

1. Conceptualization

[SafeSurfing]

URL 안전 검사 어플리케이션

Student No.	22213487
Name	권기범
E-mail	gkdnld99@yu.ac.kr

[Revision history]

Revision date	Version #	Description	Author
03/20/2025	1.00	First Draft	권기범
05/07/2025	1.01	기능 수정	권기범

= Contents =

1. Business purpose	1
2. System context diagram	3
3. Use case list	4
4. Concept of operation	5
5. Problem statement	7
6. Glossary	8
7. References	8

1. Business purpose

1) Project background

현대의 디지털 환경에서는 다양한 사이버 위협이 존재하며, 사용자가 의도치 않게 악성 웹사이트에 접속하는 경우가 빈번하게 발생한다. 이러한 위협은 개인정보 유출, 금융 사기, 멀웨어 감염 등의 심각한 피해로 이어질 수 있다. 따라서 본 프로젝트에서는 사용자가 웹사이트에 접속하기 전에 해당 URL의 안전성을 검사하고, 이를 통해 보안 사고를 예방하는 모바일 애플리케이션을 개발하는 것을 목표로 한다. 이 보고서에서는 프로젝트의 배경, 목표, 대상 시장 등을 상세히 설명하여 프로젝트의 방향성과 기대 효과를 명확히 하고자 한다.

인터넷 사용이 보편화되면서 사이버 보안 위협도 증가하는 문제는 항상 대두된다. 특히 피싱, 악성 코드 배포, 가짜 웹사이트를 통한 개인 정보 탈취 등의 공격 방식은 더욱 정교해지고 있으며, 이에 따라 사용자의 피해도 심각해지고 있다. 하지만 현재 대부분의 보안 솔루션은 사용자가 웹사이트를 방문한 후 경고를 제공하는 방식으로 작동하여, 피해를 완전히 예방하기에는 한계가 존재한다. 따라서 웹사이트 방문 전에 URL의 안전성을 미리 검사하고 위험 여부를 알려주는 기능이 필요하다고 생각하여 본 프로젝트를 구상하게 되었다. 이러한 문제를 해결하기 위해, 본 프로젝트에서는 웹사이트 URL의 안전성을 사전에 검사하는 모바일 애플리케이션을 개발하고자 한다. 사용자가 접속하려는 링크가 신뢰할 수 있는 것인지 미리 평가하고, 위험성이 높은 웹사이트일 경우 사용자에게 경고를 제공함으로써 사이버 보안 위협을 줄이는 것이 본 프로젝트의 핵심 목표이다.

이 애플리케이션은 Google Safe Browsing, VirusTotal 등의 보안 API를 활용하여 실시간으로 웹사이트의 위험도를 분석한다. 사용자가 애플리케이션을 통해 URL을 직접 입력하거나 클립보드에 복사된 링크를 자동 감지하여 즉각적인 보안 검사를 수행하는 기능을 기본적으로 제공한다. 또한, 신뢰할 수 없는 웹사이트에 대한 경고 메시지를 제공하여 사용자가 보안 위협을 사전에 인지하고 차단할 수 있도록 돕는다. 이러한 방식으로 웹사이트 방문 전 보안성을 점검할 수 있어, 피싱 사이트 접속과 악성 코드 감염 등의 피해를 예방할 수 있다.

2) Goal

본 프로젝트는 사용자가 악성 웹사이트 방문으로 인한 피해를 예방하고, 안전한 인터넷 환경을 제공하는 것을 목표로 합니다. 아래는 구현을 위한 기능 목록이다:

- 실시간 URL 검사 기능: 사용자가 입력한 웹사이트 주소를 분석하고, 악성 여부를 판단하여 결과를 제공
- 자동 감지 및 경고 기능: 클립보드에 복사된 URL을 자동 감지하여 위험 여부를 즉시 알림
- 사용자 친화적인 인터페이스: 직관적인 UI/UX 설계를 통해 누구나 쉽게 보안 검사를 수행할 수 있도록 지원
- 경량화 및 최적화: 보안 검사 기능이 모바일 기기의 성능에 영향을 미치지 않도록 최적화 진행

이 애플리케이션이 성공적으로 구현될 경우, 다음과 같은 기대 효과를 얻을 수 있다:

- 보안 사고 예방: 악성 웹사이트 방문을 사전에 차단하여 피싱 및 멀웨어 감염 위험 감소
- 사용자 보호 강화: 누구나 쉽게 URL을 검사할 수 있어, 보안 지식이 부족한 사용자도 보호 가능
- 신뢰할 수 있는 인터넷 환경 조성: 위험한 웹사이트에 대한 사용자 경각심을 높여 전반적인 사이버 보안 수준 향상

3) Target market

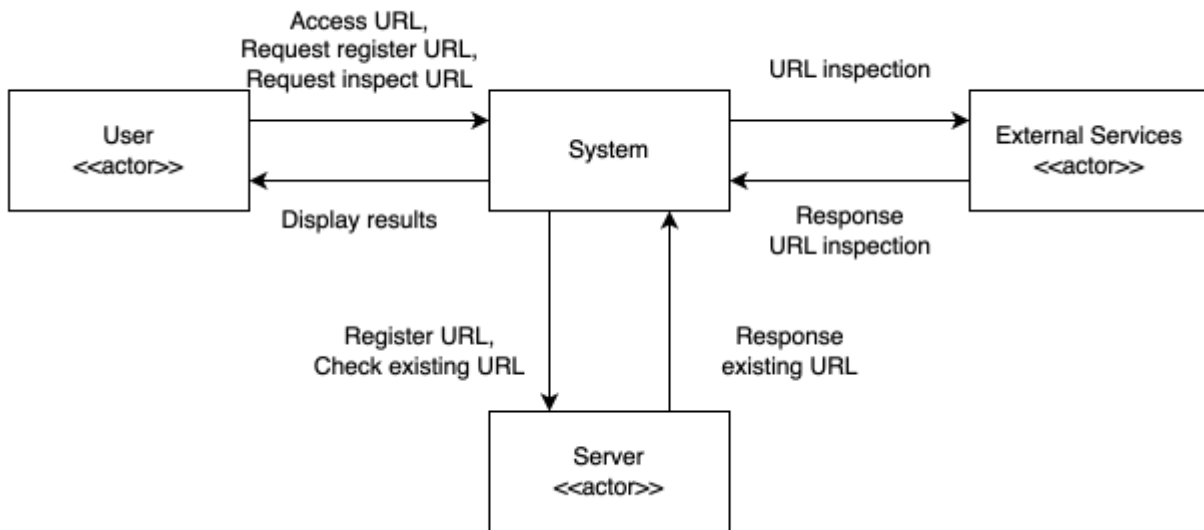
본 애플리케이션은 다양한 사용자층을 대상으로 보안 솔루션을 제공한다:

- 일반 인터넷 사용자: 웹 서핑을 자주 하며 악성 사이트 방문을 피하고 싶은 사용자
- 기업 및 직장인: 업무 중 외부 링크를 확인해야 하는 직장인 및 비즈니스 전문가
- 부모 및 보호자: 자녀가 신뢰할 수 없는 웹사이트에 접속하는 것을 방지하고 싶은 사용자

인터넷과 모바일 기기의 보급이 확대되면서 보안 위협 또한 증가하고 있다. 이에 따라 사용자가 쉽게 활용할 수 있는 모바일 보안 솔루션에 대한 수요도 지속적으로 증가한다. 현재 보안 소프트웨어는 주로 데스크톱 환경에서 제공되거나 브라우저 기반 확장 프로그램으로 개발된 경우가 많아, 모바일 환경에서 간편하게 사용할 수 있는 보안 도구는 상대적으로 부족한 상황이다.

본 애플리케이션은 이러한 시장의 필요성을 충족하기 위해, 모바일 환경에서도 간편하게 URL 보안 검사를 수행할 수 있도록 설계되었다. 특히, 사용자의 접근성이 높은 모바일 애플리케이션 형태로 제공됨으로써, 보안 지식이 부족한 일반 사용자도 손쉽게 보안 점검을 수행할 수 있다.

2. System context diagram



- | | |
|---------------------------|----------------------|
| • Access URL | URL 접근 |
| • Request register URL | 사용자 URL 등록 요청 |
| • Request inspect URL | 사용자 URL 검사 요청 |
| • Register URL | 위험한 URL 및 안전한 URL 등록 |
| • URL inspection | 시스템 URL 검사 요청 |
| • Response URL inspection | 시스템 URL 검사 결과 응답 |
| • Check existing URL | 저장된 URL 확인 요청 |
| • Response existing URL | 저장된 URL 확인 결과 응답 |
| • Display results | 검사 결과 제공 |

3. Use case list

1) Access URL

Actor	User
Description	사용자는 원하는 URL에 접근을 시도한다.

2) Request register URL

Actor	User
Description	사용자는 URL 입력 후 등록 버튼을 누른다.

3) Request inspect URL

Actor	User
Description	사용자가 URL 입력후 검사 버튼을 누른다.

4) Register URL

Actor	System
Description	시스템은 사용자가 입력한 URL을 검사 및 화이트 리스트 또는 블랙 리스트에 등록한다.

5) URL inspection

Actor	System
Description	사용자가 클릭 또는 입력하여 검사 요청한 URL을 외부 API에게 검사 요청한다.

6) Response URL inspection

Actor	External Services
Description	외부 API는 요청된 URL을 검사하여 결과를 시스템에게 전송한다.

7) Check existing URL

Actor	System
Description	시스템은 사용자가 클릭 또는 입력한 URL이 로컬 데이터베이스에 존재하는지 서버에 확인 요청한다.

8) Response existing URL

Actor	Server
Description	서버는 시스템이 요청한 URL이 로컬 데이터베이스에 존재 여부 결과를 반환한다.

9) Display results

Actor	System
Description	시스템은 검사된 URL의 안전성 검사 결과를 화면에 표시하여 사용자에게 제공한다.

4. Concept of operation

1) Access URL

Purpose	원하는 URL에 접근 시도
Approach	사용자는 원하는 URL에 접근하기 위해 클릭한다. 클릭을 하면 시스템에서 URL에 대한 검사가 발생한다.
Dynamics	사용자가 URL에 접근하기 위한 경우.
Goals	사용자가 원하는 URL에 안전하게 접근하도록 한다.

2) Request register URL

Purpose	URL 등록을 위한 버튼
Approach	사용자는 초기화 화면의 텍스트 상자에 URL 입력한 후에 등록 버튼을 누른다.
Dynamics	사용자가 URL을 등록하고 싶은 경우.
Goals	사용자가 입력한 URL 등록하는 기능을 제공한다.

3) Request inspect URL

Purpose	URL 검사를 위한 버튼
Approach	사용자는 초기화 화면의 텍스트 상자에 URL 입력한 후에 검사 버튼을 누른다.
Dynamics	사용자가 URL을 검사하고 싶은 경우.
Goals	사용자가 입력한 URL 검사하는 기능을 제공한다.

4) Register URL

Purpose	URL 등록
Approach	사용자가 입력한 URL 또는 시스템 및 외부 API에서 검사하여 위험하다고 판단된 URL을 데이터베이스에 등록한다.
Dynamics	사용자가 등록하고 싶은 URL 및 위험한 URL이 존재하는 경우.
Goals	입력되거나 위험한 URL을 데이터베이스에 저장하고 관리할 수 있도록 한다.

5) Request URL inspection

Purpose	URL 검사 요청
Approach	시스템은 사용자가 입력하거나 클릭한 URL이 데이터베이스에 존재하지 않아서 안전한지 확인할 수 없을 때, 검사하기 위해 외부 API에 해당 URL을 제출한다.
Dynamics	사용자가 제출한 URL이 데이터베이스에 존재하지 않는 경우.
Goals	URL 안전성 검사에 대한 결과를 반환받기 위해 사용한다.

6) Response URL inspection

Purpose	URL 검사 결과 응답
Approach	외부 API는 검사한 URL의 위험 여부를 판단하여 시스템에게 전달한다.
Dynamics	URL의 검사 여부를 전송하는 경우.
Goals	사용자가 입력한 URL이 안전한지 검사하여 결과를 반환하는 기능을 제공한다.

7) Check existing URL

Purpose	기존 URL 확인 요청
Approach	사용자가 입력하거나 클릭한 URL이 이미 데이터베이스에 존재하는지 서버에게 확인 요청한다. 해당 과정을 통해 검사 시간과 과정을 줄일 수 있다. 존재하지 않는다면 외부 API에게 검사를 요청한다.
Dynamics	사용자가 입력한 URL이 데이터베이스에 존재하는지 확인하는 경우.
Goals	기존에 저장된 URL을 사용하여 사용자에게 신속하게 서비스를 제공한다.

8) Response existing URL

Purpose	기존 URL 응답
Approach	서버는 데이터베이스에 URL이 존재하는지 확인하고 결과를 시스템에게 전송한다.
Dynamics	저장된 URL의 확인 결과를 반환하는 경우.
Goals	저장된 URL의 확인 결과를 시스템에게 반환한다.

9) Display results

Purpose	검사 결과 제공
Approach	시스템은 검사가 완료된 URL의 안전성 검사 결과를 화면에 표시하여 사용자가 위험한 페이지로 접근하지 못하도록 한다.
Dynamics	사용자가 요청한 URL 검사가 종료된 경우.
Goals	사용자가 요청한 URL의 검사 결과를 시각적으로 제공한다.

5. Problem statement

본 프로젝트는 웹 링크의 안전성을 검사하는 모바일 애플리케이션을 개발하는 것을 목표로 하고 있다. 그러나 시스템에는 몇 가지 중요한 한계가 존재한다.

첫째, 로컬 데이터베이스 사용으로 인해 서버를 구축하지 않으며, URL은 로컬에 저장된다. 이는 네트워크가 연결되지 않아도 사용할 수 있는 장점이 있지만, 동시에 검사할 수 있는 URL의 양과 범위에 제한이 따른다. 로컬에서만 데이터를 처리하기 때문에 대규모 데이터 처리나 외부와의 연동이 어려운 점이 한계로 작용한다.

둘째, 인터넷 연결 필요성이 있다. 실시간으로 최신 보안 정보를 반영하기 위해 인터넷 연결이 반드시 요구된다. 따라서 오프라인 환경에서는 URL 검사 기능을 사용할 수 없으며, 이는 사용자에게 불편을 초래할 수 있다.

셋째, URL 안전성 검사 알고리즘은 기존의 데이터베이스와 비교하여 검사하는 방식이다. 이로 인해 최신 악성 링크에 대한 대응이 즉시 이루어지지 않으며, 실시간 보안 위협에 대응하는 데 한계가 있다.

마지막으로, 보안성에서 취약점이 존재할 수 있다. 로컬 저장소에 URL을 저장하는 방식은 외부 서버와의 연동이나 최신 보안 업데이트를 반영하는 데 한계가 있어 보안 측면에서 완벽한 안전성을 보장하지 못한다.

따라서 본 시스템은 특정 범위 내에서 유효하지만, 완전한 보안을 제공하기 위해서는 외부 서버와의 연동, 실시간 업데이트 및 더 강력한 데이터 저장 방식이 필요하다. 현재는 모바일 기기에서만 작동하며, 제한된 환경에서만 링크의 안전성을 검사할 수 있는 한계가 있다.

6. Glossary

Terms	Description
로컬 데이터베이스	사용자의 기기에 존재하는 URL 저장소.
외부 API	로컬 데이터베이스에 존재하지 않는 URL을 검사하기 위한 외부 시스템

7. References