A	US 2007-0143289 A1 (DWORK, Cynthia et al.) 21 June 2007 See paragraphs [0050]-[0053] and figure 3.	1-10
A	US 2016-0335455 A1 (TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)) 17 November 2016 See claims 30-39 and figure 2.	1-10
A	정강수 등. 차분 프라이버시 기반 비식별화 기술에 대한 연구. 정보보호학회지. vol. 28, no. 2, pages 61-77, April 2018, non-official translation (JUNG, Kangsoo et al. Research on Deidentification Technique Based on Differential Privacy. Review of KIISC). Retrieved from <URL: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07424024&language=ko_KR> See pages 61-77.	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* 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	Date of mailing of the international search report
20 DECEMBER 2019 (20.12.2019)	**20 DECEMBER 2019 (20.12.2019)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2019/006498

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1946196 B1	08/02/2019	US 2019-0295079 A1	26/09/2019
KR 10-2018-0095896 A	28/08/2018	AU 2016-377729 A1	26/07/2018
		CA 03009567 A1	29/06/2017
		CN 106911641 A	30/06/2017
		CN 108541318 A	14/09/2018
		EP 3396576 A1	31/10/2018
		JP 2019-500799 A	10/01/2019
		US 2019-0020661 A1	17/01/2019
		WO 2017-107976 A1	29/06/2017
		ZA 201804656 B	28/08/2019
US 2007-0143289 A1	21/06/2007	US 7698250 B2	13/04/2010
US 2016-0335455 A1	17/11/2016	US 10242229 B2	26/03/2019
		WO 2015-090445 A1	25/06/2015

국 제 조 사 보 고 서

국제출원번호
PCT/KR2019/006498

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 16/2452(2019.01)i, G06F 15/16(2006.01)i, G06F 16/2453(2019.01)i, G06F 21/62(2013.01)i, H04L 29/08(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 16/2452; G06F 16/00; G06F 17/30; G06F 21/30; G06F 21/60; G06F 21/62; G06F 15/16; G06F 16/2453; H04L 29/08

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 블록체인(block chain), 분산원장(distributed ledger), 스마트 컨트랙트(smart contract), 차분 프라이버시(differential private), 질의(query)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-1946196 B1 (그래프 블록체인 리미티드) 2019.02.08 단락 [0047]-[0065] 및 도면 1 참조.	1-10
A	금융보안원, `전자금융과 금융보안`, 제8호, ISSN 2671-7093, 2017.04.26, retrieved from the Internet: <URL: http://www.fsec.or.kr/user/bbs/fsec/146/313/bbsDataView/792.do?pag> 페이지 10-30 참조.	1-10
A	KR 10-2018-0095896 A (소니 주식회사) 2018.08.28 단락 [0030]-[0049] 및 도면 1, 2 참조.	1-10
A	US 2007-0143289 A1 (CYNTHIA DWORK 등) 2007.06.21 단락 [0050]-[0053] 및 도면 3 참조.	1-10
A	US 2016-0335455 A1 (TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)) 2016.11.17 청구항 30-39 및 도면 2 참조.	1-10
A	정강수 등, `차분 프라이버시 기반 비식별화 기술에 대한 연구`, 정보보호학회지 제28권 제2호, 페이지 61-77, 2018.04 <URL:https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07424024&language=ko_KR> 페이지 61-77 참조.	1-10

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"D" 본 국제출원에서 출원인이 인용한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2019년 12월 20일 (20.12.2019)	2019년 12월 20일 (20.12.2019)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
황찬윤
전화번호 +82-42-481-3347

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2019/006498

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1946196 B1	2019/02/08	US 2019-0295079 A1	2019/09/26
KR 10-2018-0095896 A	2018/08/28	AU 2016-377729 A1	2018/07/26
		CA 03009567 A1	2017/06/29
		CN 106911641 A	2017/06/30
		CN 108541318 A	2018/09/14
		EP 3396576 A1	2018/10/31
		JP 2019-500799 A	2019/01/10
		US 2019-0020661 A1	2019/01/17
		WO 2017-107976 A1	2017/06/29
		ZA 201804656 B	2019/08/28
US 2007-0143289 A1	2007/06/21	US 7698250 B2	2010/04/13
US 2016-0335455 A1	2016/11/17	US 10242229 B2	2019/03/26
		WO 2015-090445 A1	2015/06/25