

(19) 대한민국특허청(KR) (12) 공개특허공보(A)

(51) 。 Int. Cl. ⁷
G06F 17/60

(11) 공개번호 특2003 - 0015519
(43) 공개일자 2003년02월25일

(21) 출원번호 10 - 2001 - 0049286
(22) 출원일자 2001년08월16일

(71) 출원인 문병로
서울 관악구 봉천7동 244 - 2 서울대교수아파트 가동 106호
(72) 발명자 문병로
서울 관악구 봉천7동 244 - 2 서울대교수아파트 가동 106호
(74) 대리인 박원용
이종우

심사청구 : 있음

(54) 보안성을 가지는 고객정보 공유 시스템 및 그 방법

요약

본 발명의 보안성을 가지는 고객정보 공유 시스템 및 방법은, 참여기업 자체적인 암호화를 수행하고 참여기업 소유 고객정보의 유출을 원천적으로 봉쇄하면서 암호화된 상태에서 중복가입고객 정보를 추출할 수 있는 공유시스템 및 공유방법에 관한 것이다.

본 발명의 공유시스템은 암호화수단을 제공하고 다수 참여기업들의 암호화된 가입고객정보를 전송받아 중복가입고객 정보를 추출하며, 이를 이용해서 처리된 결과의 내용을 다수의 참여기업들로 전송하는 주관사의 처리장치, 및 주관사로부터 제공된 암호화수단을 이용하여 자체 고객정보를 암호화하여 주관사의 처리장치로 전송하며, 주관사에서 추출하여 처리한 결과의 내용을 전송받는 다수 참여기업들의 처리장치를 포함함으로써, 자료의 복호화 및 해독이 불가능한 상태에서 다수 참여기업들의 중복가입고객에 대한 정보를 공유할 수 있다.

또한 위의 공유시스템을 주관사 없이 다수 참여기업들만으로 구성할 수도 있는데, 공통된 암호화수단을 이용하여 자체 가입한 가입고객정보를 암호화하는 암호화 장치, 암호화된 고객정보를 상기 다수 참여기업으로 전송하거나 하기 데이터 처리장치에서 가공 처리를 한 결과 중 필요한 정보를 다수의 참여기업들로 전송하는 전송장치, 전송장치에서 전송받은 고객정보를 이용하여 가공처리를 하는 데이터 관리장치 및 다수 참여기업들의 전송장치로부터 전송된 고객정보 또는 데이터 관리장치에서 가공 처리된 결과 중 필요한 정보를 전송받는 수신장치를 포함함으로써, 자료의 복호화 및 해독이 불가능한 상태에서 다수 참여기업들의 중복가입고객에 대한 정보를 공유할 수 있다.

또한 본 발명의 공유방법은 키없는 단방향 함수를 이용하여 암호화함으로써 보안성을 가지게 하는 제1의 방법과, 순차적 공개키 암호화기법을 이용하여 암호화함으로써 보안성을 가지게 하는 제2의 방법에 의해 달성된다.

대표도

도 2

색인어

고객, 정보공유, 보안, 암호학, 고객관계관리(CRM), 마케팅

명세서

도면의 간단한 설명

도 1은 다수 기업에 중복가입한 일반 고객의 예를 설명하기 위한 도면.

도 2는 본 발명의 일실시예에 따른 보안성을 가지는 고객정보 공유시스템의 구성도.

도 3은 본 발명의 일실시예에 따라 키없는 단방향 함수를 이용하여 암호화하는 보안성을 가지는 고객정보 공유방법의 순서도.

도 4는 본 발명의 일실시예에 따라 공개키에 의한 암호화기법을 이용하여 암호화하는 보안성을 가지는 고객정보 공유방법의 순서도.

< 도면의 주요부분에 대한 부호의 설명 >

200 : 주관사의 처리장치

210 : 암호화 관리부

220 : 데이터 관리부

221 : 데이터베이스 222 : 암호화단

223 : 고객정보 취합단 224 : 데이터 마이닝단(data mining)

230 : 서비스 관리부

300 : 참여기업의 처리장치

400 : 네트워크

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 보안 기반의 고객정보 공유에 관한 것으로, 자세하게는 참여기업 자체적인 암호화를 수행하여 참여기업 소유 고객정보의 유출을 원천적으로 봉쇄하면서 암호화된 상태에서 중복가입고객을 판별함으로써, 필요한 고객정보의 공유를 통한 마케팅(marketing) 효율의 극대화 및 공동마케팅 시장의 활성화를 추구할 수 있는, 보안성을 가지는 고객정보 공유 시스템 및 방법을 제시한 것이다.

무궁무진한 정보의 보고로서 현대인의 생활 패턴까지도 바꾸고 있는 인터넷은 은행, 티켓, 쇼핑은 기본이고 영화, 음악, 게임 등 적용되지 않는 분야가 없을 정도로 다양하고 방대하며, 통신의 발달과 함께 상상을 초월하는 속도로 급격한 변화를 주고 있다.

이와 같은 다양한 정보 및 서비스를 회원고객들에게 제공하기 위해, 인터넷 시장의 대다수 기업은 자체적으로 고객 데이터베이스를 구축하고 있다. 정도의 차이는 있지만, 이러한 고객 데이터베이스는 적게는 10만 미만에서 많게는 500만 이상의 고객을 보유하고 있다.

하지만, 개인정보의 유출을 꺼리는 가입고객들의 성향, 다양한 개인정보 보호정책, 사생활 침해의 우려 등에 의해, 각 기업들은 기업 고유의 영업 내지 마케팅에 필요한 제한적인 정보만을 고객으로부터 수집하는 것이 대부분이다.

그러나 이러한 정보수집의 어려움에도 불구하고 인터넷을 주로 사용하고 있는 고객들은 일반적으로 다수의 사이트에 중복 가입하고 있는 것이 일반적이며, 가입한 해당 사이트에 또다른 정보를 제공하고 있는 실정이다.

도 1은 다수 기업에 중복가입한 일반 고객의 예를 설명하기 위한 도면이다.

도시한 바와 같이, 고객 K가 다음의 3개 기업에 가입하여 개인 정보를 제공하였다고 하자. 위의 3개 기업에서 고객에 대한 정보는 나름대로 제한적이다. 특히 스포츠사이트인 A사(社)와 쇼핑몰 사이트인 C사(社)는 성명, 주민등록번호, 주소, 전화번호 등의 정적 정보와 고객의 상품 구매 정보 등의 동적 정보를 포함하고 있다.

이 경우 고객 K가 A, B, C 사에 동시 가입되어 있다는 정보를 알 수 있는 경우, 고객 K를 회원으로 둔 A, B, C 사는 보다 다양한 분석을 통하여 영업과 경영을 실시할 수 있다. 즉 각각의 회사에 가입하고 있는 고객 K에 대한 정보를 서로 공유할 수 있다면, 고객 K의 취향을 보다 다양하게 파악해 수준 높은 서비스 및 마케팅을 실시할 수 있게 된다.

그러나 종래의 방법으로 중복으로 가입하고 있는 중복 고객을 추출하기 위해서는 A, B, C 각 사의 전체 고객정보에 대한 공유가 필수적으로 선행되어야 한다. 하지만 이러한 과정에서 각 회사의 고객정보 유출은 심각한 문제를 야기하게 된다. 즉, 고객정보의 유출은 비단 고객의 개인 정보 침해뿐만 아니라 기업의 소중한 자산에도 큰 손실이다.

일반적으로 마케팅기법으로 고객과의 다양한 관계 유지를 통한 고객관계관리(Customer Relationship Management; CRM)가 있다. 이러한 CRM기법은 과거의 대중 마케팅(Mass Marketing), 세분화 마케팅(Segmentation marketing), 틈새 마케팅(Niche marketing)과는 구분되는 마케팅의 방법론으로서, 마케팅에 필요한 고객정보를 수집·분석·적용하는 일련의 마케팅 방식을 지칭하는 포괄적인 개념이다.

하지만 이러한 고객정보 기반에서의 CRM 기법은 양질의 고객정보를 확보하는 기능을 만족시키기에는 문제가 있다. 즉 회원으로 가입하는 대부분의 고객들은 개인 정보 유출 위험으로 자신의 정보 공개를 꺼리는 경향이 강하다. 이러한 경향 때문에 대다수의 기업들은 설문 조사 이벤트, 고객의 활동 내역 분석 등을 실시함으로써 고객 성향 분석을 통한 양질의 고객정보를 확보하기 위해 많은 자금을 투여하면서 다양한 노력을 기울이고 있는 실정이다.

또한 이러한 과정에서 기업들간의 전략적 제휴로 고객정보의 공유를 시도하고 있지만, 비중복가입 고객 등에 대한 고객정보의 유출이라는 문제를 피할 수 없다. 아울러, 전략적 제휴의 수행과정에서도 고객의 동의 및 관련회사의 인증, 공유에 따른 문제의 복잡성 등 많은 제약이 따른다. 따라서 거시적으로 보면 가입된 고객에 대한 양질의 정보가 이미 제공되어 있으면서도 적절하게 이용되지 못하고 있으며, 각 기업에서는 필요한 양질의 정보를 추가적으로 확보하기 위해 값비싼 대가를 지불하고 있는 실정이다.

따라서 중복가입된 고객에 대해 필요한 고객의 정보를 공유하면서도 각 회사자체적으로는 고객 정보의 보안을 유지할 수 있는, 상반된 개념을 수행할 수 있는 새로운 보안기법이 필요하며, 이러한 암호화기술은 인터넷의 발달과 대중성으로 인해 더욱 절실하게 요구되고 있다.

발명이 이루고자 하는 기술적 과제

따라서, 전술한 문제점을 해결하기 위한 본 발명의 목적은, 참여기업들이 동일한 방법의 암호화를 수행하여 참여기업 소유 고객정보의 유출을 원천적으로 봉쇄하면서 복호화를 하지 않은 상태에서 공통 정보를 추출함으로써, 필요한 고객 정보의 공유를 통한 마케팅 효율의 극대화 및 공동마케팅 시장의 활성화를 추구할 수 있는, 보안성을 가지는 고객정보 공유 시스템 및 방법에 대한 기술을 제공함에 있다.

본 발명을 적용할 경우 참여기업은 자사의 핵심 고객 정보의 유출을 원천적으로 봉쇄하면서 다른 기업들과 공유된 고객 정보를 통한 마케팅이라는 이득을 얻을 수 있게 된다. 따라서 고객 정보의 유출의 책임 소재가 분명하므로 여러 기업들이 참여하는 공동마케팅 시장의 활성화와 참여기업들의 마케팅 효율의 극대화의 효과를 얻을 수 있게 된다.

이를 위해 본 발명에서는 공동마케팅을 위한 복호화가 불가능한 효율적이고 안전한 시스템을 실현하기 위해서 본 발명에서 제시하는 암호화 방법은 다음의 기술적 과제들을 해결하는 것이 필요하다.

1. 암호화된 정보는 주관사이건 참여기업이건 복호화가 불가능해야 한다. (복호화 불능)
2. 암호화된 정보를 복호화하지 않은 상태에서 암호화되기 전의 정보가 서로 같은지 판별이 가능해야한다. (동일성 판별가능)

본 발명에서 이용되는 고객정보는 다른 참여기업에게 보안이 될뿐더러 정보의 동일성을 판단하는 주관사도 원천적인 정보를 알 수 없어야 한다. 기존의 암호화 기법은 주로 정보의 안전한 전송과 복호화에 초점을 맞추고 있기 때문에 단순한 적용만으로는 위의 조건을 만족시킬 수 없다. 예를 들어 각각의 참여기업이 동일한 공개키와 비밀키를 가질 경우 비밀키 하나만 입수하면 쉽게 복호화가 가능하여 보안이 취약한 시스템이 된다. 또 다른 방법으로는 참여자들끼리만 비밀키를 공유하고 주관자는 공개키만을 알고 있도록 제한하는 방법을 생각해볼 수도 있으나, 이 방법은 참여자 수가 일정 규모 이상 되면 현실적으로 보안이 어렵게 된다. 따라서, 상기 목적을 달성하기 위해서는 새로운 암호화 기법이 필요하다.

발명의 구성 및 작용

이와 같은 목적을 달성하기 위한 본 발명의 보안성을 가지는 고객정보 공유시스템은, 주관사 및 다수 참여기업들을 네트워크로 연결하는 상태에서,

암호화를 위한 암호화수단을 제공하고 다수 참여기업들의 암호화된 고객정보를 전송받아 공통 정보를 추출하며, 추출된 고객정보를 처리한 결과의 내용을 필요한 다수의 참여기업들로 전송하는 주관사의 처리장치, 및 주관사의 처리장치로부터 제공된 암호화수단을 이용하여 자체가입한 가입고객정보를 암호화하여 주관사로 전송하며, 주관사에서 추출한 고객정보를 처리한 결과의 내용을 전송받는 다수 참여기업들의 처리장치를 포함함으로써,

보안을 유지하는 상태에서 다수 참여기업들의 고객 정보를 공유하는 것을 특징으로 한다.

아울러 본 발명에 따른 보안성을 가지는 제1의 고객정보 공유 방법은, 주관사 및 다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

참여기업 자체의 고객정보를 암호화하기 위해 키없는 단방향함수를 포함한 암호화수단을 주관사의 처리 장치에서 다수

의 참여기업으로 전송하는 암호화수단 전송단계, 전송된 암호화수단 및 키없는 단방향함수를 이용하여 다수 참여기업의 처리장치에서 차체 가입고객 정보를 암호화하는 단방향함수 암호화단계, 암호화한 가입고객 정보를 주관사의 처리장치로 전송하는 고객암호화정보 전송단계, 전송된 고객암호화정보로부터 공통 정보를 추출하는 공통 정보 추출단계, 추출된 공통 정보에 대한 가입고객의 정보를 처리하여 해당 참여기업의 처리장치로 전송하는 산출물 전송단계를 포함하며,

본 발명에 따른 보안성을 가지는 제2의 고객정보 공유 방법은,

다수 참여기업 자체의 가입고객정보를 암호화하기 위해 소정의 암호화수단을 주관사의 처리장치에서 다수의 참여기업으로 전송하는 암호화수단 전송단계, 다수 참여기업의 순서를 정하고 다수 참여기업의 가입고객 정보를 암호화하기 위해 주관사 및 다수 참여기업들의 공개키를 상호 교환하는 공개키 상호교환단계, 전송된 암호화수단 및 공개키를 이용하여 다수 참여기업의 처리장치에서 차체 가입고객 정보를 암호화하는 공개키 암호화단계, 암호화한 가입고객 정보를 주관사의 처리장치로 전송하는 고객암호화정보 전송단계, 전송된 고객암호화정보로부터 공통 정보를 추출하는 공통 정보 추출단계, 추출된 공통 정보에 대한 가입고객의 정보를 처리하여 해당 참여기업의 처리장치로 전송하는 산출물 전송단계를 포함하여 진행된다.

이하 첨부된 도면들을 참조하여 본 발명에 따른, 보안성을 가지는 고객정보 공유 시스템 및 그 방법을 자세히 설명한다.

본 발명은 암호학, 고객관계관리인 CRM, 정보시스템대행업인 ASP (Application Service Provider)등에 관련된 기술이라 할 수 있다.

암호학에서 암호화란 특정 알고리즘을 이용하여 데이터를 암호문으로 변환하는 과정을 말하며, 복호화란 암호문을 원래의 데이터로 복원하는 과정을 말한다. 이때 암호화 하고자 하는 문장을 평문(plaintext)이라고 하고 암호화된 결과를 암호문 (ciphertext)이라고 한다.

대표적인 암호화 방식으로는 단일키 암호화 방식 (one - key cryptosystem)과 공개키 암호화 방식 (public - key cryptosystem)이 있다. 단일키 암호화 방식은 암호화 · 복호화에 같은 키가 사용되는 것을 의미하며, 공개키 암호화 방식은 두개의 키 즉, 비밀키와 공개키를 가진 방식을 의미한다. 이러한 암호화 방식은 주로 안전한 정보의 전송, 인증(authentication), 디지털 서명 등의 정보의 암호화 및 그에 따른 복호화에 초점이 맞추어져 있다. 즉, 정보의 암호화는 곧 원래의 평문으로의 복호화 가능성을 전제로 한다.

또한 암호학에서 단방향 함수 (one - way function)란 주어진 정보를 변환하는데 있어서 변환된 결과를 가지고 원래의 정보를 복원시키는 것이 불가능한 함수를 말한다. 안전성이 보장된 암호화 시스템은 대부분 단방향 함수로 볼 수 있는데, 이러한 암호화 시스템의 경우도 복호화에 필요한 키 값을 알면 언제든지 손쉽게 복호화하여 원래의 정보를 얻을 수 있다. 단방향 함수 가운데에서도 키 없는 단방향 함수란 원래의 정보로 복원시키기 위한 키가 존재하지 않는 단방향 함수를 의미하며, 따라서 이 경우 암호화된 정보의 복호화 가능성이 원천적으로 봉쇄되게 된다.

전술한 바와 같이 CRM(Customer Relationship Management)은 고객과의 다양한 관계 유지를 통해서 마케팅에 필요한 고객정보를 수집/분석/적용하는 마케팅 방식을 의미한다. 이러한 CRM기법은 수집한 고객정보를 중심으로 진행되기 때문에의 수집된 고객정보의 양과 질이 마케팅의 승패에 결정적인 영향을 미치게 되지만, 전술한 바와 같이 고객들이 자신의 정보를 노출시키는 것을 꺼리기 때문에 CRM을 수행하는 기업들이 큰 어려움에 처하는 문제점을 안고 있다.

ASP(Application Service Provider) 서비스란 고객사가 계약을 통해 ASP 서비스업체가 소유하는 시설을 활용하는 것으로 ASP업체는 다수의 고객에게 서비스를 제공하는 것이다. ASP시장은 전사적자원관리(ERP; Enterprise Resource Planning)나 공급망관리(SCM; Supply Chain Management), CRM 등의 영역에 급속히 확장되고 있는 실정이다.

이중에서도 전술한 CRM 분야에서 ASP 모델에 대한 관심이 증대되고 있다. ASP 모델을 공동마케팅에 적용할 경우 각 고객사들은 ASP에게 자사가 보유한 고객정보를 제공하고 ASP는 각 고객사로부터 제공받은 고객정보들을 취합하여 일관된 흐름이나 경향을 파악하는 데이터 마이닝(data mining)을 거쳐 각 고객사가 필요로 하는 마케팅 정보를 제공하게 된다. CRM의 ASP 모델은 본 발명의 대표적 응용 예가 될 수 있다. 하지만 전술한 바와 같이, 이러한 과정에서 참여기업들은 자사가 보유한 고객정보를 ASP에 제공하게 되는데 이 과정에서 고객정보의 유출이라는 문제가 발생하게 된다.

따라서, 본 발명에서는 이러한 문제점을 해결하기 위해서 중복가입고객의 정보 추출을 주관하는 ASP 주관사는 암호화된 결과를 복호화할 수 없지만, 여러 참여기업들로부터 제공받는 고객정보들의 동일성 판별이 가능하도록 암호화하는 기술을 제공하게 된다. 후술하겠지만 본 발명의 암호화과정은 해당 가입고객에 대한 정보를 원천적으로 보유하고 있는 참여기업이외에는 가입고객에 대한 정보를 확인할 수 없도록, 복호화가 불가능한 암호화 방법을 이용함을 그 핵심으로 한다.

도 2는 본 발명의 일실시예에 따른 보안성을 가지는 고객정보 공유시스템의 구성도이다.

도시한 바와 같이, 본 실시예의 보안성을 가지는 고객정보 공유시스템은 공동마케팅을 주관하는 주관사의 처리장치(200)와 참여기업의 처리장치(300)가 인터넷등의 네트워크(400)를 통해 연결되어, 서로 정보를 교환할 수 있도록 구성된다.

이러한 주관사의 처리장치(200)는, 암호화에 관련된 암호화 수단을 생성하고 관리하는 암호화 관리부(210), 수신된 암호화 고객정보들을 처리하는 데이터 관리부(220), 그리고 처리 결과를 참여기업에게 제공하는 서비스 관리부(230)로 크게 구분할 수 있다. 그리고 이 중 데이터 관리부(220)는, 중심이 되는 데이터베이스(221), 이 데이터베이스(221)와의 연동을 통해 추가적 암호화 및 복호화를 수행하는 암호화단(222), 고객정보의 보정 및 동일성 판별을 통해서 고객정보를 취합하는 고객정보 취합단(223), 그리고 취합된 고객정보를 마케팅에 필요한 서비스 정보로 가공하는 데이터 마이닝단(224 ; data mining)으로 나눌 수 있다.

본 발명에서의 공동마케팅은 유출되어서는 안 되는 고객정보들의 상호 공유라는 다소 모순적인 전제로 인해서 특수한 암호화 기법의 적용을 필요로 한다. 각 참여기업들이 가진 고객의 개인정보는 핵심적인 정보와 부수적인 정보로 나뉘어진다. 즉, 주민등록번호, 이름, 전화번호 등의 그 개인에게 고유한 정보가 핵심적인 정보가 되며, 성별, 나이, 직업, 취미, 특기, 관심분야 등의 나머지 정보들이 부수적인 정보들이 된다. 본 발명에서는 공동마케팅을 위해 이러한 고유 정보를 암호화하여 주관사에게 보내게 된다. 이때 주관사를 비롯하여 다른 참여기업들이 암호화된 정보를 복호화하지 못하게 하면서 그 정보들의 동일성은 판별할 수 있게 해주는 것이 핵심적인 것이다.

따라서 공동마케팅을 위한 암호화 수단은 다음의 조건들을 만족해야 한다. 첫째, 암호화된 정보는 복호화가 불가능해야 하며, 둘째, 암호화된 정보를 가지고 암호화되기 전의 정보가 서로 같은지 판별이 가능해야 한다.

본 발명에서는 이러한 조건들을 만족시키는 암호화를 위해서 크게 두 가지의 암호화 방식으로 진행한다. 첫번째 실시예는 각각의 참여기업에서 키 없는 단방향 함수를 이용해서 암호화하고, 주관사는 이렇게 암호화된 정보를 전송받은 후 이를 통해 중복된 고객정보를 추출하는 것이다. 그리고 두 번째 실시예는 각 참여기업과 주관사가 서로의 공개키를 공유한 상태에서 연동을 통해 순차적으로 암호화하는 공개키 암호화 기법을 이용한 암호화방식이다.

도 3은 본 발명의 일실시예에 따라 키없는 단방향 함수를 이용하여 암호화하는 보안성을 가지는 고객정보 공유방법의 순서도이다.

도시한 바와 같이, 본 실시예의 보안성을 가지는 고객정보 공유방법은 크게 암호화수단 전송단계, 단방향함수 암호화단계, 고객암호화정보 전송단계, 중복가입고객 추출단계, 그리고 산출물 전송단계로 구분할 수 있다.

본 실시예의 키 없는 단방향 함수를 이용한 암호화에 따른 고객정보 공유방법은 복호화에 필요한 키가 처음부터 존재하지 않기 때문에, 복호화 가능성은 원천적으로 봉쇄된다. 뿐만 아니라 본 실시예에서는 키 없는 단방향 함수를 이용하여 암호화를 실시하게 되므로, 암호화에 따른 추가적인 시간적 · 공간적 자원의 소모를 최소화할 수 있다.

전술한 바와 같이 단방향 함수란 간단히 말해 주어진 정보를 변환하는데 있어서 원래의 정보로 복원시키는 것이 불가능한 함수를 의미한다. 하지만 종래의 암호 시스템에서는 이러한 단방향 함수를 주로 메시지의 교환시 보안을 유지하기 위한 목적으로 사용되었기 때문에, 키 값을 가지고 있어서 이 키를 가지고 암호화와 복호화를 수행하였다. 즉 키만 알면 언제든지 암호화된 정보를 복호화할 수 있으므로 키를 공유하는 암호화 방식은 고객정보의 유출이라는 심각한 문제를 야기하였다.

하지만 본 실시예에서 사용하는 키 없는 단방향 함수는 키가 없으므로 복호화가 근원적으로 불가능하게 되며, 키를 서로 공유할 필요가 없어지므로 고객정보의 유출을 원천적으로 차단할 수 있게 된다.

가입고객정보는 전체적으로 암호화하여 것도 가능하지만, 중요정보만 선별적으로 암호화할 수 있으며 이러한 선별적 암호화는 시간적, 경제적인 이점을 제공하게 된다. 즉 개인정보의 유출 우려가 없는 부수적인 정보는 암호화하지 않고 그냥 보내게 되는데, 이 경우 암호화하지 않더라도 그 정보가 어떤 고객의 정보인지 알 수 없으므로 고객 개인의 정보에 대한 유출위험은 전혀 없게 된다. 일례로 어떠한 가입고객에 대한 주민번호, 이름, 전화번호 등 중요정보는 암호화하여 내보내고, 그 이외의 부수정보는 암호화 없이 내보내면 된다.

도 3과 같이, 먼저 주관사의 처리장치(200)는 각 참여기업의 처리장치(300)로 암호화수단을 제공하게 된다. 이러한 암호화수단에는 주관사에서 결정한 키없는 단방향 함수의 제공을 핵심으로 한다. 이 과정은 오프라인으로 이루어질 수도 있다.

이 후 각 참여기업의 처리장치는 주관사로부터 제공된 암호화수단의 키없는 단방향 함수를 이용하여 암호화하는 단방향함수 암호화단계를 진행하게 된다.

키없는 단방향 함수로는 어떠한 방법을 사용해도 무방하다. 기존의 UNIX에서는 패스워드 인증 방법으로 DES 방식을 사용하되, DES의 전형적인 사용방법과 반대로 임의의 사용자마다 상수를 하나 고정해놓고 이 상수를 패스워드를 키값으로 하여 암호화한다. NT에서는 패스워드를 MD5 해쉬함수에 적용하여 암호화한다. 이러한 방식들을 포함하여 기존에 알려진 어떠한 방법을 써도 상관없다.

단방향 함수의 한 예로 다음과 같은 방식을 사용할 수도 있다.

미국 MIT의 Rivest, Shamir, Adleman에 의해 발표된 RSA 암호화방식은, 충분히 큰 두 개의 소수를 곱해 만들어진 합성수를 이용하기 때문에 소인수분해가 거의 불가능하여 아주 안전한 것으로 알려진 암호화방식이다. 즉 길이의 차이에 따른 정도는 있겠지만, 공개키가 약 100자리(100 digit) 정도의 정수인 경우 이를 인수분해하여 비밀키를 알아낸다는 것은 현재의 기술수준으로는 거의 불가능한 것으로 판명됨으로써, 높은 안정성이 보장되고 있다. 따라서 암호화된 결과로부터 원래의 정보를 역으로 추출하는 것은 거의 불가능하며, 이러한 특성을 응용하여 아래와 같은 키 없는 단방향 함수를 만들 수 있다.

우선 전송된 고객정보를 초기값으로 하여 두 개의 랜덤소수(random number generator)를 생성한다. 일례로 암호화하려는 고객정보를 X라고 하면, 이 X를 충분히 안전한 랜덤소수생성기의 초기값(random seed)으로 하여 충분히 큰 두 개의 랜덤소수를 생성한다. 이렇게 생성된 서로 다른 두 개의 소수를 p, q라 할 때, 이 두 소수의 곱 $n (= p \cdot q)$ 이 암호화 결과값이 된다. 즉, X를 입력으로 하고 결과값 n을 출력으로 하는 키 없는 단방향 함수가 만들어진 것이다.

이렇게 각 참여기업에서 단방향함수에 의한 암호화를 수행한 후, 각 참여기업들의 처리장치(300)는 암호화한 고객정보를 주관사의 처리장치(200)로 전송하는 고객암호화정보 전송단계를 진행하게 된다.

이 후 주관사로 전송된 암호화된 고객암호화정보는 주관사의 처리장치(200)에서 후처리를 통하여 공통된 데이터를 추출하는 중복가입고객 추출단계가 진행된다.

이를 위해 주관사 처리장치의 데이터마이닝단(224)에서는 암호화된 고객정보들을 필요에 따라 취합하는 데이터마이닝(data mining)을 실시하게 된다. 먼저 데이터보정을 실시하게 된다. 본 실시예에서는 고객의 주민 번호를 암호화하여 고객정보를 취합하게 되는데 잘못된 주민 번호가 있을 경우 중복 고객의 추출에는 많은 어려움이 있게 된다. 이를 어느 정도 보정해 주기 위해 주소나 전화번호 등의 고객을 알 수 있게 해주는 추가 정보의 암호화된 정보를 활용하여 보정해 줄 수 있다. 이러한 데이터마이닝(data mining) 단계에서 보정이 필요한 경우 각 참여기업들에 데이터가 보정을 지시하고 관련된 내용을 제공받을 수 있게 된다. 이러한 보정은 본 발명의 목적인 주관자 및 다른 참여기업이 복호화가 불가능한 상태에서 개인정보의 동일성을 판단한다는 점이 충족되는 한 정보의 정확성 요구에 따라 실시할 수도 있고 실시하지 아니할 수도 있다.

이 후 고객정보를 대조하여 본 발명의 핵심적 내용인 중복고객을 추출하는 단계를 수행하게 된다. 전술한 바와 같이 지정된 방식에서 암호화된 특정정보(X)가 같다면 원래의 정보도 같게 된다. 이는 동일한 암호화 방법을 사용하는 한 여러 번 암호화를 해도 변하지 않는 특성이다. 주관사는 이미 참여기업에서 받은 암호화된 고객정보는 주관사의 처리장치(200)에서 제공한 키없는 단방향함수에 의해 암호화했으므로 이들이 일치하는지를 확인하여 중복 고객을 추출할 수 있다. 따라서 이 단계에서 특정정보, 예를 들어 주민번호가 일치된 것으로 파악된 고객은 다수의 참여기업(사이트)에 중복가입하고 있는 동일인인 것이다.

이 후 주관사는 상기 일련의 과정을 통하여 최종적으로 추출된 추출결과를 처리하여 해당 참여기업으로 전송하는 산출물 전송단계를 진행하게 된다. 또한 주관사의 처리장치(200)는 이러한 추출결과를 자체 정리한 후 데이터베이스하게 된다.

도 4는 본 발명의 일실시예에 따라 공개키에 의한 암호화기법을 이용하여 암호화하는 보안성을 가지는 고객정보 공유방법의 순서도이다.

도시한 바와 같이, 본 실시예의 공개키 암호화기법에 의한 보안성을 가지는 고객정보 공유방법은 크게 암호화수단 전송단계, 공개키 상호교환단계, 공개키 암호화단계, 고객암호화정보 전송단계, 중복가입고객 추출단계, 그리고 산출물 전송단계로 구분할 수 있다.

본 실시예에서 수행하는 주관사와의 연동을 통한 공개키 암호화 기법은 외부에 공개된 공개키로 암호화 할 수 있지만 비밀키를 모르면 복호화가 불가능하다. 따라서 본 실시예에서는 각각의 참여기업(300)이 서로 다른 공개키와 비밀키를 가지게 되는데, 각 참여기업들의 핵심정보를 모든 참여기업들의 공개키로 순차적으로 암호화하므로 모든 비밀키가 유출되지 않는 이상 복호화가 불가능하게 된다. 따라서 보안이 유지된 상태에서도 공동마케팅에 참여하는 모든 참여기업들의 고객정보는 동일성 판별가능의 조건을 만족시키게 된다. 또한 이러한 순차적인 암호화의 순서가 하나로 정해지면 각 참여기업의 정보들은 결국 같은 방식으로 암호화된 결과가 되며 따라서 본 실시예의 이러한 순차적 적용방식은 공개키 암호화 기법을 이용한 암호화 수단의 하나로 이용될 수 있다.

또한 이러한 공개키에 의한 암호화과정에서 모든 기업들의 공개키로 암호화하지 않고 고객정보 공유를 원하는 임의의 두 기업만을 대상으로 할 수도 있다. 이것은 위 순차적 암호화 방식에서 $K=2$ 인 특수한 경우에 해당된다. $K=3, 4, \dots$ 인 경우들도 마찬가지이다.

도 4에 도시된 바와 같이, 본 실시예에서도 최초 먼저 주관사의 처리장치(200)는 각 참여기업의 처리장치(300)로 암호화수단을 전송하는 암호화수단 전송단계를 수행하게 된다.

전술한 바와 같이 이러한 암호화수단은 주관사 처리장치의 암호화관리부(210)는 생성하여 전송하는 것으로, 이는 주관사에서 자체적으로 결정한 암호화방식이나 암호화함수 등 각 참여기업에서 암호화를 수행시킬 수 있는 제반내용을 포함하는 것이다. 암호화수단은 오프라인으로 전달될 수도 있다.

하지만 도 3의 실시예와 달리, 본 실시예의 방법에서는 본 고객정보 공유시스템에 참여하고 있는 다수의 참여기업에 대한 순서를 결정한 일련번호도 전송하게 된다. 즉 n 개의 참여기업이 참여하고 있다면, 주관사에서는 1부터 n 까지의 일련번호를 할당하게 되고, 이러한 할당내역은 주관사의 데이터베이스(221)에 저장하게 된다. 아울러 본 실시예의 진행과정은 주관사의 데이터베이스(221)에 모두 저장된다.

이 후 주관사로부터 일련번호가 할당되었으면 주관사와 각각의 참여기업은 자체의 공개키와 비밀키를 생성하고, 생성한 공개키를 서로 교환하는 공개키 상호교환단계를 실시하게 된다. 아울러 생성된 공개키에 암호화방식 및 복호화방식도 가지게 된다. 일례로 참여기업A는 공개키로 암호화하는 E_a 방식과 비밀키로 복호화하는 D_a 방식을 가지며, 따라서 암호화된 정보는 D_a 가 있어야 원래 정보를 알 수 있게 된다. 여기서 공개키는 서로 교환하여 공개될 수 있는 것이지만, 비밀키는 자체적으로 보유할 뿐 공개하지 않으며, 비밀키 공개에 대한 책임은 해당 참여기업에 있게 된다.

설명의 편의상 참여기업의 일련번호에 따라 1번 공개키, 1번 비밀키, 2번 공개키, ……., n 번 공개키, n 번 비밀키로 하여 서술한다.

후술하겠지만, 본 발명에서는 보안을 유지하면서 동일한 값인지를 확인할 필요가 있는 데이터(예, 주민번호)를 1번 공개키부터 n 번 공개키를 이용하여 n 회 암호화한다. 따라서 이를 원래의 주민번호로 복원하려면 1번부터 n 번까지의 비밀키를 다 가지지 않고는 복원할 수 없으며, 다만 주관사는 두 암호화된 결과가 같다는 사실만 감지할 수 있게 된다.

본 실시예에 따른 공개키에 의한 순차적 암호화 방식은 주민번호와 같이 가입고객을 구별할 수 있는 특정자료(X)를 정해진 순서대로 암호화를 해나는 방식이다. 즉 일곱번째(7th)인 제(7)참여기업의 경우 첫번째(1th)의 제1공개키로부터 제7공개키까지 연속적으로 암호화한 데이터, $E_7(E_6(E_5(E_4(E_3(E_2(E_1[X]))))))$ 를 주관사에 전송하게 된다.

이후 이렇게 암호화한 각 참여기업들의 고객정보를 참여기업의 처리장치(300)에서 주관사의 처리장치(200)로 전송하는 고객암호화정보 전송단계에서, 추가적 보안을 위해 주관사의 공개키를 이용하여 한 번 더 암호화를 해서 보낼 수도 있다. 이 경우, 주관사는 고객정보 수신 직후 자신의 비밀키로 복호화를 하는 과정을 거친다.

이 후 주관사로 전송된 암호화된 고객암호화정보는 주관사의 처리장치(200)에서 후처리를 통하여 공통된 데이터를 추출하는 중복가입고객 추출단계가 진행된다.

전체 참여기업에서 순차적 암호화 방식으로 암호화한 경우에, 주관사로 전달된 정보는 아래와 같다.

- 제(1)참여기업 : $E_1[X]$

- 제(2)참여기업 : $E_2(E_1[X])$

- 제(3)참여기업 : $E_3(E_2(E_1[X]))$

:

:

- 제(n)참여기업 : $En(En_{-1}(\cdots(E_3(E_2(E_1[X])))\cdots))$

즉, 최초 참여기업에서 연속방식에 의해 암호화된 경우, 특정된 정보에 대한 해당 참여기업까지의 암호화를 수행한 암호화정보가 주관사로 전송된다. 따라서 주관사에서는 최종적인 암호화정보, 즉 제(n)참여기업의 암호화정보인 $En(En_{-1}(\cdots(E_3(E_2(E_1[X])))\cdots))$ 에 맞도록 제(1)참여기업에서 제(n-1)참여기업까지의 정보를, 전송된 각 참여기업의 공개키를 순서적으로 적용하여 추가암호화를 실시하게 된다. 이렇게 추가암호화함으로써 각 참여기업으로부터 얻은 자료를 동일한 방식으로 암호화할 수 있고, 따라서 주관사는 각 기업 고객의 개인 정보 유출 없이 쉽게 중복 고객을 추출할 수 있다.

아울러 이러한 중복가입고객 추출단계에서 실시하는 데이터마이닝(data mining), 데이터보정, 중복가입고객의 추출 그리고 데이터베이스 등은, 도 3의 키없는 단방향 함수를 이용하여 암호화함으로써 보안성을 가지는 고객정보 공유방법에서와 같으며, 이 후 진행하는 중복가입고객정보 전송단계 및 요청고객정보 전송단계 또한 같다.

본 발명의 보안성을 가지는 고객정보 공유시스템은, 주관사의 존재 없이 다수 참여기업들만을 네트워크로 연결하는 상태에서 변형 적용될 수도 있는데, 이 경우는 위의 기술에서 주관사의 처리 장치가 참여기업의 역할로 바뀔 뿐 다른 부분들은 대부분 동일하다.

즉, 두 개 이상의 참여기업들이 네트워크로 연결된 시스템에 있어서,

공통된 암호화수단을 이용하여 자체 가입한 가입고객정보를 암호화하는 암호화 장치; 암호화된 고객정보를 상기 다수 참여기업으로 전송하거나, 아래에서 언급되는 데이터 처리장치에서 가공 처리를 한 결과 중 필요한 정보를 상기 다수의 참여기업들로 전송하는 전송장치; 전송받은 고객정보를 이용하여 가공처리를 하는 데이터 관리장치; 및 다수 참여기업들의 전송장치로부터 전송된 고객정보 또는 데이터 관리장치에서 가공 처리된 결과 중 필요한 정보를 전송받는 수신장치를 포함함으로써, 참여기업들 모두 복호화가 불가능한 상태에서 고객정보의 동일성을 판단하여 이용할 수 있는 것을 특징으로 한다.

주관사가 있는 모델과는 주관사와 관련된 부분에서 주로 차이가 나고 다른 부분들은 거의 동일한데, 주관사가 있는 모델에서 주관사의 처리장치에서 하는 작업들을 모두 각 참여기업들 자신이 하게 된다.

아울러 본 발명에 따른 보안성을 가지는 제1의 고객정보 공유 방법은, 다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

키없는 단방향함수를 이용하여 상기 다수 참여기업의 처리장치에서 자체 가입고객 정보를 암호화하는 단방향함수 암호화단계; 암호화한 가입고객 정보를 상기 다수 참여 기업 중 일부 또는 전부의 처리장치로 전송하는 고객암호화정보 전송단계; 전송된 고객암호화정보를 수신하여 중복된 정보를 추출하는 중복가입고객 추출단계; 추출된 중복정보에 대한 가입고객의 정보를 처리하여 데이터마이닝 등의 가공 처리를 하는 자료처리단계를 포함하며,

본 발명에 따른 보안성을 가지는 제2의 고객정보 공유 방법은, 다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

상기 다수 참여기업의 순서를 정하고 이들의 가입고객 정보를 암호화하기 위해 참여기업들의 공개키를 상호 교환하는 공개키 상호교환단계; 상기 단계에서 전송된 암호화수단 및 공개키를 이용하여 다수 참여기업의 처리장치에서 자체 가입고객 정보를 암호화하는 공개키 암호화단계; 암호화한 가입고객 정보를 상기 다수 참여 기업 처리장치로 전송하는 고객암호화정보 전송단계; 전송된 고객암호화정보를 수신하여 중복된 정보를 추출하는 중복가입고객 추출단계; 추출된 중복정보에 대한 가입고객의 정보를 처리하여 데이터마이닝 등의 가공 처리를 하는 자료처리단계를 포함하여 진행된다.

주관사가 있는 모델과는 주관사와 관련된 부분에서 주로 차이가 나고 다른 부분들은 거의 동일한데, 상기 공개키 상호 교환단계에서는 주관사와의 교신이 빠지며, 공개키 암호화단계 및 단방향함수 암호화단계는 동일하며, 고객암호화정보 전송단계에서는 주관사 대신 다른 참여기업에 전송하게 되며, 중복가입고객 추출단계와 자료처리단계는 주관사에서 하던 것을 각 참여사가 할 뿐 작업의 내용은 동일하다. 순차적 공개키암호화를 위한 참여기업들의 순서(일련번호)는 주관사가 없으므로 참여기업들의 자발적 협의에 의해 정해진다.

상기의 제1, 제2 공유방법은 고품질의 보안을 위한 대표적 두 가지 방법이다. 경우에 따라 다음과 같은 간단한 방법으로도 가능하다. 기업 E가 다른 기업들과 고객정보를 공유하고자 하는 경우의 예를 들어보자. 기업 E는 자신의 공개키로 자신의 고객정보를 암호화하여 상대방 기업들에 전송한다. 자료를 받은 기업은 자신의 고객정보를 기업 E의 공개키로 암호화해본다. 이렇게 하면 다른 기업들은 자신들의 고객정보와 기업 E의 고객정보와의 동일성은 간단하게 체크할 수 있다. 이 방법은 간명하기는 하나 상대방의 비밀키 하나만 알아내면 상대방의 모든 고객정보를 한꺼번에 알 수 있어 보안이 다소 취약하다. 상기의 제1, 제2 공유방법은 이보다 보안의 품질이 훨씬 높은 구현방법들의 예이다.

따라서 전술한 바와 같이, 본 발명은 보안상태에서 서로 다른 기업이나 인터넷 사이트나 가입한 중복고객을 추출하여 이용함으로써 해당 고객에 대한 양질의 서비스 제공이 가능하게 된다. 아울러 본 발명은 공개키의 공유를 통한 선별적인 암호화를 필요적으로 실시할 수 있도록 함으로써, 보안상태에서 정보의 공유라는 다소 이질적인 문제점을 기술적으로 해결하고 있다.

뿐만 아니라, 본 발명은 전술한 바와 같이 키없는 단방향 함수에 의한 암호화와, 공개키의 순차적인 적용을 통한 암호화를 실시하여 고객의 정보를 공유함으로써 실시방법을 다양화하고 있다. 아울러 이러한 실시과정에 있어서도 추가암호화, 가입고객에 관련된 정보의 전체적 또는 선별적인 암호화, 그리고 공개키와 비밀키의 이용 방법의 변화 등 본 발명의 기술 개념을 바탕으로 보다 다양하게 변경하여 실시하는 것이 가능하다.

발명의 효과

본 발명을 이용함으로써 각 기업은 자신이 갖지 않은 고객정보까지 이용할 수 있으며, 마케팅이나 전자상거래 등의 효율을 높이되 고객정보의 유출은 근원적으로 차단할 수 있게 된다. 또한 고객정보의 유출을 근원적으로 차단할 수 있기 때문에 마케팅을 위해서 정보를 상호 교환할 수 있는 새로운 시장을 형성시키는 것이 가능하다. 아울러 각 기업의 고객정보에 대한 책임소재가 분명하기 때문에 상호간의 정보공유를 통한 공동마케팅의 확산 속도를 가속화하여 마케팅 시장의 활성화와 그 효율성을 극대화시킬 것으로 예상된다.

(57) 청구의 범위

청구항 1.

주관사 및 다수 참여기업들을 네트워크로 연결하는 시스템에 있어서,

암호화를 위한 암호화수단을 제공하고 상기 다수 참여기업들의 암호화된 가입고객정보를 전송받아 중복으로 가입된 고객을 추출하며, 상기 추출된 고객정보를 이용하여 가공 처리를 한 결과 중 필요한 사항을 상기 다수의 참여기업들로 전송하는 주관사의 처리장치; 및

상기 주관사로부터 제공된 암호화수단을 이용하여 자체 가입한 가입고객정보를 암호화하여 상기 주관사로 전송하며, 상기 주관사에서 가공 처리된 정보 중 필요한 정보를 전송받는 상기 다수 참여기업들의 처리장치를 포함하여,

주관사 및 참여기업들 모두 복호화가 불가능한 상태에서 주관사가 고객정보의 동일성을 판단하여 이용할 수 있는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유시스템.

청구항 2.

제 1항에 있어서, 상기 주관사의 처리장치는

암호화에 관련된 암호화 수단을 생성하고 관리하는 암호화 관리부;

상기 암호화된 고객정보들을 처리하는 데이터 관리부; 및

상기 처리된 고객정보들을 상기 다수의 참여기업에게 제공하는 서비스관리부를 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유시스템.

청구항 3.

제 2항에 있어서, 상기 데이터 관리부는

각종의 정보를 저장하기 위한 데이터베이스;

상기 주관사의 처리장치로 전송된 고객정보의 보정 및 동일성 판별을 통해 고객정보를 취합하는 고객정보 취합단; 및

상기 취합된 고객정보를 마케팅에 필요한 서비스 정보로 가공하는 데이터 마이닝단(data mining)을 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유시스템.

청구항 4.

두 개 이상의 참여기업들이 네트워크로 연결된 시스템에 있어서,

공동된 암호화수단을 이용하여 자체 가입한 가입고객정보를 암호화하는 암호화 장치; 상기 암호화된 고객정보를 상기 다수 참여기업으로 전송하거나, 하기 데이터 처리장치에서 가공 처리를 한 결과 중 필요한 정보를 상기 다수의 참여기업들로 전송하는 전송장치;

상기 전송받은 고객정보를 이용하여 가공처리를 하는 데이터 관리장치; 및

상기 다수 참여기업들의 전송장치로부터 전송된 고객정보 또는 상기 데이터 관리장치에서 가공 처리된 결과 중 필요한 정보를 전송받는 수신장치를 포함하여,

참여기업들 모두 복호화가 불가능한 상태에서 고객정보의 동일성을 판단하여 이용할 수 있는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유시스템.

청구항 5.

제 4항에 있어서, 데이터 처리장치는

암호화에 관련된 암호화 수단을 생성하고 관리하는 암호화 관리부;

상기 암호화된 고객정보들을 전처리하여 관리하는 데이터 관리부로 이루어진 것을 특징으로 하는, 보안성을 가지는 고객정보 공유시스템.

청구항 6.

제 5항에 있어서, 상기 데이터 관리부는

각종의 정보를 저장하기 위한 데이터베이스;

상기 암호화하여 전송된 고객정보의 보정 및 동일성 판별을 통해 고객정보를 취합하는 고객정보 취합단; 및

상기 취합된 고객정보를 마케팅에 필요한 서비스 정보로 가공하는 데이터 마이닝단(data mining)을 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유시스템.

청구항 7.

주관사 및 다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

상기 다수 참여기업 자체의 가입고객정보를 암호화하기 위해 키없는 단방향함수를 포함한 암호화수단을 상기 주관사의 처리장치에서 상기 다수의 참여기업으로 전송하는 암호화수단 전송단계;

상기 단계에서 전송된 암호화수단 및 키없는 단방향함수를 이용하여 상기 다수 참여기업의 처리장치에서 자체 가입고객 정보를 암호화하는 단방향함수 암호화단계;

상기 암호화한 가입고객 정보를 상기 주관사의 처리장치로 전송하는 고객암호화정보 전송단계;

상기 전송된 고객암호화정보를 수신하여 중복된 정보를 추출하는 중복가입고객 추출단계;

상기 단계에서 추출된 중복정보에 대한 가입고객의 정보를 처리하여 해당 참여기업의 처리장치로 전송하는 산출물 전송단계를 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 8.

다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

키없는 단방향함수를 이용하여 상기 다수 참여기업의 처리장치에서 자체 가입고객 정보를 암호화하는 단방향함수 암호화단계;

상기 암호화한 가입고객 정보를 상기 다수 참여 기업 중 일부 또는 전부의 처리장치로 전송하는 고객암호화정보 전송단계;

상기 전송된 고객암호화정보를 수신하여 중복된 정보를 추출하는 중복가입고객 추출단계;

상기 단계에서 추출된 중복정보에 대한 가입고객의 정보를 처리하여 데이터마이닝 등의 가공 처리를 하는 자료처리단계를 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 9.

제 7항 또는 제8항에 있어서, 상기 단방향함수 암호화단계는

상기 전송된 암호화수단의 랜덤소수 생성기로부터 상기 고객정보를 초기값으로하여 두 개의 랜덤소수(random prime number)를 생성하는 랜덤소수 생성단계; 및

생성된 서로 다른 두 개의 소수값을 곱하여 결과값을 생성하는 결과값 생성단계를 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 10.

제 7항 또는 제8항에 있어서, 상기 단방향함수 암호화단계는

상기 참여기업에 가입한 고객정보의 전체를 암호화하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 11.

제 7항 또는 제8항, 상기 단방향함수 암호화단계는

상기 참여기업에 가입한 고객정보 중 가입고객에 필수적인 중요정보는 암호화하고, 상기 중요정보를 제외한 부수정보는 암호화하지 않은 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 12.

주관사 및 다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

상기 다수 참여기업 자체의 가입고객정보를 암호화하기 위해 소정의 암호화수단을 상기 주관사의 처리장치에서 상기 다수의 참여기업으로 전송하는 암호화수단 전송단계;

상기 다수 참여기업의 순서를 정하고 상기 다수 참여기업의 가입고객 정보를 암호화하기 위해 상기 주관사 및 상기 다수 참여기업들의 공개키를 상호 교환하는 공개키 상호교환단계;

상기 단계에서 전송된 암호화수단 및 공개키를 이용하여 상기 다수 참여기업의 처리장치에서 자체 가입고객 정보를 암호화하는 공개키 암호화단계;

상기 암호화한 가입고객 정보를 상기 주관사의 처리장치로 전송하는 고객암호화정보 전송단계;

상기 전송된 고객암호화정보를 수신하여 중복된 정보를 추출하는 중복가입고객 추출단계;

상기 단계에서 추출된 중복정보에 대한 가입고객의 정보를 처리하여 해당 참여기업의 처리장치로 전송하는 산출물 전송단계를 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 13.

제 12항에 있어서,

상기 공개키 암호화단계에서는 상기 각 참여기업에 부여한 일련의 순서에 따라 K번을 할당받은 해당 참여기업이 제1번부터 제K번까지의 공개키를 순서대로 사용하여 자신의 특정된 고객정보를 연속적으로 암호화하며,

이 경우 상기 중복가입고객 추출단계에서는 상기 해당 참여기업으로부터 암호화정보를 전송받은 주관사가 제K+1번부터 제N번까지의 공개키를 순서대로 더 사용하여 추가암호화 하여 이용하는 연속방식으로 진행되는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

여기서 K는 상기 주관사로부터 부여된 일련번호중의 하나이고, N은 참여사의 총수이다.

청구항 14.

제12항에 있어서,

상기 공개키 암호화단계에서는 상기 각 참여기업에 부여한 일련의 순서에 따라 K번을 할당받은 해당 참여기업이 제1번부터 제N번까지의 공개키를 순서대로 사용하여 자신의 특정된 고객정보를 연속적으로 암호화하여 상기 주관사의 중복 가입고객 추출단계에서는 추가적인 암호화를 하지 않도록 변형하여 운용할 수 있는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 15.

제 12항에 있어서,

상기 암호화정보 전송단계에서는 상기 주관사로 전송시의 추가적 보안을 위해 상기 공개키 암호화단계에서 암호화된 고객정보를 상기 주관사의 공개키로 암호화한 후 전송하며,

이 경우 상기 중복가입고객 추출단계에서는 상기 주관사의 비밀키로 복호화한 후 진행하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 16.

다수 참여기업들의 처리장치를 네트워크로 연결하는 시스템에 있어서,

미리 정해진 참여기업의 순서에 따라 상기 다수 참여기업의 가입고객 정보를 암호화하기 위해 상기 다수 참여기업들의 공개키를 상호 교환하는 공개키 상호교환단계;

상기 단계에서 전송된 암호화수단 및 공개키를 이용하여 상기 다수 참여기업의 처리장치에서 자체 가입고객 정보를 암호화하는 공개키 암호화단계;

상기 암호화한 가입고객 정보를 상기 다수 참여 기업 처리장치로 전송하는 고객암호화정보 전송단계;

상기 전송된 고객암호화정보를 수신하여 중복된 정보를 추출하는 중복가입고객 추출단계;

상기 단계에서 추출된 중복정보에 대한 가입고객의 정보를 처리하여 데이터마이닝 등의 가공 처리를 하는 자료처리단계를 포함하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 17.

제16항에 있어서,

상기 공개키 암호화단계에서는 미리 정해진 참여기업의 일련의 순서에 따라 K번인 해당 참여기업이 제1번부터 제N번까지의 공개키를 순서대로 사용하여 자신의 특정된 고객정보를 연속적으로 암호화 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 18.

제 12항 또는 제16항에 있어서, 상기 공개키 암호화단계는

상기 참여기업에 가입한 고객정보의 전체를 암호화하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 19.

제 12항 또는 제16항에 있어서, 상기 공개키 암호화단계는

상기 참여기업에 가입한 고객정보 중 가입고객에 필수적인 중요정보는 암호화하고, 상기 중요정보를 제외한 부수정보는 암호화하지 않은 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 20.

제 12항 또는 제16항에 있어서, 상기 중복가입고객 추출단계는

전송된 암호화된 고객정보들을 일련의 정리과정으로 취합하는 데이터마이닝(data mining)과정을 포함하여 실시하는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 21.

제7항, 제8항, 제12항, 제16항중 어느 한 항에 있어서, 상기 중복가입고객 추출단계는

고객의 중복가입 여부를 추출하지 않고도 다른 중복정보(예: 나이)를 추출하여 자료 처리에 이용할 수도 있는 변형 기능을 더 갖는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

청구항 22.

제7항 또는 제12항에 있어서, 상기 암호화수단 전송단계는

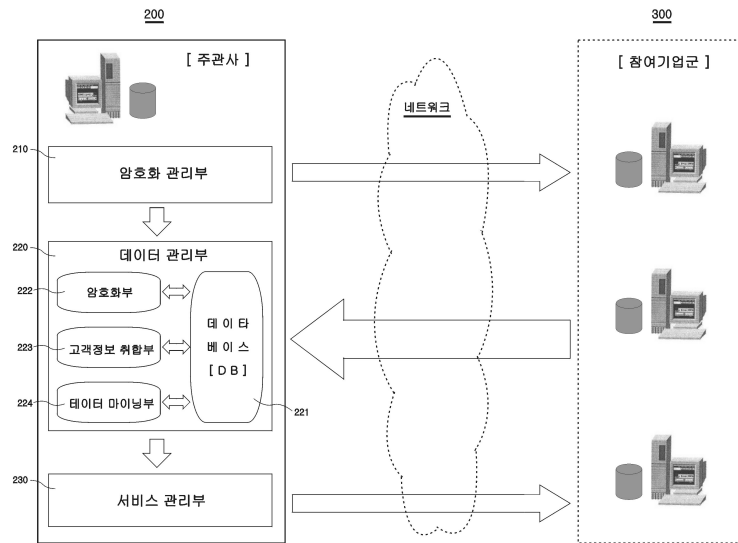
오프라인으로 제공할 수도 있는 것을 특징으로 하는, 보안성을 가지는 고객정보 공유방법.

도면

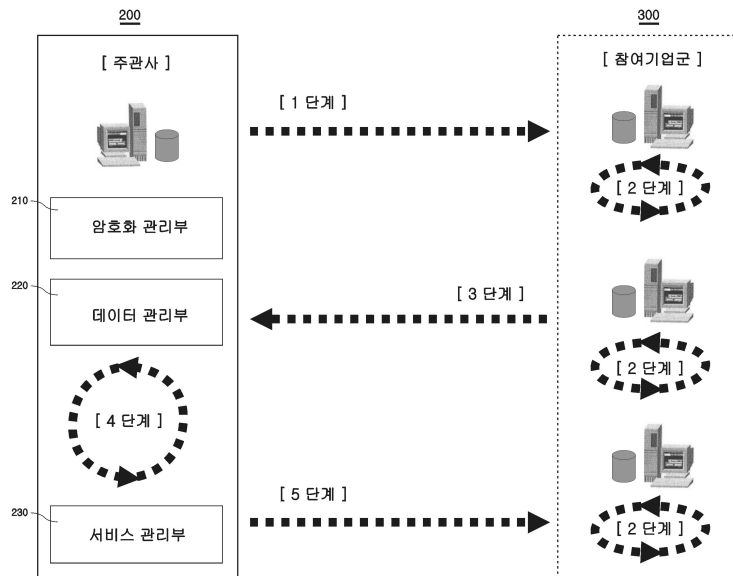
도면 1

[스포츠사이트 A]	[영화사이트 B]	[쇼핑몰사이트 C]
성명	성명	성명
주민등록번호	주민등록번호	주민등록번호
즐거하는 운동	좋아하는 남자배우	주소
좋아하는 스포츠스타	좋아하는 여자배우	전화번호
평균운동시간	가장 감명깊은 영화	메일(선택사항)
동아리가입(선택사항)	팬클럽가입(선택사항)	취미(선택사항)
상품구매정보		특기(선택사항)
		상품구매경로

도면 2



도면 3



도면 4

