Journal of the Korea Convergence Society
Vol. 9. No. 12, pp. 53-60, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.12.053

스마트 기기를 이용한 상호 협력 기반 파일 공유 시스템

정필성[1], 조양현[2*]
[1]명지전문대학 정보통신공학과 교수, [2]삼육대학교 컴퓨터・메카트로닉스공학부 교수

File Sharing Algorithm based Mutual Cooperation using Smart Device

Pil-Seong Jeong[1], Yang-Hyun Cho[2*]
[1]Professor, Dept. of Information Technology Communication, Myongji College
[2]Professor, Division of Computer & Mechatronics Engineering, Sahmyook University

요 약 정보통신 기술의 발전으로 우리는 스마트 기기를 이용하여 언제 어디서나 기업정보가 담긴 문서에 접근하고 관리가 가능하게 되었다. 근무 환경이 스마트워크 근무 환경으로 변화함에 따라서 정보의 유통범위가 넓어짐과 동시에 보안을 위한 관리에 많은 노력이 필요하게 되었다. 본 논문은 스마트 기기를 소유한 사용자들끼리 상호 협력을 통해 파일을 관리하고 공유할 수 있는 파일 공유 시스템을 제안한다. 제안하는 파일 공유 시스템은 사용자가 파일을 업로드 할 때 함께 파일을 공유할 상대를 추가하면 파일의 일부분을 서로 나눠서 보관하고 나머지는 서버에 보관하는 알고리즘을 사용한다. 업로드 할 파일을 base64로 변환 후 사용자들끼리 암호화된 파일로 나누어 가진 후 공유를 원할 때 서버로 전송한다. 파일을 보기 위해서 전용 애플리케이션을 사용하여 파일 관리와 통제가 쉬우며 높은 보안성을 가진다. 본 논문에서 개발한 시스템을 이용할 경우 보안에 많은 돈을 지불하기 어려운 중소기업에서도 효율성 높은 시스템을 구축할 수 있다.

주제어 : 파일 공유 시스템, 문서 보안, 정보 보호, 보안 기술, 스마트 기기

Abstract With the development of information and communication technology, we have been able to access and manage documents containing corporate information anytime and anywhere using smart devices. As the work environment changes to smart work, the scope of information distribution is expanded, and more efforts are needed to manage security. This paper proposes a file sharing system that enables users who have smart devices to manage and share files through mutual cooperation. Proposed file sharing system, the user can add a partner to share files with each other when uploading files kept by spliting the part of the file and the other uses an algorithm to store on the server. After converting the file to be uploaded to base64, it splits it into encrypted files among users, and then transmits it to the server when it wants to share. It is easy to manage and control files using dedicated application to view files and has high security. Using the system developed with proposed algorithm, it is possible to build a system with high efficiency even for SMEs(small and medium-sized enterprises) that can not pay much money for security.

Key Words : File Sharing System, Document Security, Information Security, Security technology, Smart Device

1. 서론

이동통신기술의 발달과 스마트기기 보급화를 통해 우리는 언제 어디서나 필요한 문서 및 사진을 쉽게 획득하고 공유할 수 있는 환경을 맞이하게 되었다. 이를 통해 사무실에서만 업무가 진행되던 업무 공간이 제한되어 있

*This study is supported by the Basic Science Research Program through the Research Foundation of Korea (NRF) funded by the Ministry of Education (No.2017R1D1A1B03030759)
*Corresponding Author : Yang-Hyun Cho (yhcho@syu.ac.kr)
Received October 2, 2018 Revised December 5, 2018
Accepted December 20, 2018 Published December 28, 2018

는 근무 환경에서 벗어나 언제 어디서나 효율적으로 업무를 처리할 수 있는 스마트워크 근무환경으로 변화하고 있다. 클라우드 서비스를 이용하여 정보의 유통 범위가 넓어지고 있는 반면 기업 문서 보안에 대한 문제점들이 많이 노출이 되고 있으며 이를 해결하기 위한 연구가 활발하게 진행되고 있다[1-5].

정부의 중소기업 기술유출 사례 및 실태조사에 따르면 기업에서는 직접적인 피해가 발생하여, 피해 규모 및 유출 건수 등에 응답한 중소기업 52개사의 기술유출 피해금액은 1,022억원이며, 건당 13.1억원의 기술유출 피해가 있는 것으로 조사되고 있다. 유출된 기술 자료로는 생산중인 제품, 연구과제 결과데이터, 최종 연구결과가 가장 많으며, 비기술 자료로는 영업정보, 원가분석정보가 높게 나왔다. 기술유출에 대한 유형으로는 내부직원의 기술유출이 25.0%로 가장 높게 나왔으며 유출수단으로는 휴대용저장장치, 핵심연력매수, 스마트폰카메라, 복사 등이 있다[6-9].

기업에서 정보유출을 막기 위해서 통합계정관리, 문서 DRM, 휴대용저장장치통제, 네트워크 통제 등 다양한 보안 시스템을 구축하고 있지만 구축을 위해 소용되는 비용이 크기 때문에 중소기업에서는 일부만 구축해서 사용하고 있는 것이 현실이다[10-12].

본 논문에서는 사용자의 스마트 기기를 이용하여 이미지 형태의 문서 파일에 접근하는 사용자를 통제하고 파일을 관리할 수 있는 사용자간 협력을 통해 파일을 공유하는 알고리즘을 제안한다. 제안 알고리즘은 이미지 파일 정보를 base64로 인코딩 후 암호화된 정보를 담당자의 스마트 기기와 서버에 나눠서 보관하고 있다가 접근을 원하는 사용자가 있을 경우 확인 후 이미지 파일을 공유해 주는 방식으로 쉽고 간단하게 이미지 파일 접근을 제어할 수 있기 때문에 실효성이 높으며 , 전용 앱을 사용하기 때문에 문서의 복사를 통제할 수 있어 보안성을 높일 수 있다는 장점이 있다. 중소기업에서 적은 비용으로도 보안 시스템구축이 가능하도록 시스템을 구현하기 위해서 파이썬 플라스크 웹 프레임워크와 Cordova 기반 하이브리드 앱 개발방식을 이용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 base64와 Cordova 하이브리드 앱 개발 기술 및 Firebase 클라우드 메시징 서비스에 관하여 알아본다. 3장에서는 이미지 파일 공유를 위한 시스템 알고리즘을 알아보며 4장에서는 이미지 공유 시스템 구현에 대해서 알아본다. 5장에서는 효용성에 대해서 평가를 진행하며 마지막으로 6장에서는 결론을 맺는다.

2. 관련 연구

2.1 Cordova

Cordova는 오픈 소스 모바일 개발 프레임워크이다. Android에서는 JAVA와, Kotlin을 이용하여 개발하고, iOS에서는 Objective-C와 Swift를 이용하여 개발하는 네이티브 개발방식을 벗어나서 크로스 개발 플랫폼을 이용하여 HTML5, CSS3, 자바 스크립트 등 표준 웹 개발 기술을 활용하여 애플리케이션을 개발하는 방식을 말한다. 레이아웃 렌더링은 플랫폼의 웹뷰를 통해 표현하며 디바이스 제어를 위해 필요한 기능은 네이티브 언어로 개발된 네이티브 API를 이용하여 제어한다. Cordova에서 제공하는 자바스크립트 API는 Table 1과 같다[13].

Table 1. Javascript API by Cordova

API	Description
Accelerometer	Read measurement value of 3-axis acceleration sensor (motion sensor) of device
Camera	Capture photos using device camera
Capture	Capture media files using the device's media capture function
Cmpass	Read direction information of device
Connection	Check device network status and read network information
Contact	Can work with device's contact list database
Device	Device-specific information such as device name, platform, version, etc
Events	JavaScript can detect events that occur on the device
File	Javascript can use the device's file system
Geolocation	Read device's current location information
Media	Ability to play and record audio files on the device
Notification	Device notification function is available
Storage	The device's database is available

Cordova에서 지원하는 플랫폼은 Android, iOS, BlackBerry, 윈도우폰, Tyzen 등이 있으며 플랫폼에 따라서 플러그인을 이용하여 가속도계, 카메라, 나침반, 연락처, 파일, 위치정보, 미디어, 네트워크, 소리, 진동 등의 디바이스 제어 하는 기능을 제공한다.

2.2 Base64

Base64는 실행파일, ZIP 파일과 같은 8비트 바이너리 데이터를 문자코드에 영향을 받지 않는 공토 ASCII 코드로만으로 표현 가능한 문자열로 인코딩하는 방식을 나타낸다. Base64 인코딩 방식은 이메일을 통해 바이너리 데이터를 전송할 때 많이 사용된다. 또한 이미지나 스타일시트 등 외부 데이터를 URI(Uniform Resource Identifier)로 표현하는 방식인 Data URI scheme에서 활용된다. Base64로 인코딩하면 파일의 크기보다 더 커지는 단점이 존재하지만 HTML에서 이미지를 표현할 때 Base64를 이용하면 서버에서 인코딩 정보를 파일로 저장하는 과정 없이 img 요소의 src 속성 값으로 바로 인코딩 정보를 사용할 수 있는 장점이 있다[14].

본 논문에서는 파일을 Base64로 인코딩하여 파일을 공유할 사람에 맞게 나눈 후 암호화하여 나눠가지는 방식을 취한다. 이렇게 하면 파일 조각을 가진 사용자 스마트폰을 모두 해킹하지 하지 않는 한 파일 정보 복구가 불가능하며 파일 조각을 전부 가져와도 암호화된 파일 조각을 복호화해야 하기 때문에 해킹에 강건한 특징을 가진다.

2.3 Firebase 클라우드 메시징

일반적으로 FCM이라고 불리는 Firebase 클라우드 메시징 서비스는 Firebase 서비스의 일부분으로서 스마트폰으로 실시간 푸시 메시지를 전송할 수 있는 기능을 제공한다. FCM SDK에서 자동으로 처리하는 알림 메시지와 클라이언트 애플리케이션에 처리하는 데이터 메시지 전송 기능을 제공한다. 자바스크립트, C++, JAVA, Objectiv-C, Swift, Python 등 다양한 언어를 지원하기 때문에 적용되는 플랫폼에 제한이 없으며 서버가 없어도 콘솔 웹에서 직접 테스트할 수 있는 기능을 제공하고 있다.

Firebase는 구글에서 제공하는 메시지 전송 서비스로서 애플에서 판매되는 기기인 아이폰, 아이패드 등으로 메시지를 전송하기 위해서 애플에서 제공하는 푸시 알림 서비스인 APNS(Apple Push Notification Service)와의 연동이 필요하다. 연동을 위해서는 개발자 계정 키를 이용한 인증 키, 앱 ID, 프로비저닝 프로파일 정보가 필요하다[15].

3. 제안 시스템 알고리즘

3.1 제안 서비스 모델

제안 시스템의 서비스 모델은 Fig. 1와 같다. 사용자는 스마트폰에 설치된 애플리케이션을 이용하여 파일 공유 서비스를 제공받는다. Restful 웹 서비스를 제공하는 API 서버와 데이터베이스 서버를 이용하며 실시간 메시지 전송을 위해 구글의 Firebase 클라우드 메시징 서비스를 이용한다.

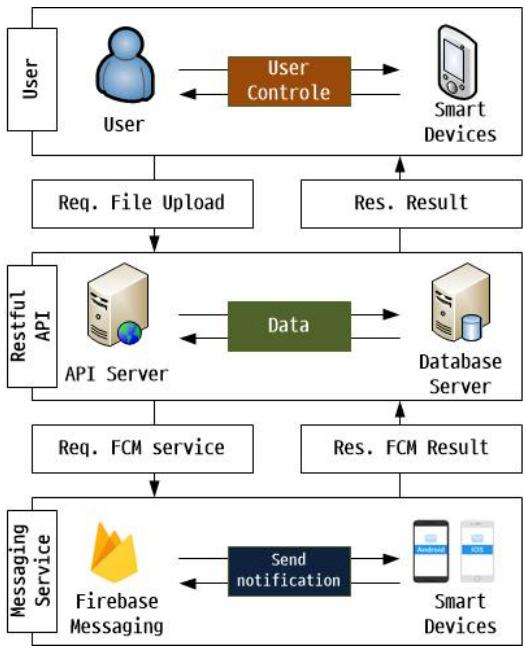

Fig. 1. Proposed service model

3.2 파일 업로드

Fig. 2는 파일 공유를 위한 업로드 절차를 나타낸다. 파일을 공유하고 싶은 사용자 목록을 함께 서버로 전송하며 서버에서는 파일을 조각내어 각 사용자에게 조각낸 파일을 공유한다. 공유 방식은 푸시 메시지를 먼저 전송 후 푸시 메시지를 받으면 애플리케이션에서 조각난 파일을 자동으로 다운로드 받도록 처리한다. 파일 공유를 위한 세부 동작은 다음과 같다.

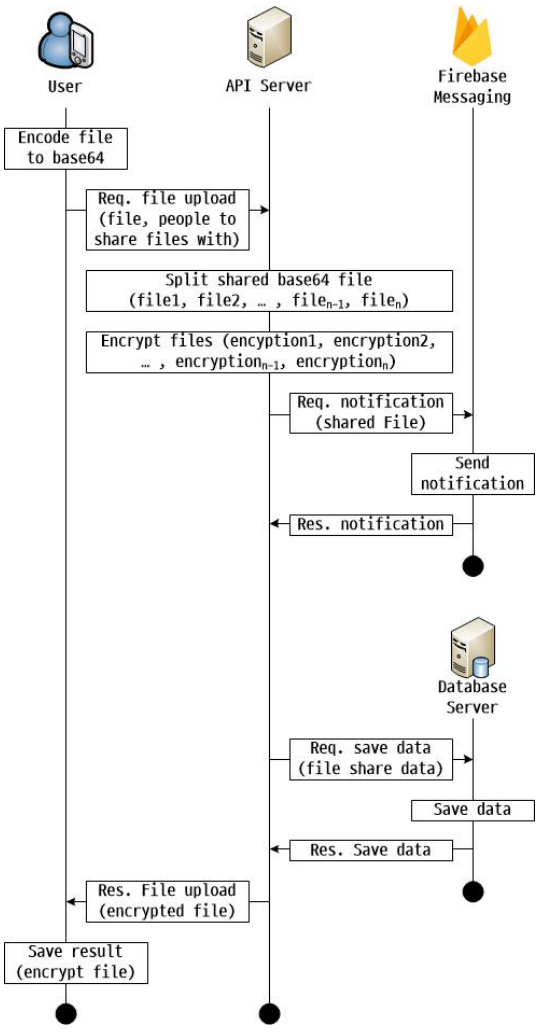

Fig. 2. User registration flow

① 사용자는 스마트폰 애플리케이션을 이용하여 공유하고 싶은 파일을 선택하고 base64 형태로 인코딩 한다.

② 파일 조각을 공유할 사용자 정보와 인코딩된 파일을 서버로 전송한다.

③ 파일을 받은 서버에서는 파일 조각을 공유할 사용자에 비례하도록 파일을 분할한 후 각각 분할된 정보를 암호화한다. 암호화 방식은 AES, RSA 방식 등을 적용할 수 있다. 파일 조각의 일부분이 없으면 복구가 어렵기 때문에 분할하여 스마트폰으로 전송하는 비율은 모바일 환경에 맞게 최소한의 비율만을 유지할 수 있도록 전체 파일 크기의 10% 씩만 사용자에게 전송하며 나머지는 전부 서버에서 보관하는 구조를 가진다.

④ 파일 조각을 공유하려는 사용자에게 푸시 메시지를 전송하기 위해서 FirebaseMessaging 서비스를 이용한다. FirebaseMessaging 서비스를 이용하면 동일한 메시지를 실시간으로 Android, iOS 스마트폰으로 전송할 수 있으며 메시지를 받은 스마트폰에서 사용자의 확인 없이도 백그라운드로 파일 조각을 API 서버로부터 다운로드 받아서 저장할 수 있는 장점이 있다. 또한 여러 사람이 파일 조각을 나누어 가짐으로서 관련된 모든 사람의 폰을 해킹하여 파일을 모아야 하며 API 서버에서 사용한 암호화 방식을 알지 못하면 복구가 어렵기 때문에 제안한 알고리즘은 보안성에 강건한 특징을 가진다.

⑤ 푸시 메시지를 전송한 것을 확인한 API 서버에서는 파일 소유자 및 공유자의 정보와 남겨진 파일 조각을 데이터베이스 서버에 저장한다.

⑥ 데이터베이스 서버에 정보가 저장된 후 API 서버에서 파일을 업로드한 사용자에게 파일의 일부분과 저장된 데이터의 Primary Key 정보를 JSON 구조로 응답한다.

⑦ 응답을 받은 스마트폰 애플리케이션에서 모바일 환경에 적합한 데이터베이스 구조인 SQLite를 이용하여 파일 정보를 저장한다. SQLite를 이용하면 백업과 복구가 용이하기 때문에 사용자가 스마트폰을 바꾸더라도 파일 열람에 문제가 발생하지 않는다.

3.3 파일 열람

Fig. 3은 분할된 파일을 열람하기를 원하는 사용자가 파일 조각을 가지고 있는 사용자로부터 파일 공유 요청을 진행한 후 파일을 열람하는 절차를 나타낸다. 파일 열람을 위해서 파일 조각을 직접 받는 것이 아니라 서버에서 수집하여 하나의 파일로 합쳐서 복구 후 전용 애플리케이션을 통해 보여주기 때문에 사용자가 파일 정보를 훔쳐낼 수 있는 방법이 없으며, 파일을 보고 있는 동안 전용 애플리케이션에서 소켓 통신을 통해 실시간으로 서버와 통신을 진행하기 때문에 네트워크를 차단하게 되면 애플리케이션에서 파일 열람을 차단하게 된다. 또한 화면 캡처와 같은 비정상적인 방법을 실시간으로 감시하는 기능을 포함한다. 사용하게 될 경우 파일 열람을 위한 세부 동작은 다음과 같다.

① 사용자가 열람하고 싶은 파일 아이디와 본인이 소유한 파일 조각을 서버로 전송한다. 파일 업로드 과정에서 이미 파일 조각을 나눠서 보관할 사용자 목록을 데이

터베이스에 저장하고 있기 때문에 파일 아이디와 파일 조각을 전송하면 된다.

② 서버에서 파일 공유 요청을 보내고 요청을 받은 사용자가 확인을 누르면 자신이 소유한 파일 조각을 서버로 전송한다.

③ 파일 조각을 공유한 사람들에게 ②번 과정을 반복한다.

④ 해킹이나 오류 상황에 확인할 수 있도록 데이터베이스에 공유 결과를 로그로 기록한다.

⑤ API 서버에서 암호화된 파일 조각을 복호화하고 하나로 합친 후 파일 열람을 요청하는 사용자 애플리케이션 화면에 보여준다.

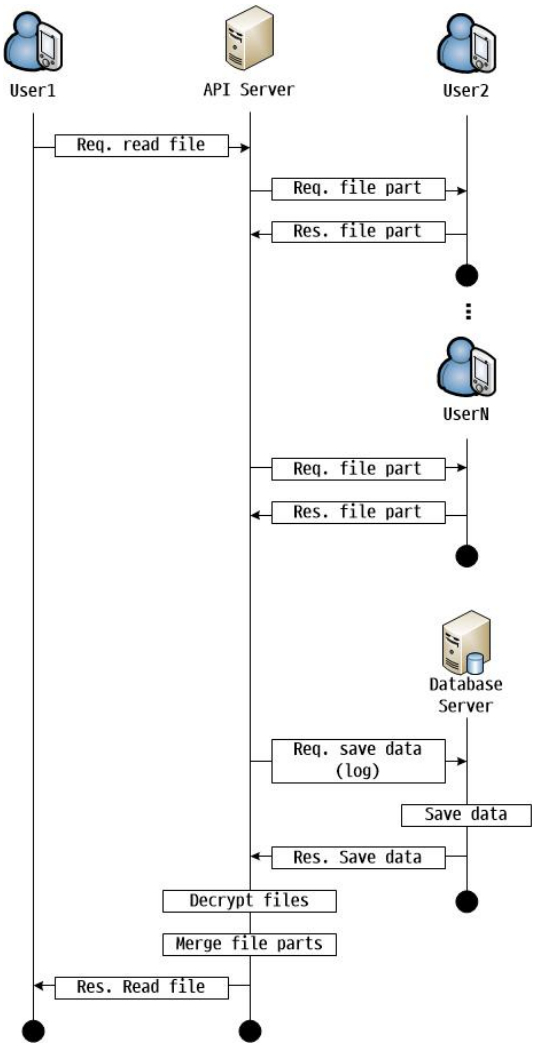

Fig. 3. User login flow

4. 제안 시스템 구현

제안 상호 협력 기반 파일 공유 알고리즘이 적용된 시스템을 구현하기 위해서 파이썬 플라스크 웹 프레임워크를 이용하여 웹 서비스와 API 서비스를 제공하는 서버를 구현하였으며 기능 모듈은 파이썬으로 구성하였다. 사용자 정보, 사용자가 공유하는 파일 정보, 로그를 기록하기 위해서 구성된 데이터베이스 서버는 MariaDB를 이용 하였다. 사용자가 사용하는 애플리케이션은 Cordova를 이용하여 동일한 소스 코드로 Android와 iOS에서 동작하는 하이브리드 애플리케이션을 구현하였다.

Table 2. USERS table scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
first_name	VARCHAR(255)	NOT NULL
last_name	VARCHAR(255)	NOT NULL
email	VARCHAR(255)	NOT NULL
password	LONGTEXT	NOT NULL
created	DATETIME	NOT NULL
updated	DATETIME	NOT NULL

Table 2는 사용자 정보를 저장하는 테이블 구조를 나타낸다. 테이블은 USERS로 하였다. 구성된 필드는 정보 구분자로 사용되는 id, 이름인 first_name, last_name, 인증에 사용되는 email, password, FCM 서비스 이용에 사용되는 fcm_token 필드로 구분된다. 생성년월일인 created, 수정년월일인 updated로 구분된다.

Table 3. IMAGES table scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
user_id	INTEGER	FOREIGN KEY(USERS.id) NOT NULL
title	VARCHAR(255)	NOT NULL
image	LONGTEXT	NOT NULL
created	DATETIME	NOT NULL

Table 3은 공유에 사용되는 테이블 구조를 나타낸다. 테이블은 IMAGES로 하였다. 구성된 필드는 정보 구분자로 사용되는 id, 외래키로서 사용자 구분자를 나타내는

user_id, 파일 정보를 알려주는 title, 파일 조각 정보를 저장하는 file, 생성년월일인 created로 구분된다.

파일 공유를 위해 사용되는 공유 정보를 저장하기 위해서 사용되는 테이블을 Table 4와 같이 구성하였다. 테이블은 RESULTS로 하였다. 구성된 필드는 정보 구분자로 사용되는 id, 외래키로서 파일을 업로드한 사용자 구분자를 나타내는 from_user_id, 외래키로서 파일을 나눠가진 사용자 구분자를 나타내는 to_user_id, 생성년월일인 created로 구분된다.

Table 4. RESULTS table scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
from_user_id	INTEGER	FOREIGN KEY(USERS.id) NOT NULL
to_user_id	INTEGER	FOREIGN KEY(USERS.id) NOT NULL
created	DATETIME	NOT NULL

Fig. 4는 사용자 등록 진행하는 화면이다. 사용자 등록을 위해서 로그인 가능 여부, 권한(사용자, 관리자), 이름, 로그인에 사용할 이메일, 비밀번호를 입력한다. 사용자 등록은 보안문서에 아무나 접근할 수 없도록 관리자가 직접 등록한다.

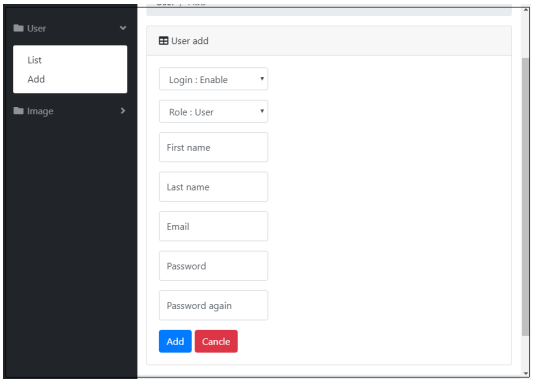

Fig. 4. User registration screen

Fig. 5는 등록된 사용자 목록을 보여주는 화면이다. 사용자 이름, 이메일, 권한, 로그인 가능 여부, 관리 기능(수정, 삭제)을 보여주고 있다.

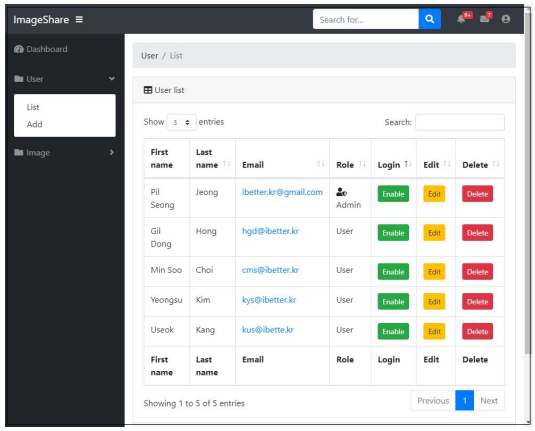

Fig. 5. User list screen

Fig. 6은 애플리케이션을 이용하여 로그인을 진행하는 화면과 로그인 후 보여주는 메인화면이다. 아이디와 비밀번호를 이용하여 로그인을 진행하면 인증 후 애플리케이션 로고와 바로 파일을 업로드 할 수 있도록 안내 화면을 보여준다.

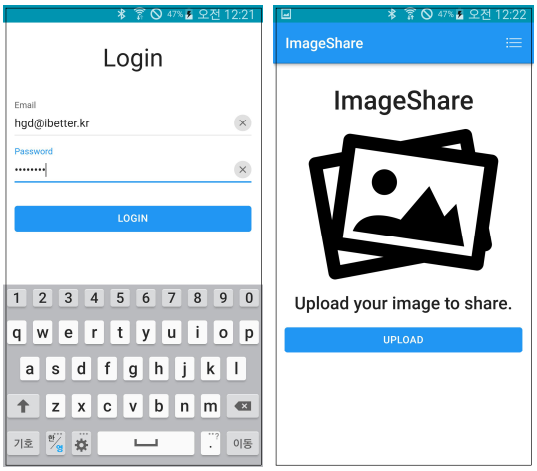

Fig. 6. Login screen and main screen

Fig. 7은 애플리케이션을 이용하여 파일을 업로드하는 화면과 함께 파일을 공유하는 사람에게 푸시 메시지를 전송하는 화면을 보여준다. 파일에 대한 간단한 설명, 함께 파일 조각을 소유할 사용자, 업로드할 파일을 선택 후 업로드를 진행한다. 파일 조각을 소유하는 사용자에게 FCM을 이용하여 메시지를 전송할 수 있도록 이메일 주소를 입력하며, 존재하지 않는 사용자의 이메일 주소를 입력하게 되면 자동으로 걸러주는 알고리즘을 적용하였

다. API 서버에서는 이메일 주소를 이용하여 사용자의 FCM 토큰을 조회하여 실시간 푸시 메시지를 전송한다.

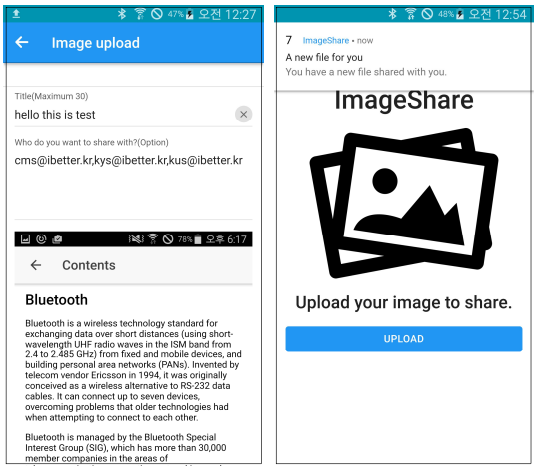

Fig. 7. File upload screen and notification screen

5. 제안 시스템 효용성 평가

본 장에서는 상호 협력을 통해 파일을 공유하는 시스템에 대한 효용성 평가를 진행한다. 효용성 평가의 기준으로 편의성, 보안성, 적용성을 제시하여 논의하였다. Table 5는 제안한 방법과 기존의 방법을 비교한 것이다.

Table 5. Comparison between proposed algorithm and other algorithm

Evaluation	Proposed	Other
Convenience	Using smart devices	Using smart devices
Security	- Access fragmented file but can not use file - high security	- Access hall information file so can use file - low security
Applicability	- Applicable to various systems - Low cost	- Applicable to specific systems - High cost

5.1 편의성

편의성이란 휴대가 용이하고 언제 어디서나 쉽고 간편하게 서비스를 이용할 수 있는 기술인지를 말한다. 본 논문에서 제시한 파일 공유 알고리즘은 스마트폰, 태블릿 PC와 같은 스마트 기기에 설치된 전용 애플리케이션을 이용하여 찍은 사진이나 라이브러리에 보관하고 있는 파일을 쉽고 간단하게 공유할 수 있는 기술로 평가할 수 있다.

5.2 보안성

보안성이란 다양한 방식의 해킹에 대한 대응력을 말한다. 기존의 파일 공유 방식은 서버에 파일을 저장해 놓고 인증을 받은 사용자가 언제 어디서나 파일에 접근할 수 있기 때문에 퇴사한 사람에 대한 지속적인 관리가 어려운 중소, 중견 기업에서는 기업 정보 유출의 문제가 발생할 수 있는 조건이 존재하였다. 본 논문에서 제시한 알고리즘은 파일을 조각으로 나누어 여러 명의 사용자가 공유하기 때문에 문서 유출이 어려우며, 파일의 일부분으로 복구가 어려운 특징을 가진다. 본 논문에서 제시한 알고리즘을 통해 기업에서 발생하는 보안 문서 유출에 대한 원천적인 문제를 막을 수 기술로 평가된다.

5.3 적용성

적용성이란 다양한 환경과 기기에 적용이 가능한 기술인지에 대한 여부를 말한다. 본 논문에서 제시한 기술은 네트워크에 연결된 스마트 기기라면 쉽게 적용이 가능하며 기능 확장을 통해 PC에서도 쉽게 클라이언트-서버 방식의 애플리케이션 구조로 적용이 가능하다. 또한 기업, 금융, 군사 등 다양한 환경에서 적용이 가능한 문서 관리 서비스로 평가할 수 있다.

6. 결론

스마트폰이 널리 보급화 되고 이동통신기술의 발달하면서 업무 공간이 제약되면 근무환경에서 언제 어디서나 스마트폰을 이용하여 문서에 접근하고 열람할 수 있는 스마트워크 근무환경으로 변화하고 있다. 하지만 보안기술의 한계성 및 정보 보호에 대한 준비 부족으로 인하여 기업, 병원, 군대의 문서가 유출되고 있으며 이에 따른 범국가적 차원으로 큰 피해를 보고 있다. 본 논문에서는 스마트폰을 이용하여 쉽게 문서에 접근하고 유출할 수 있는 상황을 대비한 상호 협력 기반 파일 공유 알고리즘을 제안하고 제안한 알고리즘을 적용한 시스템을 구현하였다. 구현된 시스템은 제안 알고리즘이 기존의 솔루션 기반 문서 관리 시스템의 문제점인 보안성, 비용 문제 및 적용성의 한계를 해결할 수 있음을 증명하기 위해서 파이썬 기반 웹 프레임워크와 Cordova 하이브리드 앱 개발 방식을 적용하여 구현하였다. 제안 시스템은 사용자가 항상 휴대하고 있는 스마트폰을 이용하여 파일을 조각으

로 나누어 암호화하여 여러 명의 사용자가 공유하며 파일 열람시에 서버에서 조각을 수집하여 전용 애플리케이션을 통해 열람하도록 하여 사용자가 파일을 유출할 수 있는 환경을 제한하였다. 향후 본 연구를 초석으로 조각으로 나눈 파일을 암호화할 때 모바일 환경에 적합한 암호화 알고리즘을 연구하여 보안성을 향상시킬 수 있는 추가 연구를 진행할 계획이다.

REFERENCES

[1] S. Y. Lee, Y. T. Cho & S. E. Yoo. (2015). An Effect of Smartwork Center Design and Smartwork on Job Satisfaction Work and Life Balance, and Work Productivity. *Journal of Korea Design Knowledge, 34,* 183-191.

[2] C. Kwan. (2018). Issues and Improvements of Secure Coding for Preventing Cyber Crime: Focus on the Private Company Systems. *Journal of Information and Security, 18(2),* 69-76.

[3] J. S. Park & J. C. Ha. (2012). Vulnerability Analysis of Security Document Management in Multi Function Peripheral and Its Countermeasure. *Journal of Korean Institute of Information Technology, 10(6),* 133-143.

[4] J. H. Lee, D. H. Lee & H. K. Kim. (2012). Decision Support System to Detect Unauthorized Access in Smart Work Environment. *Journal of the Korea Institute of Information Security & Cryptology, 22(4),* 797-808.

[5] B. H. Kang. (2018). 5 Topics for Education and Research in Business Ethics. *Journal of Digital Convergence, 16(8),* 137-150.

[6] C. Kwan. (2015). Rethinking of Situational Context and Characteristic of Industrial Secrets Leakage: Some National Security and Psychological Perspectives. *The Korean Journal of Forensic Psychology, 6(1),* 1-11.

[7] B. G. Song. (2014). Differences of Small Enterprise' Industrial Security Management System : Focus on the Trade Secrets. *The Journal of Social Science, 21(3),* 326-358.

[8] S. R. Kang, S. R. Kim, M. S. Park & J. S. Kim. (2018). Study on Windows Event Log-Based Corporate Security Audit and Malware Detection. *Journal of the Korea Institute of Information Security & Cryptology, 28(3),* 591-603.

[9] B. C. Kim. (2015). The SME Informatization Level Analysis and Design for Privacy. *Journal of Digital Convergence, 13(2),* 121-126.

[10] T. S. Jeong, M. S. Yim & J. B. Lee. (2012). A Development of Comprehensive Framework for Continuous Information Security, *Journal of Digital Convergence, 10(2),* 1-10.

[11] S. H. Lee. (2013). A Security Enhancement Method for Web Service, *Journal of Digital Convergence, 11(12),* 361-366.

[12] G. C. Ko, J. S. Jung, S. K. Choi & K. S. Han (2017). A Study on the Affecting Factors in Performance of Internal Leakage Prevention on Industrial Technology, *Journal of Digital Convergence, 15(7),* 159-167.

[13] Apache Cordova. (2018). Apache Cordova Documentation. Apache Cordova Documentation(Online). https://cordova.apache.org/docs/en/latest

[14] Mozilla. (2018). Base64 encoding and decoding. MDN web docs(Online). https://developer.mozilla.org/en-US

[15] Google. (2018). Firebase Documentation. Firebase(Online). https://firebase.google.com/docs

정 필 성(Jeong, Pil-Seong) [정회원]

- 2014년 2월 : 서울과학기술대학교 전자공학과(공학사)
- 2007년 8월 : 광운대학교 전자통신공학과(공학석사)
- 2013년 8월 : 광운대학교 전자통신공학과(공학박사)
- 2018년 3월 ~ 현재 : 명지전문대학 정보통신공학과 조교수
- 관심분야 : 사물인터넷, WSN, 임베디드 시스템
- E-Mail : ibetter.kr@gmail.com

조 양 현(Cho, Yang-Hyun) [정회원]

- 1982년 2월 : 광운대학교 전자통신공학과(공학사)
- 1985년 2월 : 광운대학교 전자통신공학과(공학석사)
- 2012년 2월 : 광운대학교 전자통신공학과(공학박사)
- 1987년 9월 ~ 1997년 8월 : LG정보통신 전송기술개발실 과장
- 1997년 9월 ~ 현재 : 삼육대학교 컴퓨터●메카트로닉스공학부 교수
- 2014년 3월 ~ 2016년 2월 : 삼육대학교 산학협력단장/연구처장
- 관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS, IoT
- E-Mail : yhcho@syu.ac.kr