Video Classification with Homomorphic Neural Network

AI와 Blockchain을 활용한 CCTV 협력 검증 시스템.. 관련..

https://youtu.be/fR0gcsFaHtU

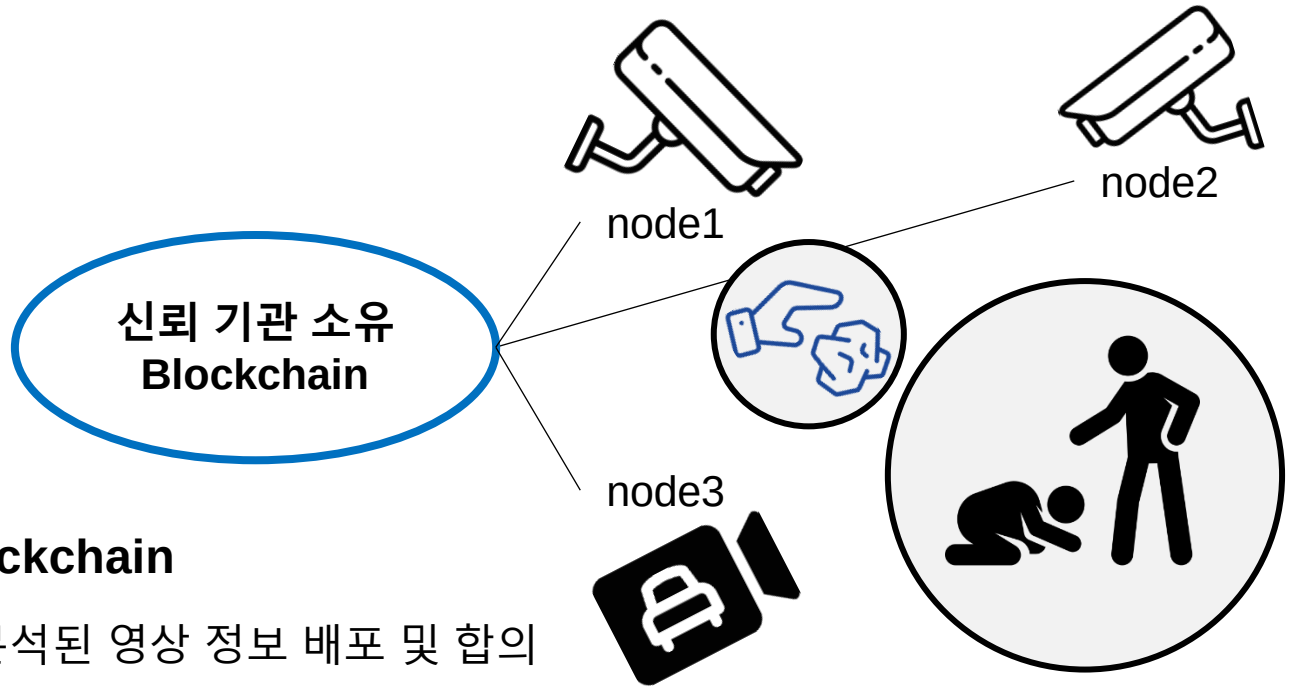
HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

시스템 구성



Blockchain

1. 분석된 영상 정보 배포 및 합의
2. 보상 지급

AI

1. 영상 분석
2. 유저 데이터 보호
3. 블록체인 성능 향상

훈련된 모델 서버
(trained model)

세부 사항

- **Deep Learning**
  1. 공공 CCTV, 차량용 블랙박스들의 **영상 분석**
     → **Object detection or Video Captioning**
     → 영상 분석 결과가 문장일 경우 문장 분석 과정이 필요 → **키워드** 레벨
  2. **개인정보 노출 방지** 필요
     → 행인 얼굴, 영상 제공자의 위치 정보 등 영상 분석 과정에서의 민감 정보 노출 방지
     but, **edge device** 상에서의 추론은 **컴퓨팅 능력 과부하**
  3. 따라서, 서버에서 학습된 모델 소유 및 **변환된 데이터** 추론
     → **masking, encryption 등등..**

폭력

예시 : 모든 노드가 폭력으로 분석

→ 키워드에 대한 비교를 통한 합의

	node 1	node 2	node 3
폭력	O	O	O
투기	X	O	X
교통사고	X	X	X

- **Blockchain**
  1. public blockchain 및 참여자 보상 지급
  2. 합의 과정
     → **해당 지역의 노드들 간의 합의** / 간단한 합의 알고리즘 (분석 키워드 비교)

기대효과

- 영상이 아닌 키워드만을 업로드하여 **블록체인의 성능 향상**
- Public blockchain을 통해 공공 기관의 CCTV 뿐만이 아니라 개인의 참여 가능
  → 다수의 참여자로 인한 **무결성 보장 및 신뢰도 향상**
- 딥러닝 기반의 영상 분석을 통한 **신뢰도 향상 및 자동화**
- 개인정보 보호가 가능한 추론 → **유저 데이터 보호**
- 어떤 사건에 대한 빠른 대처 가능 / 시간, 노동 등의 비용 절감

구현.. 계획

- 구현해야할 부분

  1. 비디오 분류

     → 마스킹 또는 암호화된 데이터에 대한 학습

     → 하나의 클래스로 하는거 되면 하나의 비디오에서 여러 키워드 검출 하는 걸로

  2. 퍼블릭 블록체인 네트워크

Video classification

* Video는 3차원 데이터 (이미지들의 시퀀스)

1. CNN으로 1-frame 단위로 분류
2. Time distributed CNN 후 RNN
3. 3D-CNN
4. CNN + RNN
5. CNN + MLP

CNN : 1-frame 단위 분류

- CNN 사용 (Inception-v3 등 image net)
- Video를 image로 쪼개서 그냥 image를 분류하는 것

Time distributed CNN + RNN

- TimeDistributed CNN

  → many output에 사용

  → 2차원 이미지에 추가 차원 (시간) 사용

- RNN (GRU or LSTM)

3차원 벡터 3개 → (batch,**3**,3)

*TimeDistributed(Dense(~))
*TimeDistributed(Conv2D(~))

3D-CNN

- 2D 이미지에 시간 차원 고려하여 3D CNN 사용
- 컨볼루션, 필터, 스트라이드, 패딩 등 똑같은 개념인데 3D CNN 레이어 사용, 커널도 3차원
  → 3차원 데이터에 대한 컨볼루션

CNN (Encoder) + RNN

- 제안 시스템에 사용할 방법

  → CNN을 encoder 개념으로 사용

- CNN output을 RNN의 input으로 설정

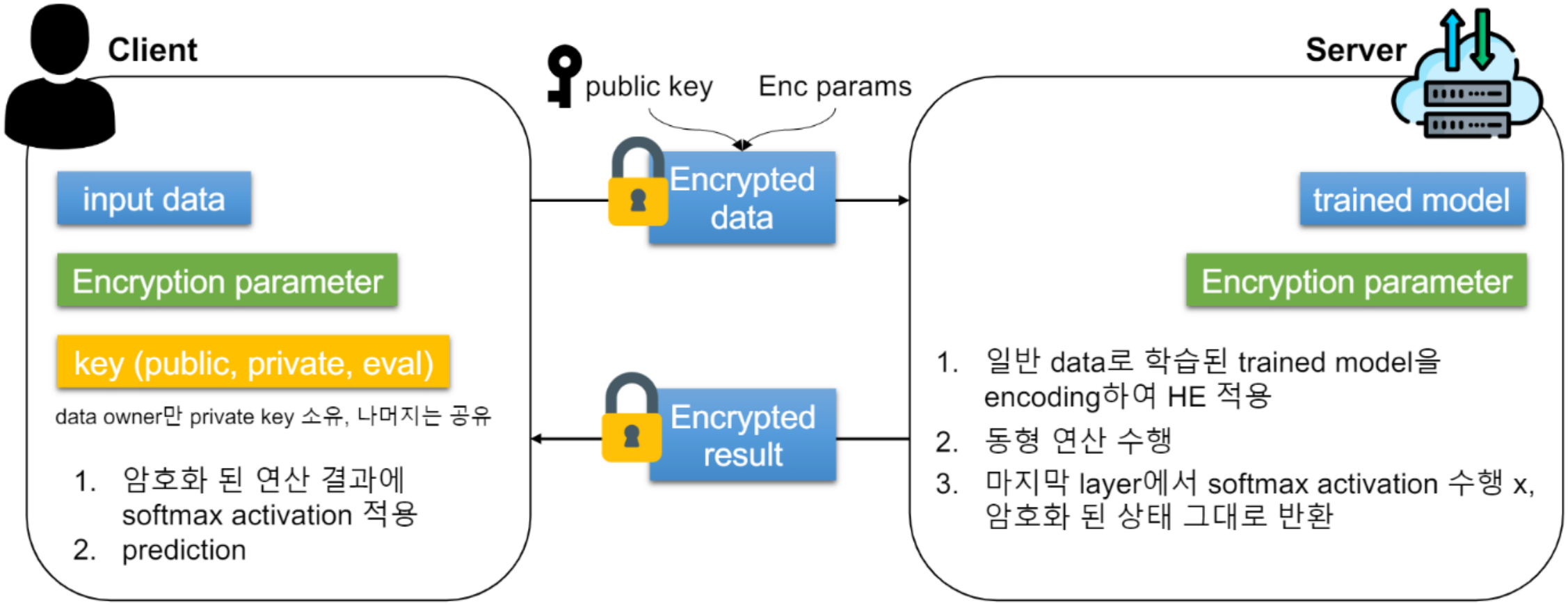
  → 2D 이미지를 학습한 후, sequence로

  → CNN output은 분류 결과가 아닌 임베딩 벡터 (latent vector)

  : 분류 모델 아니라 인코더 개념으로 사용

https://colab.research.google.com/drive/19pL3dcmxTrsD-10YJblDq01WimleY9w9#scrollTo=LR0F-diBAb47

Homomorphic Neural Network



사용된 data와 결과는 key 소유자만이 확인 가능

Homomorphic Neural Network

- homomorphic neural network를 CNN에 적용
- 학습은 일반 모델로 하고, 추론은 encrypted 모델 사용

```
ds = Dataset(verbosity = verbosity)
(train, train_labels), (test, test_labels) = ds.load(2)

exp = Exporter(verbosity = verbosity)
# exp.exportBestOf(train, train_labels, test, test_labels, params, model_name="model15", num_test=10)

model = exp.load(model_name='model15')

test = test[:coeff_mod]
test_labels = test_labels[:coeff_mod]

cn = Cryptonet(test, test_labels, model, p_moduli, coeff_mod, precision, True)
cn.evaluate()
```

load data

load model

Evaluation

1. 데이터셋
2. 모델
3. 동형암호 관련 파라미터
4. 키
5. 연산

https://github.com/MarzioMonticelli/python-cryptonet/blob/master/

동형암호 딥러닝 세미나 피피티.. :
https://github.com/solowal/CLASS/blob/master/2021/%EC%97%B0%EA%B5%AC%EC%8B%A4/%EA%B9%80%ED%98%84%EC%A7%80_DL%20with%20Homomorphic%20Encryption.pdf

진행 계획

Video Classification	Homomorphic Neural Network
데이터 구하기 (CCTV 관련..?)	RNN 구현 해보고 안되면 .. CNN을 frame 단위로 해서 앙상블이나 퓨전, 아니면 샘플링 단위를 n초에 한번으로 해서 2D-CNN 등으로..
하나의 클래스로 하는거 되면 하나의 비디오에서 여러 키워드 검출하는 것 .. 도전..	Video classification이랑 합치기

Q & A