



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년12월02일
(11) 등록번호 10-2046276
(24) 등록일자 2019년11월12일

- (51) 국제특허분류(Int. Cl.)
G06Q 50/10 (2012.01) H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
- (52) CPC특허분류
G06Q 50/10 (2013.01)
H04L 9/0838 (2013.01)
- (21) 출원번호 10-2019-0004886
- (22) 출원일자 2019년01월14일
심사청구일자 2019년01월14일
- (56) 선행기술조사문헌
KR1020030028695 A*
KR1020170136724 A*
*는 심사관에 의하여 인용된 문헌

- (73) 특허권자
임현진
서울특별시 금천구 독산로28나길 14-26 (시흥동)
- (72) 발명자
임현진
서울특별시 금천구 독산로28나길 14-26 (시흥동)
- (74) 대리인
김남혁

전체 청구항 수 : 총 9 항

심사관 : 배상진

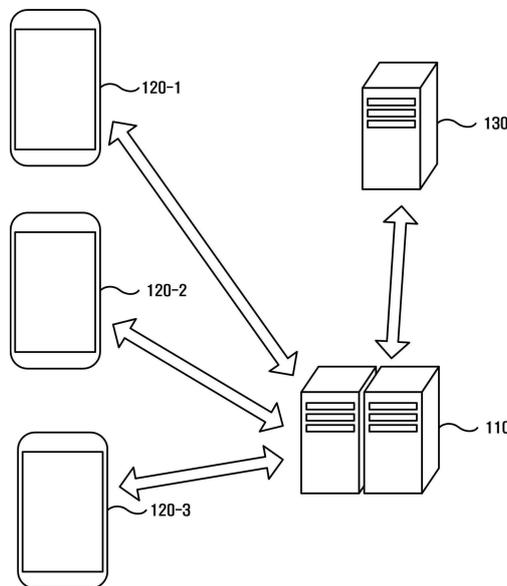
(54) 발명의 명칭 복수의 사용자의 동의 여부를 판단하여 하나의 서비스를 제공하는 서비스 제공 방법 및 장치

(57) 요약

복수의 사용자의 동의 여부를 판단하여 하나의 서비스를 제공하는 서비스 제공 방법 및 장치가 개시된다. 본 발명의 일 실시예에 따른 서비스 제공 장치는, n(n은 2이상의 자연수)개의 단말 각각에 대응되는 n개의 비밀키를 저장하는 메모리 - 상기 n개의 비밀키는, 상기 n개의 단말이 공동으로 서비스를 수행할 수 있는 서비스에 대하여

(뒷면에 계속)

대표도 - 도1



서비스를 수행하기 위한 비밀키 및 상기 n개의 단말 중 제1 단말로부터 상기 서비스를 수행하기 위한 서비스 수행 요청이 수신되면, 상기 제1 단말에 대해 전자 서명 요청 메시지를 전송하여 상기 제1 단말로부터 상기 제1 단말에서 생성된 제1 전자 서명 값을 수신하고, 수신된 상기 제1 전자 서명 값에 대한 검증을 수행하고, 상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 n개의 단말 중 상기 제1 단말을 제외한 나머지 단말들에 대해 전자 서명 요청 메시지를 전송하여 상기 나머지 단말들로부터 상기 나머지 단말들에서 각각 생성된 전자 서명 값들을 수신하고, 상기 수신된 나머지 단말들로부터 각각 수신된 전자 서명 값에 대한 검증을 수행하고, 상기 나머지 단말로부터 각각 수신된 전자 서명 값에 대한 검증이 완료되면, 상기 n개의 단말에 대해 상기 n개의 비밀키들 중 서로 다른 어느 하나의 비밀키 및 상기 서비스 수행에 대한 동의 여부 메시지를 요청하고, 기 설정된 시간 내에 상기 n개의 단말 모두로부터 비밀키 및 동의 여부 메시지를 수신하면, 상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하는지 여부를 확인하고, 상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하고, 상기 n개의 단말로 모두로부터 상기 서비스 수행을 동의한다는 메시지를 수신하면, 상기 서비스를 수행하고, 상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하지 않으면, 상기 비밀키 및 동의 여부 메시지를 재요청하는 프로세서를 포함하고, 상기 프로세서는, 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단한다.

(52) CPC특허분류

H04L 9/0894 (2013.01)

H04L 9/3247 (2013.01)

H04L 2209/56 (2013.01)

명세서

청구범위

청구항 1

n (n 은 2이상의 자연수)개의 단말 각각에 대응되는 n 개의 비밀키를 저장하는 메모리; - 상기 n 개의 비밀키는, 상기 n 개의 단말이 공동으로 서비스를 수행할 수 있는 서비스에 대하여 서비스를 수행하기 위한 비밀키-, 및

상기 n 개의 단말 중 제1 단말로부터 상기 서비스를 수행하기 위한 서비스 수행 요청이 수신되면, 상기 제1 단말에서 생성된 전자 서명값을 바탕으로 상기 제1 단말에 대한 인증을 수행하고,

상기 제1 단말의 인증이 완료되면, 상기 n 개의 단말에 대해 상기 n 개의 비밀키들 중 서로 다른 어느 하나의 비밀키 및 상기 서비스 수행에 대한 동의 여부 메시지를 요청하고,

기 설정된 시간 내에 상기 n 개의 단말 모두로부터 비밀키 및 동의 여부 메시지를 수신하면, 상기 n 개의 단말로부터 수신한 n 개의 비밀키 각각이 상기 메모리에 저장된 상기 n 개의 비밀키와 일치하는지 여부를 확인하고,

상기 n 개의 단말로부터 수신한 n 개의 비밀키 각각이 상기 메모리에 저장된 상기 n 개의 비밀키와 일치하고, 상기 n 개의 단말 모두로부터 상기 서비스 수행을 동의한다는 메시지를 수신하면, 상기 서비스를 수행하고,

상기 n 개의 단말로부터 수신한 n 개의 비밀키 각각이 상기 메모리에 저장된 상기 n 개의 비밀키와 일치하지 않으면, 상기 비밀키 및 동의 여부 메시지를 재요청하는 프로세서;를 포함하고,

상기 프로세서는,

기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하고,

상기 n 개의 단말 각각으로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지를 요청한 시점부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지를 수신한 시점에 대한 시간 정보 및 상기 n 개의 단말 각각에 대한 사용 환경 정보를 입력 데이터로 인공 지능 모델에 입력하여, 상기 기 설정된 시간을 결정하는 것을 특징으로 하는 서비스 제공 장치.

청구항 2

제1항에 있어서,

상기 서비스는

하나의 공용 계좌를 복수의 사용자가 사용하기 위한 बैं킹 서비스, 하나의 직불 카드 또는 신용 카드를 복수의 사용자가 사용하는 결제 서비스, 하나의 인터넷 서비스를 복수의 사용자가 사용하는 인터넷 서비스, 하나의 유료 서비스를 복수의 사용자가 사용하는 유료 서비스, 하나의 유료 회원제 구매 카드를 복수의 사용자가 사용하기 위한 회원제 서비스 중 적어도 하나인 것을 특징으로 하는 서비스 제공 장치.

청구항 3

제1항에 있어서,

상기 프로세서는,

기 설정된 시간 내에 상기 n 개의 단말로부터, 상기 n 개의 단말이 상기 전자 서명 요청 메시지 또는 상기 비밀키 및 동의 여부 메시지 확인하였다는 제어 신호를 수신한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하고,

기 설정된 시간 내에 상기 n 개의 단말로부터, 상기 n 개의 단말이 상기 전자 서명 요청 메시지 또는 상기 비밀키 및 동의 여부 메시지 확인하였다는 제어 신호를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 미동의한 것으로 판단하는 서비스 제공 장치

청구항 4

제1항에 있어서,

상기 프로세서는,

상기 n개의 단말 각각에 제1 인덱스 또는 제2 인덱스 중 하나를 전송하고,

기 설정된 시간 내에 상기 제1 인덱스를 전송한 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 미동의한 것으로 판단하고,

기 설정된 시간 내에 상기 제2 인덱스를 전송한 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하는 것을 특징으로 하는 서비스 제공 장치.

청구항 5

제 1항에 있어서,

상기 프로세서는,

상기 제1 단말로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 비용 이상이고, 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 미동의한 것으로 판단하고,

상기 제1 단말로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 비용 이하이고, 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하는 서비스 제공 장치.

청구항 6

제1항에 있어서,

상기 서비스는 상기 n개의 단말에 대응되는 각각의 사용자들이 공동으로 소유하고 있는 공용 계좌에 대한 대금 이체 서비스이고,

상기 프로세서는,

상기 n개의 단말 중 적어도 하나의 단말로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 상태로 상기 대금 이체 서비스가 완료되고, 상기 대금 이체 수행 후 상기 적어도 하나의 단말로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 서비스 제공 미동의 메시지를 수신한 경우, 상기 제1 단말의 사용자의 개인 계좌에서 상기 대금 이체 서비스에 대응되는 대금을 상기 공용 계좌로 입금하는 것을 특징으로 하는 서비스 제공 장치.

청구항 7

제1항에 있어서,

상기 기 설정된 시간은, 상기 n개의 단말로부터 수신한 과거 응답 시간을 바탕으로 결정되는 것을 특징으로 하는 서비스 제공 장치.

청구항 8

삭제

청구항 9

n개의 단말 중 제1 단말로부터 서비스를 수행하기 위한 서비스 수행 요청이 수신되면, 상기 제1 단말에 대해 전자 서명 요청 메시지를 전송하여 상기 제1 단말로부터 상기 제1 단말에서 생성된 제1 전자 서명 값을 수신하고,

수신된 상기 제1 전자 서명 값에 대한 검증을 수행하는 단계;

상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 n개의 단말 중 상기 제1 단말을 제외한 나머지 단말들에 대해 전자 서명 요청 메시지를 전송하여 상기 나머지 단말들로부터 상기 나머지 단말들에서 각각 생성된 전자 서명 값들을 수신하고, 상기 수신된 나머지 단말들로부터 각각 수신된 전자 서명 값에 대한 검증을 수행하는 단계;

상기 나머지 단말로부터 각각 수신된 전자 서명 값에 대한 검증이 완료되면, 상기 n개의 단말에 대해 n개의 비밀키들 중 서로 다른 어느 하나의 비밀키 및 상기 서비스 수행에 대한 동의 여부 메시지를 요청하는 단계 - 상기 n개의 비밀키는, 상기 n개의 단말이 공동으로 서비스를 수행할 수 있는 서비스에 대하여 서비스를 수행하기 위한 비밀키;

기 설정된 시간 내에 상기 n개의 단말 모두로부터 비밀키 및 동의 여부 메시지를 수신하면, 상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하는지 여부를 확인하는 단계;

상기 n개의 단말로부터 수신한 상기 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하고, 상기 n개의 단말 모두로부터 상기 서비스 수행을 동의한다는 메시지를 수신하면, 상기 서비스를 수행하는 단계;

상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하지 않으면, 상기 비밀키 및 동의 여부 메시지를 재요청하는 단계;

기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하는 단계;를 포함하고,

상기 기 설정된 시간은, 상기 n개의 단말 각각으로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지를 요청한 시점부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지를 수신한 시점에 대한 시간 정보 및 상기 n개의 단말 각각에 대한 사용 환경 정보를 입력 데이터로 인공 지능 모델에 입력하여 결정되는 것을 특징으로 하는 서비스 제공 방법.

청구항 10

하드웨어인 컴퓨터와 결합되어, 제9항의 방법을 수행할 수 있도록 컴퓨터에서 독출 가능한 기록매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 복수의 사용자의 동의 여부를 판단하여 하나의 서비스를 제공하는 서비스 제공 방법 및 장치에 관한 것으로, 보다 상세하게는, 하나의 서비스를 복수의 사용자가 함께 이용하는 경우, 서비스 수행에 대한 복수의 사용자의 동의를 얻는 방법에 관한 것이다.

배경 기술

[0002] 종래에는 하나의 서비스는 하나의 사용자만 사용하는 것이 일반적이었으나, 근래 들어, 하나의 서비스에 대하여 복수의 사용자가 서비스를 사용할 수 있는 서비스 제공 방법들이 개시되고 있다.

[0003] 이때, 한명의 사용자가 서비스를 사용하는 것이 다른 사용자에게 피해가 될 수 있는 서비스의 경우, 하나의 사용자가 서비스를 사용할 때 다른 사용자의 동의를 얻음으로써 서비스를 사용하지 않는 사용자들의 피해를 방지할 수 있다.

[0004] 예컨대 공개특허공보 제10-2017-0136724호에 개시된 바와 같이, 제공되는 서비스가 공용 계좌 기반의 대금 이체 서비스인 경우, 하나의 사용자는 다른 사용자의 동의를 얻는 경우에만 대금을 이체할 수 있을 것이다.

[0005] 그러나, 서비스를 이용하지 않는 사용자의 보호와는 별개로, 서비스를 이용하지 않는 사용자가 서비스 사용에 대한 동의 의사 또는 미동의 의사 자체를 표현하지 않는 경우, 서비스를 사용하고자 하는 하나의 사용자에게 불

측의 피해를 줄 가능성 또한 존재한다.

[0006] 따라서, 서비스를 사용하고자 하는 사용자 및 서비스를 사용하지 않는 사용자를 모두 보호할 수 있는 방법의 필요성이 요구되고 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 공개특허공보 제10-2017-0136724호, 2017.12.12

발명의 내용

해결하려는 과제

[0008] 본 발명이 해결하고자 하는 과제는 서비스를 사용하고자 하는 사용자 및 서비스를 사용하지 않는 사용자를 모두 보호할 수 있는 방법을 제공하는 것이다.

[0009] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 상술한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 서비스 제공 장치는, n (n 은 2이상의 자연수)개의 단말 각각에 대응되는 n 개의 비밀키를 저장하는 메모리 - 상기 n 개의 비밀키는, 상기 n 개의 단말이 공동으로 서비스를 수행할 수 있는 서비스에 대하여 서비스를 수행하기 위한 비밀키 및 상기 n 개의 단말 중 제1 단말로부터 상기 서비스를 수행하기 위한 서비스 수행 요청이 수신되면, 상기 제1 단말에 대해 전자 서명 요청 메시지를 전송하여 상기 제1 단말로부터 상기 제1 단말에서 생성된 제1 전자 서명 값을 수신하고, 수신된 상기 제1 전자 서명 값에 대한 검증을 수행하고, 상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 n 개의 단말 중 상기 제1 단말을 제외한 나머지 단말들에 대해 전자 서명 요청 메시지를 전송하여 상기 나머지 단말들로부터 상기 나머지 단말들에서 각각 생성된 전자 서명 값들을 수신하고, 상기 수신된 나머지 단말들로부터 각각 수신된 전자 서명 값에 대한 검증을 수행하고, 상기 나머지 단말로부터 각각 수신된 전자 서명 값에 대한 검증이 완료되면, 상기 n 개의 단말에 대해 상기 n 개의 비밀키들 중 서로 다른 어느 하나의 비밀키 및 상기 서비스 수행에 대한 동의 여부 메시지를 요청하고, 기 설정된 시간 내에 상기 n 개의 단말 모두로부터 비밀키 및 동의 여부 메시지를 수신하면, 상기 n 개의 단말로부터 수신한 n 개의 비밀키 각각이 상기 메모리에 저장된 상기 n 개의 비밀키와 일치하는지 여부를 확인하고, 상기 n 개의 단말로부터 수신한 n 개의 비밀키 각각이 상기 메모리에 저장된 상기 n 개의 비밀키와 일치하고, 상기 n 개의 단말로 모두로부터 상기 서비스 수행을 동의한다는 메시지를 수신하면, 상기 서비스를 수행하고, 상기 n 개의 단말로부터 수신한 n 개의 비밀키 각각이 상기 메모리에 저장된 상기 n 개의 비밀키와 일치하지 않으면, 상기 비밀키 및 동의 여부 메시지를 재요청하는 프로세서를 포함하고, 상기 프로세서는, 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단한다.

[0011] 이때, 상기 프로세서는, 기 설정된 시간 내에 상기 n 개의 단말로부터, 상기 n 개의 단말이 상기 전자 서명 요청 메시지 또는 상기 비밀키 및 동의 여부 메시지 확인하였다는 제어 신호를 수신한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하고, 기 설정된 시간 내에 상기 n 개의 단말로부터, 상기 n 개의 단말이 상기 전자 서명 요청 메시지 또는 상기 비밀키 및 동의 여부 메시지 확인하였다는 제어 신호를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 미동의한 것으로 판단할 수 있다.

[0012] 이때, 상기 프로세서는, 상기 n 개의 단말 각각에 제1 인덱스 또는 제2 인덱스 중 하나를 전송하고, 기 설정된 시간 내에 상기 제1 인덱스를 전송한 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 미동의한 것으로 판단하고, 기 설정된 시간 내에 상기 제2 인덱스를 전송한 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하는 것을 특징으로 할 수 있다.

- [0013] 이때, 상기 프로세서는, 상기 제1 단말로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 비용 이상이고, 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 미동의한 것으로 판단하고, 상기 제1 단말로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 비용 이하이고, 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단할 수 있다.
- [0014] 이때, 상기 서비스는 상기 n개의 단말에 대응되는 각각의 사용자들이 공동으로 소유하고 있는 공용 계좌에 대한 대금 이체 서비스이고, 상기 프로세서는, 상기 n개의 단말 중 적어도 하나의 단말로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 상태로 상기 대금 이체 서비스가 완료되고, 상기 대금 이체 수행 후 상기 적어도 하나의 단말로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 서비스 제공 미동의 메시지를 수신한 경우, 상기 제1 단말의 사용자의 개인 계좌에서 상기 대금 이체 서비스에 대응되는 대금을 상기 공용 계좌로 입금할 수 있다.
- [0015] 이때, 상기 기 설정된 시간은, 상기 n개의 단말로부터 수신한 과거 응답 시간을 바탕으로 결정될 수 있다.
- [0016] 이때, 상기 프로세서는, 상기 n개의 단말 각각으로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지를 요청한 시점부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지를 수신한 시점에 대한 시간 정보 및 상기 n개의 단말 각각에 대한 사용 환경 정보를 입력 데이터로 인공 지능 모델에 입력하여, 상기 기 설정된 시간을 결정할 수 있다.
- [0017] 한편, 상술한 과제를 해결하기 위한 본 발명의 또 다른 실시예에 따른 서비스 제공 방법은, n개의 단말 중 제1 단말로부터 상기 서비스를 수행하기 위한 서비스 수행 요청이 수신되면, 상기 제1 단말에 대해 전자 서명 요청 메시지를 전송하여 상기 제1 단말로부터 상기 제1 단말에서 생성된 제1 전자 서명 값을 수신하고, 수신된 상기 제1 전자 서명 값에 대한 검증을 수행하는 단계, 상기 제1 전자 서명 값에 대한 검증이 완료되면, 상기 n개의 단말 중 상기 제1 단말을 제외한 나머지 단말들에 대해 전자 서명 요청 메시지를 전송하여 상기 나머지 단말들로부터 상기 나머지 단말들에서 각각 생성된 전자 서명 값들을 수신하고, 상기 수신된 나머지 단말들로부터 각각 수신된 전자 서명 값에 대한 검증을 수행하는 단계, 상기 나머지 단말로부터 각각 수신된 전자 서명 값에 대한 검증이 완료되면, 상기 n개의 단말에 대해 n개의 비밀키들 중 서로 다른 어느 하나의 비밀키 및 상기 서비스 수행에 대한 동의 여부 메시지를 요청하는 단계 - 상기 n개의 비밀키는, 상기 n개의 단말이 공동으로 서비스를 수행할 수 있는 서비스에 대하여 서비스를 수행하기 위한 비밀키-, 기 설정된 시간 내에 상기 n개의 단말 모두로부터 비밀키 및 동의 여부 메시지를 수신하면, 상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하는지 여부를 확인하는 단계, 상기 n개의 단말로부터 수신한 상기 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하고, 상기 n개의 단말로 모두로부터 상기 서비스 수행을 동의한다는 메시지를 수신하면, 상기 서비스를 수행하는 단계, 상기 n개의 단말로부터 수신한 n개의 비밀키 각각이 상기 메모리에 저장된 상기 n개의 비밀키와 일치하지 않으면, 상기 비밀키 및 동의 여부 메시지를 재요청하는 단계 및 기 설정된 시간 내에 상기 나머지 단말들 중 적어도 하나로부터 상기 전자 서명 값, 상기 비밀키 값 및 상기 동의 여부 메시지 중 적어도 하나를 수신하지 못한 경우, 상기 제1 단말의 서비스 수행 요청에 동의한 것으로 판단하는 단계를 포함한다.
- [0018] 한편, 상술한 과제를 해결하기 위한 본 발명의 또 다른 실시예에 따른 컴퓨터 프로그램은, 하드웨어인 컴퓨터와 결합되어, 제8항의 방법을 수행할 수 있도록 컴퓨터에서 독출 가능한 기록매체에 저장된다.
- [0019] 본 발명의 기타 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

- [0020] 개시된 실시예에 따른 서비스 제공 장치는, 서비스를 사용하고자 하는 사용자 및 서비스를 사용하지 않는 사용자를 모두 보호할 수 있는 효과가 있다.
- [0021] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [0022] 도 1 및 도 2는 본 발명의 일 실시예에 따른 기본적인 서비스 제공 방법을 설명하기 위한 예시도이다.
 도 3은 본 발명의 일 실시예에 따른 서비스 수행 방법을 간략히 도시한 흐름도이다.
 도 4는 기 설정된 시간 내에 응답이 없는 경우, 제1 단말의 서비스 요청에 대해 묵시적으로 동의하여 서비스를 수행하는 것으로 처리하는 방법을 설명하기 위한 흐름도이다.
 도 5 내지 도 7은 본 발명의 일 실시예에 따른 묵시적 동의 여부를 판단하는 또 다른 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.
- [0024] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.
- [0025] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0026] 명세서에서 사용되는 "부" 또는 "모듈"이라는 용어는 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, "부" 또는 "모듈"은 어떤 역할들을 수행한다. 그렇지만 "부" 또는 "모듈"은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부" 또는 "모듈"은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 "부" 또는 "모듈"은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 "부" 또는 "모듈"들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 "부" 또는 "모듈"들로 결합되거나 추가적인 구성요소들과 "부" 또는 "모듈"들로 더 분리될 수 있다.
- [0027] 공간적으로 상대적인 용어인 "아래(below)", "아래(beneath)", "하부(lower)", "위(above)", "상부(upper)" 등은 도면에 도시되어 있는 바와 같이 하나의 구성요소와 다른 구성요소들과의 상관관계를 용이하게 기술하기 위해 사용될 수 있다. 공간적으로 상대적인 용어는 도면에 도시되어 있는 방향에 더하여 사용시 또는 동작시 구성요소들의 서로 다른 방향을 포함하는 용어로 이해되어야 한다. 예를 들어, 도면에 도시되어 있는 구성요소를 뒤집을 경우, 다른 구성요소의 "아래(below)"또는 "아래(beneath)"로 기술된 구성요소는 다른 구성요소의 "위(above)"에 놓여질 수 있다. 따라서, 예시적인 용어인 "아래"는 아래와 위의 방향을 모두 포함할 수 있다. 구성요소는 다른 방향으로도 배향될 수 있으며, 이에 따라 공간적으로 상대적인 용어들은 배향에 따라 해석될 수 있다.
- [0028] 본 명세서에서, 단말 또는 장치는 적어도 하나의 프로세서를 포함하는 모든 종류의 하드웨어 장치를 의미하는 것이고, 실시 예에 따라 해당 하드웨어 장치에서 동작하는 소프트웨어적 구성도 포괄하는 의미로서 이해될 수 있다. 예를 들어, 단말 또는 장치는 스마트폰, 태블릿 PC, 데스크톱, 노트북, 서버 및 각 장치에서 구동되는 사용자 클라이언트 및 애플리케이션을 모두 포함하는 의미로서 이해될 수 있으며, 또한 이에 제한되는 것은 아니다.

- [0029] 본 개시에서 사용되는 전자 서명 값 검증은 인증과 동일하거나 유사한 의미로 혼용될 수 있다.
- [0030] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [0031] 본 명세서에서 설명되는 각 단계들은 스마트폰 또는 서버에 의하여 수행되는 것으로 설명되나, 각 단계의 주체는 이에 제한되는 것은 아니며, 실시 예에 따라 각 단계들의 적어도 일부가 서로 다른 장치에서 수행될 수도 있다.
- [0032] 도 1 및 도 2는 본 발명의 일 실시예에 따른 기본적인 서비스 제공 방법을 설명하기 위한 예시도이다.
- [0033] 도 1은 본 발명의 일 실시예에 따른, 서비스 제공 장치를 설명하기 위한 전체 시스템을 설명하기 위한 예시도이다.
- [0034] 도 1에 도시된 바와 같이, 서비스 제공 시스템은, 서비스 제공 장치(110), 복수의 단말(120-1 내지 120-3) 및 공개키 검증 서버를 포함할 수 있다. 도 1에서는 복수의 단말이 3개인 것으로 설명하나 2개 또는 3개 이상의 단말로 구성될 수 있음은 물론이다. 다만, 설명의 편의를 위해 본 발명에서는 복수의 단말이 3개의 단말인 경우를 예로 하여 설명한다.
- [0035] 서비스 제공 장치(110)는 메모리 및 프로세서를 포함할 수 있다. 프로세서는 프로세서 내부에서 처리되는 신호(또는, 데이터)를 일시적 및/또는 영구적으로 저장하는 램(RAM: Random Access Memory, 미도시) 및 롬(ROM: Read-Only Memory, 미도시)을 더 포함할 수 있다. 또한, 프로세서는 그래픽 처리부, 램 및 롬 중 적어도 하나를 포함하는 시스템온칩(SoC: system on chip) 형태로 구현될 수 있다. 메모리에는 프로세서의 처리 및 제어를 위한 프로그램들(하나 이상의 인스트럭션들)을 저장할 수 있다. 메모리에 저장된 프로그램들은 기능에 따라 복수 개의 모듈들로 구분될 수 있다.
- [0036] 이때, 메모리는 복수의 단말의 개수와 같은 개수인 3개의 서로 다른 비밀키를 저장할 수 있다. 서비스 제공 장치(110)는 3개의 서로 다른 비밀키 각각을 3개의 단말(120-1 내지 120-3)에 전송할 수 있다.
- [0037] 한편, 복수의 단말(120-1 내지 120-3)은 인증에 필요한 개인키, 개인키에 대응되는 공개키 및 서비스 제공 장치(110)로부터 수신한 비밀키를 저장하고 있을 수 있다. 설명의 편의 상 제1 단말(120-1)은 제1 개인키, 제1 공개키 및 제1 비밀키를, 제2 단말(120-2)은 제2 개인키, 제2 공개키 및 제2 비밀키를, 제3 단말(120-3)은 제3 개인키, 제3 공개키 및 제3 비밀키를 저장하고 있다고 가정한다.
- [0038] 일 실시예로, 서비스 제공 장치(110)가 제1 단말(120-1)로부터 서비스 수행 요청을 수신하면, 서비스 제공 장치(110)는 제1 단말(120-1)에서 생성된 전자 서명 값을 바탕으로 제1 단말(120-1)에 대한 인증을 수행할 수 있다. 구체적으로, 서비스 제공 장치(110)가 제1 단말(120-1)로부터 서비스 수행 요청을 수신한 경우, 서비스 제공 장치(110)는 요청된 서비스에 대응하는 데이터를 특정 해시 함수의 입력값으로 인가하여 해시 값을 생성하고, 생성된 해시 값을 제1 단말(120-1)로 전송하여 전자 서명을 요청할 수 있다. 이때 서비스에 대응하는 데이터는 서비스의 종류에 대한 정보, 서비스에 필요한 비용 정보, 서비스 제공자에 대한 정보 등을 포함할 수 있다.
- [0039] 제1 단말(120-1)은 제1 개인키를 이용하여 해시값을 암호화 하여 이용하여 제1 전자 서명 값을 생성하고, 생성된 제1 전자 서명 값 및 제1 공개키를 서비스 제공 장치(110)로 전송할 수 있다.
- [0040] 서비스 제공 장치(110)는 공개키 검증 서버(130)에게 제1 단말(120-1)로부터 수신한 제1 공개키의 검증을 요청하고, 검증 결과 제1 공개키가 공개키 검증 서버(130)에서 제공된 것이 확인되면, 제1 공개키를 기초로 제1 전자 서명 값을 복호화 하고, 복호화된 값이 제1 단말로 전송된 해시 값과 동일한지 여부를 검증할 수 있다.
- [0041] 상기 검증이 완료되면, 서비스 제공 장치(110)는 제2 단말(120-2) 및 제3 단말(120-3)로 제1 단말(120-1)로 전송한 해시값과 동일한 해시값을 전송할 수 있다.
- [0042] 제2 단말 및 제3 단말(120-2, 120-3)은 제1 단말(120-1)의 검증 확인 방법과 동일한 방법을 통해 인증을 완료할 수 있다. 다만, 필수적인 과정은 아니며, 경우에 따라 생략될 수 있음은 물론이다. 즉, 제2 단말(102-2)(제3 단말(120-3))은 제2 개인키(제3 개인키)를 이용하여 해시값을 암호화 하여 이용하여 제2 전자 서명 값(제3 전자 서명 값)을 생성하고, 생성된 제2 전자 서명 값(제3 전자 서명 값) 및 제2 공개키(제3 공개키)를 서비스 제공 장치(110)로 전송할 수 있다. 서비스 제공 장치(110)는 공개키 검증 서버(130)에게 제2 단말(120-2)(제3 단말(120-3))로부터 수신한 제2 공개키(제3 공개키)의 검증을 요청하고, 검증 결과 제2 공개키(제3 공개키)가 공개키 검증 서버(130)에서 제공된 것이 확인되면, 제2 공개키(제3 공개키)를 기초로 제2 전자 서명 값(제3 전자 서명 값)을 복호화 하고, 복호화된 값이 제1 단말로 전송된 해시 값과 동일한지 여부를 검증할 수 있다.

- [0043] 인증이 완료되면, 서비스 제공 장치(110)는 각각의 단말들에게 비밀키의 전송을 요청할 수 있다. 각각의 단말은 메모리에 저장된 비밀키 및 서비스 수행에 대한 동의 여부 메시지를 서비스 제공 장치(110)로 전송할 수 있다.
- [0044] 구체적으로, 제1 단말(120-1)은 제1 비밀키 및 서비스 수행에 대한 동의 여부 메시지를 서비스 제공 장치(110)로 전송하고, 제2 단말(120-2)은 제2 비밀키 및 서비스 수행에 대한 동의 여부 메시지를 서비스 제공 장치(110)로 전송하고, 제3 단말(120-3)은 제3 비밀키 및 서비스 수행에 대한 동의 여부 메시지를 서비스 제공 장치(110)로 전송할 수 있다. 이때, 최초 서비스 수행을 요청한 제1 단말(120-1)은 서비스 수행에 대한 동의 여부 메시지를 전송하지 않을 수 있음은 물론이다.
- [0045] 서비스 제공 장치(110)는 각각의 단말들로부터 수신된 비밀키 각각이 메모리에 저장된 비밀키와 동일한지 여부를 확인할 수 있다. 동일한 경우, 서비스 제공 장치(110)는 각각의 단말로부터 수신한 메시지 동의 여부를 바탕으로 서비스를 수행할지 여부를 판단할 수 있다. 동일하지 않은 경우, 서비스 제공 장치(110)는 서비스 수행을 보류하거나, 동일하지 않은 비밀키를 전송한 단말에게 비밀키가 틀렸음을 안내하는 메시지를 전송할 수 있다.
- [0047] 도 2는 본 발명의 일 실시예에 따른 서비스 제공 장치의 구성을 상세히 도시한 블록도이다.
- [0048] 도 2에 도시된 바와 같이, 서비스 제공 장치(110)는 비밀키 저장부(211), 제1 전자 서명 요청부(212), 제1 전자 서명 수신부(213), 제1 전자 서명 검증부(214), 제2 전자 서명 요청부(215), 제2 전자 서명 수신부(216), 제2 전자 서명 검증부(217), 비밀키 전송 요청부(218) 및 서비스 수행 결정부(219)를 포함할 수 있다. 구체적으로, 각각의 구성은 프로그램의 형태로 메모리에 저장되어 프로세서에 의해 동작할 수 있다.
- [0049] 제1 전자 서명 요청부(212), 제1 전자 서명 수신부(213) 및 제1 전자 서명 검증부(214)는 서비스 수행 요청을 하는 단말(본 예서는 제1 단말(120-1)로 설명한다)의 전자 서명 값 검증을 위한 구성이며, 제2 전자 서명 요청부(215), 제2 전자 서명 수신부(216), 제2 전자 서명 검증부(217)는 나머지 단말의 전자 서명 값 검증을 위한 구성이다. 필요에 따라, 제1 전자 서명 요청부(212), 제1 전자 서명 수신부(213), 제1 전자 서명 검증부(214) 및 제2 전자 서명 요청부(215), 제2 전자 서명 수신부(216), 제2 전자 서명 검증부(217)는 하나의 전자 서명 요청부, 전자 서명 수신부 및 전자 서명 검증부로 구성되거나, 각각의 단말에 대응되는 복수의 전자 서명 요청부, 전자 서명 수신부 및 전자 서명 검증부로 구성될 수 있음은 물론이다.
- [0050] 비밀키 전송 요청부(218)는 나머지 단말의 전자 서명 값 검증이 완료되면, 복수의 단말(120-1 내지 120-3)에게 비밀키 전송을 요청하기 위한 구성이며, 서비스 수행 결정부(219)는 복수의 단말(120-1 내지 120-3)으로부터 올바른 비밀키가 전송되면, 복수의 단말(120-1 내지 120-3)이 비밀키와 함께 전송한 서비스 수행 동의 여부 메시지의 내용을 바탕으로 서비스 수행 여부를 결정할 수 있다. 예를 들어, 복수의 단말(120-1 내지 120-3)이 서비스 수행 동의 메시지를 전송하면, 서비스 수행 결정부(219)는 제1 단말(120-1)이 요청한 서비스를 수행할 수 있다. 또 다른 예로, 복수의 단말(120-1 내지 120-3)중 일부는 서비스 수행 동의 메시지를 전송하고, 나머지 일부는 서비스 수행 미동의 메시지를 전송하면, 서비스 수행 결정부(219)는 제1 단말(120-1)이 요청한 서비스를 수행하지 않을 수 있다. 또 다른 예로, 복수의 단말(120-1 내지 120-3)중 일부는 서비스 수행 동의 메시지를 전송하고, 나머지 일부는 서비스 수행 미동의 메시지를 전송하면, 서비스 수행 결정부(219)는 동의 메시지 및 미동의 메시지의 비율에 따라 제1 단말(120-1)이 요청한 서비스를 수행여부를 결정하거나, 동의 메시지 및 미동의 메시지를 전송한 단말의 기 설정된 우선순위(예를 들어, 선순위 단말이 서비스 수행 미동의 메시지를 전송하면, 차순위 단말의 동의 메시지 전송 결과와 관계 없이 서비스 수행을 거절할 수 있다.) 또는 지분율에 따라 서비스 수행 여부를 결정할 수 있다.
- [0051] 나아가, 후술하는 다양한 실시예에서와 같이, 서비스 수행 결정부(219)는 다양한 방법을 통해 복수의 단말(120-1 내지 120-3) 중 어느 하나의 비밀키가 잘못 전송되거나, 전자 서명 값 검증이 완료되지 않은 경우에 대한 서비스 수행 여부를 결정할 수 있음은 물론이다.
- [0052] 한편, 본 발명에서 설명하는 서비스는 다양한 서비스를 포함할 수 있다. 일 실시예로, 본 발명에 따른 서비스는, 하나의 공용 계좌를 복수의 사용자가 사용하는 बैं킹 서비스일 수 있다. 또는, 본 발명에 따른 서비스는, 하나의 직불카드 또는 신용 카드를 복수의 사용자가 사용하는 결제 서비스 일 수 있다.
- [0053] 또는, 본 발명에 따른 서비스는, 하나의 인터넷 서비스를 복수의 사용자가 사용하는 인터넷 서비스일 수 있다. 예를 들어, 복수의 사용자는 각각의 ID 및 비밀번호를 소유하고 있고, 복수의 사용자가 사용하는 서비스는 인터넷 쇼핑 장바구니 공유 서비스일 수 있다. 이 경우, 복수의 사용자는 상이한 ID로 로그인하지만, 로그인 후 접속되는 계정은 동일한 계정일 수 있다.

- [0054] 또는, 본 발명에 따른 서비스는, 하나의 유료 서비스를 복수의 사용자가 사용하는 유료 서비스일 수 있다. 예를 들어, 하나의 콘텐츠(E-book, 영화 감상 사이트 등)에 대한 서비스를 복수의 사용자가 이용할 수 있다.
- [0055] 또는, 본 발명에 따른 서비스는 하나의 유료 회원제 구매 카드를 복수의 사용자가 사용하기 위한 회원제 서비스 일 수 있다. 이 경우, 구매카드는 복수의 사용자 각각의 ID를 포함하는 복수개의 카드로 구성될 수 있으나, 복수개의 카드로부터 결제되는 계정은 하나일 수 있다.
- [0057] 도 3은 본 발명의 일 실시예에 따른 서비스 수행 방법을 간략히 도시한 흐름도이다.
- [0058] 도 3에 도시된 바와 같이, 제1 단말(102-1)로부터 서비스 수행 요청이 수신되면, 서비스 제공 장치(110)는 제1 단말(120-1)에 대해 전자 서명 값을 요청하여 수신하고, 제1 단말(120-1)로부터 수신한 전자 서명 값을 검증할 수 있다(S310).
- [0059] 제1 단말(120-1)로부터 수신한 전자 서명 값 검증이 완료되면, 서비스 제공 장치(120-1)는 나머지 단말(120-2, 120-3)들로부터 나머지 단말들 각각에 대해 전자 서명을 요청하여 수신하고, 수신한 전자 서명 값을 검증할 수 있다(S320). S320은 필요에 따라 생략될 수 있음은 물론이다.
- [0060] 서비스 제공 장치(110)는 모든 단말의 전자 서명 값 검증이 완료되었는지 여부를 판단할 수 있다(S330). 모든 단말의 전자 서명 값 검증이 완료되면(S330-Y), 서비스 제공 장치(110)는 모든 단말로부터 각각의 단말의 비밀 키 및 서비스 수행에 대한 동의 여부 메시지를 요청하여 수신할 수 있다(S340).
- [0061] 서비스 제공 장치(110)는 각각의 단말들로부터 수신한 비밀키를 검증할 수 있다(S350). 각각의 비밀키로부터 수신한 비밀키 검증이 완료되면(S350-Y), 서비스 제공 장치(110)는 각각의 단말들로부터 수신한 서비스 수행 동의 여부 메시지의 결과에 따라 제1 단말(120-1)이 요청한 서비스를 수행할 지 여부를 결정할 수 있다(S360).
- [0062] 한편, 모든 단말 각각의 전자 서명 값 또는 비밀키의 검증이 완료되지 않은 경우, 서비스 제공 장치(110)는 단계로 이동한다(S370). 다만, 전자 서명 값, 비밀키뿐만 아니라, 동의 여부 메시지가 수신되지 않은 경우에도 A 단계로 이동할 수 있음은 물론이다.
- [0064] 이하에서는 도 4 내지 도 7을 이용하여 본 발명에 따른 다양한 서비스 수행 결정 방법을 설명하기 위한 흐름도이다.
- [0065] 도 4는 기 설정된 시간 내에 응답이 없는 경우, 제1 단말의 서비스 요청에 대해 묵시적으로 동의하여 서비스를 수행하는 것으로 처리하는 방법을 설명하기 위한 흐름도이다.
- [0066] 구체적으로, 나머지 단말(120-2, 120-3) 중 어느 하나의 단말로부터 전자 서명 값의 검증이 완료되지 않거나 (S330-N), 모든 단말 중 어느 하나의 단말로부터 비밀키의 검증이 완료되지 않은 경우(S350-N), 서비스 제공 장치(110)는 기 설정된 시간 내에 검증이 완료되지 않은 나머지 단말들로부터 전자 서명 값 또는 비밀키의 검증이 완료되는지 여부를 판단할 수 있다(S410).
- [0067] 이때, 기 설정된 시간은 다양한 방법에 의해 결정될 수 있다. 일 실시예로, 기 설정된 시간은 사용자 설정 또는 합의에 의해 결정될 수 있다. 또 다른 실시예로, 기 설정된 시간은, 상기 복수의 단말 각각으로부터 수신한 과거 응답 시간을 바탕으로 결정될 수 있다. 이때, 과거 응답 시간이란, 단말이 전자 서명 값 또는 비밀키 요청 메시지를 수신한 시간부터 메시지 수신에 대한 응답을 완료한 시간, 또는 단말이 전자 서명 값 또는 비밀키 요청 메시지 수신을 확인한 시간부터 메시지 수신에 대한 응답을 완료한 시간일 수 있다. 예를 들어, 제1 단말(120-1)의 과거 응답 시간의 평균이 10분, 제2 단말(120-2)의 과거 응답 시간의 평균이 8분, 제3 단말(120-3)의 과거 응답 시간의 평균이 6분인 경우, 기 설정된 시간은 10분, 8분, 6분의 평균값인 8분으로 결정되거나, 10분, 8분, 6분중 가장 긴 시간인 10분 또는 가장 짧은 시간인 6분으로 결정될 수 있다. 또는 기 설정된 시간은 복수의 단말 각각에 대하여 개별적으로 결정될 수도 있음은 물론이다. 예를 들어, 제1 단말(120-1)의 과거 응답 시간의 평균이 10분, 제2 단말(120-2)의 과거 응답 시간의 평균이 8분, 제3 단말(120-3)의 과거 응답 시간의 평균이 6분인 경우, 제1 단말(120-1)의 기 설정된 시간은 10분, 제2 단말(120-2)의 기 설정된 시간은 8분, 제3 단말(120-3)의 기 설정된 시간은 6분으로 결정될 수 있다.
- [0068] 이때, 기 설정된 시간 내에 전자 서명 값 또는 비밀키의 검증이 완료되면(S410-Y), 서비스 제공 장치(110)는 전자 서명 값 또는 비밀키 검증 결과에 따라 제1 단말(120-1)이 요청한 서비스를 수행할 수 있다. 구체적으로, 서비스 제공 장치(110)는 각각의 단말이 비밀키와 함께 전송한 서비스 수행 동의 여부 메시지를 바탕으로 서비스를 수행할 지 여부를 판단할 수 있다. 상술한 바와 같이, 복수의 단말(120-1 내지 120-3)이 서비스 수행 동의 메시지를 전송하면, 서비스 수행 결정부(219)는 제1 단말(120-1)이 요청한 서비스를 수행할 수 있다. 또 다른

예로, 복수의 단말(120-1 내지 120-3)중 일부는 서비스 수행 동의 메시지를 전송하고, 나머지 일부는 서비스 수행 미동의 메시지를 전송하면, 서비스 수행 결정부(219)는 제1 단말(120-1)이 요청한 서비스를 수행하지 않을 수 있다. 또 다른 예로, 복수의 단말(120-1 내지 120-3)중 일부는 서비스 수행 동의 메시지를 전송하고, 나머지 일부는 서비스 수행 미동의 메시지를 전송하면, 서비스 수행 결정부(219)는 동의 메시지 및 미동의 메시지의 비율에 따라 제1 단말(120-1)이 요청한 서비스를 수행여부를 결정하거나, 동의 메시지 및 미동의 메시지를 전송한 단말의 기 설정된 우선순위 또는 지분율에 따라 서비스 수행 여부를 결정할 수 있다.

[0069] 한편, 기 설정된 시간 내에 전자 서명 값 또는 비밀키의 검증이 완료되지 않으면(S410-N), 서비스 제공 장치(110)는 전자 서명 값 또는 비밀키 검증이 완료되지 않은 단말이 서비스 수행 동의 메시지를 전송한 것으로 간주하고 제1 단말(120-1)이 요청한 서비스 수행 여부를 결정할 수 있다. 예를 들어, 제2 단말(120-2)은 기 설정된 시간 내에 서비스 수행을 동의 하는 메시지를 전송하였으나, 제3 단말(120-3)은 전자 서명 값 또는 비밀키 검증을 하지 않은 경우, 서비스 제공 장치(110)는 제3 단말(120-3)이 서비스 수행에 동의한 것으로 판단하고 제1 단말(120-1)이 요청한 서비스를 수행할 수 있다.

[0071] 도 5는 본 발명의 일 실시예에 따른 목시적 동의 여부를 판단하는 또 다른 방법을 설명하기 위한 흐름도이다.

[0072] 먼저, 나머지 단말(120-2, 120-3) 중 어느 하나의 단말로부터 전자 서명 값의 검증이 완료되지 않거나(S330-N), 모든 단말 중 어느 하나의 단말로부터 비밀키의 검증이 완료되지 않은 경우(S350-N), 서비스 제공 장치(110)는 검증을 완료하지 않은 단말이 기 설정된 시간 내에 전자 서명 값 또는 비밀키 요청 메시지를 확인하였는지 여부를 판단할 수 있다(S510).

[0073] 구체적으로, 제1 단말(120-1)로부터 서비스 수행을 요청 받고, 제1 단말(120-1)의 전자 서명 값 검증이 완료되면, 서비스 제공 장치(110)는 필요한 단말에 전자 서명 값을 요청하는 메시지를 전송하거나, 비밀키를 요청하는 메시지를 전송할 수 있다. 이때, 전자 서명 값을 요청하는 메시지 또는 비밀키를 요청하는 메시지는 메시지 수신 여부를 확인하는 인덱스를 더 포함할 수 있다. 즉, 서비스 제공 장치(110)는 단말의 사용자가 시스템 상의 예러로 메시지 자체를 수신하지 못하거나, 메시지를 수신하였으나, 단말을 관리하지 않는 등의 이유로 메시지의 내용을 확인하지 못하는 상황 등을 수신 여부를 확인하는 인덱스를 통해 판단할 수 있다.

[0074] 전자 서명 값 또는 비밀키 검증이 완료되지 않은 단말이 전자 서명 값 또는 비밀키 요청 메시지를 기 설정된 시간 내에 확인한 경우(S510-Y), 서비스 제공 장치(110)는 서비스 제공 장치(110)는 전자 서명 값 또는 비밀키 검증이 완료되지 않은 단말이 서비스 수행 동의 메시지를 전송한 것으로 간주하고 제1 단말(120-1)이 요청한 서비스 수행 여부를 결정할 수 있다(S520). 즉, 서비스 제공 장치(110)는 단말의 사용자가 서비스 동의와 관련된 메시지를 수신하였으나 이에 대한 응답을 의도적으로 하지 않은 것으로 판단하여 단말의 사용자가 서비스 수행을 목시적으로 동의한 것으로 판단할 수 있다. 따라서, 서비스 수행을 요청한 제1 단말(120-1)의 사용자 및 나머지 사용자의 의사를 존중하며 서비스를 수행할 수 있는 효과가 존재한다.

[0075] 다만, 전자 서명 값 또는 비밀키 검증이 완료되지 않은 단말이 전자 서명 값 또는 비밀키 요청 메시지를 기 설정된 시간 내에 확인하지 않은 경우(S510-N) 서비스 수행 장치(110)는 목시적 동의로 간주하지 않고 전자 서명 값 또는 비밀키 검증을 위한 전자 서명 값 또는 비밀키의 수신을 대기할 수 있다. 상기 과정을 통해 서비스를 요청한 단말의 서비스 수행 요구를 효과적으로 만족시킴과 동시에, 서비스에 대한 요청을 확인조차 하지 못한 채 서비스가 수행되는 것을 방지하여 나머지 단말의 사용자를 보호할 수 있다.

[0077] 도 6는 본 발명의 일 실시예에 따른 목시적 동의 여부를 판단하는 또 다른 방법을 설명하기 위한 흐름도이다.

[0078] 구체적으로, 서비스 제공 장치(110)는 서비스 수행에 필수 단말과 일반 단말을 구분하고, 기 설정된 시간 내에 필수 단말로부터 전자 서명 값 또는 비밀키를 수신하지 못한 경우에는 목시적 동의로 처리하지 않고, 일반 단말로부터 전자 서명 값 또는 비밀키를 수신하지 못한 경우에는 목시적 동의로 처리 할 수 있다.

[0079] 먼저, 서비스 제공 장치(110)는 복수의 단말들(120-1 내지 120-3)을 전자 서명 값 또는 비밀키 검증이 필수적인 필수 단말과 전자 서명 검증이 없을 경우 목시적 동의로 처리하는 일반 단말로 분류할 수 있다(S610). 분류 방법은 필요에 따라 다양할 수 있다. 일 실시예로, 서비스 제공 장치(110)는 필수 단말에게 제1 인덱스를 전송하고, 일반 단말에게 제2 인덱스를 부가한 후, 전자 서명 값 또는 비밀키를 전송 받을 때, 단말로 전송한 제1 인덱스 또는 제2 인덱스를 함께 수신하여 필요 단말과 일반 단말을 분류할 수 있다.

[0080] 또 다른 실시예로, 서비스 제공 장치(110)는 전체 단말의 우선 순위를 부가하고, 기 설정된 기준에 따라 필수 단말 및 일반 단말을 분류할 수 있다. 예를 들어, 단말이 4개가 존재하는 경우, 서비스 제공 장치는 각각의 단말에게 제1 인덱스 내지 제4 인덱스를 전송할 수 있다. 이때, 제1 인덱스에서 제4 인덱스의 순서로 우선순위가

결정될 수 있다. 서비스 제공 장치(110)는 기 설정된 기준(예를 들어 제1 인덱스 내지 제3 인덱스를 가지는 단말을 필수 단말로 지정하는 기준, 또는 제1 인덱스 및 제2 인덱스를 가지는 단말을 필수 단말로 지정하는 기준)에 따라 필수 단말 및 일반 단말을 분류할 수 있다.

- [0081] 서비스 제공 장치(110)는 제1 단말(120-1)로부터 서비스 수행 요청이 수신되면, 제1 단말(120-1)에 대해 전자 서명 값을 요청하여 수신하고, 제1 단말로부터 수신한 전자 서명을 검증할 수 있다(S620). 같은 방법으로, 서비스 제공 장치(110)는 나머지 단말들로부터 전자 서명 값을 검증할 수 있다. 비밀키 및의 검증 또한, 상술한 방법을 통해 이뤄질 수 있다. 즉, 도면에는 도시되어 있지 않으나, 서비스 제공 장치(110)는 도3의 S310~S350와 동일한 방법으로 전자 서명 값 및 비밀키를 검증할 수 있다.
- [0082] 서비스 제공 장치(110)는 필수 단말 전체로부터 전자 서명 값 및 비밀키 검증이 완료되었는지 여부를 판단할 수 있다(S630).
- [0083] 필수 단말 모두의 전자 서명 값 및 비밀키 검증이 완료되면(S630-Y), 서비스 제공 장치(110)는 기 설정된 시간 내에 일반 단말로부터 수신한 전자 서명 값 또는 비밀키가 검증되었는지를 확인하고, 기 설정된 시간 내에 일반 단말로부터 수신한 전자 서명 값 또는 비밀키가 검증되지 않으면, 전자 서명 값 또는 비밀키 검증 결과에 따라 제1 단말(120-1)이 요청한 서비스를 수행할 수 있다(S640).
- [0084] 필수 단말 모두의 전자 서명 값 및 비밀키 검증이 완료되지 않으면(S630-N), 서비스 제공 장치(110)는 필수 단말의 무응답을 묵시적 동의로 판단하지 않고, 전자 서명 값 또는 비밀키 검증을 위한 전자 서명 값 또는 비밀키의 수신을 대기할 수 있다(S650).
- [0085] 즉, 서비스 제공 장치(110)는 일반 단말이 응답하지 않는 경우, 일반 단말의 무응답은 묵시적 동의로 처리하고, 필수 단말의 무응답은 묵시적 동의로 처리하지 않을 수 있다.
- [0087] 도 7은 본 발명의 일 실시예에 따른 묵시적 동의 여부를 판단하는 또 다른 방법을 설명하기 위한 흐름도이다.
- [0088] 검증이 완료되지 않거나(S330-N), 모든 단말 중 어느 하나의 단말로부터 비밀키의 검증이 완료되지 않은 경우(S350-N), 서비스 제공 장치(110)는 기 설정된 시간 내에 나머지 단말들로부터 전자 서명 값 또는 비밀키 요청 메시지를 검증하였는지 여부를 판단할 수 있다(S710).
- [0089] 모든 단말이 전자 서명 값 및 비밀키 검증을 완료하였으면(S710-Y), 서비스 제공 장치(110)는 동의 여부 결과에 따라 제1 단말(120-1)이 요청한 서비스를 수행할 지 여부를 결정할 수 있다.
- [0090] 모든 단말이 전자 서명 값 및 비밀키 검증을 완료하지 않은 경우(S710-N), 서비스 제공 장치(110)는 제1 단말(120-1)로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 값 이상인지 여부를 판단할 수 있다(S730). 이때, 기 설정된 값은 다양한 방법에 따라 결정될 수 있다. 예를 들어, 기 설정된 값은 복수의 사용자의 합의에 의해 결정될 수 있다. 또는, 서비스 제공 장치(110)에 의해 제공되는 서비스(110)가 공동 계좌 서비스인 경우, 기 설정된 값은 공동 계좌에 존재하는 현금의 액수의 일정 비율(예를 들어 계좌 인출 가능 금액의 10%)일 수 있다. 또는, 서비스 제공 장치(110)에 의해 제공되는 서비스(110)가 공동 계좌 서비스인 경우, 기 설정된 값은 복수의 사용자 각각이 공동 계좌에 입금한 금액의 비율에 따른 값일 수 있다.
- [0091] 제1 단말(120-1)로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 값 이상인 경우(S730-Y), 서비스 제공 장치(110)는 전자 서명 값 또는 비밀키의 수신을 대기할 수 있다(S750). 다만, 제1 단말(120-1)로부터 수신한 서비스 수행 요청에 대응되는 비용이 기 설정된 값 미만인 경우(S730-N), 서비스 제공 장치(110)는 미응답한 단말이 서비스 수행에 대하여 묵시적 동의를 한 것으로 보고, 나머지 단말들의 전자 서명 값 또는 비밀키 검증 결과에 따라 제1 단말(120-1)이 요청한 서비스를 수행할 수 있다.
- [0092] 즉, 작은 비용의 경우에도 모든 서비스 이용에 대하여 모든 사용자의 동의를 얻는 것은 서비스 요청 사용자에게 가혹한 일이므로, 서비스 제공 장치(110)는 기 설정된 값 미만의 비용에 대하여는 기 설정된 시간 미응답시 서비스 수행을 처리할 수 있어 서비스 요청자를 보호할 수 있다.
- [0094] 한편, 상술한 다양한 실시예는 독립적으로 적용될 수 있으나 필요에 따라 서로 결합되어 적용될 수 있음은 물론이다.
- [0095] 일 실시예로, 도 5의 실시예에서, 단말 중 일부가 기 설정된 시간 내에 메시지를 확인하지 않은 경우라도, 제1 단말(120-1)의 서비스 수행 요청에 대응되는 비용이 기 설정된 값 미만이거나, 필수 단말 모두가 전자 서명 값 및 비밀키 검증을 완료하였거나, 메시지를 확인한 경우, 서비스 제공 장치(110)는 무응답한 일반 단말을 묵시적

동의로 판단하고 서비스 수행 여부를 결정할 수 있다.

- [0096] 또 다른 실시예로, 도 6의 실시예에서, 필수 단말 중 일부가 전자 서명 값 및 비밀키 검증을 완료하지 않은 경우라도, 제1 단말(120-1)의 서비스 수행 요청에 대응되는 비용이 기 설정된 값 미만이면, 서비스 제공 장치(110)는 무응답한 일반 단말을 묵시적 동의로 판단하고 서비스 수행 여부를 결정할 수 있다.
- [0097] 또 다른 실시예로, 도 7의 실시예에서, 제1 단말(120-1)의 서비스 수행 요청에 대응되는 비용이 기 설정된 값 이상인 경우라도, 필수 단말 모두가 전자 서명 값 및 비밀키 검증을 완료한 경우, 서비스 제공 장치(110)는 무응답한 일반 단말을 묵시적 동의로 판단하고 서비스 수행 여부를 결정할 수 있다.
- [0099] 한편, 본 개시에 따른 다양한 값 또는 조건은 인공 지능 모델을 통해 획득될 수 있다.
- [0100] 예를 들어, 서비스 제공 장치(110)는 복수의 단말 각각으로부터 전자 서명 값, 비밀키 값 및 동의 여부 메시지를 요청한 시점부터 전자 서명 값, 비밀키 값 및 동의 여부 메시지를 수신한 시점에 대한 시간 정보 및 복수의 단말 각각에 대한 사용 환경 정보를 입력 데이터로 인공 지능 모델에 입력하여, 기 설정된 시간을 결정할 수 있다.
- [0101] 또는, 서비스 제공 장치(110)는 각각의 단말로부터 사용 환경 정보를 수신하고, 사용 환경 정보를 입력 데이터로 인공 지능 모델에 입력하여 기 설정된 시간을 결정할 수 있다. 이때, 사용 환경 정보란, 사용자의 단말 사용 시간에 대한 정보, 사용자가 단말의 다른 기능을 사용하고 있는지 여부에 대한 정보, 시간 정보 등을 포함할 수 있다.
- [0102] 즉, 서비스 제공 장치(110)는 사용자가 전자 서명 값 및 비밀키 검증 완료에 소요되는 시간 뿐만 아니라, 사용자의 단말 사용 습관을 학습하여, 서비스 수행 요청을 받은 시점에서 단말의 사용자가 서비스 수행에 대한 동의가 가능한 상태인지 등을 판단할 수 있다. 예를 들어, 제2 단말(120-2)의 사용자는 오후 3시부터 오후 6시까지 단말을 사용하지 않는 빈도가 높다면, 서비스 제공 장치(110)는 묵시적 동의 여부를 인정하기 위한 기 설정된 시간이 만료되는 시점을 오후 6시 이후로 설정할 수 있다)
- [0103] 또는, 서비스 제공 장치(110)는 과거 복수의 단말 사용자들의 서비스 수행 요청에 대한 동의/미동의 여부와 관련된 데이터를 입력 데이터로 입력하여 서비스 요청에 대한 단말 사용자의 동의/미동의 여부를 판단할 수 있다. 이때, 서비스 수행 요청에 대한 동의/미동의 여부와 관련된 데이터는 서비스의 공유, 서비스를 수행하는데 소요되는 비용, 동의 및 미동의 여부 등과 관련된 정보일 수 있다. 즉, 서비스 제공 장치(110)는 사용자가 서비스 수행 요청에 대한 응답을 하지 않는 경우, 사용자의 과거 정보를 바탕으로 현재 요청된 서비스를 동의할 것인지 미동의할 것인지 여부를 판단할 수 있다. 일 실시예로, 서비스 제공 장치(110)는 각각의 단말로부터 단말을 주로 사용하는 시간에 대한 정보, 메시지 수신을 확인하는 시간에 대한 정보, 결제에 동의한 서비스에 대한 정보, 결제에 동의한 서비스의 비용에 관한 정보 등을 바탕으로 요청된 서비스를 동의할 것인지 미동의할 것인지 여부를 판단할 수 있다. 예를 들어, 복수의 단말 중 어느 하나의 단말이 특정 비용(예를 들어 5만원) 이하인 서비스에 대하여 항상 서비스 수행에 동의하였다면, 서비스 제공 장치(110)는 복수의 단말 중 어느 하나의 단말이 전자 서명 값 또는 비밀키 값을 기 설정된 시간 동안 제공하지 않더라도 해당 단말이 서비스 요청에 동의할 것이라고 판단할 수 있다. 또는, 복수의 단말 중 어느 하나의 단말이 특정 서비스(예를 들어, 영화 감상 서비스) 이하인 서비스에 대하여 항상 서비스 수행에 동의하였다면, 서비스 제공 장치(110)는 복수의 단말 중 어느 하나의 단말이 전자 서명 값 또는 비밀키 값을 기 설정된 시간 동안 제공하지 않더라도 해당 단말이 서비스 요청에 동의할 것이라고 판단할 수 있다.
- [0104] 동의/미동의에 대한 판단 결과는, 상술한 묵시적 동의 조건을 만족하는 경우 사용될 수 있다. 예를 들어, 제2 단말(120-2)이 전자 서명 값 또는 비밀키에 대한 검증을 기 설정된 시간 동안 완료하지 않은 경우, 서비스 제공 장치(110)는 인공 지능 모델을 이용하여 판단된 판단 결과에 따라 서비스 수행에 동의하거나, 미동의 할 수 있다.
- [0105] 상술한 인공 지능 모델을 이용하기 위하여, 서비스 제공 장치(110)는 인공 지능 모델을 학습시키기 위한 데이터 학습부 및 학습된 인공 지능 모델을 사용하기 위한 데이터 인식부의 구성을 포함할 수 있다. 데이터 학습부 및 데이터 인식부는 적어도 하나는 인공 지능(AI; artificial intelligence)을 위한 전용 하드웨어 칩 형태로 제작될 수도 있고, 또는 기존의 범용 프로세서(예: CPU 또는 application processor) 또는 그래픽 전용 프로세서(예: GPU)의 일부로 제작될 수도 있다. 이 때, 인공 지능을 위한 전용 하드웨어 칩은 확률 연산에 특화된 전용 프로세서로서, 기존의 범용 프로세서보다 병렬처리 성능이 높아 기계 학습과 같은 인공 지능 분야의 연산 작업을 빠르게 처리할 수 있다.

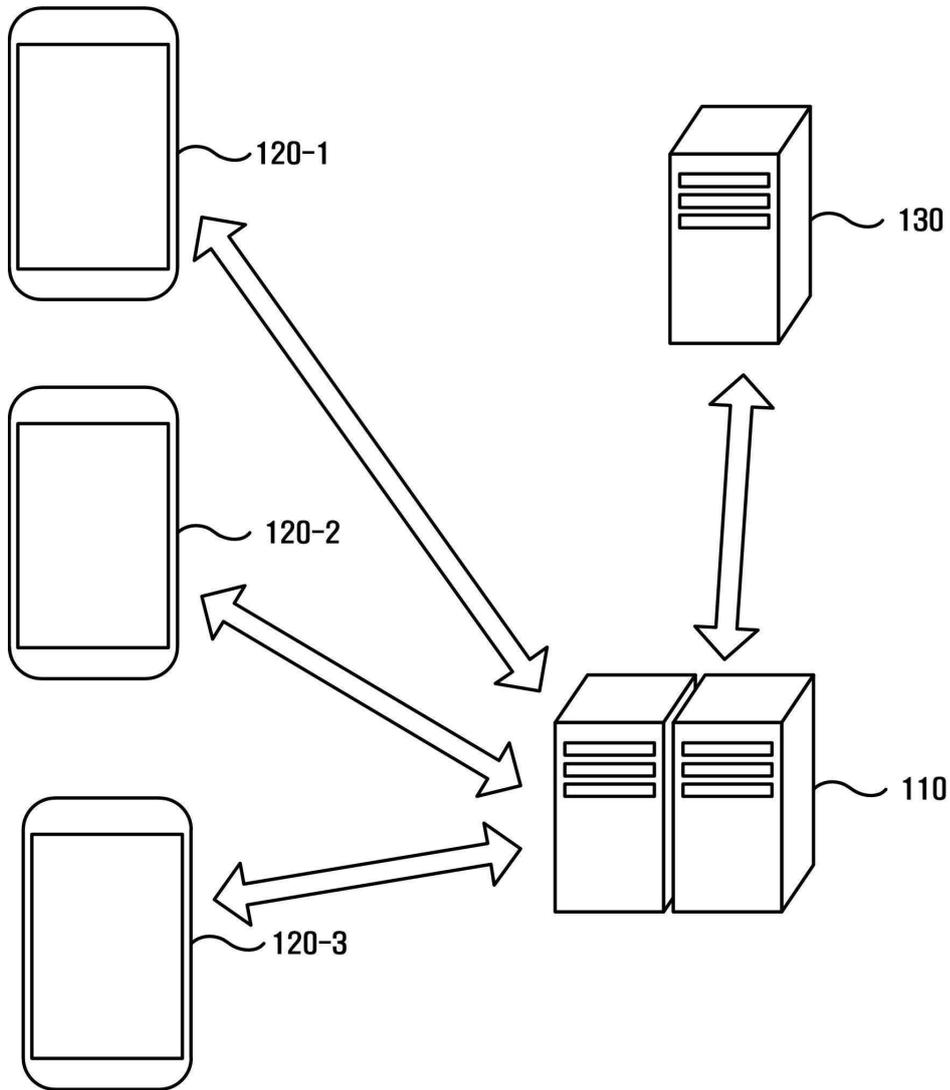
- [0106] 이러한 인공 지능 모델은 DNN(Deep Neural Network), RNN(Recurrent Neural Network), BRDNN(Bidirectional Recurrent Deep Neural Network)과 같은 모델을 사용할 수 있으나, 이에 한정되는 것은 아니다.
- [0108] 본 발명의 실시예와 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 판독가능 기록매체에 상주할 수도 있다.
- [0109] 본 발명의 구성 요소들은 하드웨어인 컴퓨터와 결합되어 실행되기 위해 프로그램(또는 애플리케이션)으로 구현되어 매체에 저장될 수 있다. 본 발명의 구성 요소들은 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있으며, 이와 유사하게, 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블러(assembly) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다.
- [0110] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이지 않은 것으로 이해해야만 한다.

부호의 설명

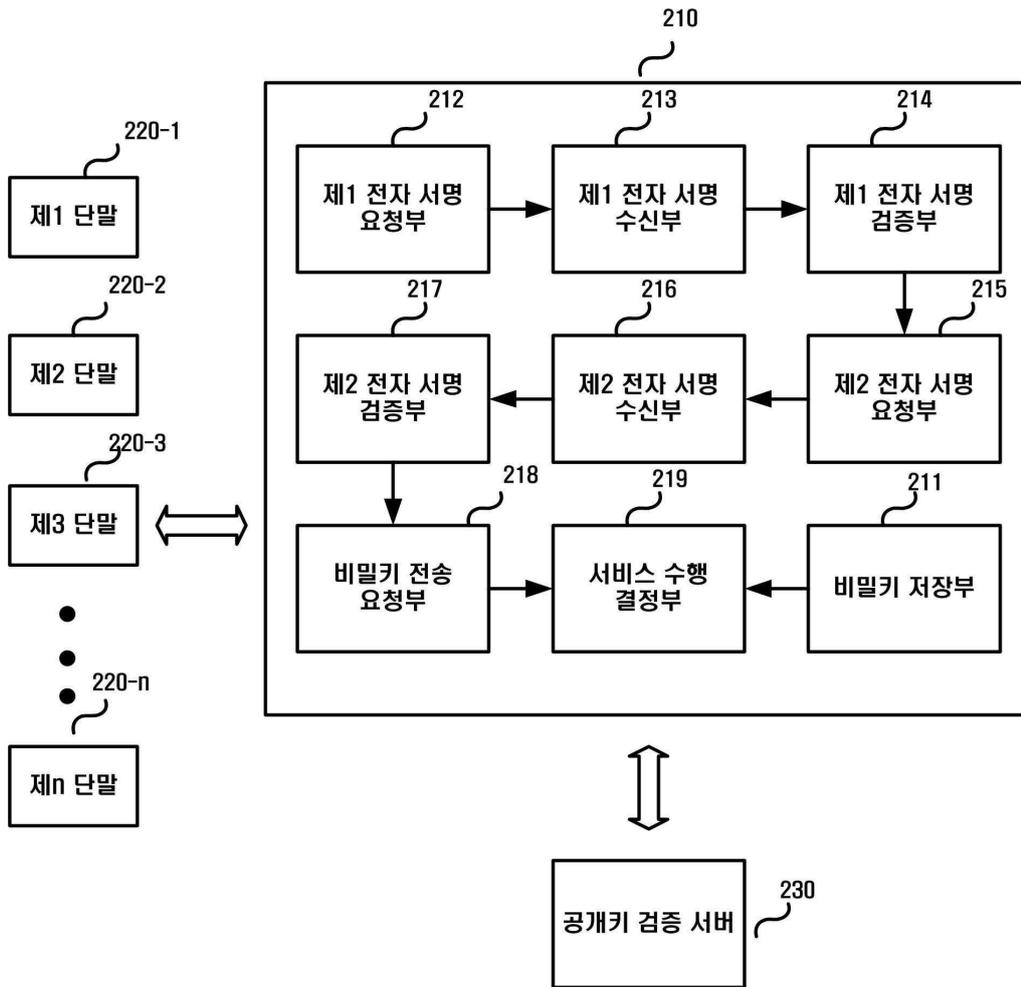
- [0111] 110 : 서비스 제공 장치
- 120-1: 제 1 단말
- 120-2: 제2 단말
- 120-3: 제3 단말
- 130: 공개키 검증 서버

도면

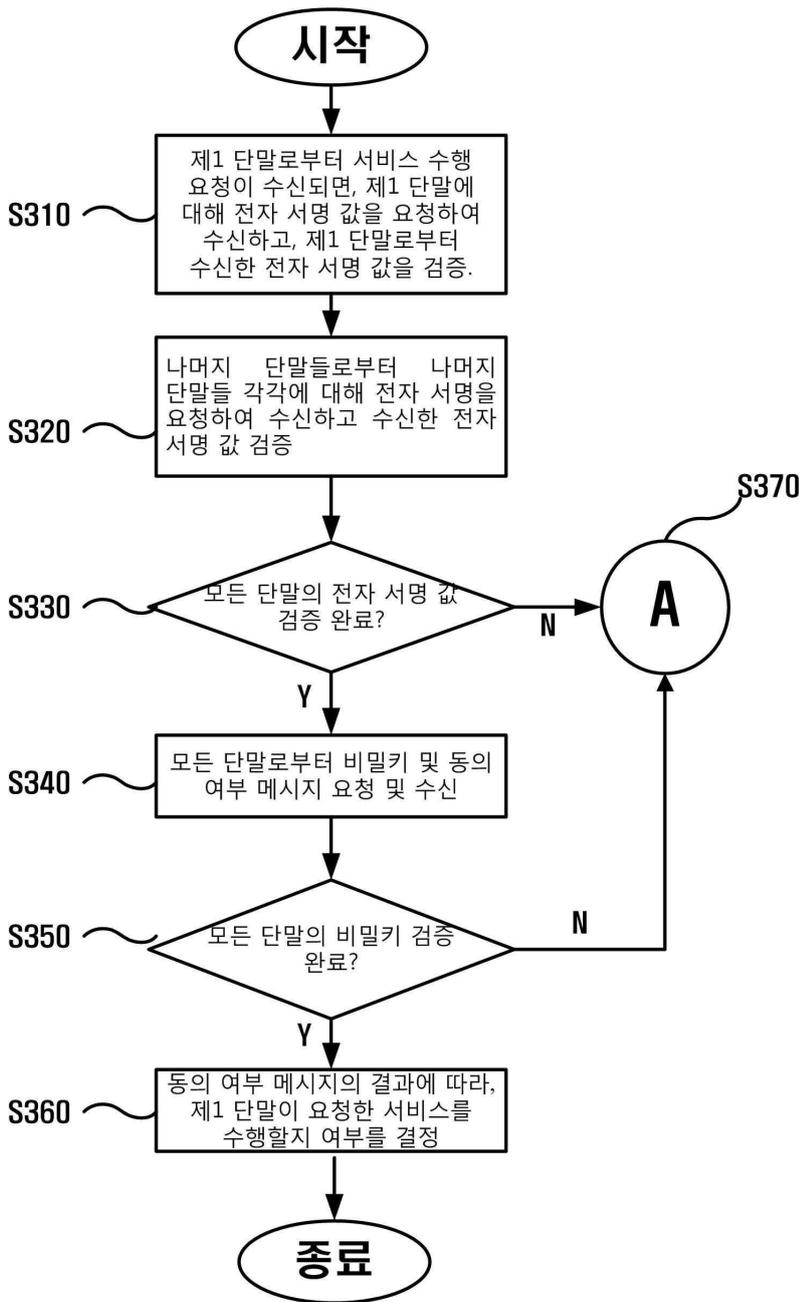
도면1



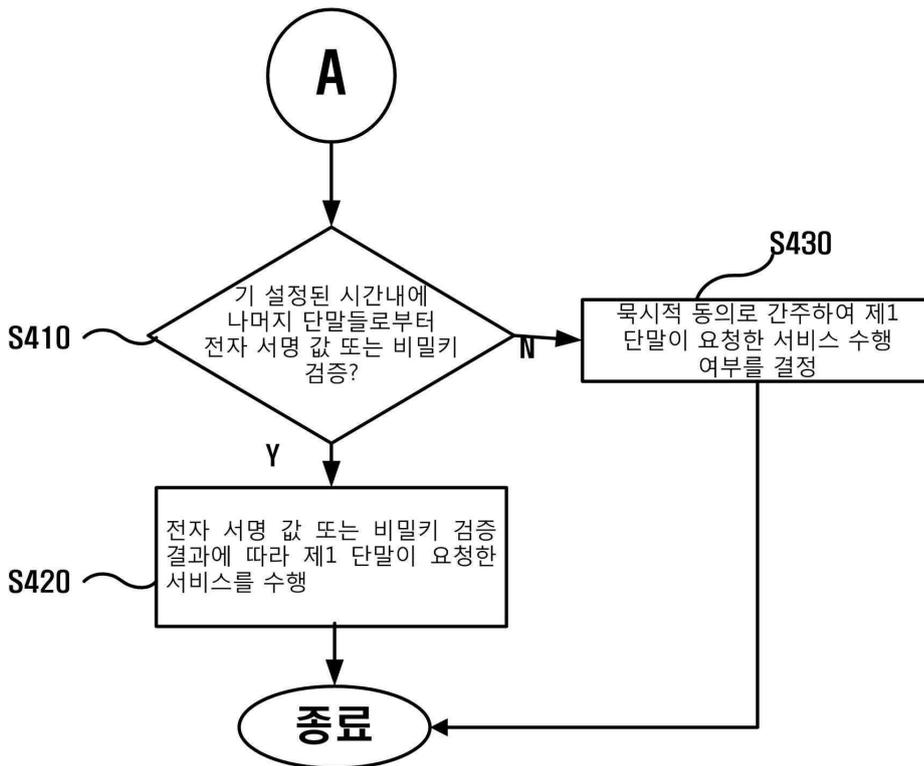
도면2



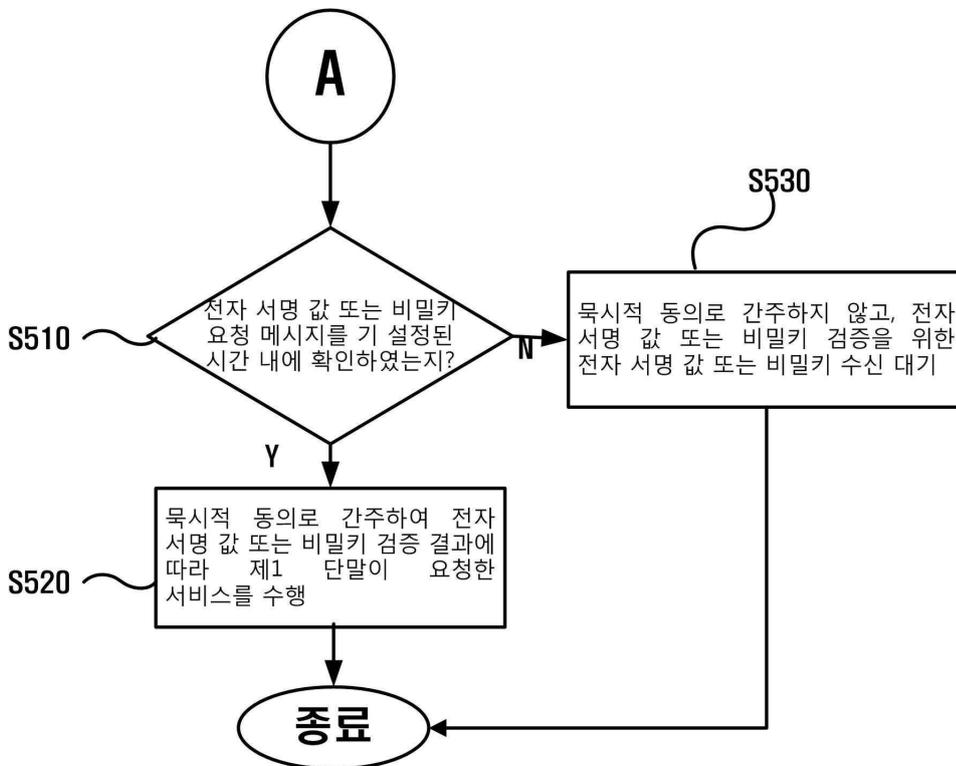
도면3



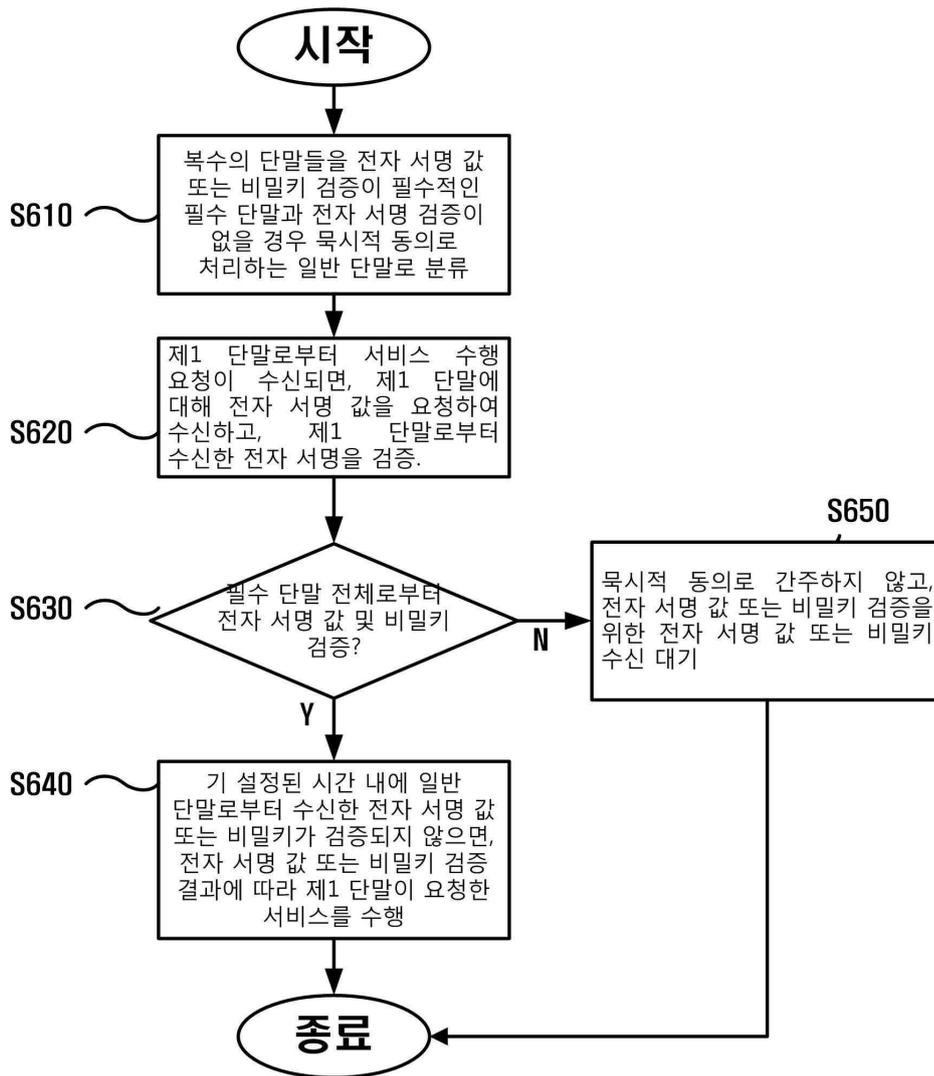
도면4



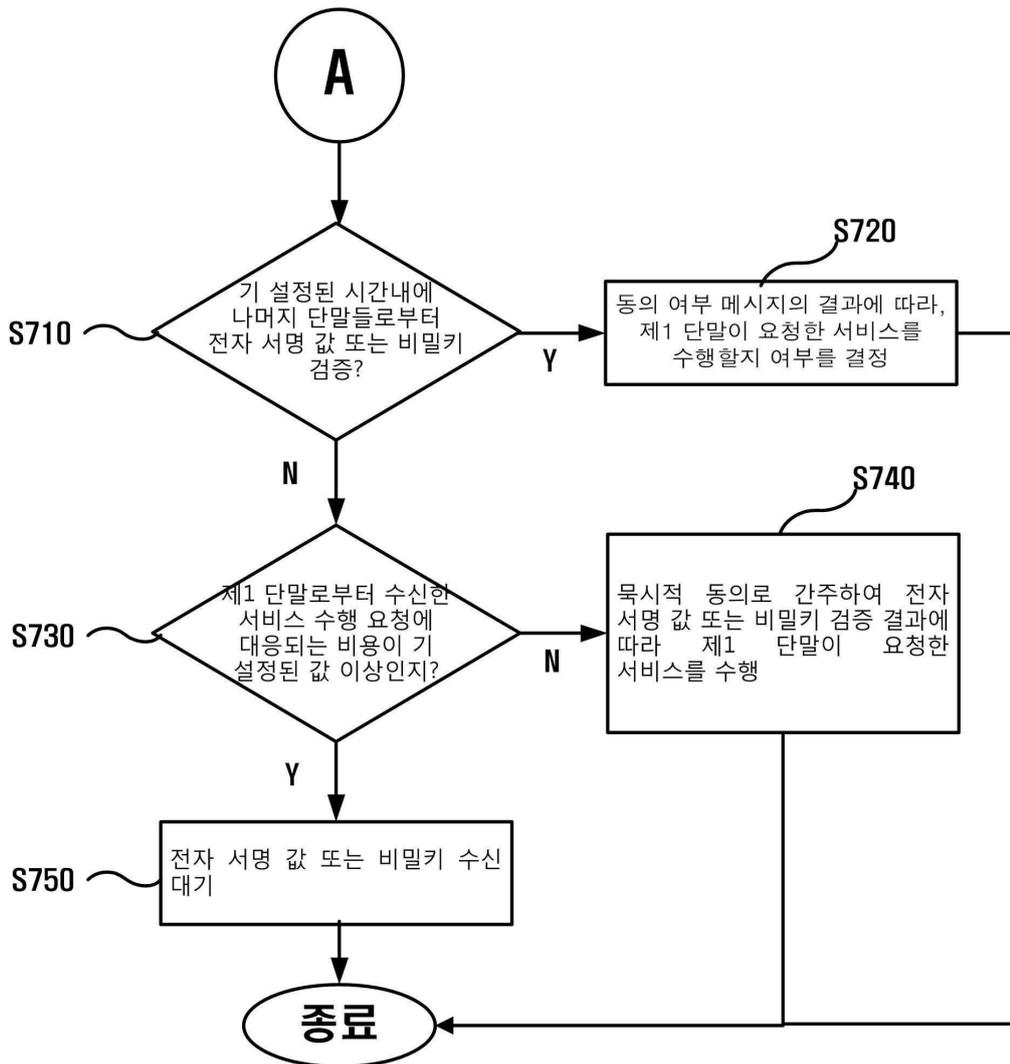
도면5



도면6



도면7



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제9항

【변경전】

상기 서비스를 수행하기

【변경후】

서비스를 수행하기