Social Poll 시스템 환경을 위한 Today Poll 시스템의 설계 및 구현

박지호, 박성욱, 이선호, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail : [corex, swpark, sunho431, imylee]@sch.ac.kr

Design and Implementation of Today Poll System for the Social Poll System Environment

Ji-Ho Park, Sung-Wook Park, Sun-Ho Lee, Im-Yeong Lee
Dept. of Computer Software Engineering, Soonchunhyang University

요 약

모바일 인터넷 통신망의 급속한 발전과 스마트폰 보급률이 늘어남에 따라 언제 어디서나 빠르게 인터넷에 접속할 수 있는 정보 인프라가 갖추어졌다. 더불어 이를 이용하는 사용자 간의 사회적 네트워크 소통 시스템이 최근 주목받고 있다. 하지만 단순한 메시지나 사진, 음성이나 동영상 등의 데이터를 교환하는데 그치고 있다. 이러한 시스템 환경에서는 다른 사용자의 피드백이 필요한 질문이나 설문, 투표와 같은 요청이 발생하였을 때 만족스러운 결과를 얻기까지 여러 번의 복잡한 메시지 교환이 이루어져야 한다. 본 논문에서는 이러한 불편을 해결하기 위하여 질문자의 물음에 답변하는 일반적인 설문조사 방식이 아닌 투표 할 수 있는 후보에 대한 추천을 응답자들이 직접 하는 것이 가능하도록 하는 시스템을 설계 및 구현하였다.

1. 서론

현재 무선통신망은 상당히 빠른 속도를 지원하고 있다. 이러한 빠른 모바일 인터넷 환경 속에서 애플사의 아이폰에 의해 스마트폰 시장이 활성화 되었다. 그리하여 이제는 휴대전화는 통화하거나 문자를 보내는 용도만으로 쓰이지 않게 되었다.[1-2]

사람들과 소통하는 방법에서 스마트폰과 같은 모바일 기기가 등장하면서 조금 더 편리해진 것은 사실이나 직접적인 경험이 수반된 후에야 얻어지는 고급 정보는 얻기가 쉽지 않다. 예를 들어 교내 또는 사내 식당의 식단표는 쉽게 구할 수 있지만, 해당 식단에 쓰인 음식재료의 조리 상태 등 구체적인 정보는 직접 경험해본 사람 이외에는 알기가 쉽지 않다. 이런 사소하지만, 자세한 정보를 여러 사람에 의해 생성하고 가공하고 공유하고자 한다. 아울러 그러한 공유의 기록을 남긴다면 언제든지 검색을 통해 고품질의 정보를 기대할 수 있을 것이다.

본 연구는 누군가의 경험으로 얻어진 자세한 정보를 모아서 필요로 하는 시간과 장소에 존재할 수 있도록 한다. 단순히 질문에 대한 답변만을 얻는 방법 외에 여러 사람의 경험에 기반을 두어 질문자와 답변자가 함께 질문의 완성도를 높여 좀 더 효율적인 경험 공유의 수단으로 활용하고자 Social Poll 시스템 환경을 위한 Today Poll 시스템을 설계 및 구현하였다.

본 논문에서는 2장에서 기존 연구에 대해 기술하고 3장에서 보안 요구사항에 대해 기술하며 4장은 이를 만족하는 제안방식에 대해 기술한다. 5장은 제안한 방식의 구현에 대해 기술하고 6장에서는 제안한 시스템을 분석한다. 마지막으로 7장에서 결론을 맺는다.

2. 기존 연구

본 장에서는 기존 연구 방식에 대하여 알아본다.

2.1 기존의 연구 방식

사람들의 의견, 생각, 경험, 관점 등을 공유하기 위해 사용하는 온라인 도구와 플랫폼을 소셜 미디어라 한다. 이러한 소셜 미디어는 텍스트, 이미지, 오디오, 비디오 등의 다양한 형태를 보이고 있는데 가장 대표적인 소셜 미디어로는 블로그(Blogs-자신의 생각, 견해나 주장 같은 것을 차곡차곡 적어서 올려놓은 글들의 모음), 소셜 네트워크 서비스(Social Network Service-온라인 인맥구축 서비스), 메시지 보드(Message Boards-온라인 토론을 위한 장소), 팟캐스트(Podcasts-원하는 그룹을 선택하여 자동으로 구독할 수 있도록 함으로써 방송을 전달하는 방법), 위키스(Wikis-집단지성에 의한 정보가공), 비디오 블로그(vlog-비디오의 형식으로 인터넷에 올리는 블로그) 등이 있다.

기존의 소셜 미디어들은 콘텐츠를 단순히 공유 공간에 게시하여 공유하거나 여러 사람이 참여하여 특정 주제에 대해서 콘텐츠를 완성해 나가는 방식을 채택하고 있다. 이

러한 방식은 콘텐츠가 필요한 사람보다 콘텐츠를 생산하는 사람에게 초점이 맞춰져 있다고 할 수 있다. 블로그나 메시지 보드는 일방적인 정보 제공을 하며 콘텐츠 소비자는 댓글 형식으로 참여를 제한받는다. 비디오 블로그 또한 대동소이하며 위키스의 경우 콘텐츠가 완성되는데 상당히 오랜 시간과 노력이 필요한 단점이 있다. 또한, 기존 방식에서는 정보 제공자의 이익을 위한 편향적인 정보제공이나 정보 조작 등 보안 문제와 함께 1인 미디어에 의한 정보의 질 저하 문제가 발생하기도 한다. 이상적인 소셜 미디어는 사용자들이 콘텐츠를 소비하는 동시에 생산도 하는 참여형 소비자(Prosumer)활동을 어느 한 쪽에 치우치지 않도록 지원해야 한다.

본 제안 방식에서는 질문자의 물음에 답변하는 일반적인 설문조사 방식이 아닌 투표 할 수 있는 후보에 대한 추천을 응답자들이 직접 하는 것으로 참여형 소비자의 활동을 투표의 형식을 통해 나타나게끔 한다. 아울러 특정 개인이나 단체의 이익을 위해 투표 결과를 조작하거나 투표의 대상을 제한하는 등 악의적인 정보 조작을 방지하기 위해 보안 기능을 강화 하였다. 기존의 콘텐츠 생산자 측면의 기능을 유지한 채 소비자 측면에서 필요로 하는 편의성과 함께 수준 높은 정보를 보다 안전하게 제공하게 될 것이다.

3. 보안 요구사항

본 장에서는 Social Poll 시스템에서 요구하는 보안사항에 대하여 알아본다.

3.1 보안 요구사항

본 연구는 기밀성, 무결성, 사용자 인증, 부인방지에 대하여 다음과 같은 보안 요구사항을 가진다.

- 기밀성 : 개설된 투표에 대해서 찬성/반대표를 행사하거나 서버에서 인증서를 클라이언트에 전송하기 위해 제3자가 인증서를 취득하지 못하도록 기밀성이 보장되어야 하며, 제3자의 도용을 방지할 수 있어야 한다.
- 무결성 : 사용자가 인증서를 발급받거나 투표를 하는 과정에서 인증서나 투표참여 정보 전송 도중 인증서와 투표참여 정보의 내용에 대한 위·변조 및 삭제 등과 같은 공격에 의해 정보가 변경되지 않아야 한다.
- 사용자 인증 : 인증서는 아이디/비밀번호를 기본으로 하여 생성된 것이므로 인증서를 통하여 허가된 사용자인지 식별하고 검증할 수 있어야 한다.
- 부인방지 : 사용자에 의해 서명된 투표 정보가 서버로 보내졌다는 사실에 대한 부인을 방지할 수 있어야 한다.

3.2 모바일 콘텐츠 요구사항

본 연구의 시스템은 Android OS를 통하여 사용자의 투표 정보를 서버로 전송하므로 일반적인 모바일 콘텐츠로서의 요소가 필요하여 다음과 같은 요구사항을 가지게 된다.

- 상호작용성 : 클라이언트와 서버 간의 원활한 통신이 이루어져야 한다. 서버는 클라이언트로부터 받은 데이터로 사용자를 인증하고 인증서를 생성할 수 있어야 하며, 클라이언트는 서버로부터 받은 데이터를 이용함으로써 시스템 사용에 영향을 줄 수 있어야 한다.
- 즉시연결성 : 사용자는 시간 및 공간의 제약 없이 스마트폰을 이용하여 서버와의 통신이 가능해야 하며, 서비스를 원활히 받을 수 있어야 한다. 모바일 콘텐츠의 가장 큰 장점이라고도 할 수 있는 즉시연결성을 만족함으로써 언제 어디서나 Social Poll 환경에 접근할 수 있어야 한다.

4. 제안방식

본 연구에서 제안하는 방식은 기존의 SNS나 인터넷에서 이루어지는 설문/투표에서 흔히 투표를 제안하며 투표를 개설하는 투표 개설자가 일방적으로 투표 후보에 대해서 미리 정하고 투표 참여자들은 정해진 투표후보들에 대해서만 투표권을 행사하는 기존 방식을 벗어나 투표 참여자들이 투표 후보를 추천하는 방안을 제안한다.

4.1 시스템계수

제안방식은 다음과 같은 시스템 계수를 사용한다.

- *request*[*]= *를 요청함
- *KU** = *의 공개키
- *KR** = *의 개인키
- *KS* = 서버와 클라이언트 간의 세션키
- *E**[] = *의 키로 암호화
- *D**[] = *의 키로 복호화
- *H[]* = 단 방향 암호화
- *C* = 클라이언트
- *S* = 서버
- *ID* = 아이디
- *PW* = 비밀번호
- *FAV* = 선호정보
- *A* = 인증서
- *P* = 투표 참여 정보
- || = 연접

4.2 투표후보 추천 방식

투표가 개설됨과 동시에 투표권자가 개설된 투표의 목적에 맞는 투표후보를 등록하게 된다. 투표가 개설되는 과정에서 투표후보에 대한 등록이 가능하며 이 때문에 투표가 개설자의 의도와는 전혀 다른 방향으로 흘러가는 것을 어느 정도 완화 시킬 수 있다.

4.3 세션키 분배와 인증서 발급

Today Poll 시스템을 이용해서 사용자 등록, 인증서

발급 그리고 투표 정보 전송을 위해 PKI(Public Key Infrastructure)를 이용한 서버와 클라이언트 간의 세션키 분배를 통하여 통신 내용을 안전하게 암호화 하여 통신을 수행하며 프로토콜은 다음과 같다.

4.3.1 세션키 분배

Step 1. 클라이언트가 서버에게 공개키를 요구한다.

$C->S$: $request[KU_S]$

Step 2. 서버가 클라이언트에게 공개키를 전송한다.

$S->C$: KU_S

Step 3. 클라이언트가 생성한 세션키를 서버의 공개키로 암호화하여 전송 한다.

$C->S$: $E_{KU_S}[KS]$

Step 4. 서버의 개인키로 암호문을 복호화하여 세션키를 확인한다.

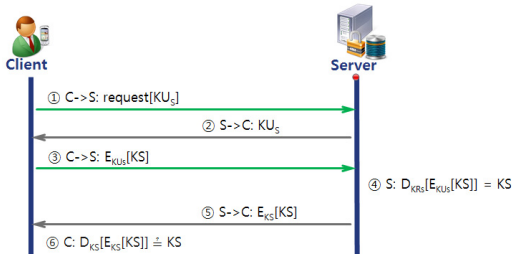
S: $D_{KR_S}[E_{KU_S}[KS]]$

Step 5. 클라이언트의 세션키로 세션키를 암호화하여 서버에게 전송한다.

$S->C$: $E_{KS}[KS]$

Step 6. 클라이언트는 암호문을 복호화하여 세션키를 확인한다.

C: $D_{KS}[E_{KS}[KS]] \stackrel{?}{=} KS$



(그림 1 세션키 분배)

4.3.2 사용자 등록과 인증서 발급

Step 7. 클라이언트가 사용자의 아이디, 단방향 암호화된 비밀번호, 공개키, 선호정보를 연접하여 세션 키로 암호화하여 서버에 전송한다.

$C->S$: $E_{KS}[ID||H[PW]||KU_c||FAV]$

Step 8. 서버는 전송받은 암호문을 세션 키로 복호화하여 가입정보를 DB에 저장한다.

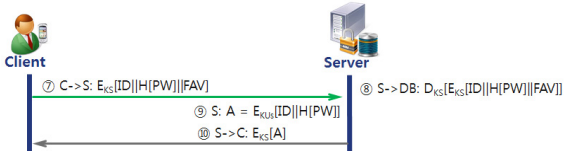
$S->DB$: $D_{KS}[E_{KS}[ID||H[PW]||FAV]]$

Step 9. 서버에서 서버의 공개키로 아이디와 비밀번호를 암호화하여 인증서를 생성한다.

S: $A = E_{KU_S}[ID||H[PW]]$

Step 10. 서버에서 사용자의 인증서를 세션키로 암호화하여 클라이언트에게 전송한다.

$S->C$: $E_{KS}[A]$

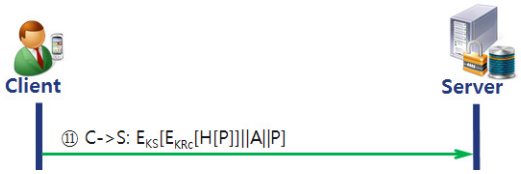


(그림 2 사용자 등록과 인증서 발급)

4.3.3 투표정보 전송

Step 11. 투표에 참여할 때 클라이언트는 투표 참여 정보의 해쉬를 자신의 개인키로 서명한 뒤 인증서와 투표 참여 정보와 함께 세션 키로 암호화 하여 서버에 전송한다.

$C->S$: $E_{KS}[E_{KR_C}[H[P]]||A||P]$



(그림 3 투표정보 전송)

4.4 시나리오

제안방식은 Android OS를 가진 스마트폰의 애플리케이션을 클라이언트로 하여 Windows서버와 연동하며 진행된다. Today Poll 서버를 통해 현재 진행되고 있는 투표 리스트를 보여주고, 스마트폰 애플리케이션을 이용해서 투표를 개설하거나 이미 개설된 투표에 대해 추천, 또는 투표 후보를 등록하고 여러 투표후보에 대해서 표를 행사하는 방법을 제공한다.

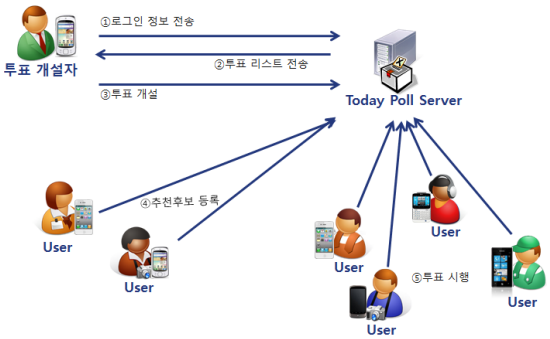
Step 1. Today Poll 애플리케이션에서 회원가입 후 아이디와 비밀번호를 입력하여 서버에 전송한 후 로그인 한다.

Step 2. 정상적인 로그인이 완료되면 현재 진행되고 있는 투표의 리스트를 서버로부터 내려받는다.

Step 3. 투표 개설자는 상세한 내용(예: 6박 7일 여행지로 어디가 좋을까?)을 적어서 투표를 개설한다.

Step 4. 사용자는 선택한 투표에 대해 추천을 하거나 추천후보를 등록한다.

Step 5. 등록되어 있는 투표후보들에 대해서 투표를 시행한다.



(그림 4 시나리오)

5. 제안방식 구현

4장에서 설계한 내용을 기반으로 투표 후보를 투표권자가 등록 가능하며 다른 사용자와 자신의 경험을 공유할 수 있는 Social Poll 시스템 환경을 위한 Today Poll 시스템을 구현하였다.

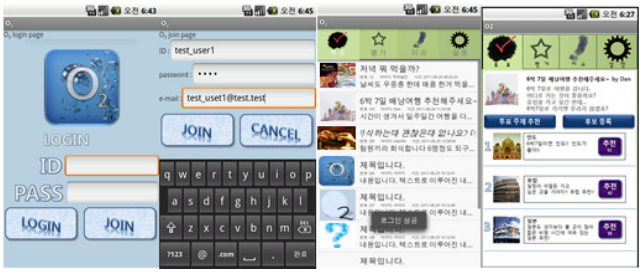
5.1 서버 현황 및 클라이언트 접속

서버에서는 전반적인 통신의 흐름을 알 수 있으며, 클라이언트의 접속 및 전송받는 데이터의 내용을 알 수 있고, 회원 목록과 투표목록에 대한 조회 및 관리를 할 수 있다.

5.2 투표 참여

투표의 참여는 모바일 클라이언트를 통해서 이루어진다. 안드로이드 마켓에서 클라이언트 애플리케이션을 내려받아서 설치한 뒤에 아이디/비밀번호 입력으로 사용자 인증을 거치고 나서 투표를 개설하거나 이미 개설된 투표를 추천, 또는 투표 후보들에 대한 추천이나 등록을 통해서 투표에 참여하게 된다.

(그림 5) 서버 현황



(그림 6) 모바일 클라이언트

6. 제안방식 분석

본 연구의 제안방식은 보안 요구사항을 충족함으로써 다음과 같은 이점을 제공한다. 본 장에서는 3장에서 언급한 요구사항에 따라 제안방식을 분석한다.

・기밀성 : 외부의 공격으로부터 안전하기 위해 공개키 방식을 이용하여 클라이언트는 서버에게 서버의 공개키를 요청하고 서버는 클라이언트에게 자신의 공개키를 전달한다. 클라이언트는 세션키를 생성하여 세션키를 서버의 공개키로 암호화하여 보내고 서버는 인증서를 생성하여 세션키로 암호화하여 보냄으로써 제3자가 인증서를 취득하지 못하도록 하여 기밀성을 제공한다.

・무결성 : 사용자의 개인키로 서명된 투표 정보를 다시 세션키로 암호화하여 전송한다. 투표정보의 해쉬값을 비교함으로써 무결성을 제공한다.

・사용자 인증 : 모바일 클라이언트의 아이디/비밀번호와 인증서를 이용하여 사용자 인증을 제공한다.

・부인방지 : 공개키 기반 구조를 토대로 전자서명을 생성하게 되는데, 이때 사용자의 개인키는 사용자만이 가지고 있으므로 부인방지를 제공한다.

7. 결론 및 향후 연구 방향

본 논문에서 제안한 방식은 투표를 받을 후보등록에 대한 결정권을 제 3자에게 양도 하는 것이 가능하여 투표의 성향이 불공정 투표와 같이 특정 지어지는 것을 미리 방지하는 것이 가능하다. 아울러 여러 사람의 참여로 인해 투표 개설자가 생각지 못한 부분을 보완할 수 있는 아이디어가 제안될 것이라 기대된다. 이것은 설문의 경우 선택가능한 항목 제일 마지막에 기타 의견을 적도록 배려하는 것을 적극적으로 확대한 것이라 이해해도 무방하다. 아이디/비밀번호 방식을 토대로 인증서 생성 및 발급 시스템을 구현하여 시스템의 안정성을 높이고, 부인방지, 무결성, 기밀성 등을 제공하여 투표의 신뢰성을 높였다. 또한, 스마트폰과 같은 모바일 기기를 통하여 일상생활과 밀접하게 투표를 개설하고 추천하거나 후보를 추천하고 등록하는 등의 투표에 참여 하는 것이 언제 어디서나 가능하게 하였다. 따라서 지속적으로 관련 연구가 진행되어 뒷받침된다면 개인의 질의부터 단체나 기업의 의견수렴 등 많은 비용이 드는 기존의 투표 시스템을 대체하는 공신력 있고 접근성이 뛰어난 전자투표 시스템으로 자리를 잡을 수 있게 된다.

소셜 미디어의 가장 큰 목적인 의견이나 생각, 경험, 관점 등에 관한 정보의 공유를 위하여 본 논문에서 제안한 투표자의 후보추천 참여 외에도 많은 수의 가치 있는 제안이 이루어져서 의견이나 경험 외에도 좀 더 효율적으로 다양한 관점에서 여러 정보를 수집하고 공유할 수 있는 진보된 수단에 대한 연구가 지속되어야 할 것으로 예상된다.

참고문헌

[1] “Wikipedia”, ko.wikipedia.org, 2010. 11.

[2] 제갈병직, “스마트폰 시장과 모바일OS 동향”, Semiconductor Insight, 2010. 5.

[3] 최용락, 소우영, 이재광, 이임영, “컴퓨터통신보안 3rd”, 그린출판사, 2006. 1.

[4] 최재규, “C# Programming Bible with .Net frame-work 3.0”, 영진닷컴, 2009. 1.

[5] 이두진, “안드로이드 앱 개발 완벽 가이드”, PCBOOK, 2011. 2.

[6] 윤성우, “TCP/IP 소켓 프로그래밍”, 프리렉, 2003. 4.

[7] 임치환 “모바일 기술을 활용한 전자투표시스템의 설계”, 대한인간공학회 학술대회논문집, pp.403~407, 2011. 5.

[8] 박희운, 이임영, “전자투표상에서의 부정행위 방지에 관한 연구”, 통신정보보호학회논문지 제8권, 제4호, 1998. 12.

[9] FKII 조사연구팀, “소셜미디어(Social Media)란 무엇인가”, 정보통신연구진흥원, 학술정보 정보산업지, 2006권 6호, 52~55, 2006.