

---

# System Model (Sequence Diagram) Document

Project Name	바이너리프로그램에서 제어구조를 식별하는 도구개발
-----------------	----------------------------

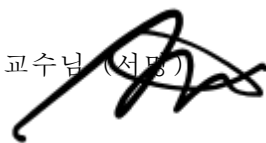
14 조

202002514 안상준

202202602 손예진

202202487 박혜연

지도교수: 조은선 교수님 (서명)



# Document Revision History

---

REV#	DATE	AFFECTED SECTION	AUTHOR
1	2025/04/28	초안 작성	안상준
2	2025/04/29	서명 추가 및 1.2 내용 수정	안상준

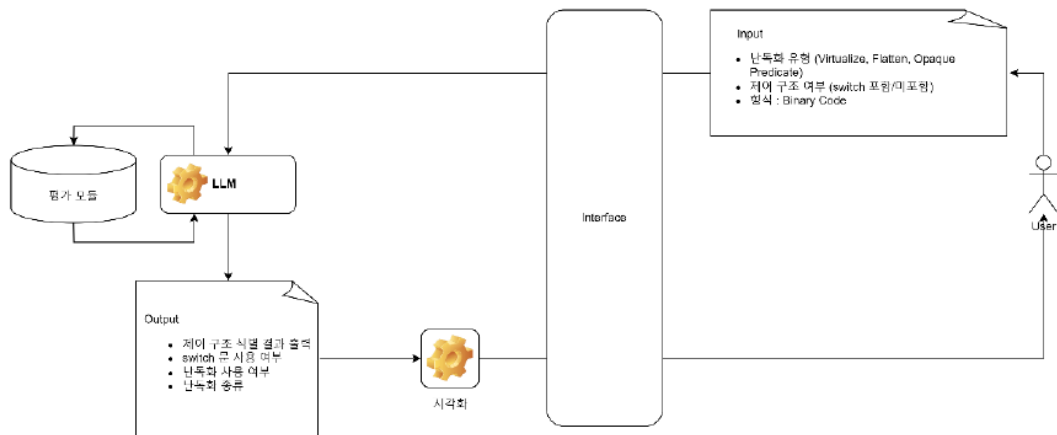
# Table of Contents

---

1.	INTRODUCTION.....	5
1.1.	연구 배경.....	5
1.2.	연구 목적.....	5
1.3.	연구 질문/ 가설.....	5
2.	USE CASE DIAGRAM.....	6
2.1.	소프트웨어 활용 사례.....	6
2.2.	문제 해결에 대한 사용 사례 DIAGRAM.....	7
3.	SEQUENCE DIAGRAM.....	7
3.1.	해결 방법에 대한 알고리즘 순서도.....	7
4.	AI 도구 활용 정보.....	9

# List of Figure

그림 1. 유스케이스 다이어그램 .....7



# 1. Introduction

## 1.1. 연구 배경

악성코드로 인한 사이버 위협이 증가되고 있다. 악성코드는 주로 난독화를 하여 해석하기 어렵게 만드는데 적용되는 난독화는 다양하며 점점 발전하고 있다. 하지만 이를 범용성 있게 분석할 수 있는 역난독화 도구는 존재하지 않는다.

최근 LLM이 다양한 분야에서 사용되고 있으나, 난독화/역난독화 등의 보안 분야에서는 다른 분야에 비해 활용도가 떨어지는 것으로 보인다. 이는 데이터셋의 부족과 LLM의 신뢰성 문제가 주된 원인으로, 해당 문제를 보완해냄으로써 LLM을 사용한 역난독화 도구를 개발해낸다면 가상화 기반의 난독화로 만들어진 악성코드의 분석에 활용할 수 있을 것으로 여겨진다.

## 1.2. 연구 목적

본 연구의 목적은 [LLM을 이용하여 가상화 난독화된 코드에서 제어구조(loop-switch)를 식별하는 연구]을 통해 [가상화 난독화의 역난독화에 필요한 제어구조 탐지 기술 개발]을 수행하는 것이다. 특히, [악성코드 분석 및 역난독화 연구 분야]의 [여러 난독화 기법에 대해 범용적으로 적용 가능한 도구의 부재 문제]를 해결하거나, [가상화 난독화의 역난독화의 가능]의 효과성을 검증함으로써 [LLM 기반 역난독화 가능성 최초 검증, 제어구조 식별 방법론 제시] 기여를 목표로 한다. 이를 통해 [가상화 난독화 기반 악성코드에 대한 분석 효율성 향상 및 역공학 기술 발전에 기여]를 도출하고자 한다.

## 1.3. 연구 질문/ 가설

본 연구는 다음과 같은 연구 질문에 답하고자 한다:

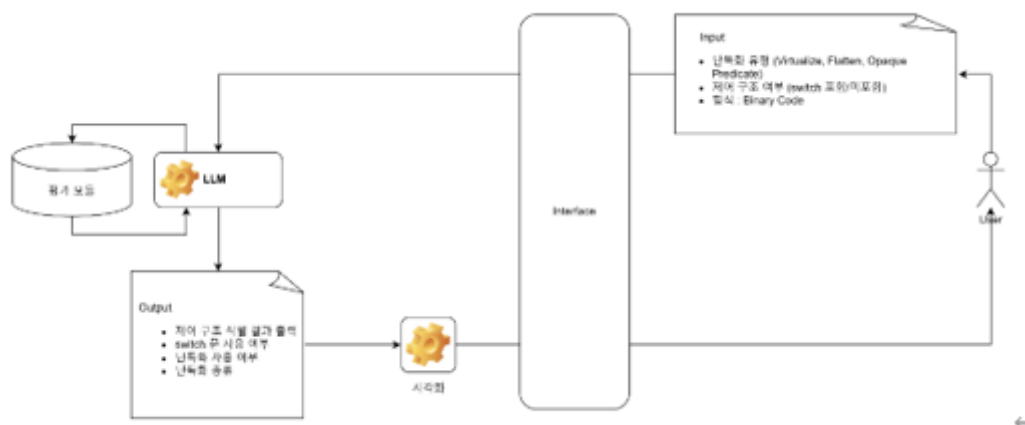
- RQ1.  
[LLM 기반 제어구조 식별 도구]를 활용한 [가상화 난독화 코드 분석]이 기존의 방식에 비해 [제어구조 식별 정확도]에 어떠한 영향을 미치는가?
- RQ2.  
[LLM 기반 제어구조 식별 도구]는 [난독화 난이도나 코드 복잡도]에 따라 [제어구조 식별 성능]에 차이를 보이는가?

본 연구는 다음과 같은 가설을 설정할 수 있다:

- H1.  
[LLM 기반 제어구조 식별 도구]를 활용한 [가상화 난독화 코드 분석]이 기존의 방식보다 [제어구조 식별 정확도]를 유의미하게 향상시킬 것이다.
- H2.  
[LLM 기반 제어구조 식별 도구]는 [다양한 난독화 난이도 및 코드 복잡도 조건]에서도 [안정적인 제어구조 식별]에 성과 향상을 보일 것이다.

## 2. Use Case Diagram

## 2.1. 소프트웨어 활용 사례



## 2.2. 문제 해결에 대한 사용 사례 Diagram

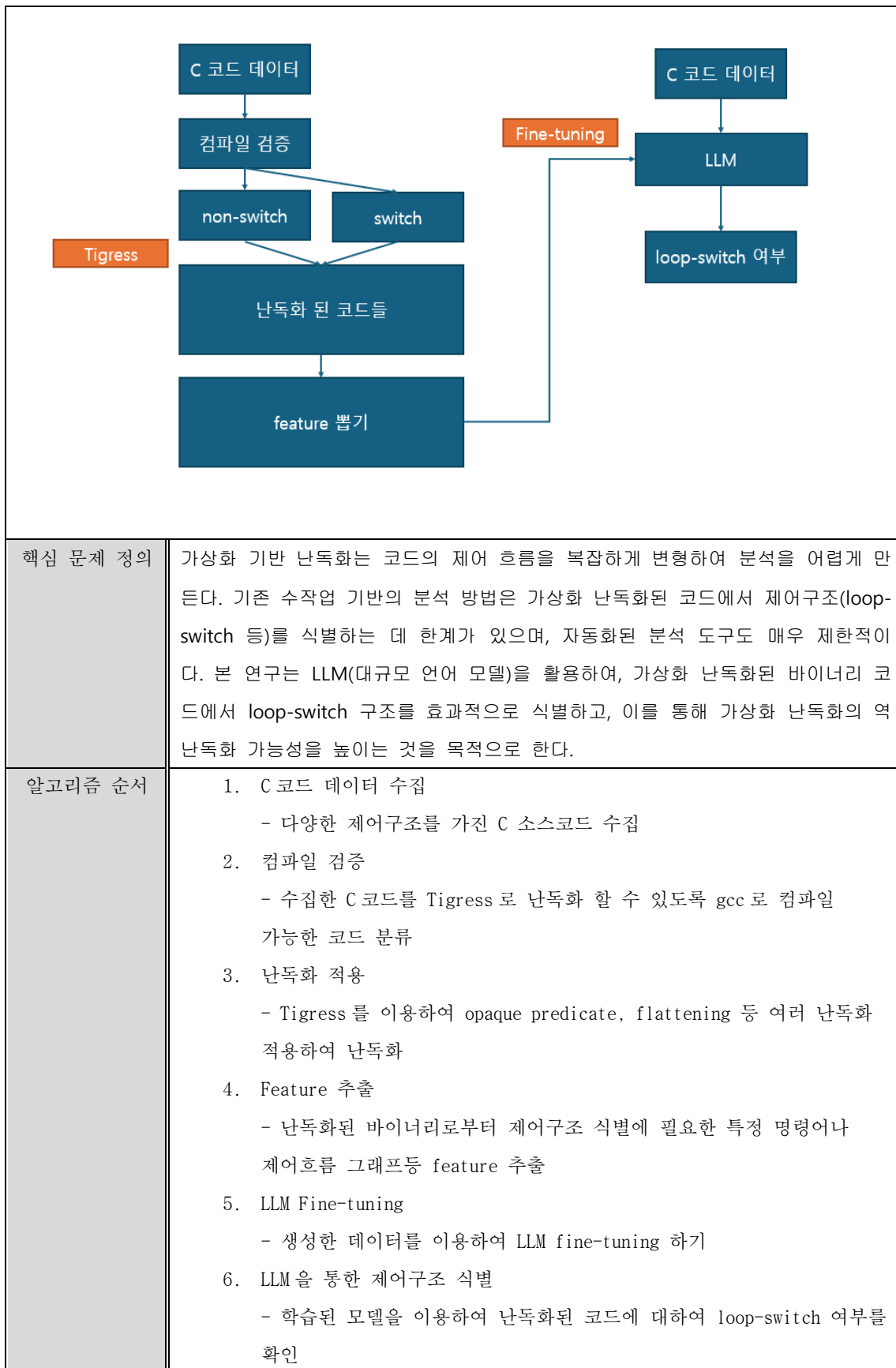


그림 1. 유스케이스 다이어그램

## 3. Sequence Diagram

### 3.1. 해결 방법에 대한 알고리즘 순서도

연구가설 (or 연구질문)	<ul style="list-style-type: none"> <li>• H1. LLM 기반 제어구조 식별 도구를 사용하면 기존 수작업 분석 방식보다 난독화된 코드에서 loop-switch 구조를 더 높은 정확도로 식별할 수 있을 것이다.</li> <li>• H2. LLM 기반 제어구조 식별 도구는 난독화 난이도와 코드 복잡도에 상관없이 일관된 식별 성능을 보일 것이다.</li> </ul>
-------------------	---





	<p>7. 결과 분석 및 해석</p> <ul style="list-style-type: none"> <li>- 난독화 난이도, 코드 복잡도에 따라 성능 차이를 분석</li> <li>- 제어구조 식별 여부와 가상화난독화 연구지원 가능성 논의</li> </ul>
--	--

## 4. AI 도구 활용 정보

사용 도구	gpt-4o	
사용 목적	알고리즘 순서도에서 순서를 작성하기 위하여 사용	
프롬프트	<ul style="list-style-type: none"> <li>● 알고리즘 순서도를 보고 순서를 작성해줘</li> </ul>	
반영 위치	1. Sequence Diagram (p.9~10)	
수작업	있음(알려준 내용 기반으로 수정하여 작성)	
수정		