

# 사용자 경험 (UX)에 기반한 안전하고 편리한 스마트워크 서비스

이현동\*, 오준철\*, 정목동\*

\*부경대학교 컴퓨터공학과

e-mail : win4class@hanmail.net, jcoh@gsti.co.kr, mdchung@pknu.ac.kr

## Secure and Convenient Smartwork Services based on User Experiences

Hyundong Lee\*, Juncheol Oh\*, Mokdong Chung\*

\*Dept of Computer Engineering, Pukyong National University

### 요 약

최근의 비즈니스 컴퓨팅 환경은 스마트워크 도입으로 이동성 보장 및 업무의 효율성이 높아지고 있는 반면에, 보안이 취약하다는 문제점과 더불어 복잡한 사용자 인터페이스로 인해서 사용자의 불편 사항도 증가하고 있다. 이를 해결하기 위해서 본 논문에서는 안전하고 편리한 스마트워크 서비스 제공을 위한 사용자 경험 (UX) 기반의 사용자 인터페이스 및 보안 시스템을 제안하고, 스마트워크 서비스 시나리오를 통해서 제안하는 시스템을 평가한다. 안전하고, 편리한 스마트워크 서비스의 활용을 통하여 유연한 근무 체계 확립과 동시에 업무 생산성을 향상시킬 수 있을 것으로 기대된다.

### 1. 서론

1980년대 후반, 우리나라의 잠재성장률은 약 10% 수준이었으나, 최근 저 출산, 고령화에 따른 경제활동 인구의 감소와 선진국과 비교하여 노동시간 대비 낮은 생산성 등의 원인으로 인하여 3% 수준으로 하락하며 경제 성장률의 둔화를 보이고 있다[1].

이에 인력 자원의 역할 및 근무형태 등을 고려하여 적합하고 유연한 근무형태를 통해 생산성 향상 및 저 출산, 고령화와 같은 사회적인 문제를 해결하는 방안으로서 모바일 오피스, 재택 근무, 원격 근무 등의 기능을 모두 포함하고 있는 스마트워크 도입의 중요성이 커지고 있다.

스마트워크 도입으로 이동성 보장 및 업무의 효율성이 높아지고 있는 반면에, 보안이 취약하다는 문제가 발생하고 있다. 또한, 공인인증서 및 OTP(One-Time Password) 등의 귀찮은 사용자 인증 및 복잡한 사용자 인터페이스로 인해서, 사용자의 불편 사항이 증가하고 있다.

본 논문에서는 스마트워크 환경에서 안전한 업무를 수행하기 위한 보안 서비스 및 사용자 경험(UX) 기반의 사용자 인터페이스를 제안한다.

본 논문의 구성은 다음과 같다. 2절 관련 연구에서는 스마트워크 서비스 제공을 위한 기본 기술들을 살펴보고, 3절에서는 스마트워크 서비스를 위한 사용자 경험(UX)기반의 사용자 인터페이스 및 보안 서비스를 제공하는 스마트워크 서비스 구성을 살펴본다. 4절에서는 시나리오 및 제안 시스템 평가하고, 마지막으로 5절에서는 결론 및 향후 연구 방향을 제시한다.

### 2. 관련연구

#### 2.1 스마트워크 서비스

스마트워크 서비스는 종래의 사무실 개념을 탈피하여 시간과 장소에 얽매이지 않고 언제 어디서나(anytime, anywhere) 편리하고 똑똑하게 근무함으로써 업무 효율성을 향상시킬 수 있는 미래지향적인 업무 환경이다[2].

그림 1은 스마트워크 서비스의 특징을 나타낸다.



그림 1. 스마트워크 서비스의 특징[2]

#### 2.2 스마트워크 서비스의 보안 이슈

스마트워크의 한 유형인 재택근무의 경우 기존 사무실에 비해 보안에 취약하다. 또한, 최근 들어 각광을 받고 있는 스마트폰 및 스마트패드를 이용하는 모바일 근무 역시 외근자 위주의 업무처리가 가능한 수준의 서비스만 이용할 수 있으며, 보안에 대한 취약성이 존재한다. 이를 해

결하기 위한 보안 기술로는 안티바이러스, 침입차단, 통합 PC 보안, DB/콘텐츠 보안, 접근관리 및 가상사설망(VPN) 등이 있다. 스마트워크의 또 다른 유형인 스마트워크센터의 보안에는 다양한 소속의 근로자들이 공용으로 사용하기 때문에 출입보안, 서버보안, 문서 출력보안, 공용 PC환경 보안, 방음시설 등이 있다.

표1은 스마트워크의 서비스의 보안 검토사항이다. 스마트워크 보안의 경우 기업별, 시스템별, 업무 내용별 적용 정책이 다양하므로, 수준에 따른 보안 정책을 고려해야 한다[3].

표 1. 스마트워크 서비스의 보안 검토 사항

분류	보안 이슈에 대한 검토사항
단말 부분	<ul style="list-style-type: none"> <li>• 단말기의 도난 및 분실로 인한 개인정보 또는 업무정보의 유출</li> <li>• 스마트폰 소유자가 악의적으로 업무 정보를 외부로 유출할 가능성 존재</li> </ul>
응용 프로그램 및 플랫폼 부분	<ul style="list-style-type: none"> <li>• 개인정보 유출: 스마트폰의 블루투스 및 애플리케이션을 통해 이용자가 인지하지 못한 채 SMS, 통화기록, 위치정보 등의 개인정보 유출 가능</li> <li>• 장치이용 제한: 콘텐츠 삭제, 아이콘 변경 등을 통해 기기의 사용을 불가능하게 만들거나 일부 기능을 마비시키는 공격 수행</li> <li>• 부정 과금 유발: 바이러스 감염 등으로 비정상인 요금 유발, 등의 문제 발생</li> <li>• 모바일 DDoS: 감염된 좀비 단말기는 특정 사이트에 트래픽을 유발함으로써 부정 과금 유발 및 웹사이트 마비, 단말이용 불능 야기</li> </ul>
네트워크 및 서버 부분	<ul style="list-style-type: none"> <li>• 네트워크 구간에서 패킷 스니핑을 통한 해킹</li> <li>• 스마트폰, 노트북 등 휴대단말을 경유하여 내부 인트라넷 서버에 접속함으로써 보안 위협</li> <li>• 악성코드에 의한 정보 전송, 무선 구간의 도청</li> </ul>

### 2.3 퍼지 알고리즘

1965년 Lotfi A. Zadeh가 ‘퍼지 집합(Fuzzy sets)’을 발표하면서, 퍼지 연구가 활성화되었다. 퍼지 논리는 고전적인 이진 논리처럼 소속을 분명히 하는 것이 아니라, 어느 정도 속하는지를 바탕으로 지식을 표현하는 일련의 수학 원리이다[4].

Fuzzy 알고리즘은 수집한 상황정보를 분석하기 위해서 특정 상태 집합에 어느 정도 포함되는지를 정의한 소속도 함수를 사용한다. 환경 변수  $x$ 에서 수집된 상황정보  $e$ 를 퍼지화한 상태는 다음 식1과 같이 정의한다.

$$fuzzification_x(e) = \sum_{s^x} u_{s^x}(e) / s^x \quad (1)$$

$S^x$ 는 환경 변수  $x$ 의 상태를 의미하고,  $u_{s^x}(e)$ 는 해당 상태에 대한 퍼지 소속도 함수(0, 1 사이)를 의미한다.

본 논문에는 가장 흔히 쓰이는 퍼지 추론 기법인 Mamdani 방법을 이용하여, 애매모호한 상황에 따른 사용자 경험 정보를 분석한다. Mamdani 퍼지 추론의 과정은 4 단계로 진행된다. 입력 변수의 퍼지화, 규칙 평가, 출력으로 나온 규칙의 통합, 마지막으로 역퍼지화이다[5].

### 2.4 사용자 경험 (UX: User eXperience)

최근에는 다양한 센서를 활용하여 기기와 사용자가 소통하는 방식을 직관적으로 바꾸려는 시도가 계속 되고 있다. 특히 제한적인 화면으로 입력이 불편한 스마트폰 환경에서의 입력 방식은 사용자에게 편의성을 제공하며 좀 더 쉽고 직관적으로 전달하려는 노력들이 계속되고 있다.

사용자 경험(UX) 기술은 사용자의 상황과 성향을 고려하여 적합한 콘텐츠를 골라 우선적으로 제공하는 기술이다[6]. 사용자 경험 기술을 통하여 모바일 기기는 매우 개인화된 기기로 사용자 개인 정보나 지리적 정보 획득이 용이해, 상황기반 개인화 및 맞춤형 서비스를 제공할 수 있다.

### 3. 안전하고 편리한 스마트워크 서비스

#### 3.1 스마트워크 서비스 구성

안전하고 편리한 스마트워크 서비스를 제공하기 위해서 제안하는 시스템은 사용자의 경험 정보를 수집 및 분석하여 사용자 인터페이스 화면을 제공하는 Smartwork Server와 사용자 인증 및 접근제어, 데이터 암호·복호화 서비스를 제공하는 Security Server로 구성한다. 그림 2는 제안하는 시스템의 내부 구성을 나타낸다.

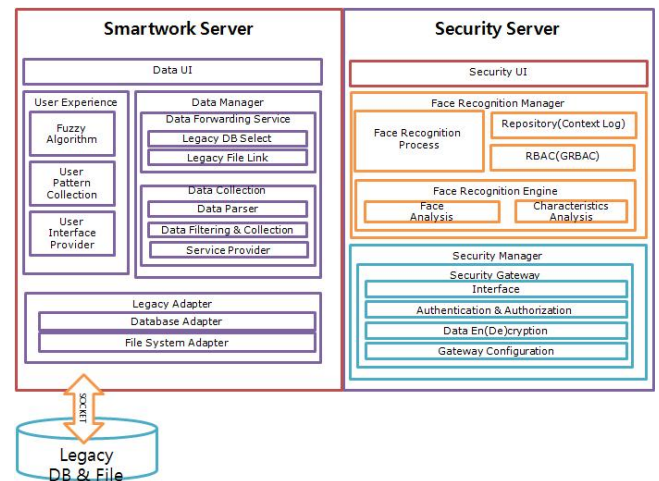


그림 2. 스마트워크 서비스 구성

#### 3.1.1 Smartwork Server

레거시 시스템과 연결 및 레거시 시스템의 대용량 데이터를 스마트워크 서비스에 적합한 형태로 가공하고, 필터링하는 기능을 수행한다. 또한, 사용자의 경험 정보를 수집하고 퍼지 알고리즘을 이용하여 분석하여 동적인 사용자 인터페이스 화면을 제공한다.

- Data UI: 스마트워크 서비스 제공을 위한 화면 제공
- User Experience: 사용자 경험 정보를 수집, 분석, 추론
- Data Manager: 레거시 시스템의 대용량 데이터를 수집하여, 스마트워크 서비스에 필요한 데이터만 필터링하는 기능 수행
- Legacy Adapter: 레거시 DB 및 파일 시스템과 연계를 위한 어댑터 제공

### 3.1.2 Security Server

스마트워크 서비스 환경에서 기본 인증 (아이디/패스워드)을 검증하고, 접근 제어 및 데이터 암호·복호화의 기본적인 보안 서비스를 제공한다. 또한, 인증 과정에서 사용자 편의성을 제공하기 위해서 추가 인증 방식인 얼굴인식 기반의 인증 서비스를 제공한다.

- Security UI: 사용자 인증 화면 및 보안 관리자가 보안 설정을 하기 위한 화면 제공
- Face Recognition Manager: 사용자 얼굴 정보를 분석하는 기능 수행
- Security Manager: 기본 인증, 접근제어, 데이터 암호·복호화 서비스 제공

### 3.2 스마트워크 서비스의 환경

고정 환경 또는 이동 환경에서 스마트워크 서비스 사용자는 업무 관련 정보에 접근하기 위해서 사용자 기본 인증을 시도한다. 인증이 성공되면, 스마트워크 서비스를 받을 수 있다. 하지만, 중요한 정보에 접근할 경우, 한 번의 아이디/패스워드 인증으로는 보안성이 취약하다. 이런 문제를 해결하고자 제안하는 논문에서는 중요한 정보를 접근할 경우, 사용자 편의성과 안전성을 보장하기 위해서 얼굴인식 기반의 추가 인증 서비스를 제공함으로써 보안성을 강화한다.

또한, 스마트워크 서비스를 사용하면서 축적한 사용자의 경험 정보를 바탕으로, 사용자가 자주 사용하는 메뉴를 동적으로 재구성함으로써 사용자의 편의성을 향상시킨다.

다음 그림 3은 스마트워크 서비스의 환경을 나타낸다.

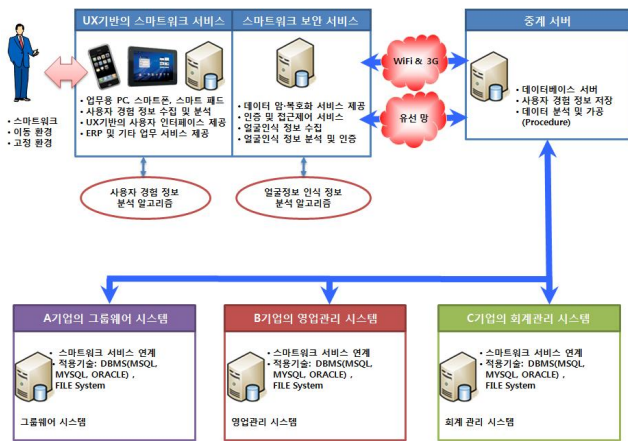


그림 3. 스마트워크 서비스 환경

## 4. 스마트워크 서비스 시나리오 및 시스템 평가

### 4.1 스마트워크 서비스 시나리오

스마트워크 서비스 환경에서 사용자 인증 및 접근제어, 데이터 암호·복호화 서비스를 제공함으로써, 안전한 스마트워크 서비스를 제공한다. 뿐만 아니라, 추가 인증 시 사용자가 편리한 얼굴인식 기반의 인증 서비스를 제공함으로써, 사용자 인증의 번거로움을 줄였다. 그림4와 같은 스마트워크 서비스의 시나리오 과정을 통하여 편의성 및 안전성을 보장한다.

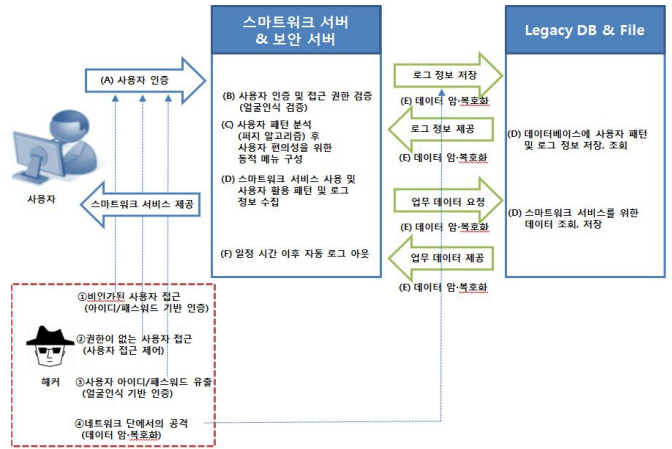


그림 4. 스마트워크 서비스의 시나리오

- A단계: 사용자가 기본 인증 (아이디/패스워드) 과정을 거친다. 중요한 정보에 접근할 경우, 추가적 인증 방식인 얼굴인식 기반 인증 서비스를 통하여 스마트워크 서비스를 요청한다.
- B단계: 보안 서버가 인증 정보를 검증한 후, 인증 성공 시 사용자 권한을 검증한다. 인증 실패 시 사용자에게 재 인증을 요청한다.
- C단계: 권한이 있는 스마트워크 메뉴 중에서 사용자가 자주 사용하는 정보를 퍼지 알고리즘으로 분석 한 후, 동적으로 메뉴를 구성하여 스마트워크 서비스를 제공한다. 만일, 사용자가 초기에 접근할 경우에는 사용자 패턴 및 로그 정보가 없기 때문에, 기본 업무 메뉴를 제공한다.
- D단계: 사용자가 스마트워크 서비스를 사용하는 도중에 실시간으로 사용하는 패턴 및 로그 정보를 수집한다. 수집한 정보는 사용자의 재접속 시 동적 메뉴를 구성하는데 활용한다.
- E단계: 사용자의 화면(UI)을 제공하는 클라이언트와 데이터가 저장되어 있는 서버단의 정보는 데이터 암호·복호화 기술을 적용하여 정보의 기밀성 및 무결성을 보장한다.
- F단계: 사용자가 일정 시간 사용하지 않을 경우, 자동적으로 사용자 계정의 접속을 로그아웃 한다.

### 4.2 스마트워크의 보안 침해 대응 과정

스마트워크 서비스는 Security Server를 통하여 보안 서비스를 제공한다. 이를 통하여 다음과 같은 보안 공격에 대응할 수 있다.

- ①비인가된 사용자 접근: 기본적인 인증인 아이디/패스워드 기반의 인증 과정을 수행한다. 또한 사용자가 일정 시간 사용하지 않을 경우에 로그아웃 기능을 제공하여, 비인가된 사용자의 접근을 차단한다.
- ②권한이 없는 사용자 접근: 접근제어 기법인 RBAC(Role Base Access Control)를 사용하여, 사용자 권한별로 정보를 제공하기 때문에, 권한 오남용을 방지 할 수 있다.
- ③사용자 아이디/패스워드 유출: 중요한 정보를 조회할 경우, 보조 인증 수단인 얼굴인식 기반의 인증 과정을 추

가적으로 수행하기 때문에, 보안 위협에 대응한다,

- ④네트워크 단에서의 공격: 클라이언트와 서버단의 통신에서는 데이터 암호화 기술을 적용하여, 데이터 기밀성 및 무결성을 보장하여, 정보의 유출을 방지한다.

#### 4.2 스마트워크의 사용자 편의성 제고

제안하는 Smartwork Server의 User Experience 모듈에서 상황에 따른 사용자의 경험 정보를 수집하고 퍼지 알고리즘을 이용하여, 사용자가 자주 접속하는 메뉴를 분석한다. 분석된 정보를 바탕으로 사용자가 원하는 메뉴를 동적으로 제공함으로써, 사용자의 스마트워크 서비스 편의성을 제고할 수 있다. 사용자 편의성을 향상시키는 개념도는 그림5와 같다.

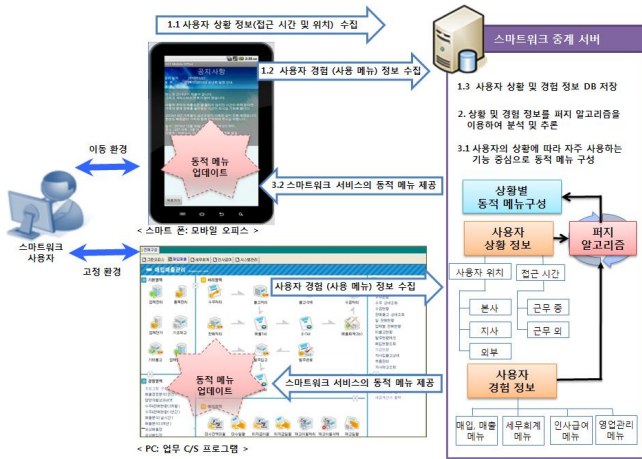


그림 5. 스마트워크 서비스의 사용자 편의성 제고 개념도

- ①사용자의 상황(접근 시간, 사용자 위치)정보와에 스마트워크 서비스 사용 과정에서의 행동 패턴 및 사용 메뉴 정보를 데이터베이스에 저장한다.
- ②저장된 사용자의 상황 정보와 경험 정보를 퍼지 알고리즘을 활용하여 상황별로 사용자가 자주 사용하는 메뉴의 우선순위를 추론한다.
- ③추론된 메뉴의 우선순위 정보를 바탕으로 자주 사용하는 기능 중심으로 메뉴를 동적으로 구성하여 스마트워크 서비스 사용자에게 제공한다.

수집한 사용자 경험 정보는 동적인 메뉴 구성 외에 사용자별 메뉴 사용에 대한 통계 및 스마트워크 서비스 유지 보수 정책 수립에도 활용 할 수 있다.

#### 4.3 제안하는 스마트워크 서비스의 평가

스마트워크 서비스는 업무 환경의 이동성을 보장하기 때문에, 사용자 편의성과 안전성이 중요시 되고 있다. 하지만, 기존의 ERP 시스템과 모바일 오피스의 경우에는 고정된 형태의 동일한 메뉴 제공 및 스마트워크 서비스 시작시 한 번의 인증 서비스를 제공하고 있기 때문에, 편의성 및 안전성의 요구사항을 만족하지 못하고 있다.

하지만, 제안하는 시스템은 사용자 경험 정보 기반의 동적 메뉴 제공과 중요 정보 접근 시 편리한 얼굴인식 기반의 추가 인증 서비스를 제공함으로써 사용자의 편의성 및

정보의 안전성이 향상된다.

표2는 기존 ERP 시스템과 제안하는 스마트워크 서비스의 정성적인 비교를 나타낸다.

표 2. 기존 ERP 시스템과 제안하는 스마트워크 서비스 비교

항목	기존 ERP 시스템	스마트워크 서비스(제안)
사용성	복잡하고 어렵다	쉽고, 간편하다
보안성	한 번의 인증 과정 (아이디/패스워드, OTP, 공인인증서)	기본(아이디/패스워드) 인증 서비스와 편리한 얼굴인식 기반의 추가 인증 제공
메뉴 구성 방식	SAP/ORACLE을 모방한 메뉴 다운 또는 트리 방식	VISUAL 업무 프로세스 형태의 메뉴 구성으로 직관적이고 쉬운 업무 프로세스 파악
비계량 요소	파일 첨부 등 비계량적인 요소를 배제	사내 공지사항, 전자 업무 일지, 파일첨부기능 등 비계량적인 요소 고려

#### 5. 결론 및 향후 연구

사용자 경험 정보 수집과 퍼지 알고리즘을 이용하여 자주 사용하는 기능 중심의 동적 메뉴 구성과 스마트워크 환경에서의 기본 보안 서비스 및 편리한 인증 방식인 얼굴 인식기반 추가 인증 서비스를 제안하였다. 이를 통하여 스마트워크 환경에서 사용자는 편리하고, 안전한 업무를 수행할 수 있다. 또한, 이러한 스마트워크의 안전성과 편의성을 통하여 유연한 근무 체계 확립과 동시에 업무 생산성을 향상시킬 수 있다.

향후에는 제안하는 스마트워크 서비스를 산업 현장에서 필드 테스트를 통해 정량적 평가를 수행하고자 한다. 정량적인 평가를 통해 수집된 사용자별 업무 단축 시간 및 사용 메뉴를 찾기 위한 마우스 클릭 변화율 정보를 사용자 경험 분석 과정에서 피드백으로 추가하는 방안을 연구하고자 한다.

#### Acknowledgments

“본 논문은 중소기업청에서 지원하는 2011년도 산학연공동기술개발사업(No.00046702)의 연구수행으로 인한 결과물임을 밝힙니다.”

#### 참고문헌

- [1] 김정언, “스마트워크 추진 현황과 활성화 방안”, 한국통신정책연구원, 2010.11.
- [2] 김꽃마을, “스마트워크 활성화 정책방향”, *TTA Journal*, Vol.134, 2011.03.
- [3] “기업을 위한 스마트워크 도입·운영 가이드북”, 방송통신위원회&한국정보화진흥원, 2011.01.
- [4] L.A.Zadeh, “Fuzzy sets”, *Information and Control*, Vol.8, June. 1965, pp.338-353.
- [5] E.H.Mamdani and S.Assilian, “An experiment in linguistic synthesis with a fuzzy logic controller”, *International journal of Man Machine Studies*, 7(1), November. 1975. pp.1-13.
- [6] Tullis, Tom, Albert, Bill, *Measuring the User Experience*, Elsevier Science Ltd, 2008.