명세서

발명의 명칭: 개인 데이터 관리 시스템 및 그 방법

기술분야

[1] 본 발명은 개인 데이터 관리 시스템 및 그 방법에 관한 것으로, 보다 상세하게 유저의 개인 데이터를 해당 유저의 단말기나 특정 서버에 저장하지 않고 랜덤하게 분산 저장하여 관리하고 필요시 복수의 인증절차를 거쳐 해당 유저 단말기에서 개인데이터를 복구함으로써 해킹 가능성이 대폭 낮춤을 물론이고, 해당 유저 단말기의 분실시에도 데이터가 유출되지 않도록 한 개인 데이터 관리 시스템 및 그 방법에 관한 것이다.

배경기술

[2] 최근, 데이터 통신기술이 급속하게 발전함에 따라 개인 휴대단말기를 통해 온라인으로 이체와 결제 등과 같은 각종 금융 처리를 수행하는 바, 금융처리를 위해서는 개인을 식별할 수 있는 식별정보가 필요하고 그 식별정보를 포함한 개인 정보는 금융서버에 저장되어져 있다.

[3] 따라서, 하나의 금융서버에는 몇백만건의 대량 개인 정보가 저장되어져 있으므로 금융서버는 해커들이 노릴만한 표적이 되었다. 실제로 많은 금융서버가 해킹되어 다수의 개인정보가 불법적인 사용을 위해 유통되고 있다.

[4] 금융서버가 해커에게 표적이 되는 가장 큰 이유는 활용 가능한 개인정보가 매우 대량이라는 것 때문이다. 즉, 시간적인 노력을 들이더라도 해킹 성공시 활용할 수 있는 개인정보를 대량으로 얻을 수 있으므로 빈번하게 해커의 표적이 되는 것이다.

[5] 한편, 최근의 개인 휴대 단말기는 카메라와 무선 인터넷이 가능하므로 각종 사생활이 담긴 데이터를 저장하고 있으나, 매우 빈번하게 개인 사생활 데이터가 인터넷에 유출되어 곤욕을 치룬다. 특히, 스타 연예인의 경우에는 개인 사생활 데이터의 유출시 전 국민에게 미치는 그 파급 효과가 매우 크다고 할 수 있다.

[6] 이를 방지하기 위한 다양한 보안 기술이 출시되고 있지만, 현실적으로 서버에 저장된 데이터를 해킹하는 것이 불가능하지 않으며, 개인 휴대 단말기에 저장된 데이터도 해킹하여 유출시킬 수 있다는 문제가 있었다.

발명의 상세한 설명

기술적 과제

[7] 본 발명은 상기한 종래 기술의 사정을 감안하여 이루어진 것으로, 유저의 개인 데이터를 해당 유저의 단말기나 특정 서버에 저장하지 않고 랜덤하게 분산 저장하여 관리하고 필요시 복수의 인증절차를 거쳐 해당 유저 단말기에서 개인데이터를 복구함으로써 해킹 가능성이 대폭 낮춤을 물론이고, 해당 유저 단말기의 분실시에도 데이터가 유출되지 않도록 한 개인 데이터 관리 시스템 및 그 방법을 제공함에 그 목적이 있다.

과제 해결 수단

[8] 상기한 목적을 달성하기 위해, 본 발명의 바람직한 실시예에 따르면 a) 유저 단말기(2)에 탑재된 개인데이터 관리 어플리케이션(6)이 구동신호를 수신하는 과정과; b) 데이터 분산 선택신호가 인가되는 지를 상기 개인데이터 관리 어플리케이션(6)이 판단하는 과정과; c) 특정 데이터가 선택되는 지를 판단하는 과정과; d) 상기 개인데이터 관리 어플리케이션(6)이 데이터 전송 대상 정보를 데이터 관리서버(10)에 요청하는 과정과; e) 상기 데이터 관리서버(10)가 데이터 전송 대상정보를 상기 개인데이터 관리 어플리케이션(6)으로 제공하는 과정과; f) 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터를 소정개수로 분할 처리하는 과정과; g) 각 분할데이터를 데이터 전송 대상 단말기측으로 임의 매칭시켜 전송하는 과정이 포함되어 구성된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[9] 바람직하게, 상기 e) 과정은 상기 데이터 관리서버(10)가 대상이 되는 단말기 식별정보 풀(Pool)에서 소정 개수를 랜덤하게 추출하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[10] 바람직하게, 상기 f) 과정은 상기 개인데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로부터 제공받은 데이터 전송 대상 단말기중 일부를 랜덤하게 추출함으로써 최종 대상 단말기를 결정하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[11] 바람직하게, 상기 g) 과정은 상기 개인데이터 관리 어플리케이션(6)이 별도의 데이터 백업 대상 단말기로 분할된 백업 데이터를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[12] 바람직하게, 상기 g) 과정 다음으로, h) 상기 개인데이터 관리 어플리케이션(6)이 데이터 복구모드가 선택되는 지 판단하는 과정과; i) 특정 데이터 복구신호가 수신되면, 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터의 분할 데이터를 분산 저장하는 대상 단말기 정보를 추출하는 과정과; j) 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터 저장 대상 단말기로 데이터 전송 요청을 수행하여 데이터를 수신받는 과정과; k) 데이터 수신이 완료되면, 상기 개인데이터 관리 어플리케이션(6)이 데이터를 복구하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[13] 바람직하게, 상기 k) 과정중, 일부 단말기로부터 일정시간 경과시까지 데이터 수신이 이루어지지 않으면 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터의 백업 저장 대상 단말기 정보를 추출하는 과정과; 상기 개인데이터 관리 어플리케이션(6)이 해당 백업 저장 대상 단말기측으로 데이터 전송 요청을 수행하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[14] 바람직하게, 상기 g) 과정 다음으로, 상기 개인데이터 관리 어플리케이션(6)이

상기 데이터 관리서버(10)로 데이터 전송 대상 단말기 정보를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[15] 바람직하게, 상기 h) 과정과 i) 과정의 사이에는, l) 상기 개인 데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로 복구할 데이터 정보를 전송하고 해당 데이터의 인증 유저 정보를 요청하는 과정과; m) 상기 데이터 관리서버(10)가 해당 개인 데이터 관리 어플리케이션(6)으로 해당 데이터의 인증 유저정보를 전송하는 과정과; n) 상기 개인 데이터 관리 어플리케이션(6)이 해당 인증 유저의 단말기(2)로 개인 인증정보 입력을 요청하는 과정과; o) 해당 인증 유저의 단말기(2)에서의 개인 인증 성공시 해당 인증 유저의 유저 단말기(2)는 상기 개인 데이터 관리 어플리케이션(6)으로 인증 확인신호를 전송하는 과정이 더 포함되는 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[16] 바람직하게, 상기 m) 과정은 상기 데이터 관리서버(10)가 해당 개인 데이터 관리 어플리케이션(6)으로 단문 메시지 또는 이메일을 통해 인증 유저정보를 전송하는 과정인 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[17] 바람직하게, 상기 o) 과정중 인증 실패신호가 상기 인증 유저의 단말기(2)로부터 수신되면, 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로 인증 실패 정보를 전송하는 과정과; 기설정 시간 초과시까지 인증 신호가 수신되지 않으면, 해당 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로 신규 인증 유저 정보를 요청신호를 전송하는 과정과; 상기 데이터 관리서버(10)가 해당 개인 데이터 관리 어플리케이션(6)으로 신규 인증 유저정보를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[18] 바람직하게, 상기 k) 과정은 기설정시간 경과시까지 특정 분할 데이터가 미수신되는 지를 판단하는 과정과; 특정 분할 데이터의 미수신시, 백업 데이터를 저장하는 유저 단말기 정보를 추출하는 과정과; 상기 개인 데이터 관리 어플리케이션(6)이 해당 백업 데이터를 저장하는 유저 단말기(2)측으로 데이터 전송을 요청하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[19] 바람직하게, 데이터를 분할하여 전송하는 전송 유저 단말기(2-1)와, 분할 저장된 데이터를 복구 시도하는 수신 유저 단말기(2-3)가 각각 상이한 경우, 상기 전송 유저 단말기(2a)는 상기 수신 유저 단말기(2-3)측으로 전송 유저 단말기(2-1)가 분할하여 저장하는 데이터와, 수신 인증정보와, 나머지 분할 데이터의 저장 단말기 정보를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법이 제공된다.

[20] 한편, 본 발명은 유저 인증으로 구동되며, 유저가 선택한 특정 데이터를 다수개로 자동 분리하여 데이터 관리서버(10)로부터 전송된 특정 식별번호의 다수 유저 단말기(2)로 분산하여 전송하고, 유저의 복구 명령에 따라 해당 분산데이터를 취합하여 복구시키는 개인 데이터 관리 어플리케이션(6)이 설치된

유저 단말기(2)와; 상기 개인 데이터 관리 어플리케이션(6)을 설치한 유저 단말기의 식별정보를 저장하고, 상기 유저 단말기(2)로부터 데이터 분산 신호를 인가받아, 데이터 분산 저장의 대상이 되는 특정 유저의 단말기 식별정보를 추출하여 상기 유저 단말기(2)로 전송 처리하는 데이터 관리서버(10)로 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[21] 바람직하게, 상기 데이터 관리서버(10)는 특정 유저의 단말기 식별정보 추출시, 대상이 되는 단말기 식별정보 풀(Pool)에서 소정 개수를 랜덤하게 추출하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[22] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로부터 제공받은 유저의 단말기 식별정보들중 소정 개수를 랜덤하게 추출하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[23] 바람직하게, 데이터를 분산하여 전송하는 상기 유저 단말기(2)와, 데이터를 분산 저장하는 유저 단말기(2)와, 상기 데이터 관리서버(10) 사이에 전송되는 데이터는 암호화된 데이터인 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[24] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 다수개로 분할된 데이터중 어느 한 데이터는 해당 유저 단말기(2)에 저장하고, 그 외의 데이터는 특정 식별번호의 다수 유저 단말기(2)로 분산하여 저장되도록 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[25] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 데이터를 분산 저장하는 다수의 유저 단말기(2) 및 데이터 관리서버(10)와 통신하는 통신모듈(20)과; 개인 식별정보 인증을 통해 유저를 인증하는 유저 인증부(22)와; 상기 데이터 관리서버(10)로 데이터를 분산 저장할 저장 대상정보를 자동으로 요청하는 저장대상 정보 요청부(24)와; 유저가 선택한 특정 데이터를 분할 처리하는 데이터 분할 처리부(28)와; 통신하는 데이터에 대해 암호화 및 복호화를 수행하는 암호/복호 처리부(32)와; 분할 처리된 데이터중 일부 데이터를 저장하고, 각 분할 처리된 데이터를 저장하고 있는 저장 대상 정보를 저장하는 데이터 저장부(34)와; 상기 데이터 관리서버(10)와 통신하여 데이터 저장 대상정보를 제공받고, 특정 데이터를 분할하여 일부 데이터는 저장하고, 그 외 데이터는 다수의 데이터 저장 대상 단말기로 전송하여 분산 저장되게 처리하고, 복구시 해당 저장 대상 단말기측으로 특정 데이터의 전송 요청신호를 전송하여 복구를 수행하는 제어부(36)가 포함된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[26] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 상기 데이터 관리서버(10)로부터 수신한 저장 대상정보중 일부를 랜덤하게 추출하는 대상 랜덤 추출부(26)를 더 포함하여 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[27] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 분할된 데이터들과 해당 데이터를 저장할 대상이 랜덤하게 매칭되게 처리하는 대상 랜덤 매칭부(30)를 더 포함하여 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[28] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 다수의 데이터 전송 대상의 단말기로 분할 데이터를 전송하고, 동일한 분할 데이터를 백업 대상인 단말기측으로 전송하여 백업 저장되게 처리하고, 데이터 복구시 일정시간내 특정 분할 데이터의 복구가 이루어지지 않으면 백업 데이터를 통한 복구 처리를 수행하도록 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[29] 바람직하게, 상기 데이터 관리서버(10)는 특정 데이터의 복구시 인증이 필요한 단일의 인증 유저 정보를 데이터 분산 저장시 등록하고, 상기 개인 데이터 관리 어플리케이션(6)의 데이터 복구 요청시 해당 인증 유저정보를 개인 데이터 관리 어플리케이션(6)으로 제공하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[30] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로부터 인증 유저정보를 제공받으면 해당 인증 유저의 유저 단말기(2)측으로 개인 인증정보 입력을 요청하게 구성되고, 개인 인증 성공시 해당 인증 유저의 유저 단말기(2)는 상기 개인 데이터 관리 어플리케이션(6)으로 인증 확인신호를 전송하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[31] 바람직하게, 상기 데이터 관리서버(10)가 상기 개인 데이터 관리 어플리케이션(6)으로 전송하는 인증 유저 정보는 문자 메시지 또는 이메일을 통해 전송되게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[32] 바람직하게, 상기 개인 데이터 관리 어플리케이션(6)은 기설정 시간 경과시까지 인증 유저의 인증 확인정보가 수신되지 않으면, 상기 데이터 관리서버(10)로 신규 인증 유저정보를 요청하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[33] 바람직하게, 상기 유저 단말기(2)는 원 데이터를 분할하는 전송 유저 단말기(2-1)와, 해당 원 데이터를 복구하는 수신 유저 단말기(2-3)가 각각 서로 다르게 구성된 경우, 상기 전송 유저 단말기(2-1)는 수신 유저 단말기(2-3)로 전송 유저 단말기(2-1)가 분할하여 저장하는 데이터와, 수신 인증정보와, 나머지 분할 데이터의 저장 단말기 정보를 전송하도록 구성된 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

[34] 바람직하게, 분산데이터를 저장하는 상기 다수의 유저 단말기(2)는 서버나 PC 또는 무선 단말기중 어느 하나인 것을 특징으로 하는 개인 데이터 관리 시스템이 제공된다.

발명의 효과

[35] 본 발명에 따른 개인 데이터 관리 시스템 및 그 방법은 개인 데이터를 분할하여 다수의 유저 단말기에 분산 저장함으로써 데이터 관리서버나 이메일 서버 또는 SNS 서버가 해킹되어도 데이터를 전혀 얻지 못하거나 분할 데이터의 일부만을 얻을 수 있어서 해킹의 의미가 없고, 서버가 해킹되었다고 할지라도 다수의 제 2 유저단말기를 해킹하지 않으면 모든 분할데이터를 얻을 수 없고, 특정 데이터와 관련된 다수의 유저 단말기를 해킹한다고 해도 결국 개인 한명의 특정 데이터만을 얻을 수 있으므로 해커에게 실익이 매우 적어서 보안 성능을 강화시킬 수 있다는 장점이 있다.

도면의 간단한 설명

[36] 도 1은 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템의 구성을 도시한 모식도,

[37] 도 2는 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템을 통한 데이터 저장대상 선정상태를 도시한 도면,

[38] 도 3은 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템을 통한 데이터 분할 저장 및 복구상태를 도시한 도면,

[39] 도 4는 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템에 포함된 개인 데이터 관리 어플리케이션의 구동을 도시한 블록구성도,

[40] 도 5는 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템의 신호흐름을 도시한 플로우챠트,

[41] 도 6은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템의 구성을 도시한 모식도,

[42] 도 7은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템의 구조를 개념적으로 도시한 도면,

[43] 도 8은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템을 통한 인증대상 유저 선정상태를 도시한 도면,

[44] 도 9, 10, 11은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템을 통한 데이터 복구과정을 도시한 플로우챠트,

[45] 도 12는 본 발명의 제 3실시예에 따른 개인 데이터 관리 시스템의 구성을 도시한 모식도이다.

발명의 실시를 위한 최선의 형태

[46] 이하, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템에 대해 도면을 참조하여 상세하게 설명한다.

[47] 도 1은 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템의 구성을 도시한 모식도, 도 2는 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템을 통한 데이터 저장대상 선정상태를 도시한 도면, 도 3은 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템을 통한 데이터 분할 저장 및 복구상태를 도시한 도면이다.

[48] 이를 참조하면, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템은 유저의 개인 데이터를 해당 유저의 단말기나 특정 서버에 저장하지 않고 랜덤하게 분산 저장하여 관리하고 필요시 복수의 인증절차를 거쳐 해당 유저 단말기에서 개인데이터를 복구함으로써 해킹 가능성이 대폭 낮춤을 물론이고, 해당 유저 단말기의 분실시에도 데이터가 유출되지 않도록 한 시스템이다.

[49] 즉, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템은 어느 한 저장수단에 유저가 저장하고자 하는 데이터의 전체를 일괄적으로 저장하지 않고 전체 데이터를 다수개로 분할하여 분산 저장시킴으로 인해서, 어느 한 저장수단이 해킹된다고 하여도 해당 데이터의 유출을 우려하지 않도록 한 시스템이다.

[50] 보다 상세하게, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템은 유저 인증으로 구동되며, 유저가 선택한 특정 데이터를 다수개로 자동 분리하여 데이터 관리서버(10)로부터 전송된 특정 식별번호의 다수 유저 단말기(2)로 분산하여 전송하고, 유저의 복구 명령에 따라 해당 분산데이터를 취합하여 복구시키는 개인 데이터 관리 어플리케이션(6)이 설치된 유저 단말기(2)와; 상기 개인 데이터 관리 어플리케이션(6)을 설치한 유저 단말기의 식별정보를 저장하고, 상기 유저 단말기(2)로부터 데이터 분산 신호를 인가받아, 데이터 분산 저장의 대상이 되는 특정 유저의 단말기 식별정보를 추출하여 상기 유저 단말기(2)로 전송 처리하는 데이터 관리서버(10)로 이루어진다.

[51] 이때, 상기 유저 단말기(2)는 분할 이전의 원 데이터(4)를 저장하고 실제로 해당 원데이터(4)를 분할하여 분할된 데이터를 별도의 저장수단에 전송하고, 다시 분할된 데이터를 원 데이터(4)로 복구시키는 데이터 분할 및 복구용 유저 단말기(2)와; 상기 유저 단말기(2)로부터 전송하는 분할 데이터(8)를 저장하는 저장용 유저 단말기(2)로 구분할 수 있다.

[52] 즉, 이러한 유저 단말기(2)는 그 내부에 개인 데이터 관리 어플리케이션(6)을 설치함으로써, 데이터의 분할 및 전송을 수행할 수도 있고, 분할된 데이터를 수신받아 저장할 수도 있으며, 분할된 데이터를 복구할 수도 있게 된다.

[53] 따라서, 상기 유저 단말기(2)는 굳이 그 기능에 따른 구분이 필요하지 않지만, 설명의 편의상 데이터를 분할하여 전송하고, 다시 분할된 데이터를 복구시키는 유저 단말기(2)는 별도의 코드(예, A001)를 부여하였으며, 분할된 데이터를 전송받아 각각 저장하는 유저 단말기(2)도 별도의 코드(예, B001, C001, D001, E001)를 부여하여 도시한다.

[54] 그리고, 이하 설명의 편의를 위해 A001로 코드가 부여된 유저 단말기(2)를 제 1 유저단말기(2-1)라고 명명하고, B001-E001로 코드가 부여된 유저 단말기(2)는 제 2 유저단말기(2-2)로 명명한다.

[55] 한편, 상기 데이터 관리서버(10)는 특정 유저의 단말기 식별정보 추출시, 대상이 되는 단말기 식별정보 풀(Pool)에서 소정 개수를 랜덤하게 추출하게 구성된다.

[56] 즉, 상기 제 1 유저단말기(2-1)가 데이터를 분할하여 저장하고자 하는 저장 대상에 대한 정보를 상기 데이터 관리서버(10)에 요청하면, 상기 데이터 관리서버(10)는 미리 분할 데이터를 저장할 수 있는 저장 대상에 대한 정보를 추출하여 상기 제 1 유저단말기(2-1)로 전송한다.

[57] 따라서, 상기 데이터 관리서버(10)는 분할 데이터를 저장하는 저장 대상에 대한 정보를 저장하고 있으며, 저장 대상이란 상기 제 2 유저단말기(2-2)를 의미한다.

[58] 또한, 상기 데이터 관리서버(10)는 다수의 분할 데이터 저장대상 단말기인 제 2 유저 단말기(2-2)의 식별정보를 저장하고 있는 바, 다수의 제 2 유저 단말기(2-2)중 일부 식별정보의 제 2 유저 단말기(2-2)를 랜덤하게 추출하여 상기 제 1 유저 단말기(2-1)측으로 제공한다.

[59] 바람직하게, 상기 제 1 유저 단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로부터 제공받은 유저의 단말기 식별정보들중 소정 개수를 랜덤하게 추출하게 구성된다.

[60] 즉, 상기 데이터 관리서버(10)가 제 2 유저 단말기(2-2)의 식별정보를 랜덤하게 추출하여 제 1 유저 단말기(2-1)로 제공한 것과 동일하게, 상기 제 1 유저 단말기(2-1)도 상기 데이터 관리서버(10)로부터 제공된 식별정보중 일부의 제 2 유저 단말기(2-2)를 랜덤하게 추출하고, 그 추출 정보를 상기 데이터 관리서버(10)로 전송한다.

[61] 이를 통해, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템에 포함된 상기 데이터 관리서버(10)는 상기 제 1 유저 단말기(2-1)가 저장하고자 하는 어느 한 분할 데이터도 저장하지 않고, 단지 해당 분할 데이터가 어느 단말기에 저장되어져 있는 지에 대한 정보만 보유할 뿐이므로, 해커에 의해 불법적으로 해킹당하더라도 해커가 유저의 데이터를 확보할 수 없다.

[62] 한편, 상기 제 1 유저 단말기(2-1)에는 예컨대, 전체의 원 데이터(4)중 분할된 일부 분할 데이터(8: 예컨대, D-1)를 저장하고 있고, 다수의 분할 데이터를 저장하고 있는 저장 대상이 되는 제 2 유저 단말기(2-2)(예, B001, C001, D001, E001...)의 식별정보만 저장하고 있으므로 해커가 해킹한다고 하여도 유저가 숨기고자 하는 데이터의 일부 분할 데이터만 확보할 수 있을 것이다.

[63] 즉, 상기 제 1 유저단말기(2-1)에 설치된 상기 개인 데이터 관리 어플리케이션(6)은 다수개로 분할된 데이터중 어느 한 데이터는 해당 제 1유저 단말기(2-1)에 저장하고, 그 외의 데이터는 특정 식별번호의 다수의 유저 단말기(2) 즉, 제 2 유저단말기(2-2)로 분산하여 저장되도록 구성된다.

[64] 이때, 분산데이터를 저장하는 상기 다수의 제 2 유저 단말기(2-2)는 서버나 PC 또는 무선 단말기중 어느 하나이다.

[65] 또한, 상기 원 데이터(4)를 분할하여 저장하는 어느 한 제 2 유저 단말기(2-2)(예, B001)에는 어느 한 일부 분할 데이터(8: 예컨대, D-3)를 저장하고 있으며, 어느 한 제 2 유저 단말기(2-2)(예, C001)에는 어느 한 일부 분할 데이터(8: 예컨대, D-2)를 저장하고 있으며, 어느 한 제 2 유저 단말기(2-2)(예, D001)에는 어느 한 일부 분할

데이터(8: 예컨대, D-5)를 저장하고 있고, 어느 한 제 2 유저 단말기(2-2)(예, E001)에는 어느 한 일부 분할 데이터(8: 예컨대, D-4)를 저장하고 있으므로, 마찬가지로 어느 한 상기 제 2 유저단말기(2)를 해킹한다고 하여도 일부 분할 데이터만을 확보할 수 있을 것이다.

[66] 특히, 통상적으로는 어느 한 서버에 다수의 유저 데이터가 저장되어져 있으므로 해킹시 해킹에 소요되는 노력에 응당하는 댓가를 얻을 수 있겠지만, 본 발명은 상기 데이터 관리서버(10)를 해킹하여도 해커가 얻을 수 있는 원 데이터(4)가 전혀 저장되어져 있지 않고, 어느 한 개인 데이터를 얻기 위해서는 무수한 유저 단말기(2)를 해킹해야 하므로 현실적으로 해커가 얻을 수 있는 댓가가 거의 없게 된다.

[67] 한편, 일반 통신 데이터의 송수신시와 동일하게, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템은 데이터를 분산하여 전송하는 상기 유저 단말기(2)와, 데이터를 분산 저장하는 유저 단말기(2)와, 상기 데이터 관리서버(10) 사이에 전송되는 데이터가 암호화된 데이터이다.

[68] 한편, 바람직하게 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템은 어느 한 제 2 유저단말기(2-2)가 분실되거나 또는 응답하지 못할 경우를 가정하여, 데이터 백업 구조로 설계되어져 있다.

[69] 즉, 상기 제 1 유저단말기(2-1)에 탑재된 상기 개인 데이터 관리 어플리케이션(6)은 다수의 데이터 전송 대상의 단말기 예컨대, 상기 제 2 유저단말기(2-2)로 분할 데이터를 전송하고, 동일한 분할 데이터를 백업 대상인 또 다른 제 2 유저단말기(2-2)측으로 전송하여 백업 저장되게 처리하고, 데이터 복구시 일정시간내 특정 분할 데이터의 복구가 이루어지지 않으면 백업 데이터를 통한 복구 처리를 수행하도록 구성된다.

[70] 따라서, 상기 제 1 유저단말기(2-1)에 설치된 상기 개인 데이터 관리 어플리케이션(6)은 분할 데이터를 저장하는 상기 제 2 유저단말기(2-2)의 식별정보와, 백업 데이터를 저장하는 상기 제 2 유저단말기(2-2)의 식별정보를 각각 저장하고 있다.

[71] 도 4는 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템에 포함된 개인 데이터 관리 어플리케이션의 구동을 도시한 블록구성도이다.

[72] 이를 참조하면, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 데이터를 분산 저장하는 다수의 유저 단말기(2) 및 데이터 관리서버(10)와 통신하는 통신모듈(20)과; 개인 식별정보 인증을 통해 유저를 인증하는 유저 인증부(22)와; 상기 데이터 관리서버(10)로 데이터를 분산 저장할 저장 대상정보를 자동으로 요청하는 저장대상 정보 요청부(24)를 포함하여 구성된다.

[73] 또한, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 유저가 선택한 특정 데이터를 분할 처리하는 데이터 분할 처리부(28)와; 통신하는 데이터에 대해 암호화 및 복호화를 수행하는 암호/복호 처리부(32)와; 분할 처리된 데이터중 일부 데이터를 저장하고, 각 분할 처리된 데이터를 저장하고 있는 저장 대상

정보를 저장하는 데이터 저장부(34)와; 상기 데이터 관리서버(10)와 통신하여 데이터 저장 대상정보를 제공받고, 특정 데이터를 분할하여 일부 데이터는 저장하고, 그 외 데이터는 다수의 데이터 저장 대상 단말기로 전송하여 분산 저장되게 처리하고, 복구시 해당 저장 대상 단말기측으로 특정 데이터의 전송 요청신호를 전송하여 복구를 수행하는 제어부(36)를 포함하여 구성된다.

[74] 한편, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 상기 데이터 관리서버(10)로부터 수신한 저장 대상정보중 일부를 랜덤하게 추출하는 대상 랜덤 추출부(26)를 더 포함하여 구성된다.

[75] 또, 상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 분할된 데이터들과 해당 데이터를 저장할 대상이 랜덤하게 매칭되게 처리하는 대상 랜덤 매칭부(30)를 더 포함하여 구성된다.

[76] 상기한 구성의 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템의 기능과 작용을 첨부된 도면을 참조하여 상세하게 설명한다.

[77] 도 5는 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템의 신호흐름을 도시한 플로우차트이다.

[78] 먼저, 본 발명의 제 1실시예에 따른 개인 데이터 관리 시스템에 포함된 유저 단말기(2) 예컨대, 상기 제 1 유저 단말기(2-1)를 소유한 유저가 특정 데이터를 분산 저장하기 위해 상기 개인데이터 관리 어플리케이션(6)을 구동하고, 비밀번호 등과 같은 개인 인증정보를 입력하여 인증을 수행한다.

[79] 인증이 성공하면, 상기 개인데이터 관리 어플리케이션(6)은 데이터 분산모드가 선택되는 지를 판단한다.

[80] 데이터 분산 모드가 선택된 경우, 상기 개인데이터 관리 어플리케이션(6)은 특정 데이터에 대한 분산 선택신호가 인가되는 지를 판단한다.

[81] 특정 데이터가 선택되면, 상기 개인데이터 관리 어플리케이션(6)이 데이터 전송 대상 정보를 데이터 관리서버(10)에 요청한다.

[82] 즉, 분할된 데이터를 저장하기 위한 저장 대상의 식별정보를 상기 데이터 관리서버(10)에 요청하면, 상기 데이터 관리서버(10)는 다수의 분할 데이터 저장대상 단말기인 제 2 유저 단말기(2-2)의 식별정보를 저장하고 있는 바, 다수의 제 2 유저 단말기(2-2)중 일부 식별정보의 제 2 유저 단말기(2-2)를 랜덤하게 추출하여 상기 제 1 유저 단말기(2-1)의 개인 데이터 관리 어플리케이션(6)으로 제공한다.

[83] 그러면, 상기 개인데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로부터 제공받은 데이터 전송 대상 단말기중 일부를 랜덤하게 추가로 추출함으로써 최종 대상 단말기를 결정한다.

[84] 그리고, 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터를 소정개수로 분할 처리하여, 각 분할데이터를 데이터 전송 대상 단말기인 제 2 유저단말기(2-2)로 임의 매칭시켜 전송한다.

[85] 이때, 상기 개인데이터 관리 어플리케이션(6)이 별도의 데이터 백업 대상

단말기로 분할된 백업 데이터를 전송한다.

[86] 즉, 즉, 상기 제 1 유저단말기(2-1)에 탑재된 상기 개인 데이터 관리 어플리케이션(6)은 다수의 데이터 전송 대상의 단말기 예컨대, 상기 제 2 유저단말기(2-2)로 분할 데이터를 전송하고, 동일한 분할 데이터를 백업 대상인 또 다른 제 2 유저단말기(2-2)측으로 전송하여 백업 저장되게 처리한다.

[87] 한편, 상기 제 1 유저 단말기(2-1)에 설치된 상기 개인데이터 관리 어플리케이션(6)은 데이터 복구모드가 선택되는 지 판단하는 바, 특정 데이터 복구신호가 수신되면, 상기 개인데이터 관리 어플리케이션(6)은 해당 데이터의 분할 데이터를 분산 저장하는 대상 단말기 정보, 예컨대 제 2 유저단말기(2-2)의 식별정보를 추출한다.

[88] 그리고, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)이 해당 데이터 저장 대상 단말기 예컨대, 제 2 유저단말기(2-2)들로 데이터 전송 요청을 수행한다.

[89] 다수의 분할 데이터들의 수신이 완료되면, 상기 개인데이터 관리 어플리케이션(6)은 원 데이터를 복구한다.

[90] 이때, 일부 상기 제 2 유저단말기(2-2)로부터 일정시간 경과시까지 데이터 수신이 이루어지지 않으면 상기 개인데이터 관리 어플리케이션(6)은 해당 데이터의 백업 저장 대상 단말기 정보를 추출한다.

[91] 그리고, 상기 개인데이터 관리 어플리케이션(6)이 해당 백업 저장 대상 단말기측으로 데이터 전송 요청을 수행하여 원 데이터(4)를 복구한다.

[92] 이하, 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템에 대해 도면을 참조하여 상세하게 설명한다.

[93] 도 6은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템의 구성을 도시한 모식도, 도 7은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템의 구조를 개념적으로 도시한 도면, 도 8은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템을 통한 인증대상 유저 선정상태를 도시한 도면이다.

[94] 이를 참조하면, 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템은 제 1실시예에 추가로 오프라인 인증 과정을 포함한 시스템이다.

[95] 오프라인 인증을 포함한 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템은 상기 제 1 유저 단말기(2-1)에서 데이터 복구를 시도할 경우 추가적인 인증과정을 더 포함시킨 것으로, 상기 제 1 유저 단말기(2-1)에서 분할한 어느 한 분할 데이터(8)를 저장하고 있는 어느 한 제 2 유저단말기(2-2)중 한 단말기에서 사용자 인증을 수행하는 인증과정을 수행하도록 한 시스템이다.

[96] 즉, 상기 제 1 유저단말기(2-1)에서 특정 데이터의 복구를 시도하면, 어느 한 제 2 유저단말기(2-2)의 사용자 인증을 그 제 2 유저단말기(2-2)에 탑재된 상기 개인 데이터 관리 어플리케이션(6)이 수행하고, 그 인증 성공신호를 상기 제 1 유저 단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)으로 전송하면 비로서, 상기 제 1 유저 단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)이 해당

데이터의 복구를 명령할 수 있도록 구성된다.

[97] 이때, 인증 대상이 되는 특정 제 2 유저단말기(2-2)의 소유자를 인증 유저라고 일컬으며, 상기 데이터 관리서버(10)는 상기 제 1 유저단말기(2-1)를 통해 분할된 특정 데이터의 식별정보에 매칭되게 인증 유저의 정보를 난수처리모듈(12)을 통해 랜덤하게 생성시켜 저장한다.

[98] 또한, 그 인증 유저의 정보는 상기 제 1 유저단말기(2-1)에는 저장되어져 있지 않으므로 해커가 상기 제 1 유저단말기(2-1)를 해킹하여 데이터를 복구하려고 하여도 인증 유저 정보가 없이는 데이터 복구가 실행되지 않는다.

[99] 즉, 상기 데이터 관리서버(10)는 특정 데이터의 복구시 인증이 필요한 단일의 인증 유저 정보를 데이터 분산 저장시 등록하고, 상기 제 1 유저단말기(2-1)의 개인 데이터 관리 어플리케이션(6)이 데이터 복구를 요청하면 해당 인증 유저정보를 개인 데이터 관리 어플리케이션(6)으로 제공한다.

[100] 따라서, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로부터 인증 유저정보를 제공받으면 해당 인증 유저의 유저 단말기(2)(예컨대, 제 2유저단말기(2-1))측으로 개인 인증정보(예컨대, 비밀번호나 지문, 홍채정보 등) 입력을 요청하게 구성되고, 개인 인증 성공시 해당 인증 유저의 제 2 유저단말기(2-2)는 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)으로 인증 확인신호를 전송한다.

[101] 특히, 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템은 상기 데이터 관리서버(10)가 상기 개인 데이터 관리 어플리케이션(6)으로 전송하는 인증 유저 정보는 문자 메시지 또는 이메일을 통해 전송되게 구성된다.

[102] 즉, 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템에는 오프라인 개념에 추가하여, 이종통신 개념이 포함된 바, 상기 데이터 관리서버(10)에서 상기 제 1 유저단말기(2-1)로 인증 유저의 식별정보를 전송할 때 해당 제 1 유저단말기(2-1)를 소유한 유저의 이메일로 그 인증 유저의 식별정보를 전송하면, 해커가 비록 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)의 비밀번호를 알아내었다고 하여도 해당 유저의 이메일 전송서버(40)를 해킹하지 못하면 데이터를 복구시킬 수 없다.

[103] 한편, 인증 유저의 대상이 된 특정 제 2 유저단말기(2-2)는 유저의 인증정보 입력을 통해 상기 개인 데이터 관리 어플리케이션(6)의 유저 인증이 성공해야 하지만, 일정 시간이 경과하도록 인증 유저의 인증 성공신호가 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)로 수신되지 않을 수도 있다.

[104] 그 경우, 상기 개인 데이터 관리 어플리케이션(6)은 기설정 시간 경과시까지 인증 유저의 인증 확인정보가 수신되지 않으면, 상기 데이터 관리서버(10)로 신규 인증 유저정보를 요청하게 구성하는 것도 가능하다.

[105] 상기한 구성의 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템의 기능과 작용을 첨부된 도면을 참조하여 상세하게 설명한다.

[106] 도 9, 10, 11은 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템을 통한 데이터 복구과정을 도시한 플로우챠트이다.

[107] 먼저, 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템은 분할되어 원격지에 분산 저장된 분할 데이터를 복구하는 과정에 특정한 유저의 인증을 수행하는 오프라인 인증개념과, 이종 통신 개념을 더 포함시킨 것이다.

[108] 오프라인 인증개념이란 특정 유저가 직접 비밀번호 입력이나 지문, 홍채와 같은 정보를 입력하여 유저 인증을 수행하도록 한 것으로, 개인 데이터 관리 회원으로 가입되어 유저 단말기(2)에 상기 개인 데이터 관리 어플리케이션(6)을 설치한 유저라면 누구든 인증 유저의 대상이 될 수 있고, 상기 데이터 관리서버(10)가 랜덤하게 그 인증 유저를 지정한다.

[109] 인증 유저의 지정은 제 1 유저단말기(2-1)로부터 데이터 복구 요청이 있는 시점에 데이터 관리서버(10)가 수행하는 것이다.

[110] 바람직하게, 상기 제 1 유저단말기(2-1)가 특정 데이터의 분할 데이터를 저장하고 있는 다수의 제 2 유저단말기(2-2)의 식별정보를 저장할 수도 있지만, 제 1 유저단말기(2-1)는 해당 정보를 상기 데이터 관리서버(10)에 전송하여 저장하고, 상기 제 1 유저단말기(2-1)에서는 해당 데이터의 저장 대상 단말기인 제 2 유저단말기(2-2)의 정보를 삭제할 수도 있다.

[111] 만약, 삭제된 상태라면, 데이터 복구시 상기 제 1 유저단말기(2-1)의 상기 개인데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로 복구하고자 하는 특정 데이터의 식별정보(예컨대, Pig 2013)를 전송하고, 동시에 인증 유저의 식별정보를 요청한다.

[112] 그러면, 상기 데이터 관리서버(10)는 상기 개인 데이터 관리 어플리케이션(6)을 설치한 어느 한 유저의 식별정보(예컨대, 전화번호)를 추출하여 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)으로 전송한다.

[113] 이때, 바람직하게 본 발명의 제 2실시예에 따른 개인 데이터 관리 시스템에는 오프라인 개념에 추가하여, 이종통신 개념이 포함된 바, 상기 데이터 관리서버(10)에서 상기 제 1 유저단말기(2-1)로 인증 유저의 식별정보를 전송할 때 해당 제 1 유저단말기(2-1)를 소유한 유저의 이메일로 그 인증 유저의 식별정보를 전송하면, 해커가 비록 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)의 비밀번호를 알아내었다고 하여도 해당 유저의 이메일 전송서버(40)를 해킹하지 못하면 데이터를 복구시킬 수 없다.

[114] 다음으로, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 해당 인증 유저의 식별정보를 갖는 제 2 유저단말기(2-2)로 인증 요청신호를 전송하는 바, 바람직하게 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)으로 인증 요청신호를 전송하는 것이다.

[115] 그러면, 제 2 유저단말기(2-2)를 소유한 유저는 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)에 인증정보를 입력하여 인증을 수행하게 하는 바, 바람직하게 상기 개인 데이터 관리 어플리케이션(6)의

비밀번호를 입력하면 된다.

[116] 비밀번호 인증이 성공하면, 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)은 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)으로 인증 성공신호를 전송한다.

[117] 그러면, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 해당 분할 데이터를 저장하는 다수의 제 2 유저단말기(2-2)로 데이터 복구신호를 전송한다. 바람직하게 복구하고자 하는 데이터의 식별정보도 함께 전송한다.

[118] 그러면, 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)은 해당 분할데이터(8)를 상기 제 1 유저단말기(2-1)로 전송한다.

[119] 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 분할된 데이터가 모두 수신되었는 지를 판단하여 분할 데이터의 수신이 완료되면 데이터를 복구한다.

[120] 반면에, 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)이 개인 인증정보를 입력받았지만 비밀번호 불일치 등으로 개인 인증에 실패한 경우라면, 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)은 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)으로 인증 실패 정보를 전송하고, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 다시 상기 데이터 관리서버(10)로 인증유저의 인증 실패정보를 전송한다.

[121] 또한, 일정시간이 경과될 시점까지 상기 제 1 유저단말기(2-1)로 인증 성공신호가 수신되지 않을 수도 있다.

[122] 그 경우에도 마찬가지로, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로 인증 신호 미수신에 대한 정보를 전송할 수 있으며, 두 경우 공히 상기 데이터 관리서버(10)로 하여금 신규한 인증 유저의 식별정보를 요청한다.

[123] 또한, 도 11에 도시된 바와 같이 인증이 성공되었지만, 일정시간이 경과할 시점까지 분할 데이터가 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)으로 미수신된 경우라면, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)이 미수신된 해당 분할 데이터의 백업 데이터를 저장한 제 2 유저단말기(2-2)의 식별정보를 추출하여, 해당 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)으로 백업 데이터의 전송을 요청할 수 있다.

[124] 한편, 백업 데이터를 저장한 제 2 유저단말기(2-2)의 식별정보를 상기 데이터 관리서버(10)에 저장하고, 상기 제 1 유저단말기(2-1)에는 그 식별정보를 저장하지 않게 설계할 수도 있다.

[125] 이 경우에는 도 11에 도시된 바와 같이, 상기 제 1 유저단말기(2-1)의 상기 개인 데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로 미수신된 분할데이터의 백업 데이터를 요청할 수 있다.

[126] 그러면, 상기 데이터 관리서버(10)는 해당 분할 데이터의 백업 데이터를 저장한 제 2 유저단말기(2-2)의 식별정보를 추출하여, 해당 상기 제 2 유저단말기(2-2)의 상기 개인 데이터 관리 어플리케이션(6)으로 백업 데이터의 전송을 요청하여 수신받고, 수신된 백업데이터를 다시 상기 제 1 유저단말기(2-1)으로 전송하여 데이터 복구가 이루어질 수 있게 할 수 있다.

[127] 이하, 본 발명의 제 3실시예에 따른 개인 데이터 관리 시스템에 대해 도면을 참조하여 상세하게 설명한다.

[128] 도 12는 본 발명의 제 3실시예에 따른 개인 데이터 관리 시스템의 구성을 도시한 모식도이다.

[129] 이를 참조하면, 본 발명의 제 3실시예에 따른 개인 데이터 관리 시스템은 다수의 상기 제 2 유저 단말기(2-2)에 저장된 제 1 유저 단말기(2a: 이하 2-1로 기술함)의 분할 데이터를 제 1 유저단말기(2-1)에 원 데이터(4)로 복구하지 않고, 제 1 유저 단말기(2-1)가 지정한 특정 제 3 유저 단말기(2b: 이하 2-3으로 기술함)에 복구하도록 한 시스템이다.

[130] 이러한 기능은 이메일 전송 또는 SNS를 통한 특정 데이터의 특정 유저로의 전송시 데이터 보안 유지에 매우 효과적이다.

[131] 즉, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)은 이메일 전송시 자동으로 구동되어 전송할 원 데이터(4)를 다수개로 분할하고, 일부 분할 데이터(예, D-1)를 수신측인 제 3 유저단말기(2-3)의 개인데이터 관리 어플리케이션(6)으로 직접 전송하고, 해당 데이터를 열람할 수 있는 열람 인증정보(바람직하게, 비밀번호)를 함께 전송한다.

[132] 그리고, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)은 나머지 분할 데이터를 다수의 상기 제 2 유저단말기(2-2)의 개인데이터 관리 어플리케이션(6)으로 전송하여 저장시킨다.

[133] 그 상태에서, 상기 제 3 유저단말기(2-3)의 개인데이터 관리 어플리케이션(6)에 해당 데이터를 열람할 수 있는 비밀번호가 입력되면, 그 제 3 유저단말기(2-3)의 개인데이터 관리 어플리케이션(6)은 해당 비밀번호 정보를 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)으로 전송한다.

[134] 그러면, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)은 해당 비밀번호를 인증하여 정당한 데이터 열람자인지를 인증하게 되고, 비밀번호가 일치한 경우 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)은 해당 데이터를 분산 저장하고 있는 다수의 상기 제 2 유저단말기(2-2)로 해당 데이터 전송신호를 발생시킨다.

[135] 그러면, 상기 제 2 유저단말기(2-2)의 개인데이터 관리 어플리케이션(6)은 해당 분할 데이터(8)를 각각 상기 제 3 유저단말기(2-3)의 개인데이터 관리 어플리케이션(6)으로 전송한다.

[136] 그로인해, 상기 제 3 유저단말기(2-3)의 개인데이터 관리 어플리케이션(6)은 해당 데이터를 복구할 수 있게 된다.

[137] 이러한 기능은 이메일 서버와 연동하여 작동될 수 있다.

[138] 즉, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)에서 이메일 전송을 클릭하게 되면, 해당 유저가 미리 지정한 이메일 어플리케이션(미도시)이 자동으로 구동되게, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)에서 신호를 발생시킨다.

[139] 그리고, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)은 특정 데이터에 대해 분할한 어느 한 분할 데이터(예컨대, D-1)를 해당 이메일에 자동 첨부시키고, 비밀번호와 저장 장소 정보 예컨대, 제 2 유저단말기(2-2)의 개인데이터 관리 어플리케이션(6)의 식별정보는 해당 이메일의 내용란에 입력하여 전송한다.

[140] 또는, 이메일 대신 단문 메시지로도 전송 가능하다.

[141] 이때, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)에는 해당 이메일 수신자의 이메일 정보와 함께 해당 수신자의 단말기인 제 3 유저단말기(2-3)의 식별정보, 제 2 유저단말기(2-2)의 개인데이터 관리 어플리케이션(6)의 식별정보가 함께 저장되어져 있어야 한다.

[142] 그리고, 상기 제 1 유저단말기(2-1)의 개인데이터 관리 어플리케이션(6)은 남은 분할 데이터를 상기 제 2 유저단말기(2-2)로 전송한다.

[143] 그 상태에서, 제 3 유저가 상기 개인데이터 관리 어플리케이션(6)을 통해 해당 데이터의 복구명령을 상기 제 2 유저단말기(2-2)의 개인데이터 관리 어플리케이션(6)으로 발생시키면, 상기 제 2 유저단말기(2-2)의 개인데이터 관리 어플리케이션(6)은 상기 제 3 유저단말기(2-3)로 분할 데이터들을 전송한다.

[144] 그로인해, 상기 제 3 유저단말기(2-3)의 개인데이터 관리 어플리케이션(6)은 분할 데이터를 모두 수신하게 되고, 상기 제 1 유저가 전송한 비밀번호를 입력하게 되면 해당 데이터가 화면에 출력되게 된다.

[145] 그러면, 본 발명을 이메일 전송방식에 적용할 때와 마찬가지로, SNS 서버(미도시)가 해킹되지 않는 한, 제 1 유저단말기(2-1)가 제 3 유저단말기(2-3)로 SNS를 통해 전송하는 분할 데이터를 해커가 획득할 수 없으며, SNS 서버가 해킹되었다고 할지라도 다수의 제 2 유저단말기(2-2)를 해킹하지 않으면 모든 분할데이터를 얻을 수 없고, 각 유저 단말기(2)를 해킹한다고 해도 개인 한명의 특정 데이터만을 얻을 수 있으므로 해커에게 실익이 없게 된다.

[146] 한편, 본 발명의 실시예에 따른 개인 데이터 관리 시스템 및 그 방법은 단지 상기한 실시예에 한정되는 것이 아니라 그 기술적 요지를 이탈하지 않는 범위내에서 다양한 변경이 가능하다.

청구범위

[청구항 1] a) 유저 단말기(2)에 탑재된 개인데이터 관리 어플리케이션(6)이 구동신호를 수신하는 과정과;
b) 데이터 분산 선택신호가 인가되는 지를 상기 개인데이터 관리 어플리케이션(6)이 판단하는 과정과;
c) 특정 데이터가 선택되는 지를 판단하는 과정과;
d) 상기 개인데이터 관리 어플리케이션(6)이 데이터 전송 대상 정보를 데이터 관리서버(10)에 요청하는 과정과;
e) 상기 데이터 관리서버(10)가 데이터 전송 대상정보를 상기 개인데이터 관리 어플리케이션(6)으로 제공하는 과정과;
f) 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터를 소정개수로 분할 처리하는 과정과;
g) 각 분할데이터를 데이터 전송 대상 단말기측으로 임의 매칭시켜 전송하는 과정이 포함되어 구성된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 2] 상기 1항에 있어서,
상기 e) 과정은 상기 데이터 관리서버(10)가 대상이 되는 단말기 식별정보 풀(Pool)에서 소정 개수를 랜덤하게 추출하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 3] 상기 1항에 있어서,
상기 f) 과정은 상기 개인데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로부터 제공받은 데이터 전송 대상 단말기중 일부를 랜덤하게 추출함으로써 최종 대상 단말기를 결정하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 4] 상기 1항에 있어서,
상기 g) 과정은 상기 개인데이터 관리 어플리케이션(6)이 별도의 데이터 백업 대상 단말기로 분할된 백업 데이터를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 5] 상기 1항에 있어서,
상기 g) 과정 다음으로,
h) 상기 개인데이터 관리 어플리케이션(6)이 데이터 복구모드가 선택되는 지 판단하는 과정과;
i) 특정 데이터 복구신호가 수신되면, 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터의 분할 데이터를 분산 저장하는 대상 단말기 정보를 추출하는 과정과;
j) 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터 저장 대상 단말기로 데이터 전송 요청을 수행하여 데이터를 수신받는 과정과;

k) 데이터 수신이 완료되면, 상기 개인데이터 관리 어플리케이션(6)이 데이터를 복구하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 6] 제 5항에 있어서,
상기 k) 과정중, 일부 단말기로부터 일정시간 경과시까지 데이터 수신이 이루어지지 않으면 상기 개인데이터 관리 어플리케이션(6)이 해당 데이터의 백업 저장 대상 단말기 정보를 추출하는 과정과;
상기 개인데이터 관리 어플리케이션(6)이 해당 백업 저장 대상 단말기측으로 데이터 전송 요청을 수행하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 7] 상기 1항에 있어서,
상기 g) 과정 다음으로, 상기 개인데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로 데이터 전송 대상 단말기 정보를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 8] 제 5항에 있어서,
상기 h) 과정과 i) 과정의 사이에는,
l) 상기 개인 데이터 관리 어플리케이션(6)이 상기 데이터 관리서버(10)로 복구할 데이터 정보를 전송하고 해당 데이터의 인증 유저 정보를 요청하는 과정과;
m) 상기 데이터 관리서버(10)가 해당 개인 데이터 관리 어플리케이션(6)으로 해당 데이터의 인증 유저정보를 전송하는 과정과;
n) 상기 개인 데이터 관리 어플리케이션(6)이 해당 인증 유저의 단말기(2)로 개인 인증정보 입력을 요청하는 과정과;
o) 해당 인증 유저의 단말기(2)에서의 개인 인증 성공시 해당 인증 유저의 유저 단말기(2)는 상기 개인 데이터 관리 어플리케이션(6)으로 인증 확인신호를 전송하는 과정이 더 포함되는 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 9] 제 8항에 있어서,
상기 m) 과정은 상기 데이터 관리서버(10)가 해당 개인 데이터 관리 어플리케이션(6)으로 단문 메시지 또는 이메일을 통해 인증 유저정보를 전송하는 과정인 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 10] 제 8항에 있어서,
상기 o) 과정중 인증 실패신호가 상기 인증 유저의 단말기(2)로부터 수신되면, 상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로 인증 실패 정보를 전송하는 과정과;
기설정 시간 초과시까지 인증 신호가 수신되지 않으면, 해당 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로 신규 인증 유저 정보를 요청신호를 전송하는 과정과;

상기 데이터 관리서버(10)가 해당 개인 데이터 관리 어플리케이션(6)으로 신규 인증 유저정보를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 11] 제 5항에 있어서,
상기 k) 과정은 기설정시간 경과시까지 특정 분할 데이터가 미수신되는지를 판단하는 과정과;
특정 분할 데이터의 미수신시, 백업 데이터를 저장하는 유저 단말기 정보를 추출하는 과정과;
상기 개인 데이터 관리 어플리케이션(6)이 해당 백업 데이터를 저장하는 유저 단말기(2)측으로 데이터 전송을 요청하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 12] 제 1항에 있어서,
데이터를 분할하여 전송하는 전송 유저 단말기(2-1)와, 분할 저장된 데이터를 복구 시도하는 수신 유저 단말기(2-3)가 각각 상이한 경우, 상기 전송 유저 단말기(2a)는 상기 수신 유저 단말기(2-3)측으로 전송 유저 단말기(2-1)가 분할하여 저장하는 데이터와, 수신 인증정보와, 나머지 분할 데이터의 저장 단말기 정보를 전송하는 과정이 더 포함된 것을 특징으로 하는 개인 데이터 관리 방법.

[청구항 13] 유저 인증으로 구동되며, 유저가 선택한 특정 데이터를 다수개로 자동 분리하여 데이터 관리서버(10)로부터 전송된 특정 식별번호의 다수 유저 단말기(2)로 분산하여 전송하고, 유저의 복구 명령에 따라 해당 분산데이터를 취합하여 복구시키는 개인 데이터 관리 어플리케이션(6)이 설치된 유저 단말기(2)와;
상기 개인 데이터 관리 어플리케이션(6)을 설치한 유저 단말기의 식별정보를 저장하고, 상기 유저 단말기(2)로부터 데이터 분산 신호를 인가받아, 데이터 분산 저장의 대상이 되는 특정 유저의 단말기 식별정보를 추출하여 상기 유저 단말기(2)로 전송 처리하는 데이터 관리서버(10)로 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 14] 제 13항에 있어서,
상기 데이터 관리서버(10)는 특정 유저의 단말기 식별정보 추출시, 대상이 되는 단말기 식별정보 풀(Pool)에서 소정 개수를 랜덤하게 추출하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 15] 제 13항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로부터 제공받은 유저의 단말기 식별정보들중 소정 개수를 랜덤하게 추출하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 16] 제 13항에 있어서,
데이터를 분산하여 전송하는 상기 유저 단말기(2)와, 데이터를 분산

저장하는 유저 단말기(2)와, 상기 데이터 관리서버(10) 사이에 전송되는 데이터는 암호화된 데이터인 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 17] 제 13항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 다수개로 분할된 데이터중 어느 한 데이터는 해당 유저 단말기(2)에 저장하고, 그 외의 데이터는 특정 식별번호의 다수 유저 단말기(2)로 분산하여 저장되도록 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 18] 제 13항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 데이터를 분산 저장하는 다수의 유저 단말기(2) 및 데이터 관리서버(10)와 통신하는 통신모듈(20)과;
개인 식별정보 인증을 통해 유저를 인증하는 유저 인증부(22)와;
상기 데이터 관리서버(10)로 데이터를 분산 저장할 저장 대상정보를 자동으로 요청하는 저장대상 정보 요청부(24)와;
유저가 선택한 특정 데이터를 분할 처리하는 데이터 분할 처리부(28)와;
통신하는 데이터에 대해 암호화 및 복호화를 수행하는 암호/복호 처리부(32)와;
분할 처리된 데이터중 일부 데이터를 저장하고, 각 분할 처리된 데이터를 저장하고 있는 저장 대상 정보를 저장하는 데이터 저장부(34)와;
상기 데이터 관리서버(10)와 통신하여 데이터 저장 대상정보를 제공받고, 특정 데이터를 분할하여 일부 데이터는 저장하고, 그 외 데이터는 다수의 데이터 저장 대상 단말기로 전송하여 분산 저장되게 처리하고, 복구시 해당 저장 대상 단말기측으로 특정 데이터의 전송 요청신호를 전송하여 복구를 수행하는 제어부(36)가 포함된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 19] 제 18항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 상기 데이터 관리서버(10)로부터 수신한 저장 대상정보중 일부를 랜덤하게 추출하는 대상 랜덤 추출부(26)를 더 포함하여 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 20] 제 18항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 그 내부에, 분할된 데이터들과 해당 데이터를 저장할 대상이 랜덤하게 매칭되게 처리하는 대상 랜덤 매칭부(30)를 더 포함하여 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 21] 제 13항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 다수의 데이터 전송 대상의

단말기로 분할 데이터를 전송하고, 동일한 분할 데이터를 백업 대상인 단말기측으로 전송하여 백업 저장되게 처리하고, 데이터 복구시 일정시간내 특정 분할 데이터의 복구가 이루어지지 않으면 백업 데이터를 통한 복구 처리를 수행하도록 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 22] 제 13항에 있어서,
상기 데이터 관리서버(10)는 특정 데이터의 복구시 인증이 필요한 단일의 인증 유저 정보를 데이터 분산 저장시 등록하고, 상기 개인 데이터 관리 어플리케이션(6)의 데이터 복구 요청시 해당 인증 유저정보를 개인 데이터 관리 어플리케이션(6)으로 제공하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 23] 제 22항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 상기 데이터 관리서버(10)로부터 인증 유저정보를 제공받으면 해당 인증 유저의 유저 단말기(2)측으로 개인 인증정보 입력을 요청하게 구성되고, 개인 인증 성공시 해당 인증 유저의 유저 단말기(2)는 상기 개인 데이터 관리 어플리케이션(6)으로 인증 확인신호를 전송하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 24] 제 22항에 있어서,
상기 데이터 관리서버(10)가 상기 개인 데이터 관리 어플리케이션(6)으로 전송하는 인증 유저 정보는 문자 메시지 또는 이메일을 통해 전송되게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 25] 제 23항에 있어서,
상기 개인 데이터 관리 어플리케이션(6)은 기설정 시간 경과시까지 인증 유저의 인증 확인정보가 수신되지 않으면, 상기 데이터 관리서버(10)로 신규 인증 유저정보를 요청하게 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 26] 제 13항에 있어서,
상기 유저 단말기(2)는 원 데이터를 분할하는 전송 유저 단말기(2-1)와, 해당 원 데이터를 복구하는 수신 유저 단말기(2-3)가 각각 서로 다르게 구성된 경우, 상기 전송 유저 단말기(2-1)는 수신 유저 단말기(2-3)로 전송 유저 단말기(2-1)가 분할하여 저장하는 데이터와, 수신 인증정보와, 나머지 분할 데이터의 저장 단말기 정보를 전송하도록 구성된 것을 특징으로 하는 개인 데이터 관리 시스템.

[청구항 27] 제 13항에 있어서,
분산데이터를 저장하는 상기 다수의 유저 단말기(2)는 서버나 PC 또는 무선 단말기중 어느 하나인 것을 특징으로 하는 개인 데이터 관리 시스템.