가짜 앱 탐지 및 공식 앱 정보 공유 프레임워크 개발

김진욱[O], 노유정[*], 정원태[**], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과,
[**]목포대학교 정보보호기술학협동과정
e-mail: {wlsdnr0816[O], dnjsxo4354[**]}@mokpo.ac.kr, shdbwjd08@naver.com[*], carpedm@mnu.ac.kr[*]

A Framework Development for Fake App Detection and Official App Information Sharing

Jinwook Kim[O], Yujeong No[*], Wontae Jung[**], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University,
[**]Interdisciplinary Program of Information & Protection, Mokpo National University

● 요 약 ●

스마트폰은 앱을 통하여 사람들에게 다양하고 유용한 기능을 제공하며, 새로운 앱들이 계속해서 개발되어 출시되고 있다. 그러나 이러한 긍정적인 측면에서 불구하고, 사람들의 편리한 사용에 대한 욕구를 이용하여, 신종 앱 사기와 같은 범죄가 발생하고 있으며, 이를 악용하여 금전적으로 피해를 주거나 개인정보를 탈취하는 범죄로가 증가되는 추세이다. 이와 같은 앱으로 인한 범죄를 대응하기 위하여, 신종 앱 사기 범죄를 분석하고 해결하는 방안이 요구되는 실정이다. 따라서 본 논문에서는 신종 앱 사기 범죄에 악용되는 가짜 앱을 탐지하고, 공식 기관에서 제공하는 정보를 기반으로 가짜 앱과 공식 앱에 대한 대량의 정보를 공유하는 프레임워크를 개발한다. 개발한 프레임워크를 통하여, 정보를 공유한 사람들에게 가짜 앱에 대한 정보를 알려주고, 공식 기관의 앱을 확인하는 안전한 모바일 환경을 제공할 것으로 사료된다.

키워드: 가짜 앱(fake app), 공식 앱(official app), 앱 탐지(app detection), 정보 공유 프레임워크(information sharing framework)

I. 서론

스마트폰이 발전함에 따라, 모바일 애플리케이션은 지속적으로 성장하는 추세이다[1]. 모바일 앱은 휴대성으로 인하여, 고정된 장소가 아닌 이동하는 상황에서 사람들이 원하는 은행 업무, 버스 도착 시간 알림, 게임, 음악 스트리밍과 같은 서비스를 쉽게 이용할 수 있으며, 이러한 앱을 개발하는 것도 개발자가 아닌 일반인이 유튜브나 책을 통하여 혼자서 개발할 수 있는 풍부한 환경을 제공한다. 이에 따라, 개발자나 일반인이 쉽게 앱을 개발하여 앱스토어에 등록할 수 있으며, 사람들이 앱스토어에 등록된 앱을 설치함으로써, 자신이 개발한 앱을 다수의 사람들에게 배포하는 것이 가능하다.

그러나, 이러한 긍정적인 측면에도 불구하고, 누구나 쉽게 앱을 등록할 수 있는 점을 악용함으로써, 악성 앱이나 가짜 앱을 통한 피해사례가 증가하고 있다[1]. 이러한 문제점을 해결하기 위하여, 악성 앱이나 가짜 앱을 탐지하고 차단하는 다양한 방법이 제안되었다. 그럼에도 불구하고, 다양한 탐지 방법 중 패턴 기반 탐지 방법은 탐지 속도가 빠른 장점은 있지만, 신종 및 변종 앱을 탐지하기 위한 대응 시간이 필요한 단점이 있으며[2], 대량의 새로운 앱들과 가짜 앱들에 대한 정보가 부족한 한계점으로 인하여, 신종 앱 사기와 같은 범죄가 발생한다.

이러한 문제점을 해결하기 위하여, 사용자들에게 안전한 모바일 앱 환경을 제공하기 위한 방안이 요구되는 실정이며, 본 논문에서는 신종 앱 사기 범죄에 대응하고, 피해 방지를 최소화하기 위한 방안으로, 가짜 앱을 탐지하고, 공식 기관 및 사람들로부터 제공되는 정보를 기반으로 가짜 앱과 공식 앱에 대한 대량의 정보를 공유하는 프레임워크를 개발한다.

Ⅱ. 프레임워크 설계 및 개발

본 논문에서 제안하는 정보 공유를 활용한 안전한 모바일 앱 환경을 제공하기 위하여, 프레임워크에는 API 통신 기술, 암호화 기술, 텍스트 마이닝 기술을 포함한다. 각 기능을 자세히 살펴보면, API(Application Programming Interface) 서버 통신 기술은 앱과 데이터베이스, 기능들의 상호 통신 방법을 규정하고 지원하는 기술로[3], 앱에서 계정 확인 및 피해사례 게시글 내용, 앱 데이터 정보, 앱 검사와 같은 기능을 요청하는 경우, API 서버에서 각 기능을 제공한다. 암호화 기술은 사용자가 등록한 피해사례들에 포함된 개인정보의 유출을 방지하기 위하여, 개인정보와 관련된 데이터를 암호화하는 기술이다[4]. 텍스트 마이닝 기술은 특정 목적을 위하여 텍스트를 추출하여 분석하고 처리하는 기술로[5], 등록된 게시글의 데이터를 분석하여 가짜 앱에 대한 정보를 추출하여 저장하기 위한 목적으로 활용된다. 이러한 기술들을 제공하는 프레임워크에서의 정보 공유 및 수집을 통한 앱 탐지 과정을 그림 1에 나타내었다.

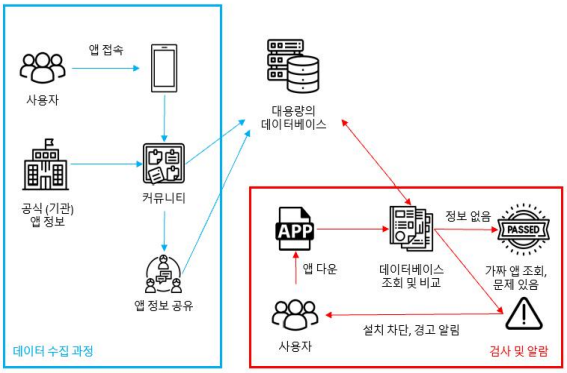

Fig. 1. 제안하는 프레임워크에서의 가짜 앱 탐지 과정

그림을 살펴보면, 사용자는 개발된 프레임워크에 접속하는 앱을 통하여 커뮤니티 공간에서 앱 정보를 공유하며, 커뮤니티에는 공식 기관에서 제공하는 공식 앱에 대한 정보와 가짜 앱에 대한 정보가 공유되고, 커뮤니티에 등록된 게시글은 텍스트 마이닝 기술을 통하여 공식 및 가짜 앱에 대한 정보를 추출하여 데이터베이스에 저장된다.

가짜 앱 탐지과정을 살펴보면, 사용자가 새로운 앱을 설치하는 경우, 백그라운드에서 앱에 대한 정보를 수집하고, 그 정보를 데이터베이스로부터 조회한다. 조회된 정보가 가짜 앱이거나 공식 앱이 아닌 경우에는 설치를 차단하고 사용자에게 알리며, 사용자는 경고를 통하여 가짜 앱을 식별할 수 있다. 만약 데이터베이스로부터 앱 정보가 조회되지 않는 경우에는 가짜 앱이 아닌 것으로 판단하여 정상적으로 설치를 진행한다. 이러한 탐지과정을 통하여, 사용자는 가짜 앱을 식별할 수 있으며, 앱을 설치하지 않음으로써, 안전한 모바일 앱 환경을 조성할 것으로 사료된다.

Ⅲ. 결론

본 논문은 신종 앱 사기 범죄와 같은 위협을 방지하고 피해를 최소화하기 위하여, 가짜 앱과 공식 앱에 대한 대량의 정보를 공유하는 프레임워크를 개발하였다. 가짜 앱을 탐지하기 위하여, 가짜 앱 및 공식 앱에 대한 정보를 데이터베이스에 저장하여, 새로 설치되는 앱의 정보를 기반으로 가짜 앱의 설치를 차단하고 사용자에게 알리는 기능을 제공한다.

공식 앱을 확인할 수 없는 경우를 대비하여, 사용자들로부터의 앱 정보를 공유하는 기능을 제공하며, 커뮤니티 기능, 피해사례 등록 기능, 앱 검색 기능을 통하여, 추가적인 가짜 앱에 대한 정보를 최신으로 유지하는 방안을 제공한다. 이러한 기능들을 통하여, 가짜 앱 및 공식 앱에 대한 정보 부족으로 인하여 발생하는 문제점을 해결할 수 있을 것으로 판단되며, 신종 앱 사기와 같은 범죄부터 안전한 모바일 앱 환경을 제공할 것으로 사료된다.

향후 연구로는, 본 논문에서 개발한 프레임워크의 한계점인 앱 정보 수집 자동화 기술과 앱 정보 최신화, 악성 앱 탐지와 같은 기능을 보완함으로써, 더욱 보안성 및 안전성이 향상된 프레임워크를 개발할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542, NRF-2021R1A4A2001810).

REFERENCES

[1] H. Byeon, "Model for preventing the spreading of spyware by using the smartphone users' app list and damage symptoms," Master's Thesis, Korea University, Jun. 2011.

[2] S. Myeong, "A Study on Android Malware Detection using Selected Features," Master's Thesis, Ajou University, Dec. 2021.

[3] Red Hat, "RESTful API (RESTful API)," https://www.redhat.com/ko/topics/api/what-is-a-rest-api, Retrieved from 26 Jun. 2023.

[4] Telecommunications Technology Association, "encryption," https://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=042591-2, Retrieved from 26 Jun. 2023.

[5] D. Eo, "Comparison of Learning Methods in Text Mining with Big Data," Master's Thesis, Inje University, Dec. 2014.