스마트폰 자동 녹음 앱을 이용한 생활 안전 도우미 설계 및 구현

문정경* · 황득영** · 김진묵*

요 약

급변하는 사회의 변화로 말미암아 강력 범죄가 급격하게 증가하고 있다. 하지만 이에 대한 경찰 인력의 부족, 현장 출동을 하더라도 범죄 상황에 대한 파악 등을 위한 시간 지연 등의 문제가 심각하다. 이미 오래전부터 관련 연구자들이 이를 해결하고자 많은 연구방법들을 제안하였다. 하지만 현실적으로 기존에 제안된 연구방법들이 아직도 부족한 점이 많다. 그러므로 본 연구에서는 스마트폰과 초고속 인터넷서비스 기술을 활용해서 범죄 상황에 대한 신속한 파악과 푸쉬 서비스를 사용해서 보안 서비스를 제공하고자 한다. 제안한 시스템은 스마트폰 사용자가 사전에 설정한 단축키를 누르면 주변에서 발생하는 음성 정보를 실시간으로 녹음하고, 저장된 음성 정보와 LBS 정보를 인증 과정을 거쳐 서버에 저장한다. 그리고 서버는 저장된 음성 정보와 LBS 정보를 푸쉬 서비스를 사용해서 가족들에게 알린다. 현재까지 우리는 제안시스템에 설계를 마쳤다. 그리고 스마트폰 사용자 앱과 인증 서버를 구현했다. 그리고 인증 서버에서 푸쉬 서비스를 사용해서 사용자 가족에게 메시지를 전달해서 알릴 수 있는 상태이다. 하지만 향후 연구를 통해 좀 더 제안한 연구가 타당성을 검토해야만 한다.

Design and Implement of Secure helper using Smart-phone Auto recording App

Jeong-Kyung Moon* · Deuk-Young Hwang** · Jin-Mook Kim*

ABSTRACT

The violent crime has increased dramatically in our society. This is because our society has to change quickly. Strong police force, but this is not enough to solve the crime. And there are a lot of police to investigate the situation difficult to go out to the crime scene. So inevitably increase in the risk of crime. Researchers have conducted a number of studies to solve this problem. However, the proposed study how realistic are many points still lacking. herefore, we to take advantage of smartphones and high-speed Internet access technology to provide security services using the push service for rapid identification and crime situation in this study. Therefore, we would like to provide rapid service to identify criminal security situation using smart-phone app and push services on the high speed internet environments. The proposed system is to record the voice information received from the smart phone near the user presses the hot key is set in advance in real-time, and stores the audio information stored in the LBS information to the server through the authentication procedure. And the server uses the stored voice data and LBS Push service information to inform their families. We have completed the design of the proposed system. And it has implemented a smart phone app, the user authentication server. And using the state in which the push service from the authentication server by transmitting a message to a user to inform a family. But more must examine whether the proposed research is relevant in future studies.

Key words : App, Voice-recording, Smart-Phone, Security service, Authentication, Push service

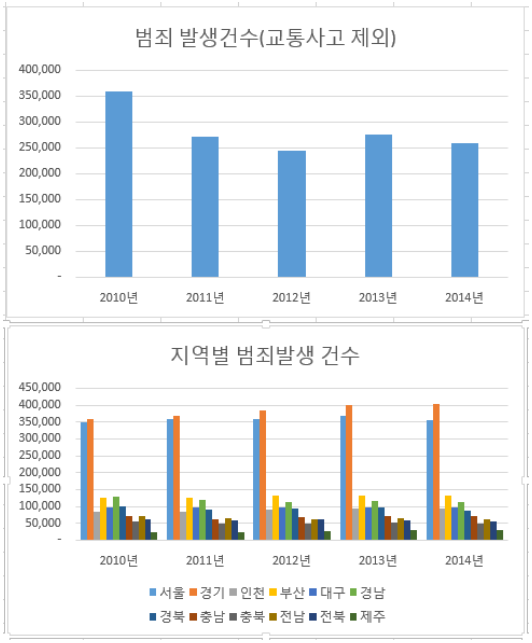
접수일(2015년 12월 23일), 게재확정일(2015년 12월 29일)

* 선문대학교 / IT교육학부
** 강원대학교 삼척캠퍼스 / 컴퓨터공학과(교신저자)

1. 서 론

최근 들어 핵-가족화로 인해서 1가구 1세대가정이나 2명 이하의 구성원으로 이루어진 가정이 증가하면서 강력범죄, 지능범죄, 풍속범죄의 발생건수가 증가하고 있다. 특히 서울이나 경기 지역과 같이 대도시 주변의 범죄의 발생 건수가 매우 크게 증가하고 있는 추세이다[13].

아래의 (그림 1)은 2010년부터 2014년 사이에 경찰청에서 발표한 전체범죄 발생 건수 및 지역별 범죄 발생 건수 자료를 재-구성한 것이다.



(그림 1) 최근 5년간 범죄발생 건수 및 추세

전체 범죄의 발생건수는 2012년을 기점으로 다소 감소하는 추세이다가 2014년으로 바뀌면서 점점 범죄 발생이 증가하고 있는 추세이다. 이것은 최근 들어 우리 사회의 경제가 다소 어려워지고, 외국인들의 국내 유입과 묻지마 범죄가 증가하는 사회적인 현상 때문인 것으로 이해된다. 더욱이 최근 들어 컴퓨터나 스마트폰 등을 이용한 소셜 네트워크 서비스를 범죄의 도구로 이용하는 경우도 증가하는 추세이다[3, 11].

그러므로 본 논문에서는 스마트폰을 이용해서 범죄의 발생 상황을 녹음하고 실시간으로 지정된 서버와 가족들이나 인근의 경찰에게 전달함으로써 범죄 발생 시 즉각적인 사고처리가 가능하도록 하고자 한다.

이를 위해서 스마트 폰에서 자동 녹음 앱을 설계 및 개발하고, 실시간 음성 녹음 데이터와 위치 정보를 지정된 서버로 전송 및 저장할 수 있는 자동 음성 녹음 서버를 설계 및 구현한다. 그리고 구글이 제공하는 푸쉬 서버 오픈소스를 활용해서 가족들과 경찰에게 범죄 상황 데이터를 문자 메시지로 전달할 수 있다.

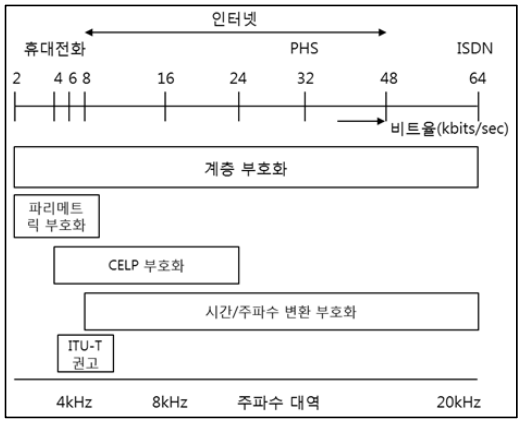
본 논문의 구성은 다음과 같다. 2장은 본 연구에서 사용한 요소기술들인 스마트폰 자동 녹음 앱을 설계하기 위한 녹음 기술과 푸쉬 서버 기술에 대해서 설명한다. 3장은 제안시스템인 스마트폰 자동 녹음 앱과 음성 데이터 저장 서버의 구성 요소들에 대해서 설명한다. 추가로 스마트폰 녹음 앱과 데이터 저장 서버 사이의 동작 절차에 대해서 설명한다. 4장은 제안시스템의 구현 결과에 대해서 설명하였고, 마지막으로 5장은 결론 및 향후 연구에 대해서 설명하였다.

2. 관련 연구

2.1 스마트폰 녹음 관련 기술들

일반적으로 음성 데이터를 녹음하기 위해서 음성신호 압축 코덱으로 MP3, AAC, OGG, WAV 등을 사용한다. 본 연구에서는 앞에서 나열한 다양한 음성신호 압축 코덱 표준기술들 중에서 MPEG4 기술을 사용하고자 한다. MPEG 부호화 기술은 범용 음악 신호의 고음질 방식과 통신에 목표를 둔 음성신호 방식으로 나눌 수 있

다. 그 중에서도 MP3는 디지털 음성 신호를 고효율로 압축, 부호화하기 위한 규격이다. 주로 음성신호만을 저장하는데 사용된다. 그리고 MPEG4는 음성부호화, 인터넷 휴대통신, 음성 합성, 음악합성(MIDI)등을 포함하는 표준 규격이다. 음성신호 부호화 방식에는 시간주파수 변환 부호화 방식, 음성신호 주체인 CELP(Code Excited Linear Prediction) 부호화, 파라메트릭 부호화, 그리고 계층부호화 등이 있다[2].



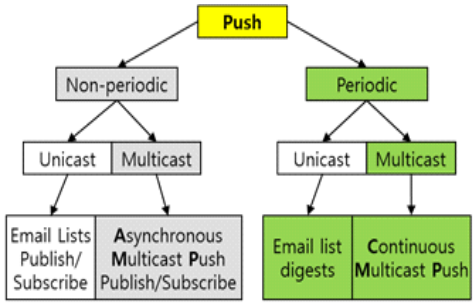
(그림 2) MPEG4 음성신호 부호화 방식

특히 음성신호 녹음기술은 주변에서 발생하는 잡음에 따라서 그 성능이 크게 좌우된다. 따라서 안정적인 성능확보를 위해서 다양한 잡음 제거 빔포밍 기술들이 연구되고 있다. 그중에서 GSC(generalized sidelobe canceller) 빔포밍 알고리즘은 LCMV(linearly constrained minimum variance) 알고리즘을 기능적으로 분해해놓은 형태와 동등하고 알려져 있으며, AMC(adaptation mode controller)만 제대로 동작하면 LCMV 보다 더 나은 성능을 얻을 수 있다고 한다[5, 6].

2.2 음성 데이터 전달을 위한 푸쉬 서버

푸쉬 서버란 구글이 제공하는 오픈소스 기술이다. 이 기술을 사용하면 스마트폰 사용자의 요구에 서버에 저장된 데이터를 사용자가 원하는 스마트폰이나 기기에게 문자메시지를 전달할 수 있다. 이때 위치 정보와 같은 텍스트 정보와 함께 서버에 사전에 녹음되어 있는 음성신호도 함께 전달할 수 있다. 이와 같은 전송 방식은 클라이언트 측의 검색 시간과 노력을 절감시킬 수 있다[7,8,9,10].

웹 서버에서 푸쉬 서버 기능을 구현하는 방법으로는 풀링(PULLING), 롱-풀링(LONG PULLING), 스트림방식(STREAM) 등이 있다.풀링 방식은 클라이언트가 반복적으로 서버에게 전달할 콘텐츠가 있는지 물어보는 방식이다. 롱-풀링 방식은 클라이언트가 서버에게 전달할 콘텐츠가 있는지 여부를 한번 물어보고, 서버 응답이 있을 때까지 계속 기다리는 방식이다. 마지막으로 스트림 방식은 클라이언트가 서버에게 단 한번 콘텐츠 요청을 하고, 서버는 보내고자 하는 콘텐츠가 있으면 언제든 보낼 수 있는 방식이다.



(그림 3) 푸쉬 서버의 데이터 전달 방식

모바일에서 사용하는 대표적인 푸쉬 서비스는 단문메시지(SMS)와 장문메시지(MMS), 그리고 애플이 제안한 APNS(Apple Push Notification Service)와 구글의 C2DM(Cloud to Device Messaging)방식이 있다.

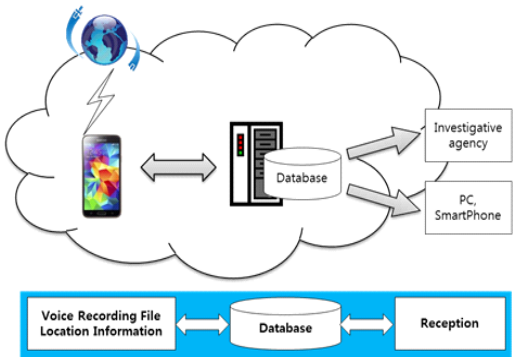
위의 (그림 3)은 푸쉬 서버의 기능을 주기적인 방식과 비-주기적인 방식으로 나누어 데이터의

전송 양식을 보여준다. 그리고 유니 캐스트와 멀티 캐스트 방식으로 구분해 나타낼 수도 있다. 또한 일정한 주기 없이 멀티 캐스트 하는 Asynchronous Multicast Push(AMP)[]와 주기적으로 멀티캐스트 하는 Continuous Multicast Push(CMP) 방식이 있다.

3. 제안시스템

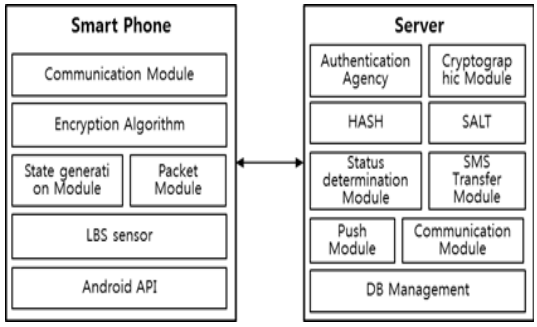
3.1 제안시스템 구조

(그림 4)는 본 논문에서 제안하고자 하는 스마트폰 자동 녹음 앱을 설치한 스마트폰과 스마트폰 사용자의 위치정보와 음성신호를 저장하기 위한 서버 역할을 하는 데이터베이스, 사용자가 저장한 정보를 푸쉬 서버를 통해서 전달하기 위한 데이터 수집 에이전트 등으로 구성된다.



(그림 4) 제안시스템 구조

제안시스템에서는 일반적인 상황에서도 사용자가 원할 때 음성신호를 저장할 수 있는 녹음 기능과 통화 내용을 녹음할 수 있는 녹음 에이전트를 갖는다. (그림 5)는 제안시스템에서 스마트폰 자동 녹음 앱의 구성요소들과 서버의 구성요소들을 나타내고 있다.



(그림 5) 제안시스템 구성요소들

본 논문에서 제안하는 스마트폰 자동 녹음 앱을 구성하는 요소들은 6개로 구성된다. 본 연구에서 사용한 스마트폰은 안드로이드 운영체제를 기반으로 하는 것을 전제 조건으로 하기 때문에 안드로이드 API 모듈, 일반적인 통신을 위한 통신 모듈, 스마트폰과 서버 사이에 데이터를 암호화해서 전달하기 위한 암호화 알고리즘(LEA128, HASH, SALT)을 갖는다. 상황정보를 판별하기 위한 모듈, 전송할 음성신호와 위치정보를 포함하는 텍스트 정보를 일정한 크기로 구분해서 전달하는 패킷 관리 모듈, 위치 정보를 인식하기 위한 LBS 센서 모듈로 구성하였다.

3.2 제안시스템 동작절차

본 논문에서는 스마트폰과 서버, 사용자의 가족사이에서 암호화된 데이터 전달과 사용하는 기기들에 대한 인증 서비스를 위한 7 단계로 구성된 동작절차로 구성하였다.

제안시스템은 크게 3가지 동작 단계를 갖는다. 첫 번째 동작단계는 동작절차 1과 동작절차 2로 구성된다.

첫 번째 동작절차는 각 디바이스가 인증서버에게 인증을 요청하고 토큰을 받는 단계이다.

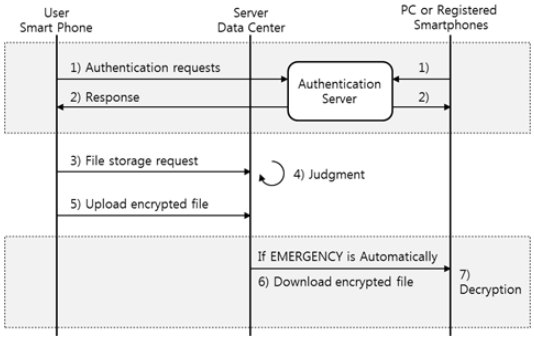
1) 인증요청(Authentication requests)

{U_Info | (U_Info)' }

- U_Info = User_ID | User_PWD | Device_ID(n) | TS

U_Info는 User ID와 Password, n개의 Device ID 그리고 타임스탬프(Timestamp)를 나열한 정보이다. (U_Info)' 는 MD5알고리즘을 사용한 HASH값이다. 이 두 자료를 임시 발급한 세션키(session key)로 암호화하여 전송한다.

인증서버(Authentication Server)는 전달받은 자료를 복호화하여 인증을 진행한다. 그리고 테이블에 사용자 정보를 저장한다.



(그림 6) 제안시스템의 동작절차

2) 인증서버의 응답(Response)

{(U_Info) | Salt(s_key) | (s_key)' | TS}

두 번째 동작절차는 인증서버의 응답이다. 정상적인 디바이스임이 확인되면 상호간 사용할 비밀키를 생성한다. LEA 알고리즘으로 생성된 비밀키를 사용하여 U_Info를 암호화 한다. 생성된 비밀키는 SALT를 수행한다. 그리고 생성된 비밀키의 HASH값을 발생시킨다. 암호화된 정보와 SALT된 비밀키, 그리고 비밀키 해시값을 나열한 후 임시 발급받은 세션키로 다시 한번 암호화한 후 전송한다.

SALT는 해쉬함수로 암호 앞이나 뒤에 임의의 문자를 넣어 길이를 같게 하는 알고리즘이다. 해시값은 메시지를 압축하는 방식이다. 이것은 비밀키의 변조나 대체를 방지한다.

두 번째 단계는 파일 업로드 단계이다. 이는 동작절차 3부터 동작절차 5까지의 절차를 갖는다.

3) 데이터 저장 요청(File storage request)

{(F_Info) | (F_Info)' | TS }

* F_Info = Vo_file | Lb_info | St_info | TS

스마트폰에 저장된 음성파일, GPS로부터 받은 위치정보, 일반인지 긴급인지 판단하는 상태정보 그리고 Timestamp를 나열하여 LEA알고리즘으로 암호화한다. 그리고 F_info에 대한 HASH값을 만들어 나열한 후 세션키로 암호화하여 전송한다. 상태정보값은 일반일 때는 0, 긴급일때는 1로 저장한다. HASH 값과 F_info를 비교하여 일치하면 무결성이 보장된다.

4) 확인(Judgement)

서버는 전달받은 정보가 변조되지 않았는지 확인한다. 그리고 St_info 값을 분석하여 1이면 긴급 0이면 일반으로 처리하여 저장한다. St_info의 값이 1이면 저장 후 6) 과정을 바로 수행한다.

5) 암호화파일 업로드(Upload encrypted file)

{(F_Info) | (F_Info)' | TS }

* F_Info = Vo_file | Lb_info | St_info | TS

동작절차 4에 이어 파일이 종료될 때까지 업로드된다.

세 번째 단계는 파일 다운로드 단계이다. 동작절차 6과 동작절차 7로 구성된다.

6) {SMS_ Device_ID(-n) | (F_Info) | (F_Info)' }

St_info 값이 0이면 이미 등록된 디바이스에서 요청이 있을 때마다 앱을 사용하여 수동적인 다운로드가 가능하다. 그러나 St_info 값이 1이면 저장을 진행한 후, 자료를 업로드한 디바이스를 제외한 미리 등록된 디바이스로 위험 상황이 자동 전송된다. 이때, 문자자료와 암호화된 F_info 그리고 HASH 알고리즘으로 처리된 F_info를 세션키로 암호화하여 전송한다.

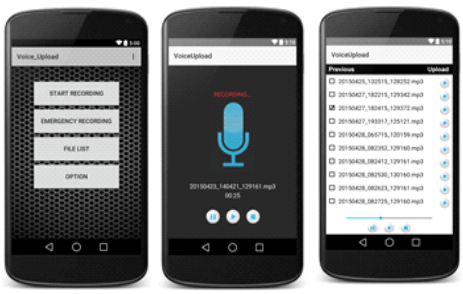
7) {SMS_ Device_ID(-n) | (F_Info) | (F_Info)' }

전송받은 디바이스에서는 세션키로 복호화한 후 문자와 파일정보를 확인할 수 있다.

본 논문에서 제안한 방법은 MITA (가로채기)에 의해 정보가 유출되더라도 내용을 알 수 없도록 LEA 128 암호 알고리즘을 사용해 암호화 한 후 데이터를 전달한다[4,12].

4. 구현 결과

본 논문에서 제안한 스마트폰 자동 음성녹음 앱의 구현 결과는 (그림 7)과 같다.



(그림 7) 제안시스템 구현결과

제안시스템은 위급한 상황에서도 사용하기 편리하도록 단축키로 메인 버튼을 2초 이상 누르면 자동 음성 녹음 앱이 실행하도록 설계하였다.

제안시스템을 사용하는 사용자는 위급 상황시 스마트폰의 메인 메뉴 버튼을 2초 이상 누름으로써 범죄자가 인식하지 못하도록 주변의 음성 정보와 위치 정보를 사전에 등록해 둔 사용자의 가족이나 가까운 경찰서로 실시간 정보를 전송할 수 있다. 이를 통해서 범죄자를 자극하지 않으면서 안전하게 구조 정보를 전달함으로써 범죄로부터 회피할 수 있을 것으로 예상된다.

5. 결론 및 향후연구

스마트폰을 사용한 녹음은 다양하게 사용되어지고 있다. 현재까지 개발된 스마트폰 음성 녹음 앱들을 앱스토에서 검색하고 분석해 본 결과, 첫 번째는 고음질로 음성을 녹음하는 앱과 비밀녹취를 위한 앱으로 크게 2가지 종류로 구분할 수 있다.

본 논문에서는 기존의 스마트폰 음성 녹음 앱들이 제공하는 일반적인 고음질 음성 녹음이나 비밀 녹취의 기능뿐만 아니라 긴급한 구조 상황에서 범죄자를 자극하지 않으면서 자신이 위험상황에 빠져 있음을 가족이나 가까운 경찰서에 알릴 수 있는 앱을 개발하고자 하였다.

연구의 초기 단계로 안드로이드 운영체제를 사용하는 스마트폰에서 오픈 API를 사용해서 일반적인 음성 녹음 기능을 구현하였고, 두 번째로 위급한 상황일 때 단축 버튼만으로 음성 정보를 녹음할 수 있도록 구현했다. 세 번째로 위급한 상황인 경우에 음성 정보 뿐만 아니라 위치정보까지 함께 인증을 확인한 후 전달할 수 있는 서버를 구축하였다. 마지막으로 구글에서 제공하는 오픈 소스로 푸쉬 서버를 구축한 후 사전에 등록한 가족이나 가까운 경찰서에 음성정보와 위치 정보를 문자 메시지로 전송할 수 있다.

하지만 아직까지 본 연구와 관련해서 수행해야 할 내용이 많이 남아 있는 상황이다.

향후 연구로 음성 정보와 위치 정보를 문자 메시지로 푸쉬할 수 있는 기능에 추가로 스트림 방식을 사용한 푸쉬 기능을 구현하고자 한다. 이를 통해서 실시간 음성 정보를 전달할 수 있게 하고자 한다.

두 번째로 사전에 등록된 가족 외에 가까운 경찰서에 위급 상황을 알리기 위한 방법론을 검토해 적용하고자 한다.

본 연구에서 제안한 향후 연구 2가지 이외에도 여러 가지 향후 연구들이 존재하고, 아직은 연구가 초기 단계이므로 미흡한 점들이 다수 존재한다. 이에 대한 해결책을 마련하기 위해서 법적, 행정적 절차 등에 대한 검토도 추가 진행할 것이다. 연구의 타당성을 검토하기 위해서 암호화된 데이터가 중간자 공격에 안전함도 검증해야 하고, 해쉬 데이터의 무결성 검증도 수행해야 할 것으로 생각한다.

참고문헌

[1] Yang-Gu Lee, Young-Soo Cho, Myeong-In Ji, Ju-Young Kim, Sang-Jun Park, Development of LBS Platform for High Density Location Recognige Service based on Smart-phone, The Journal of The Korean Institute of Communication Science, 30(2), pp.3-10, 2013.1.

[2] Euiseon Kang, Jeonghun Kim, SmartPhone Recording System for Mobile Office Environment, The Korean Contests Association, Vol.13, No.9, 2013. 9.

[3] Hyeyoung Gim, YeBeet Jang, Hyunnah Park, Seoungho Ryu, Smartphone users' application use and Privacy Concerns, The Conference of The HCI Society, pp.1150-1152, 2011.1.

[4] Andrey Bogdanov, Nicky Mouha, Elmar Tischhauser, Deniz Toz, Kerem Varici, Vesselin Velichkov, Meiqin Wang, Qingju Wang, and Vincent Rijmen, "Security Evaluation of the Block Cipher LEA Final Report," COSIC, Belgium, pp.3-30, July, 2011.

[5] Michi Skichi, World of MPEG-4, Youngpungmungo, 1999.10.

[6] Gannot et al., Signal enhancement using beamforming and nonstationarity with applications to speech, IEEE Trans. Signal Process., Vol. 49, No. 8, pp. 1614-1626, 2001.

[7] E. Bozdag, A. Meshbah, A Comparison of Push and Pull Techniques for Ajax, 9th IEEE International Workshop on WSE 2007, pp.15-22, 2007.

[8] G. Pour, The push to make software engineering respectable, IEEE Computer, Vol.33, No.5, pp.35-43, 2000.

[9] Jörg Nonnenmacher, Emst W. Biersack, Asynchronous Multicast Push: AMP, Proc. Of International Conference on Computer Communications, 1997.

[10] Pablo Rodriguez Rodriguez, Ernst W. Biersack, Continuous multicast push of web documents over the Internet, Network, IEEE, Vol.12, Issue2, pp.18-31, 1998..

[11] Seung-young Ma, Jung-ho Ju, Jong-sub Moon, The security requirements suggestion based on cloud computing security threats for server virtualization system, Journal of The Korea Institute of Information Security & Cryptology VOL.25, NO.1, Feb. 2015.

[12] TTAK.KO-12.0223. 128-Bit Block Cipher LEA, Telecommunications Technology Association. Pp.1-24. 2013.12.

[13] The Police Goverment of Korea, Account of Crime Data on Web-site, http://www.police.go.kr/portal/main/contents.do?menuNo=200197

[저 자 소 개]

문 정 경(Jeong-Kyung Moon)

1993년 2월 배재대학교 원예학과 (학사)
2006년 2월 단국대학교 인터넷정보학과(공학석사)
2013년 2월 공주대학교 컴퓨터공학과 (공학박사)
2012년 3월 ~ 현재 : 선문대학교 IT교육학부 계약교수

email : moonjk@sunmoon.ac.kr

김 진 묵 (Jin-Mook Kim)

1998년 2월 배재대학교 전자계산학과 (이학사)
2000년 2월 배재대학교 컴퓨터공학과 (공학석사)
2006년 2월 광운대학교 컴퓨터과학과 (공학박사)
2006년 9월 ~ 2008년 2월 선문대학교 컴퓨터공학과 연구교수
2006년 9월 ~ 현재 선문대학교 IT교육학부 부교수

E-Mail : calf0425@sunmoon.ac.kr

황 득 영 (Deuk-Young Hwang)

1988년 2월 광운대학교 전자계산학과(이학사)
1990년 2월 광운대학교 전자계산학과(공학석사)
1999년 2월 광운대학교 전자계산학과 (공학박사)
1990년 3월 ~ 1994년 2월 전주 기전대학교 전자계산학과 조교수
1994년 3월 ~ 현재 강원대학교 삼척캠퍼스 컴퓨터공학과 교수

email : dyhwang@kangwon.ac.kr