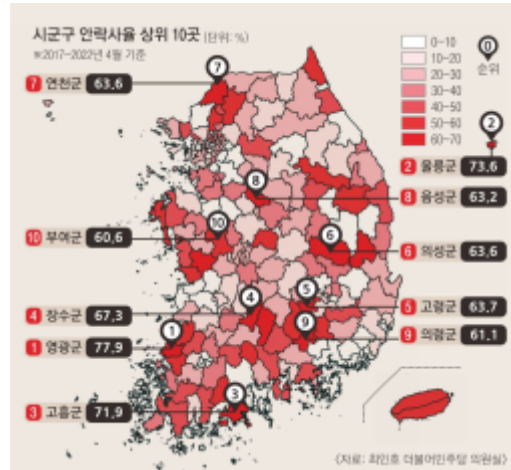


『제11회 소프트웨어 개발보안 경진대회』 소개팅 개발기획서

팀명	차우차우	개발언어	Python3
프로젝트명	Llama3 기반 유기동물-인간 유대형성 및 입양률증가를 위한 SNS		
프로젝트 소개	<p>목표는 유기동물들을 사람들에게 감정적으로 연결시켜 펫샵 대신 보호소에서 입양할 수 있도록 하는 것이다. 이를 위해 입양 대기 유기동물 공공 데이터와 LLMs를 이용해 각 개체의 가상 페르소나를 구축하고, 주기적인 포스팅과 DM을 통해 마치 동물들이 실제 활동하는 것과 같은 SNS를 만들어 사람들의 관심을 유도할 계획이다. SNS, 유기동물 입양연결플랫폼, 후기공유커뮤니티로의 역할을 목표한다.(Keyword: LLMs, SNS, 페르소나)</p>		
팀 소개 및 팀원별 역할	<p>● 팀 소개</p> <p>1) 팀원: 곽병혁 2) 학력: GIST 전기전자컴퓨터공학부 4학년 재학 3) 이력: -24.7.12: GISTxHDF, Micro Design Challenge Hackathon 대상 -22.5.26: 해군본부, 2022 해군창업경진대회 우수상 -22.2.17: 성균관대, 2022 S-TOP(SungKyun Tech.Open Party) 우수상 -20.11-21.11: 중소벤처기업부, 청년창업사관학교 1억원 펀딩 -20.11.21: 울산광역시, 2020울산지역대학 창업우수아이디어 공모전 1위 -20.4-21.4: 창업진흥원, 예비창업패키지 7천만원 펀딩 -19.11.8: UNIST, UNIST Startup Competition 3위 -18.3.24: ATAST, International Festival of Engineering Science and Technology in Tunisia (Silver medal) -2018: 충남교육청 과학교육원, 충청남도발명경진대회 우수상 -17.11.3: KSS, Intel Korea, 대한민국과학기술경진대회 2위 -2017: 충남교육청 과학교육원, 충청남도발명경진대회 우수상 -17.9.4: 미래창조과학부, 제63회 전국과학전람회 환경부장관상</p> <p>4) 기술스택: Django, FastAPI, React.js, Vue.js, AWS(EC2, S3), Docker, K3S, Docker Swarm, Figma</p> <p>1) 팀원: 김재윤 2) 학력: GIST 전기전자컴퓨터공학부 4학년 재학 3) 이력: 2023.04 - 2023.9. Tlab 교통정책연구소, 개발인턴 4) 기술스택: Django, React.js</p> <p>● 팀 역할</p> <p>전원 풀스택 개발을 지향하며, 각자 기능별 구현을 진행합니다.</p> <p>1) 곽병혁: 풀스택개발, AI, CI/CD, Cloud, 디자인 2) 김재윤: 풀스택개발, AI</p>		

1 추진 배경 및 필요성

전국 유기동물 현황은 22년 11만 2587마리, 23년 11만 2179마리로 매년 10만 마리 이상을 유지하고 있다. 유기동물의 증가는 동물보호소의 부담을 증가시키며, 결국 무기한 유기동물을 관리할 수 없는 현실적 문제에 부딪혀 매년 수만 마리의 생명이 안락사를 당하고 있는 실정이다.



[Figure 1] 시군구 안락사율 상위 10곳

사람들은 도심 속의 버려진 유기묘와 유기견들이 발생시키는 소음, 쓰레기, 위생 문제 등으로부터 불편을 겪고, 유기동물들은 10일이라는 짧은 법정 보호기간동안 갇혀있다 소중한 생명을 잃는다. 반려동물에 대한 인식이 커지며 동물들은 이미 가족 구성원으로 자리 잡았고, 이제 공동체의 지속가능성을 위해 유기동물문제는 해결은 필수적이다. 하지만 대부분의 사람들은 길거리를 떠돌던 유기동물보다는 펫샵에서 판매하는 어리고 예쁜 동물들을 선호한다. 이들이 곧 안락사 당할 운명이라는 것이 모두를 설득할 수는 없다. 사람들은 자신과 무관한 죽음에는 무관심하기 때문이다. 어떻게 이들을 설득할 수 있을까? 우리팀은 판다 “푸바오”의 사례로부터 유기동물의 입양률을 높일 수 있는 아이디어를 떠올렸다. 올해 3월, 푸바오가 중국으로 반환된다는 소식에 사람들은 “가지마 푸바오”를 외치며, 눈물을 흘렸다. 대부분 휴대폰 영상 혹은 이미지로나 접했을 자신과 아무 관련 없는 판다에게 이렇게 감정이입 할 수 있다는 사실은 흥미롭다.



[Figure 2] 중국으로 반환되는 푸바오를 배웅하는 행렬 (서울신문 24.4.3)

우리의 목표는 모든 유기동물들을 누군가의 푸바오로 만드는 것이다. 사람들이 원래라면 아무도 모른 채 사라졌을 생명들에 관심을 가지고 슬퍼할 수 있도록, 그리고 펫샵으로 향했을 발걸음이 보호소로 향할 수 있도록 하는 것이 우리의 목표이다.

2 주요 기능 및 개발환경

● 개요:

동물들 각각이 포스팅하는 형태의 SNS를 구성한다. 각각의 동물 개체들에 농림축산검역본부에서 제공하는 국가동물보호정보시스템의 공공데이터를 바탕으로 구성된 고유한 페르소나(성격/특성/행동알고리즘)를 구축/주입하고, 이를 토대로 주기적인 포스팅과 DM이 이루어지는 SNS를 만든다. 사람들은 SNS를 통해 입양 대기 중인 유기동물들과 유대를 쌓고, 프로필 상 입양정보를 통해 더 빠르게 입양을 결심하게 될 것이다. 아래 가상의 예시를 통해 우리의 서비스를 이해할 수 있을 것이다.

가상유저설정: 유기동물엔 그다지 관심이 없지만 귀여운 동물 쇼츠나 릴스를 즐겨보는 23세 여성 김뜻돌씨.

1) 뜻돌씨는 “차우차우”에서 동물들의 사진과 포스팅되는 동물들의 글, 이미지 소비한다. (뜻돌) 인스타에서 사람들이 자신의 애완동물을 자랑하는 것을 구경하는것도 재밌지만, “차우차우”에선 동물들이 정말 자신의 일상을 이야기하는 것 같아 재미있다.

2) 뜻돌씨는 어제 마음에 드는 한 고양이를 팔로우했다. (뜻돌) 계속 보다보니 마음이 가는 고양이가 있어 팔로우했다. 팔로우를 하니 더 자주 보여서 점점 정이 드는 것 같다. 오늘도 “모모”라는 치와와를 새로 팔로우했다.

3) 뜻돌씨는 오늘 “모모”에게 DM을 걸어보았다. (뜻돌) 계속 구경만 하다가 오늘은 “모모”에게 DM을 걸어보았다. 새로운 친구가 생긴 기분이다.

4) 뜻돌씨는 문득 “모모”의 프로필에 있는 보호기간을 떠올렸다. (뜻돌) “모모”의 보호기간이 3일밖에 남지 않았다. 3일 후엔 어떻게 되는걸까? 뜻돌씨는 ‘모모’를 입양하고 싶었지만, 기숙사에 사는 뜻돌씨에겐 여의치않다.

5) 뜻돌씨는 “모모”를 좋아해주는 모모의 다른 팔로워들과 팔로우를 맺고, 모모에 대한 이야기를 나누기 시작했다. 모모의 입양에 대한 이야기가 시작되었고, 결국 자취중인 32세 회사원 김복남씨가 모모를 입양하기로 결심했다.

6) ‘모모’의 계정엔 이제 새로운 글이 올라오지 않지만, 김복남씨(32)는 “차우차우”에 모모의 이야기를 계속해 올리고 있다. 사람들은 “차우차우”에서 계속해 모모를 지켜보고, 원래라면 아무도 모른채 그 생명을 다했을 다른 수많은 “모모”를 지켜보고 있다.

● 기술스택 및 모델(계획):

Backend: Django Restframework

Frontend: React.js

AI: Llama3.cpp, EEVE-Korean-Instruct-10.8B-v1.0, Hugging Face, langchain

CI/CD: Docker Swarm (여유가 된다면 Swarm 대신 k8s로 전환하고, Jenkins와 Argo를 도입하려한다. 획일화되고 안정된 배포프로세스는 실수에서 비롯되는 보안문제를 막는다.)

DB: MySQL, Redis

Cloud: AWS EC2, S3

● 주요기능

주요기능은 두 가지로 요약된다. 1) 입양 대기 중인 동물들의 주기적인 포스팅을 볼 수 있다. 2) 입양 대기 중인 동물들과 실시간 DM을 나눌 수 있다. 이를 위한 구현 과정상의 가장 큰 도전과제는 아래와 같다:

1) LLMs 모델을 서버에 어떻게 통합할 것인가

LLMs를 이용해 많은 동물들의 페르소나를 구축하고, 이를 바탕으로 주기적인 포스팅과 실시간 DM이 이루어지게 하려면 상당한 리소스가 요구된다. 이를 위해 META의 오픈소스 Llama3-8B 모델을 Fine-tuning하고 AI 추론과정에 INT4bit 포맷 양자화를 활용해 FP32bit 포맷으로부터 근사된 모델을 로컬/서버 상에서 구동될 수 있도록 한다.

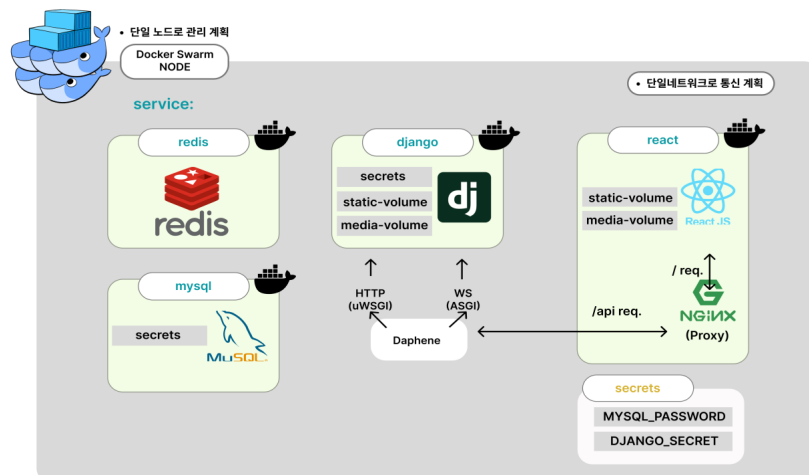
2) LLMs 모델을 서비스에 어떻게 이용할 것인가?

포스팅과 DM기능은 LLMs를 이용해 콘텐츠를 생성한다는 점은 같지만 UX관점에서 다른 접근이 필요하다. 유저의 몰입을 상승시키기 위해 콘텐츠 생성 시 히스토리 관리는 구현 중 가장 중요하게 고려되어야 한다.

DM은 유저와의 빠른 상호작용이 요구되며 이를 위해 redis로 히스토리를 관리할 계획이다. 반면 포스팅의 경우 빠른 응답이 요구되지 않는다. redis 대신 관계형DB를 통해 히스토리를 관리해 개연성을 유지한다.

● 서비스 아키텍처

유저-동물 상호작용외에 유저-유저 상호작용을 위해 웹소켓을 이용한 통신구현이 필요하다. HTTP protocol과 WS protocol을 위해 필요한 uWSGI interface와 ASGI interface를 Daphne에서 모두 처리할 계획이다. Daphne은 ASGI 서버지만, Nginx를 프록시 서버로 활용해 ws, http요청을 처리한 경험이 있다. 같은 방식으로 구현하려 한다. Container orchestration을 위해 docker swarm을 사용할 계획이며, 단일 노드내의 서비스마다 단일 컨테이너를 두어 redis, django, react, db 환경을 분리해 보안과 안정성을 강화할 계획이다. 계획에 대한 간략한 도식을 Figure 3에서 확인할 수 있다.



[Figure 3] 서비스 구조 계획: 이해를 위한 비약, 생략이 있음

● 보안기획

개발 중 신경써야할 보안계획들을 정리하였다. 서버개발시에 우리는 Django를 사용하므로 많은 문제들이 프레임워크에서 이미 사전차단된다. 이외의 쉽게 간과하고 넘어갈 만한 문제점들을 미리 체크리스트로 구성하였다.

- **SQL Injection:** 최대한 Django ORM(queryset)을 사용해 injection을 막고, raw query 사용시에 SQL Injection 처리
- **인증권한관리:** 케이스별 사용자인증과 권한검사를 구체화 및 강화
- **XSS 방지:** django에서 제공하는 escape기능을 이용해 <, >, &, W, “ 같은 문자열 관리
- **CSRF 공격방어:** POST 요청에 대한 CSRF token 발급 및 체크
- **DBD 공격방어:** SNS 기능 내 파일업로드 기능이 필요하므로 DBD 대응이 필요하다. 규정 확장자 외 확장자 차단정책, 실행권한 제거등으로 대응한다. 확장자 검사시 파일명 전체검사 실시 (ex. test.txt.asp 같은 입력시 .txt에서 검사가 종료되면 업로드될 수 있다.)
- **DBD 공격(종단문자유회) 방어:** DBD공격을 인지해도 자주 발생하는 취약점이 종단문자에 대한 비교려이다. %00가 포함된 뒷문자열은 웹서버에서 파일 저장시 null 인식된다. 이를 이용하면 허용하는 확장자와 원하는 확장자사이에 %00을 이용해 업로드공격이 가능하다. 이에 대한 대응이 필요하다.
- **DB 접속 인증:** redis는 기본적으로 인증이 필요 없는 상태로 설정되어 있어, 불특정 다수가 DB에 접속할 수 있다. 인증을 추가한다.
- **DB 데이터 도청 방지:** redis는 기본적으로 평문 통신을 사용하므로, 네트워크 상에서 데이터가 쉽게 도청될 수 있다. 따라서 TLS/SSL을 활성화하여 통신을 암호화한다.
- **DB 명령어 권한 제한:** redis는 LUA 스크립트를 실행할 수 있으며, 이를 통해 악의적인 명령어가 실행될 수 있다. 기본적으로 redis의 기본포트 6379에 대한 접근을 클라우드에서 네트워크ACL과 보안그룹을 통해 제한하겠지만 redis 자체에서도 ACL(Access Control List)을 사용하여 특정 명령어에 대한 접근 및 LUA 스크립트 실행 권한을 특정 사용자에게만 부여한다.
- 서버에서 막아야할 입력을 클라이언트단에서 추가적으로 차단해 제한을 강화한다. 이는 사용자경험 향상으로 이어질 것이다.
- 세션 및 토큰 만료시간을 명확히 한다.

3 활용방안 및 기대효과

유기동물입양서비스는 이전부터 다양하게 시도되어 왔다. 포인핸드(pawinhand.kr)는 유기동물입양플랫폼으로 유기동물들을 소개하거나, 매거진 발매, 입양자를 위한 쇼핑물 등을 운영한다. 비마이펫툴즈(tools.mypetlife.co.kr)은 품종과 지역 필터를 통해 유저가 대기 중인 유기동물을 검색할 수 있게 하고, 커뮤니티와 쇼핑물을 구성해 운영된다. 이외에도 깃허브에서 유기동물과 관련된 많은 서비스들의 개발시도들을 엿볼 수 있다. 하지만 모든 시도들이 유기동물의 검색 및 유저와의 매칭 정도 이외의 서비스를 제공하지 못한다. 우리는 유기동물문제를 해결하기 위해선 근본적으로 사람들의 인식개선이 이루어져야 한다고 판단했고, “가지마 푸바오”라는 실사례의 심리학적 접근을 통해 차별화된 서비스를 제공한다.

가법게는 동물애호가들에게 새로운 오락거리를 제공함과 동시에 동물입양에 대한 경로와 입양자커뮤니티로써 작동할 수 있을 것이고, 더 나아가서는 유기동물에 대한 인식개선, 생명존엄에 대한 의식환기 그리고 실질적인 입양률 증가로 이어질 수 있는 서비스를 기대한다.