캡스톤 디자인 2분반

도비: 악성 도메인 탐지 서비스

목차 table of contents

도비 프로젝트

프로젝트 소개

도비

도비 프로젝트는 **딥러닝** 기술을 활용하여,
악성 도메인을 **실시간**으로 **탐지**하고 사용자 보호를 강화하는 보안 솔루션입니다.

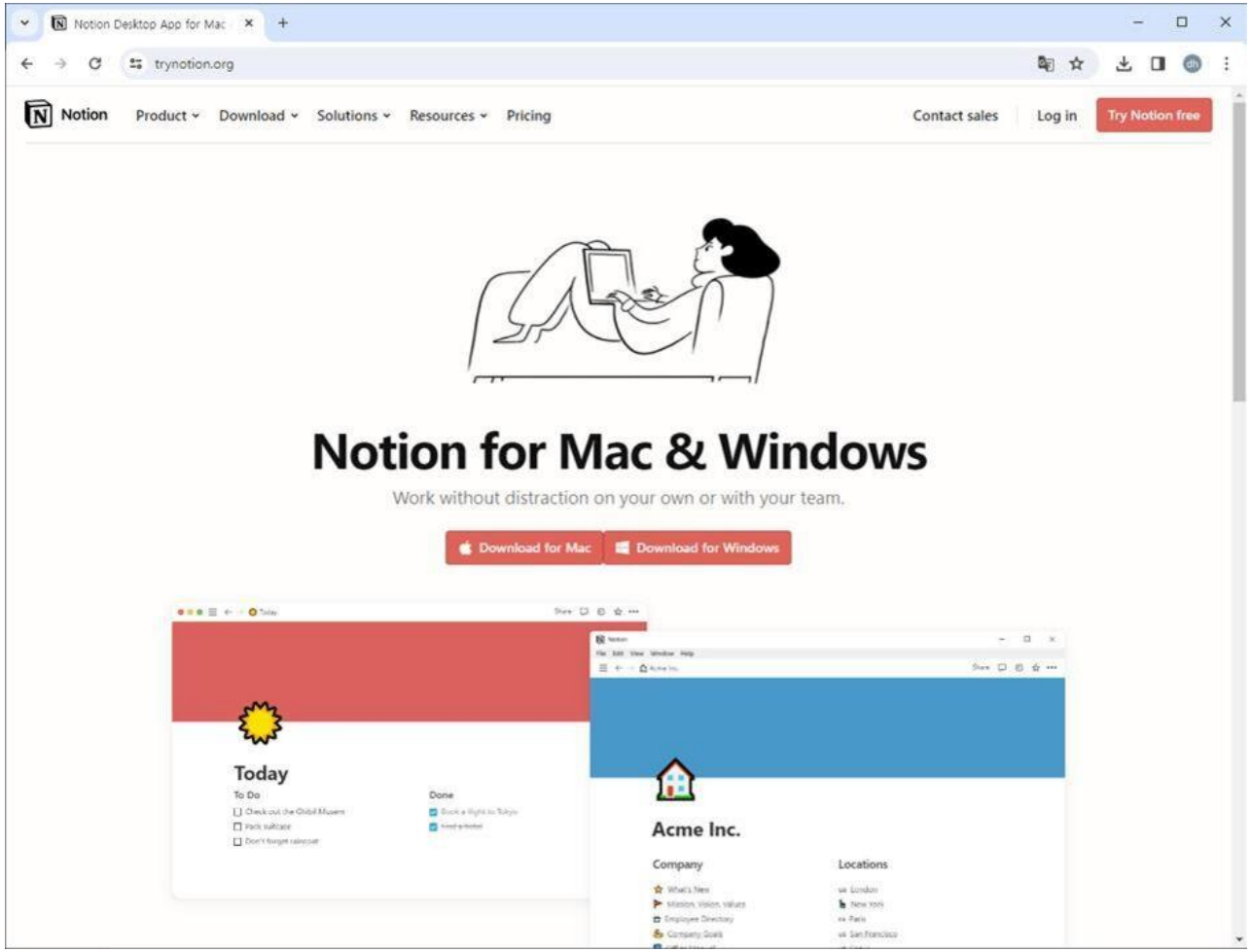
악성 도메인

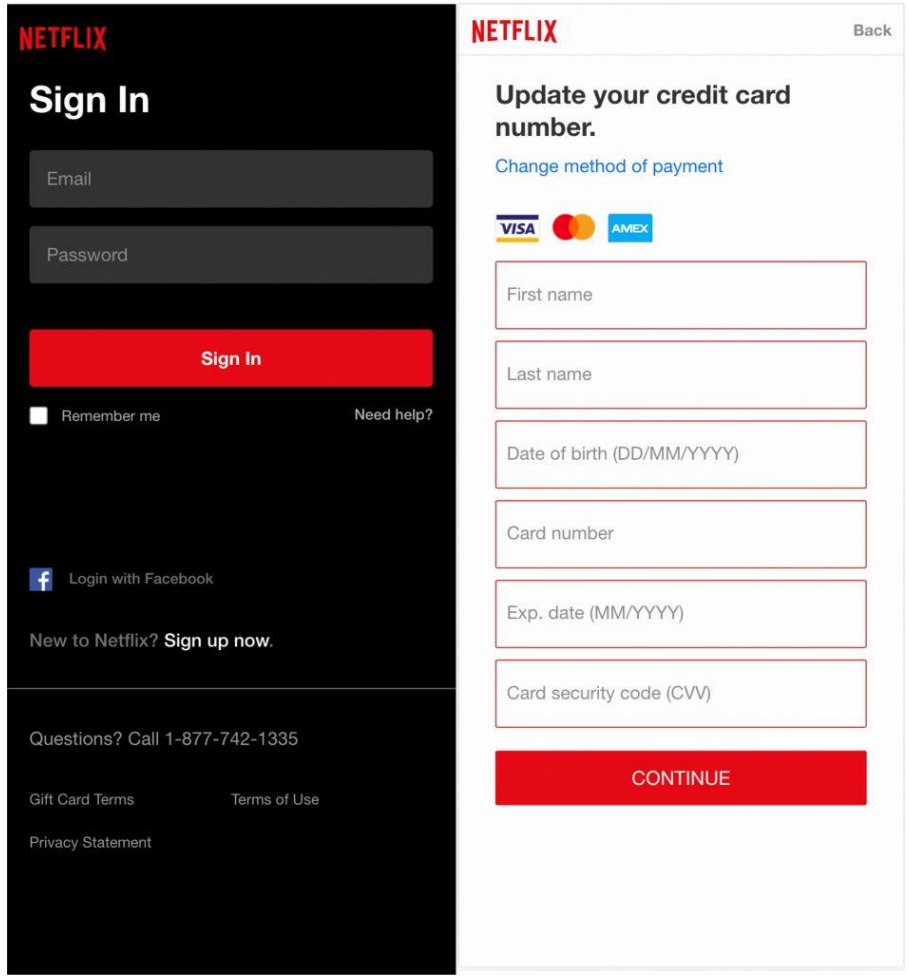
인터넷상에서 사용자를 속이거나 악의적인 목적을 수행하는 도메인으로,
주로 피싱, 악성 코드 배포, 개인정보 탈취 등의 활동에 이용된다.

ex)
1. 유명 사이트를 사칭한 악성 도메인 피해 사례
2. 정부 기관 및 공공 기관을 사칭한 악성 도메인 피해 사례
3. 생성형 AI를 통한 이메일에 악성 도메인 공격이 포함된 사례

악성 도메인

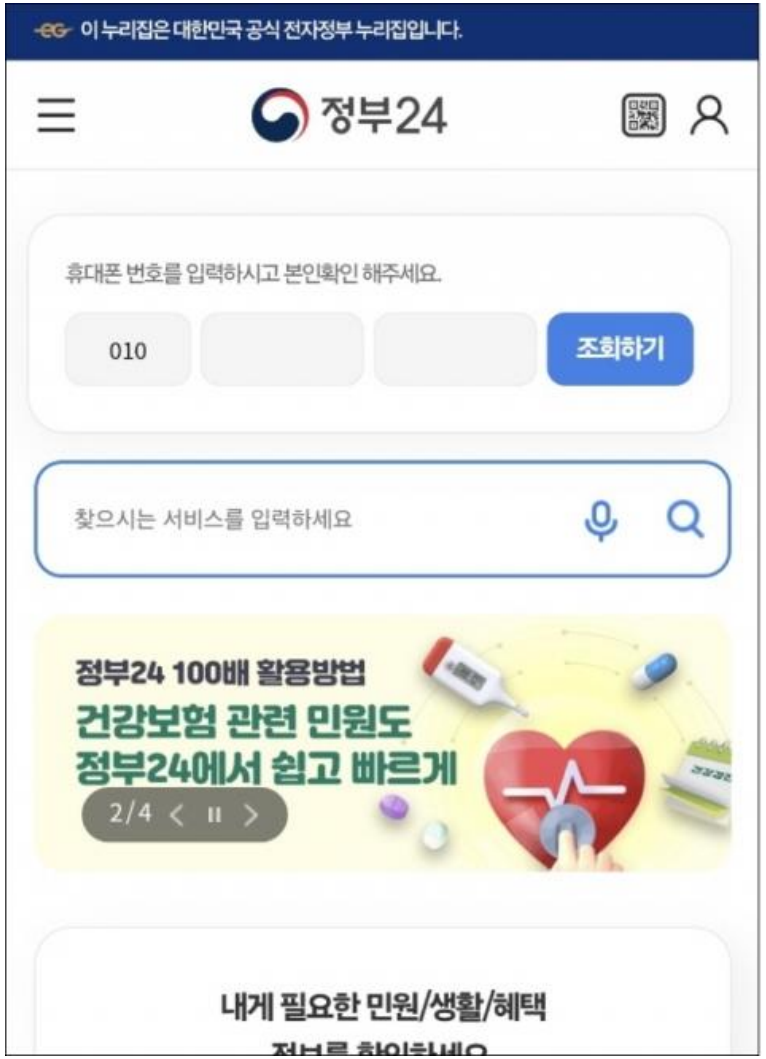
유명 사이트를 사칭한 악성 도메인 피해 사례

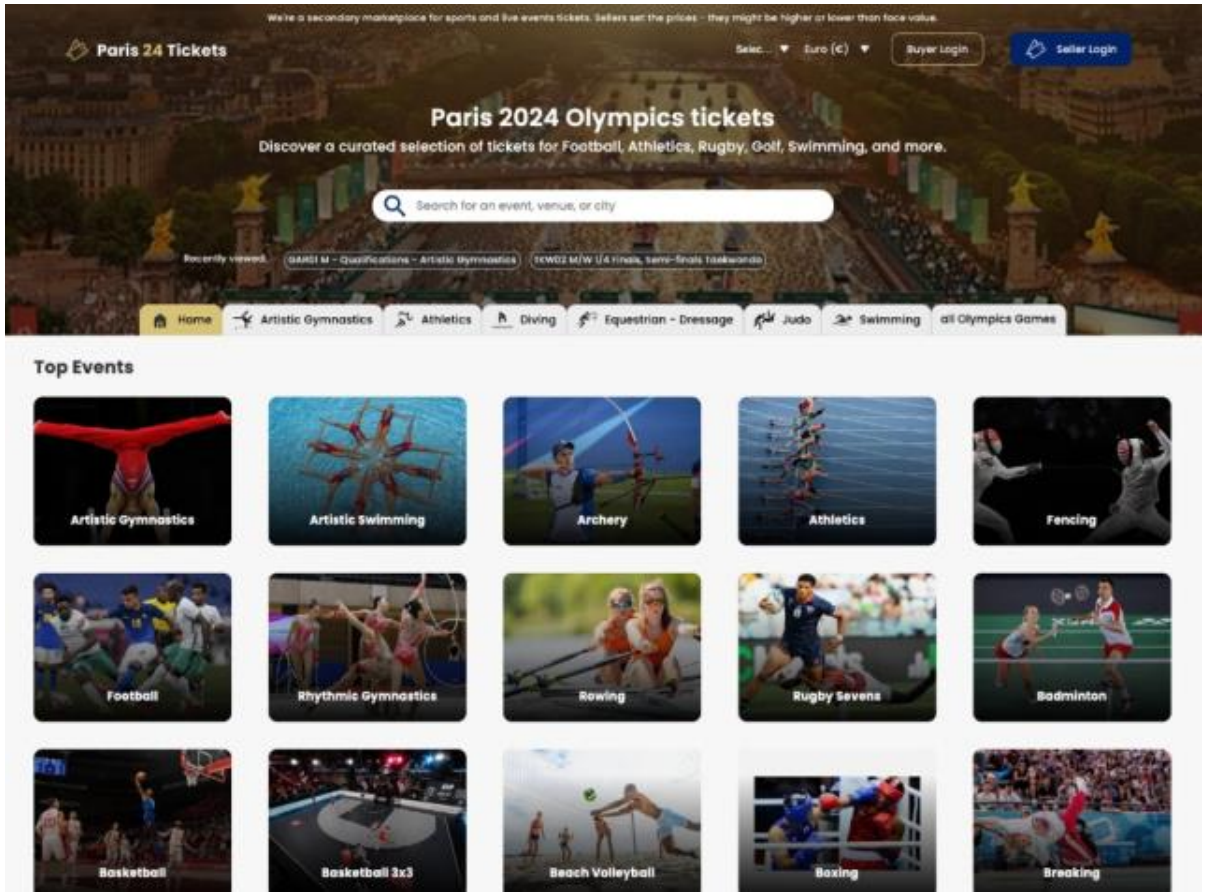




악성 도메인

정부 기관 및 공공 기관을 사칭한 악성 도메인 피해 사례

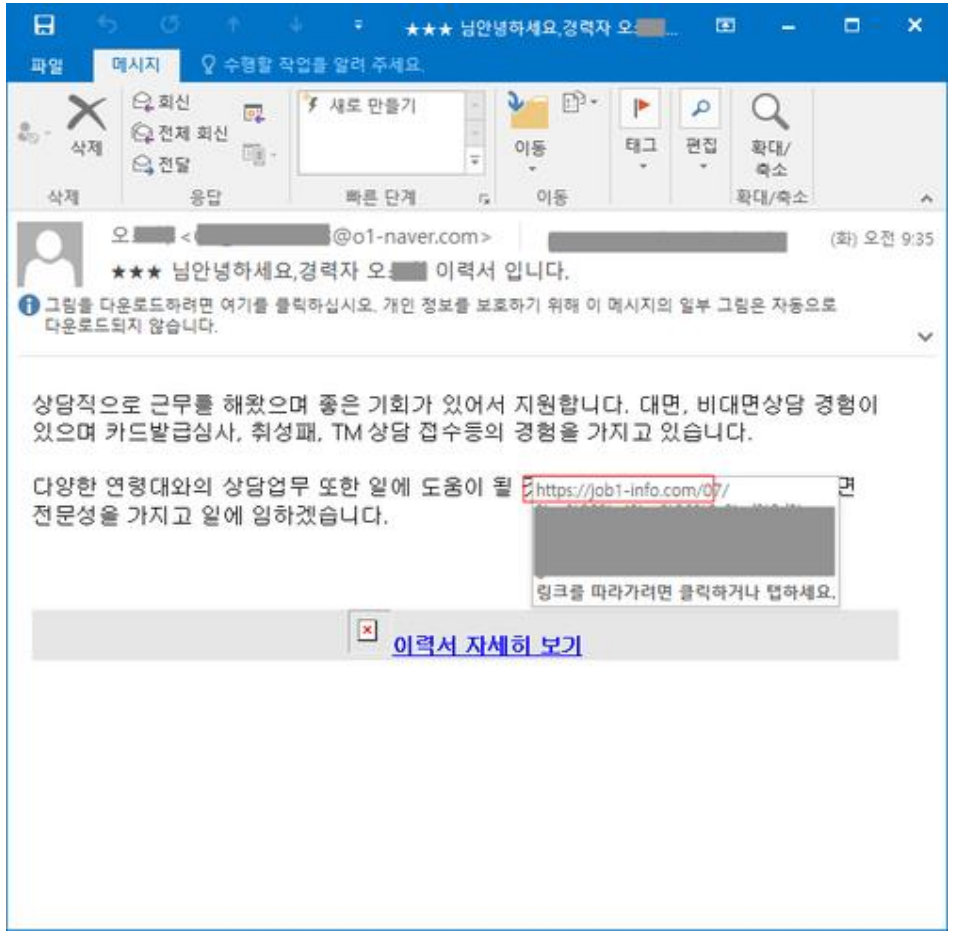




캡스톤디자인

악성 도메인

생성형 AI를 통한 이메일에 악성 도메인 공격이 포함된 사례



과학기술정보통신부 2024년 사이버 보안 위협 전망

< 2024년 사이버 보안 위협 전망 >

▲ **파해자체를모르게하는은밀하고지속적인SW공급망공격**⇒SBOM[주1]과함께HBOM[주2] 고려

▲ **생성형 인공 지능(AI)를 악용한 사이버 범죄 가능성 증가** ⇒ 진위여부 식별 연구 개발(R&D) 필요성 증대

▲ **OT[주3]/ICS[주4] 및 IoT 환경의 보안 위협 증가** ⇒ 관리되지 않은 장비, 공격표면 정리 중요

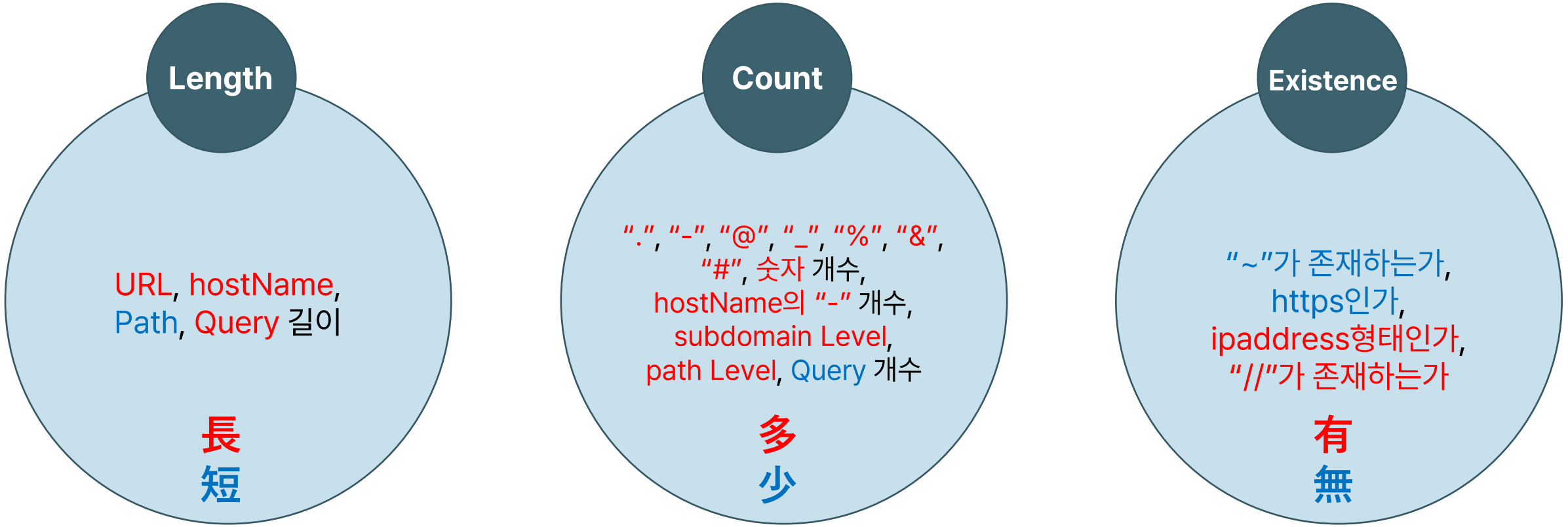
▲ **정치.사회적이슈를악용하는사이버위협 고조**⇒ 민관 더 높은 경각심과 경계 태세 유지 필요

DGA

Domain Generation Algorithm
무작위 도메인 이름을 생성하는 알고리즘

```
earnestnessbiophysicalohax.com
pbmnestnessbiophysicalohax.com
williamseasily.com
printingthatlabel.com
shoulderracerecognizeblue.com
emergencyadaptselectdoubt.com
windowtherefore.net
severadifference.net
```

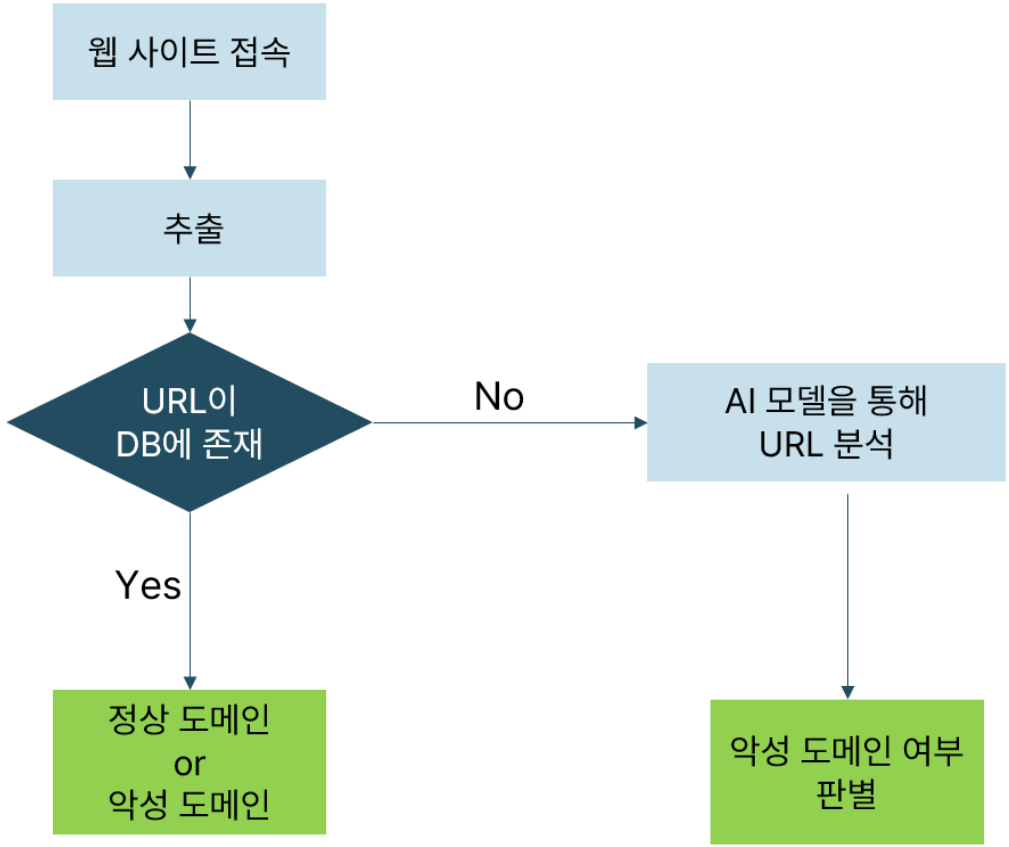
DGA


Length
URL, hostName,
Path, Query 길이
長
短
Count
“.”, “-”, “@”, “_”, “%”, “&”,
“#”, 숫자 개수,
hostName의 “-” 개수,
subdomain Level,
path Level, Query 개수
多
少
Existence
“~”가 존재하는가,
https인가,
ipaddress형태인가,
“//”가 존재하는가
有
無

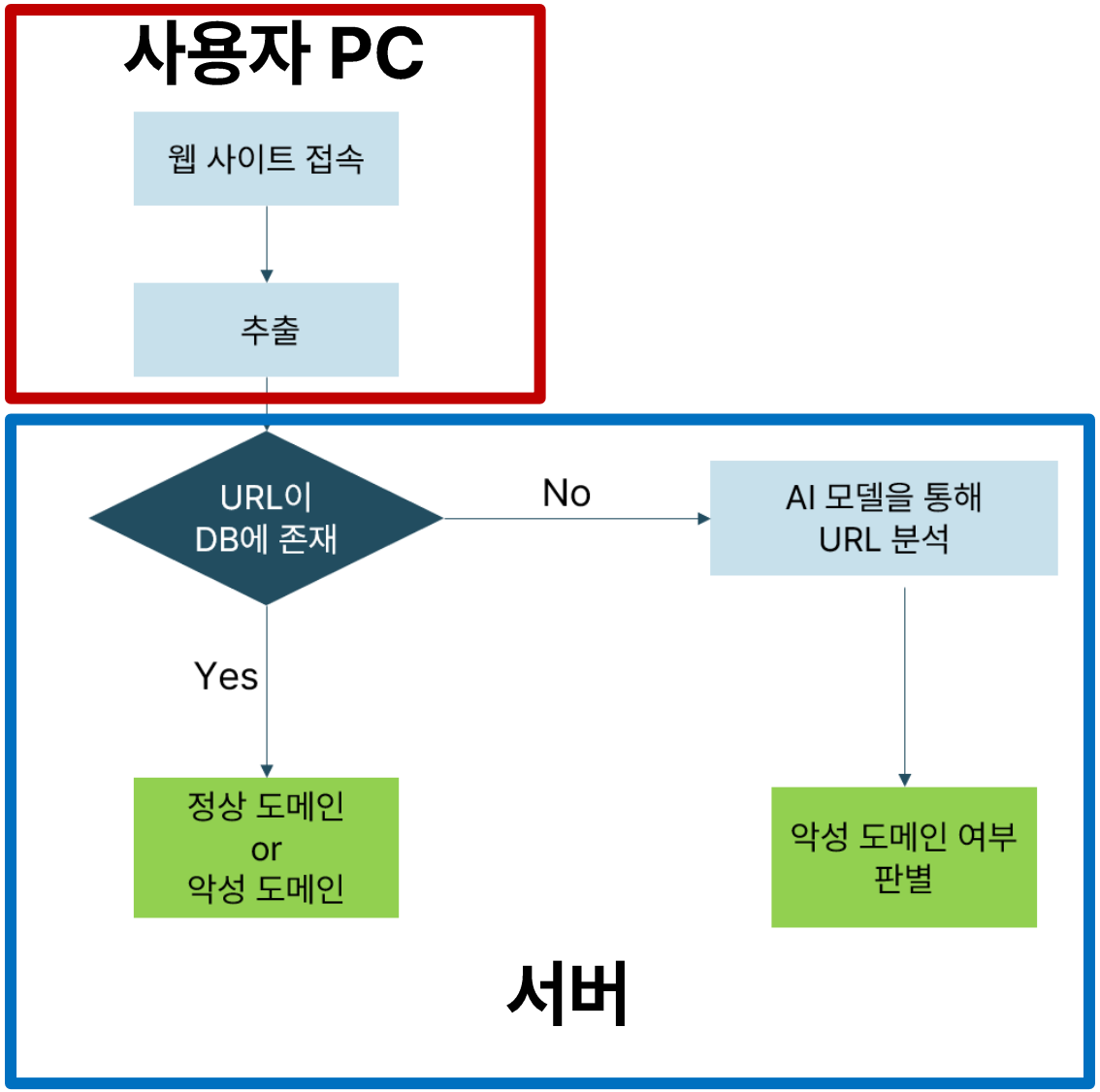
도비

악성 **도**메인 탐지 서**비**스
그리고
도메인 **비**서

도비 동작 다이어그램


웹 사이트 접속
추출
URL이
DB에 존재
No
AI 모델을 통해
URL 분석
Yes
정상 도메인
or
악성 도메인
악성 도메인 여부
판별

도비 동작 다이어그램


사용자 PC
웹 사이트 접속
추출
URL이
DB에 존재
No
AI 모델을 통해
URL 분석
Yes
정상 도메인
or
악성 도메인
악성 도메인 여부
판별
서버

도비 프로젝트 특장점

1. 대규모 동시 접속 환경에서의 안정성	2. 고성능 데이터 처리와 실시간 탐지
3. 확장성과 유연성	4. 사용자 중심 설계

프로젝트 설계

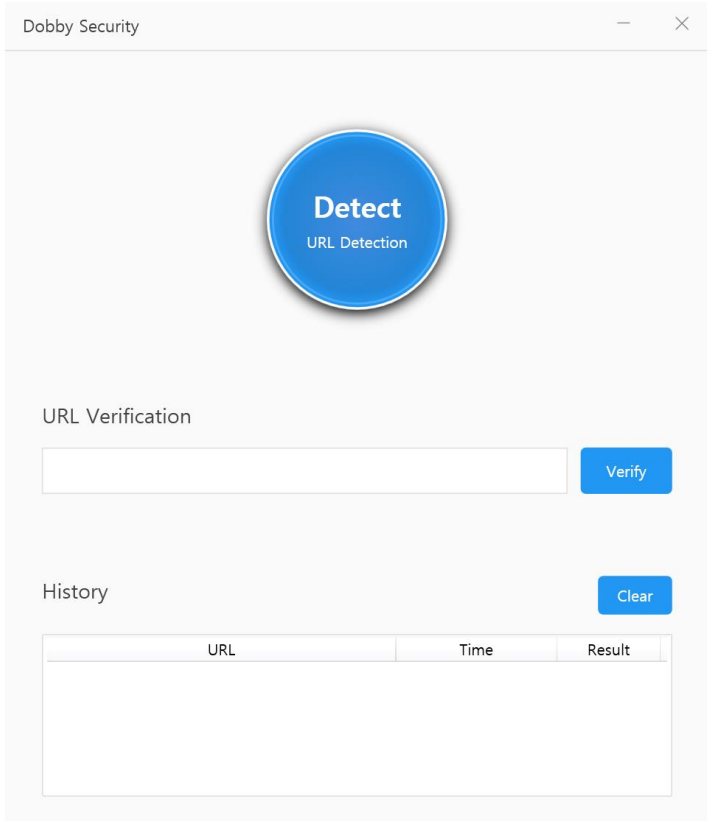
도비 기능 설계

메인 페이지

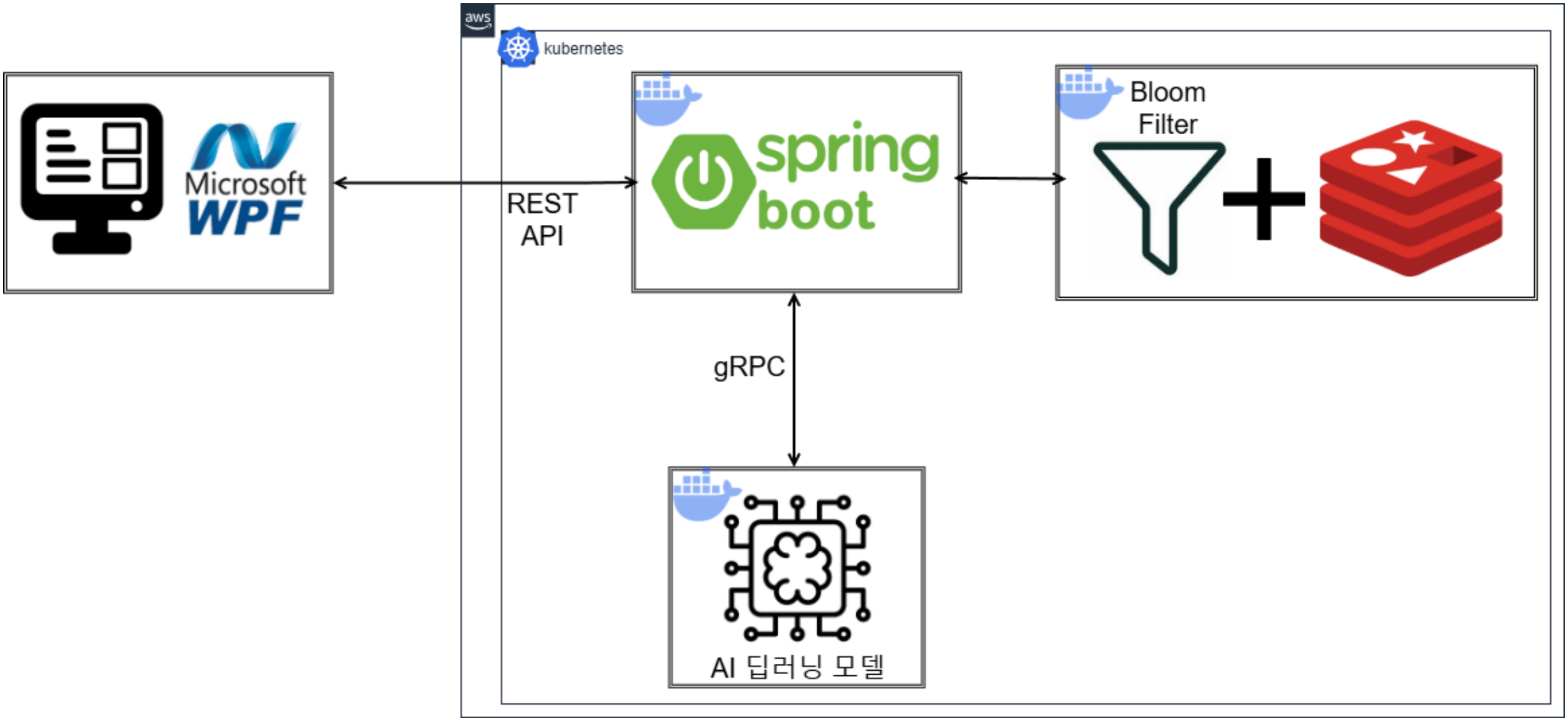
- 버튼
  - 탐지 ON/OFF 버튼
- URL 검사 입력 창
  - 사용자 입력을 통한 검사
- 히스토리
  - 탐지 결과 히스토리
- 백그라운드 실행
  - 종료 버튼 클릭 시 시스템 트레이로 최소화

악성 도메인 탐지

- 실시간 수집
  - 웹 서핑 중 실시간 URL 수집
- URL 검사
  - 수집한 URL 정상/악성 여부 판별
- 사용자 알림
  - 악성 도메인으로 판단된 경우, 사용자에게 알림



도비 시스템 아키텍처

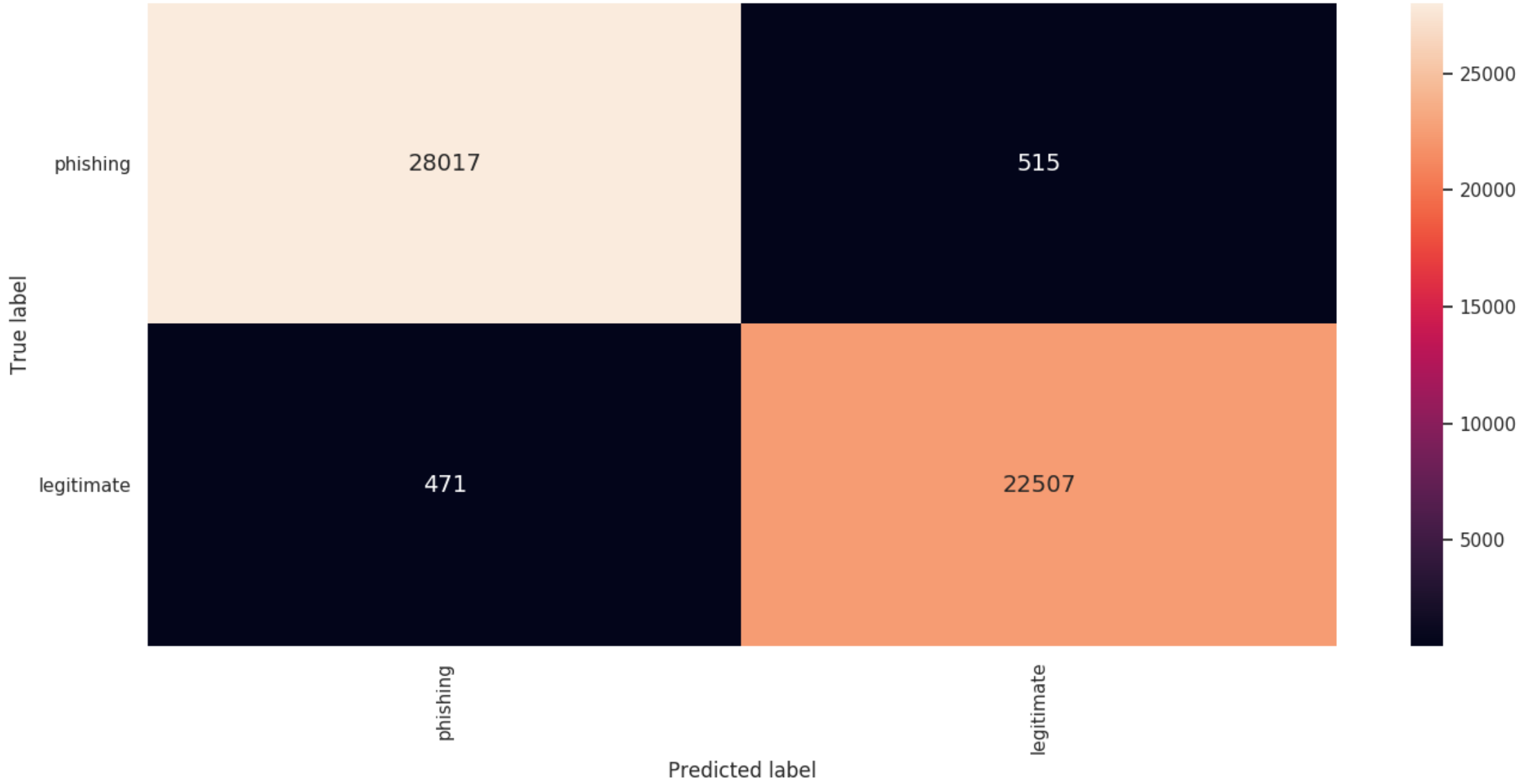

aws
kubernetes
Microsoft
WPF
REST
API
spring
boot
Bloom
Filter
gRPC
AI 딥러닝 모델

프로젝트 시연

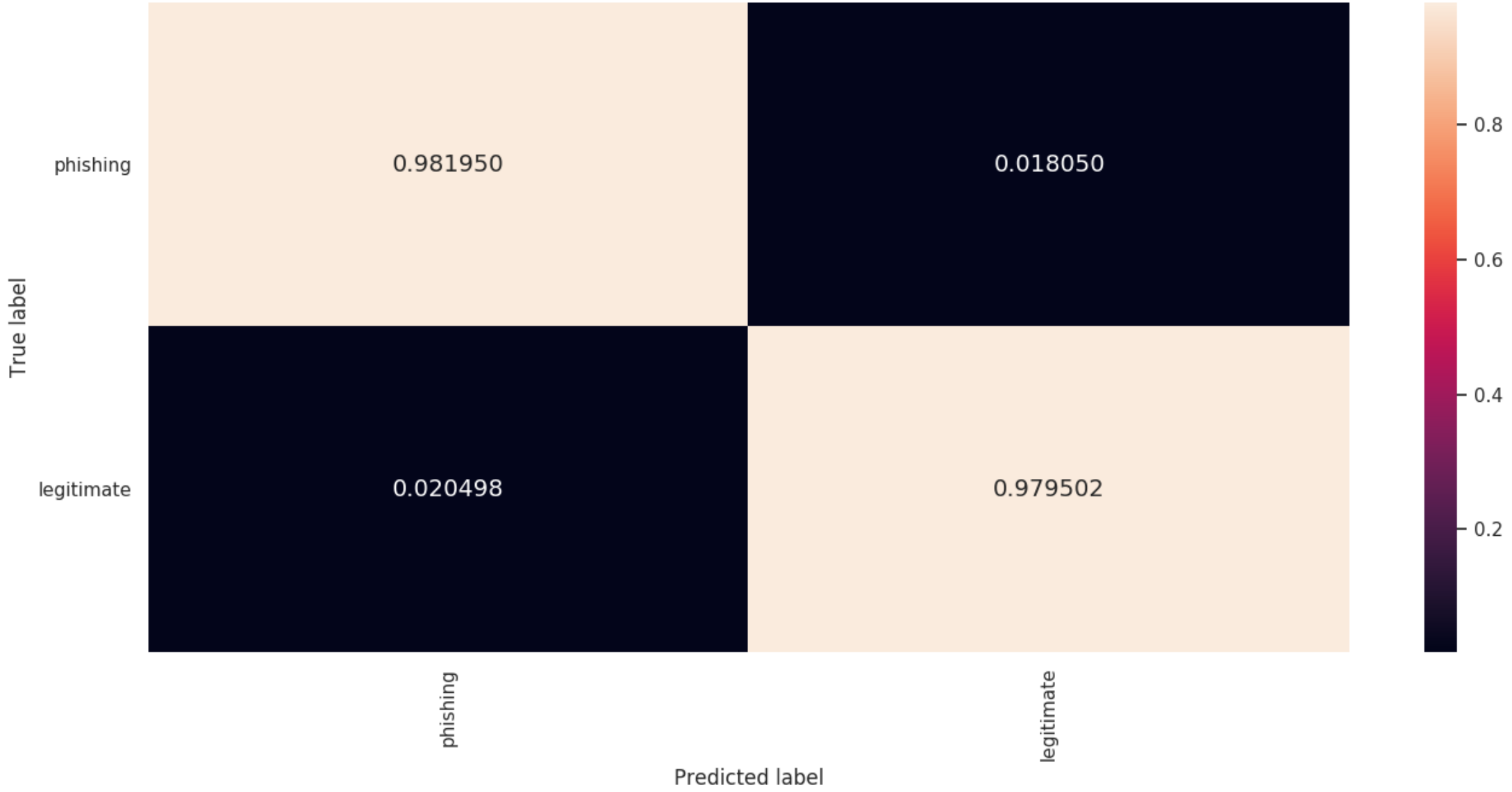
https://drive.google.com/file/d/1PTEusXlo0Oh13yQLV6RRcEI9e_zP4CcQ/view?usp=sharing

Q&A

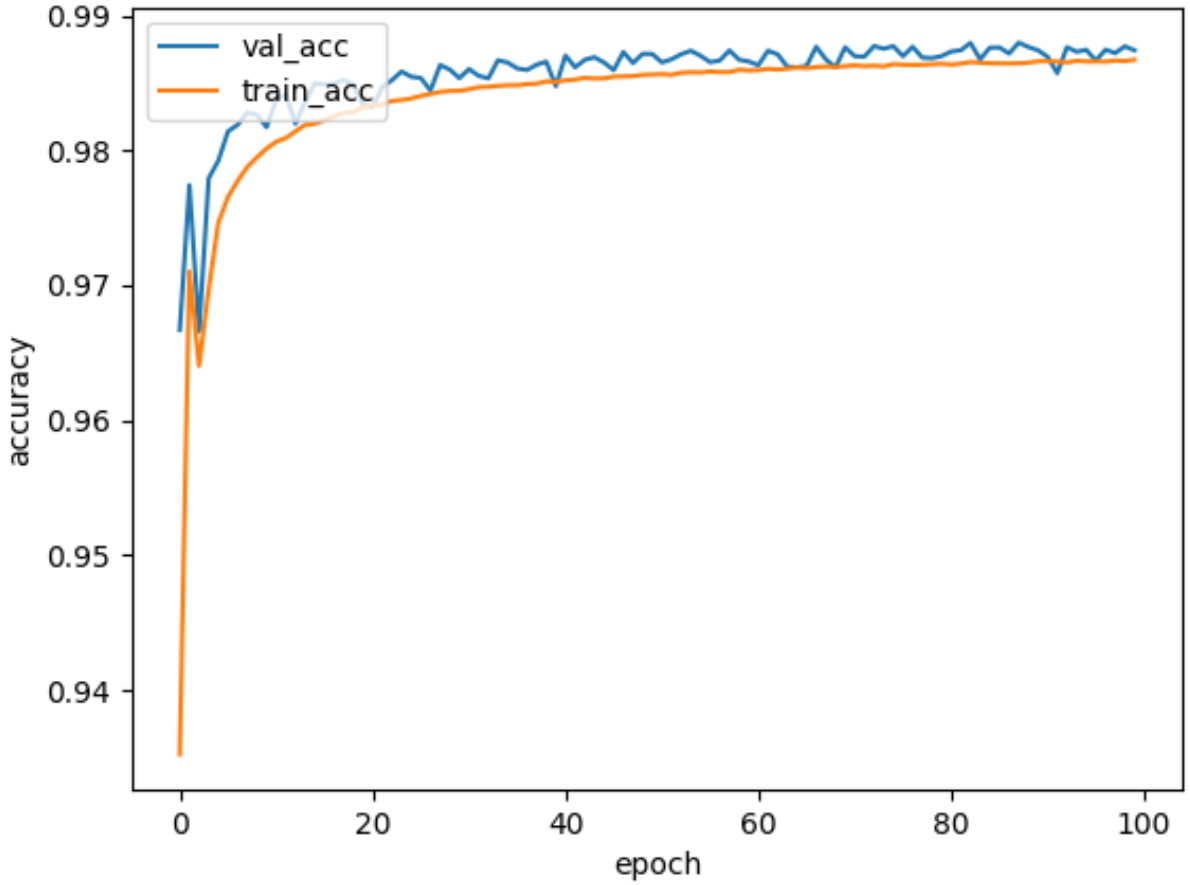
Appendix 1 – 딥러닝

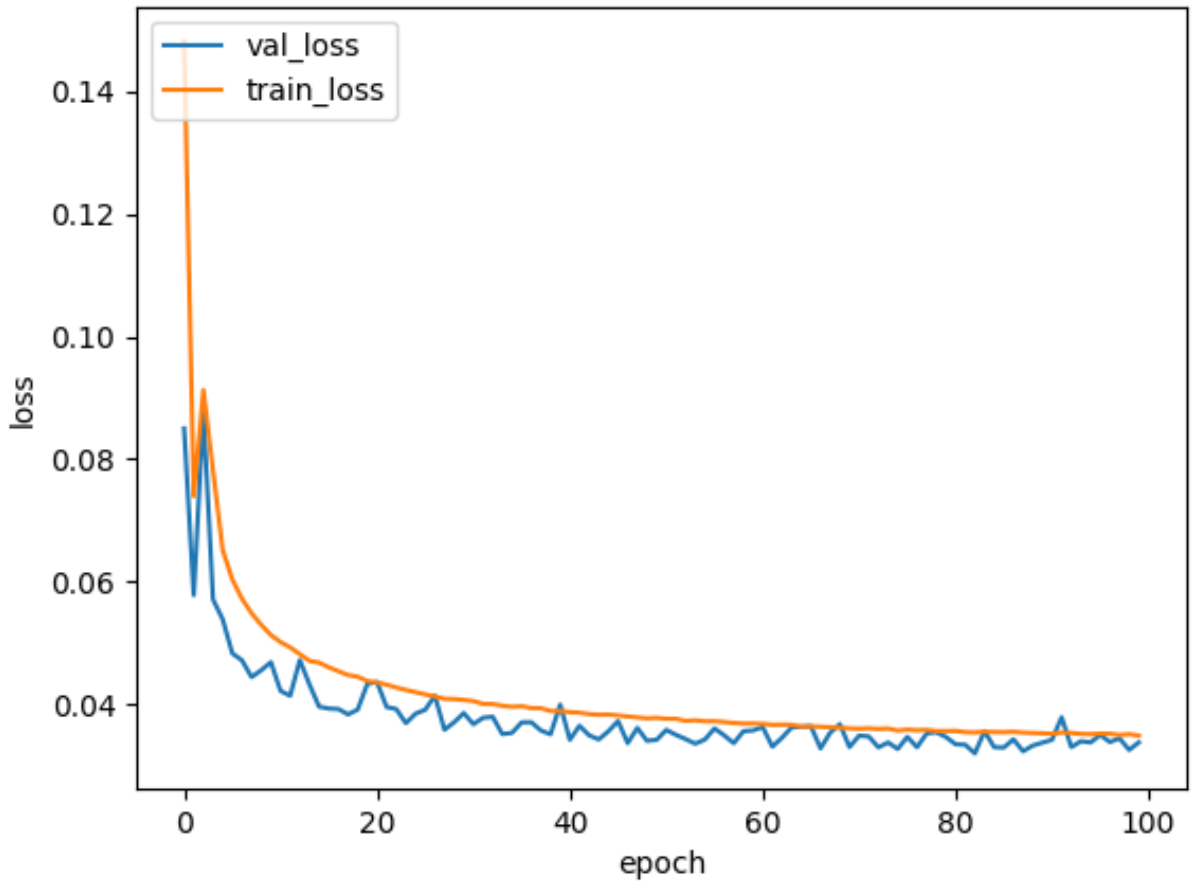


Appendix 1 – 딥러닝

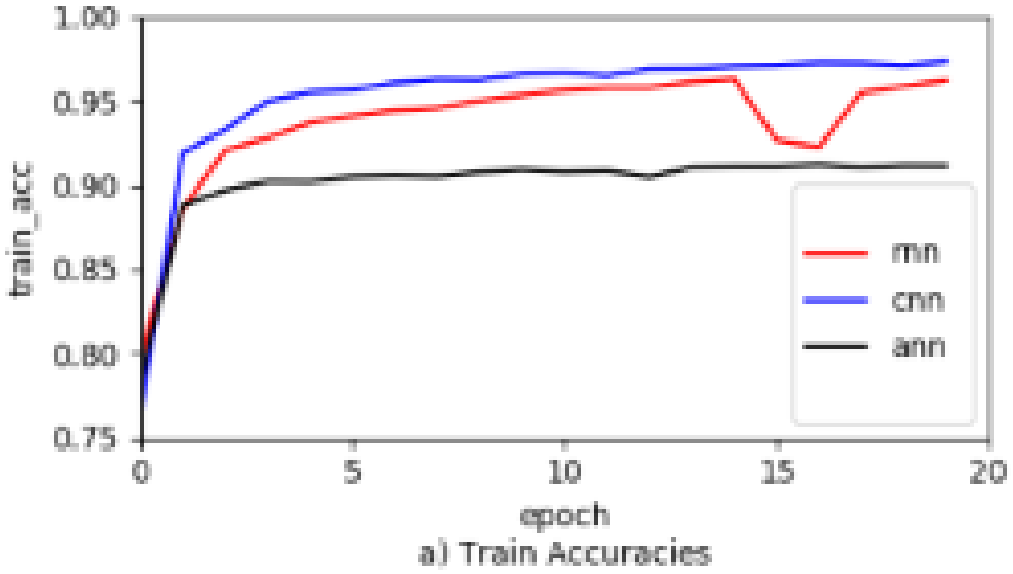


Appendix 1 – 딥러닝

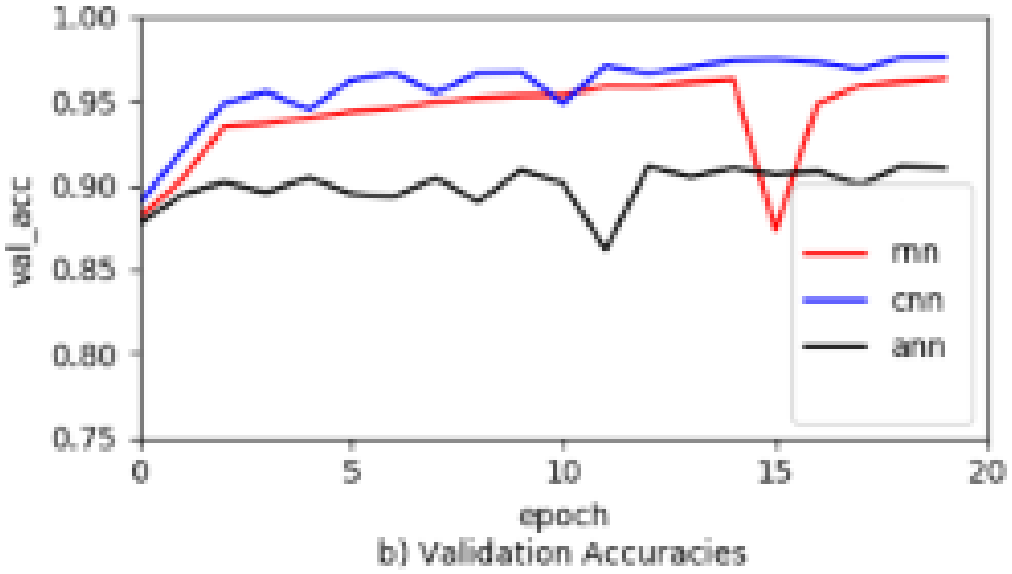




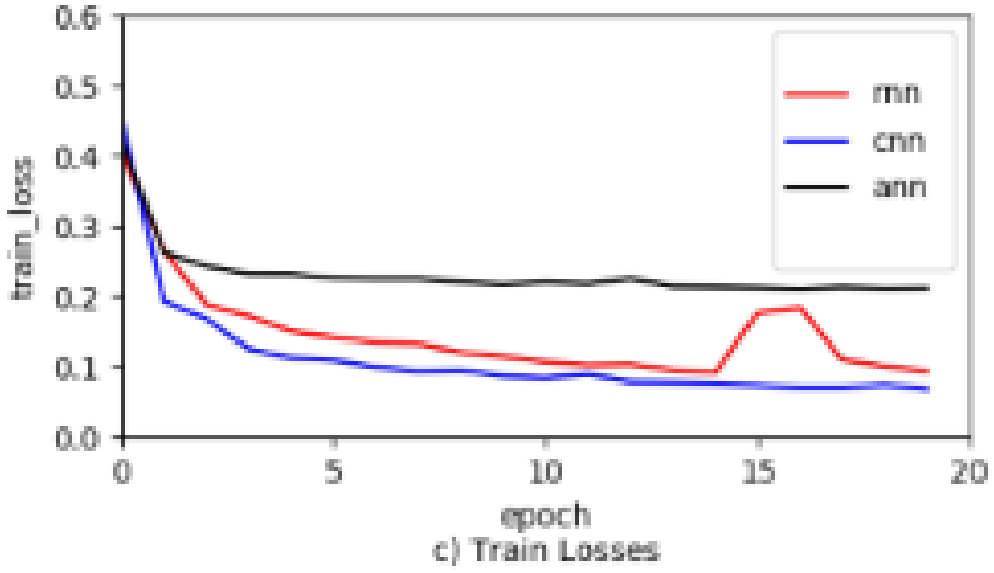
Appendix 1 – 딥러닝



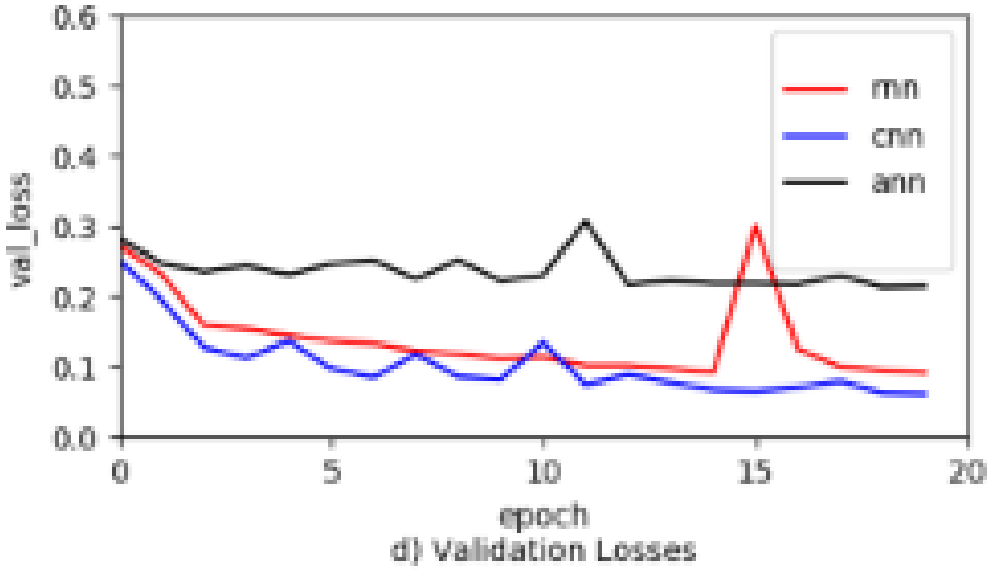
a) Train Accuracies



b) Validation Accuracies



c) Train Losses



d) Validation Losses

Appendix 1 – 딥러닝

Layer (type)	Output Shape	Param #
embedding_1 (Embedding)	(None, 200, 50)	4900
conv1d_1 (Conv1D)	(None, 198, 128)	19328
max_pooling1d_1 (MaxPooling1	(None, 66, 128)	0
dropout_1 (Dropout)	(None, 66, 128)	0
conv1d_2 (Conv1D)	(None, 66, 128)	114816
dropout_2 (Dropout)	(None, 66, 128)	0
conv1d_3 (Conv1D)	(None, 66, 128)	82048
dropout_3 (Dropout)	(None, 66, 128)	0
conv1d_4 (Conv1D)	(None, 66, 128)	49280

Layer (type)	Output Shape	Param #
max_pooling1d_2 (MaxPooling1	(None, 22, 128)	0
dropout_4 (Dropout)	(None, 22, 128)	0
conv1d_5 (Conv1D)	(None, 22, 128)	82048
dropout_5 (Dropout)	(None, 22, 128)	0
conv1d_6 (Conv1D)	(None, 22, 128)	49280
max_pooling1d_3 (MaxPooling1	(None, 7, 128)	0
dropout_6 (Dropout)	(None, 7, 128)	0
conv1d_7 (Conv1D)	(None, 7, 128)	49280
max_pooling1d_4 (MaxPooling1	(None, 2, 128)	0
dropout_7 (Dropout)	(None, 2, 128)	0
flatten_1 (Flatten)	(None, 256)	0
dense_1 (Dense)	(None, 2)	514

Total params: 451,494
Trainable params: 451,494
Non-trainable params: 0

CNN Embedding > Conv1D > MaxPooling1 > Dropout > Conv1D > Dropout > Conv1D > Dropout > Conv1D > MaxPooling1 > Dropout > Conv1D > Dropout > Conv1D > MaxPooling1 > Dropout > Conv1D > MaxPooling1 > Dropout > Flatten > Dense

Appendix 2 – 시스템 성능 측정 SC_1

Summary Report

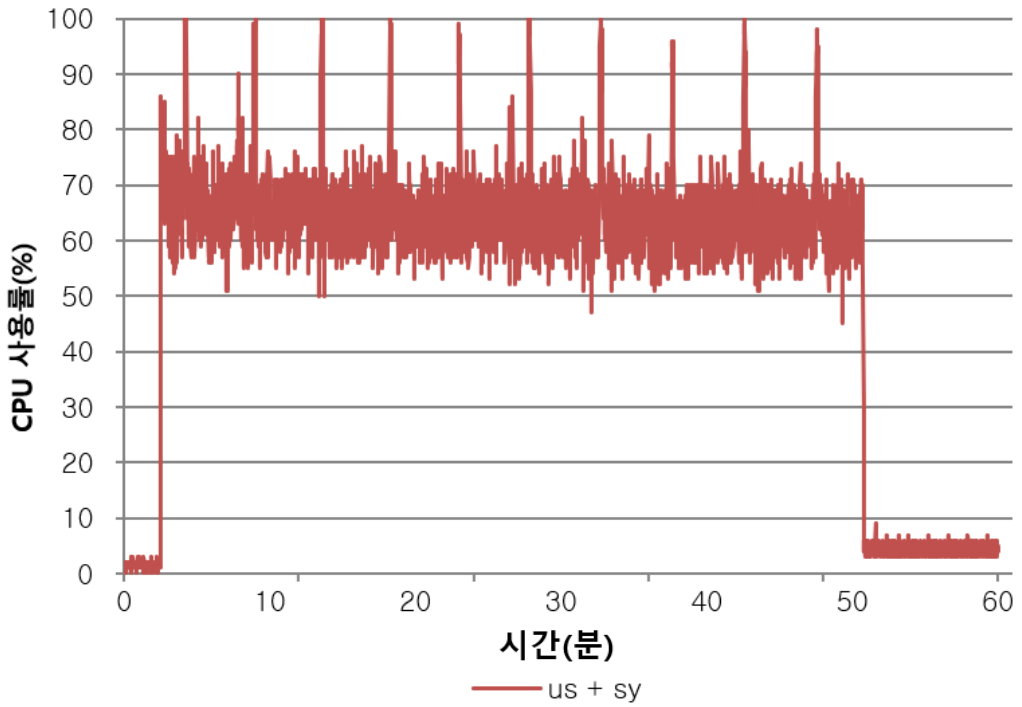
Name: Summary Report

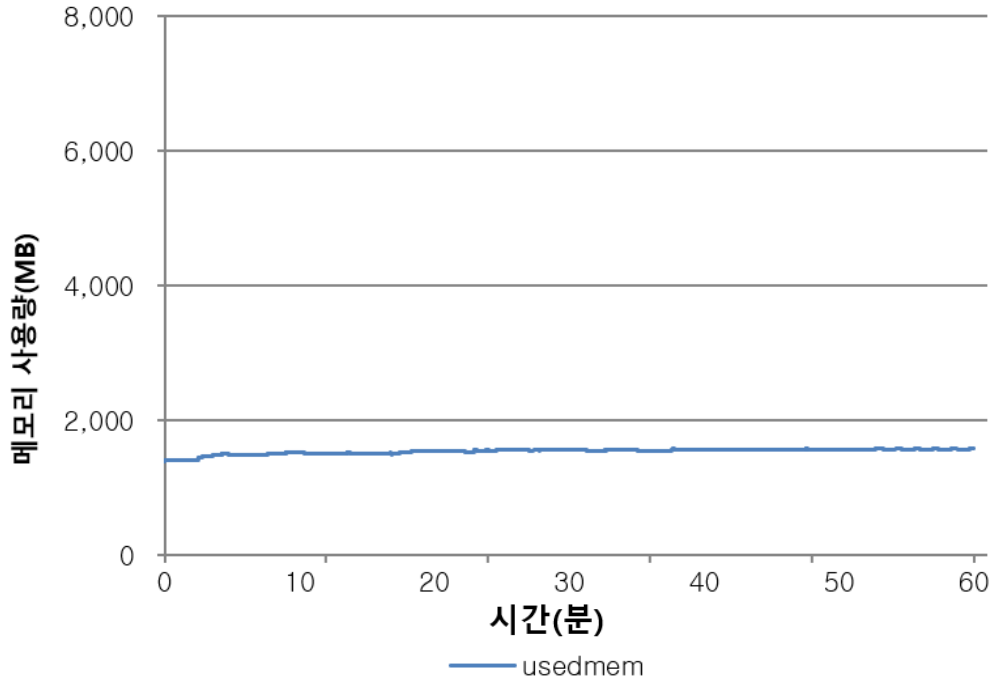
Comments:

Write results to file / Read from file

Filename Browse... Log/Display Only: Errors Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	118557	2028	4	8160	2374.22	0.00%	32.9/sec	6.16	5.55	191.5
TOTAL	118557	2028	4	8160	2374.22	0.00%	32.9/sec	6.16	5.55	191.5





Appendix 2 – 시스템 성능 측정 SC_2

Summary Report

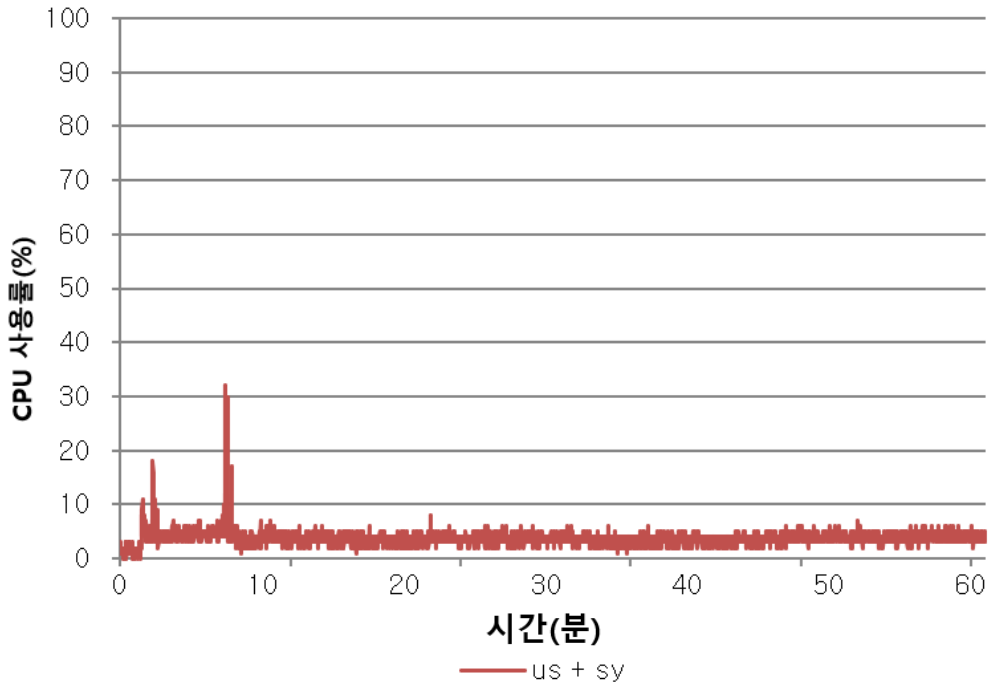
Name: Summary Report

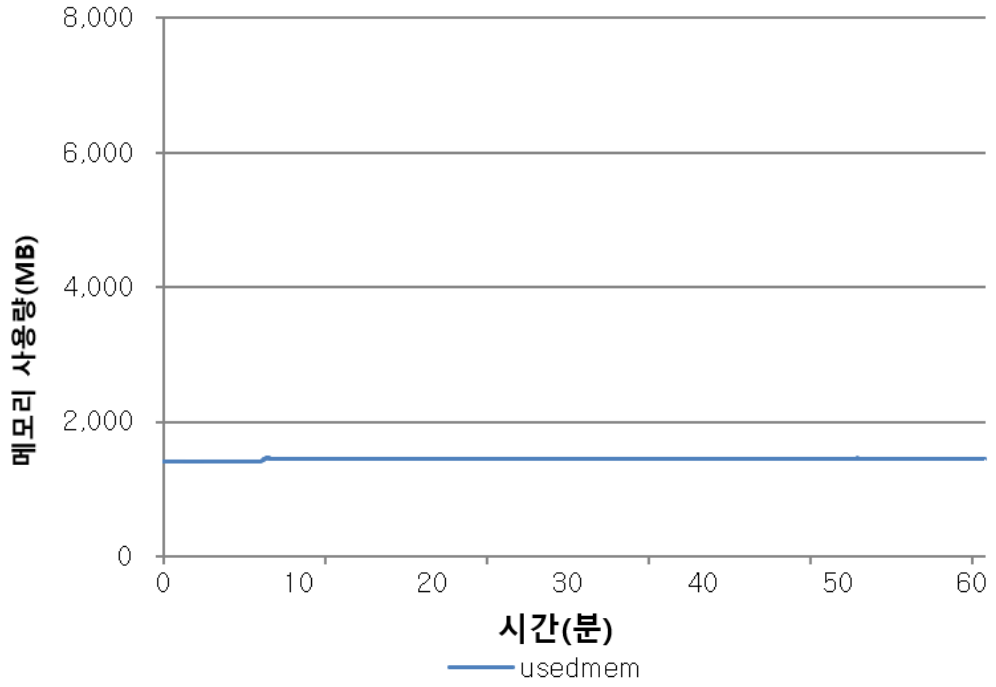
Comments:

Write results to file / Read from file

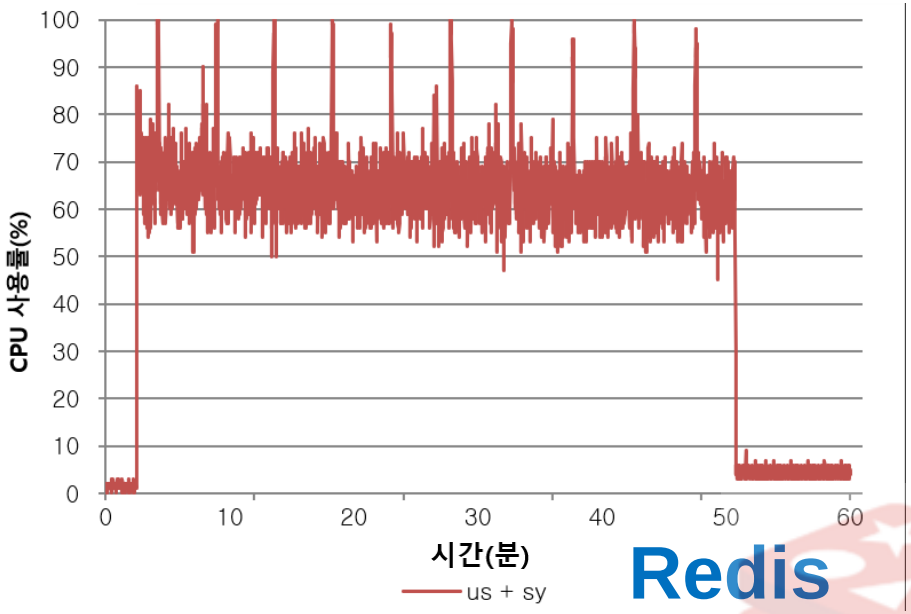
Filename Browse... Log/Display Only: Errors Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	353879	9	4	262	6.61	0.00%	98.3/sec	18.39	18.92	191.6
TOTAL	353879	9	4	262	6.61	0.00%	98.3/sec	18.39	18.92	191.6

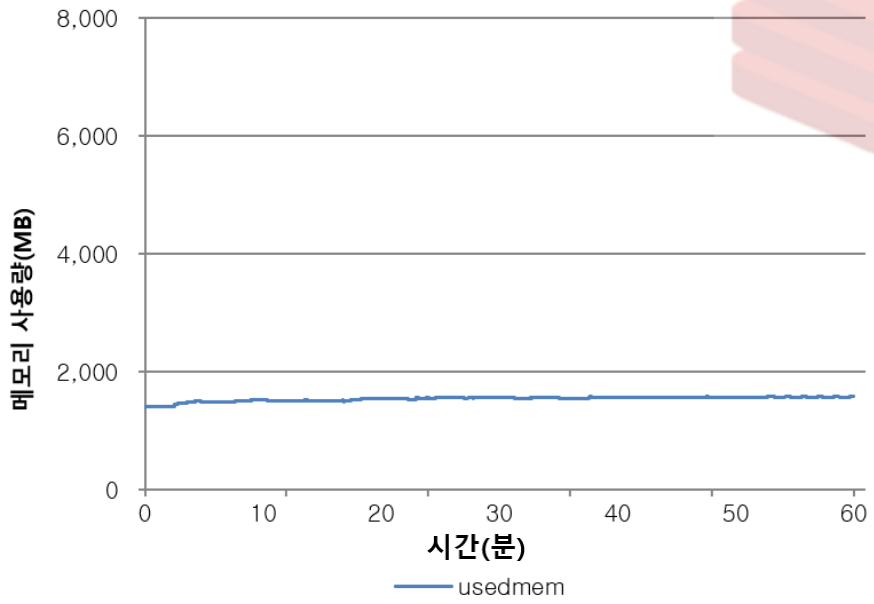


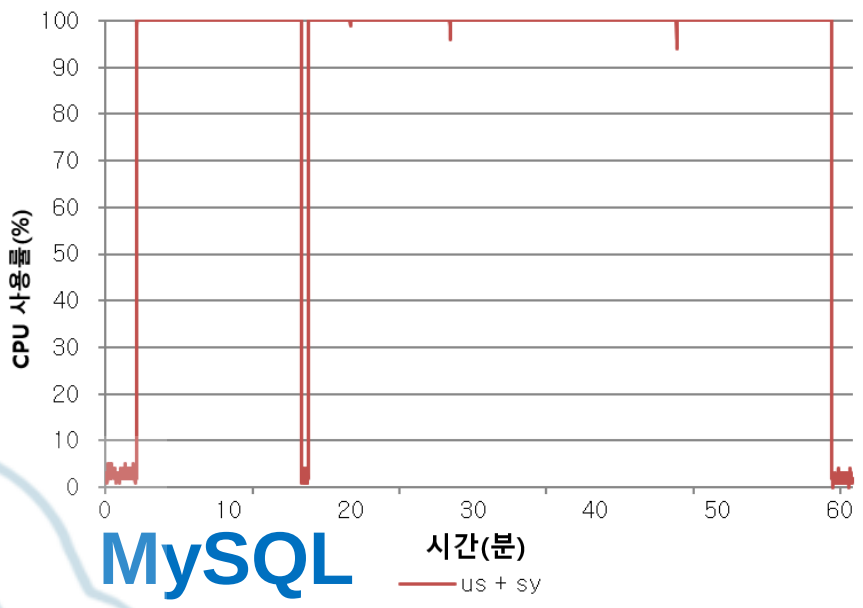


Appendix 2 – 시스템 성능 측정 SC_1 비교

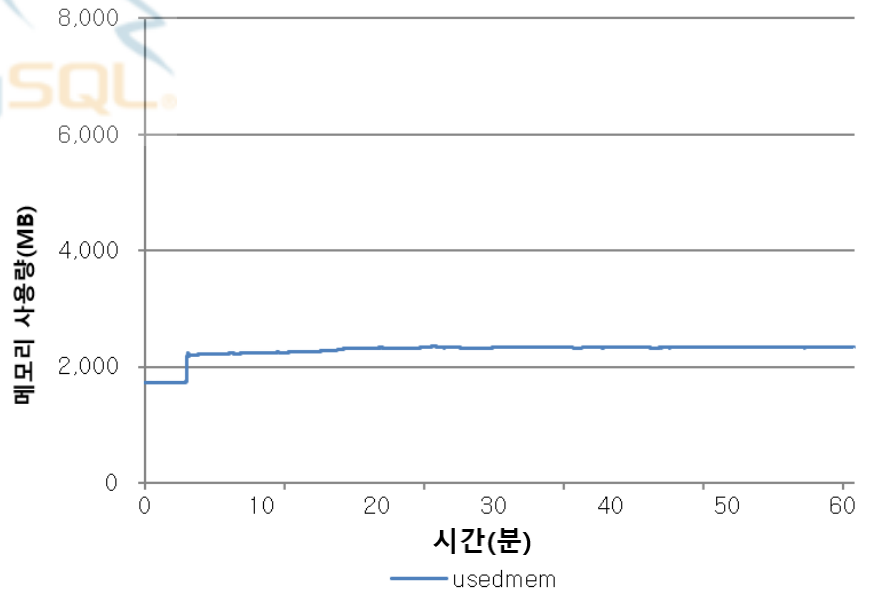


Redis





MySQL



Appendix 2 – 시스템 성능 측정 SC_1 비교

Redis

Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename Browse... Log/Display Only: Errors Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	118557	2028	4	8160	2374.22	0.00%	32.9/sec	6.16	5.55	191.5
TOTAL	118557	2028	4	8160	2374.22	0.00%	32.9/sec	6.16	5.55	191.5

MySQL

Summary Report

Name: Summary Report

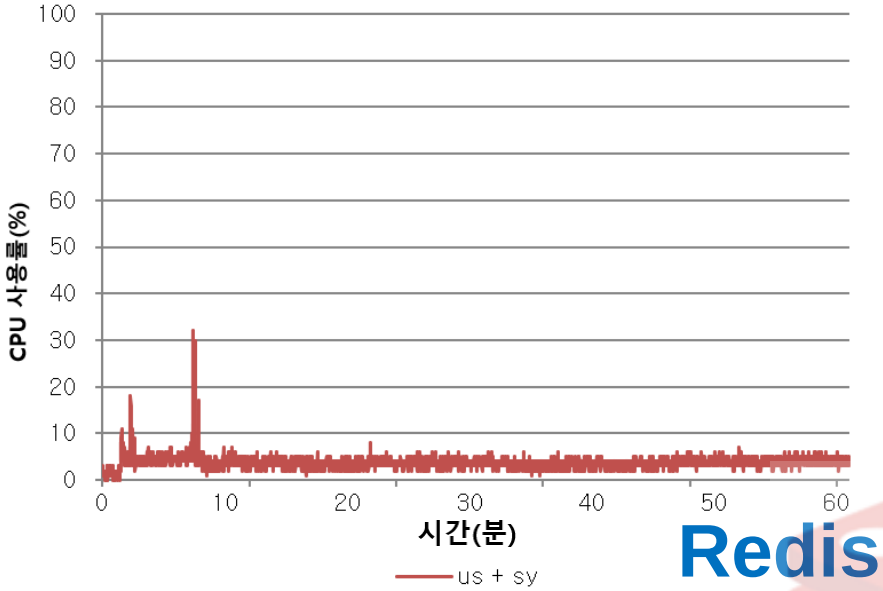
Comments:

Write results to file / Read from file

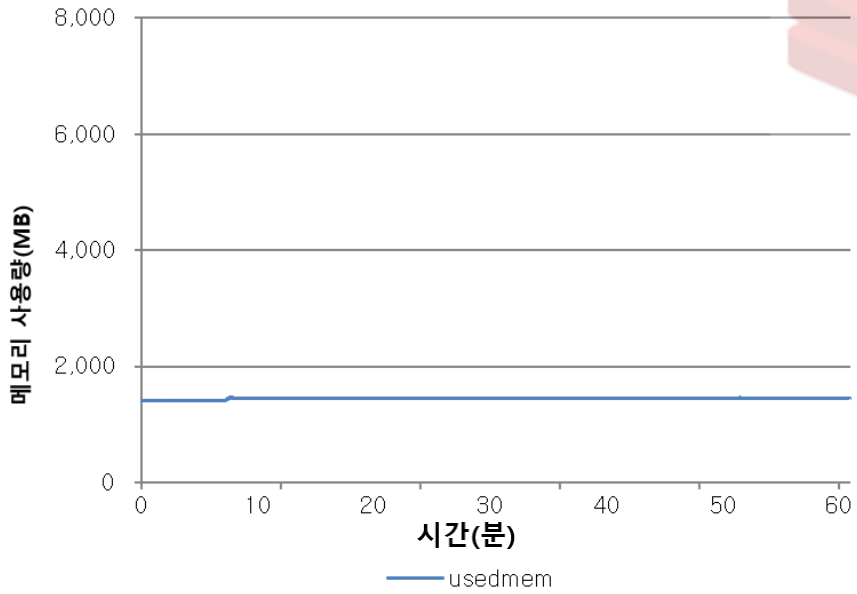
Filename Browse... Log/Display Only: Errors Successes Configure

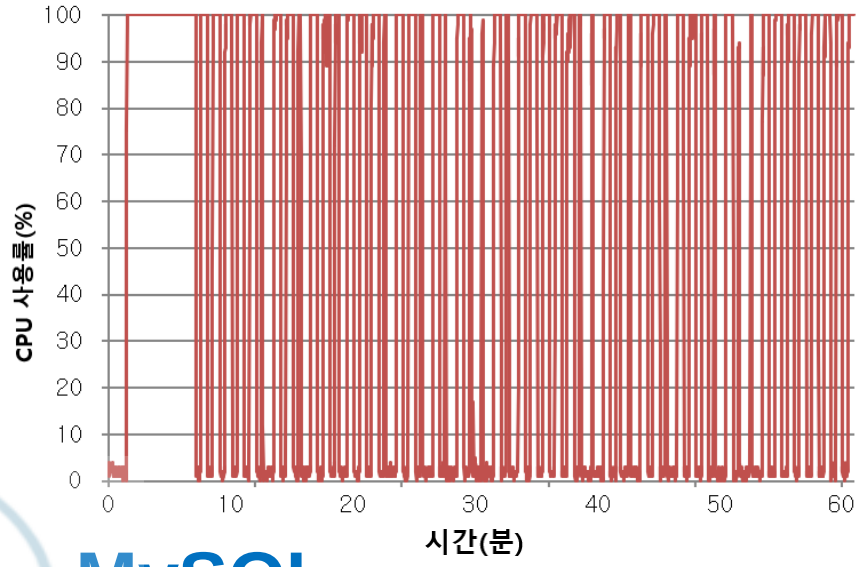
Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	9934	35372	7172	235275	18972.93	52.65%	2.7/sec	0.60	0.46	223.9
TOTAL	9934	35372	7172	235275	18972.93	52.65%	2.7/sec	0.60	0.46	223.9

Appendix 2 – 시스템 성능 측정 SC_2 비교

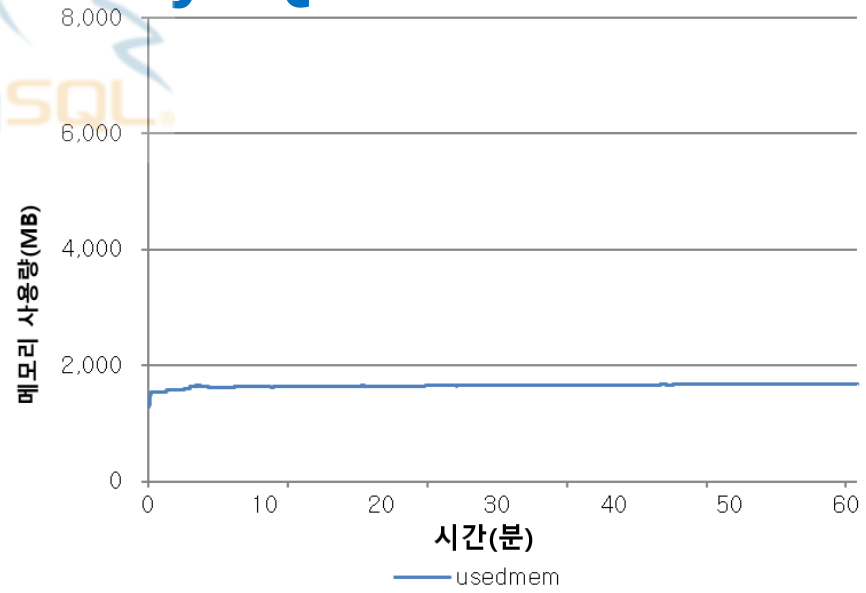


Redis





MySQL



Appendix 2 – 시스템 성능 측정 SC_2 비교

Redis

Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename Browse... Log/Display Only: Errors Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	353879	9	4	262	6.61	0.00%	98.3/sec	18.39	18.92	191.6
TOTAL	353879	9	4	262	6.61	0.00%	98.3/sec	18.39	18.92	191.6

MySQL

Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename Browse... Log/Display Only: Errors Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	3241	114141	8129	959024	143755.87	28.42%	48.4/min	0.16	0.15	209.0
TOTAL	3241	114141	8129	959024	143755.87	28.42%	48.4/min	0.16	0.15	209.0

Appendix 3 – Bloom Filter 참고 자료

		실제 포함 여부	
		True	False
분류 결과	True	True Positive	False Positive
	False	False Negative	True Negative