2021 Paper Review Project

# 7월 5주차 논문 리뷰 미팅

ICT 융합학부
2020055414 지훈

선정 논문

# Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems

# 네트워크 침입 감지 시스템을 무력화시키는 현실적인 공격 모델링

Pubilished on
Cornell University & Association for Computin Machinery(ACM)

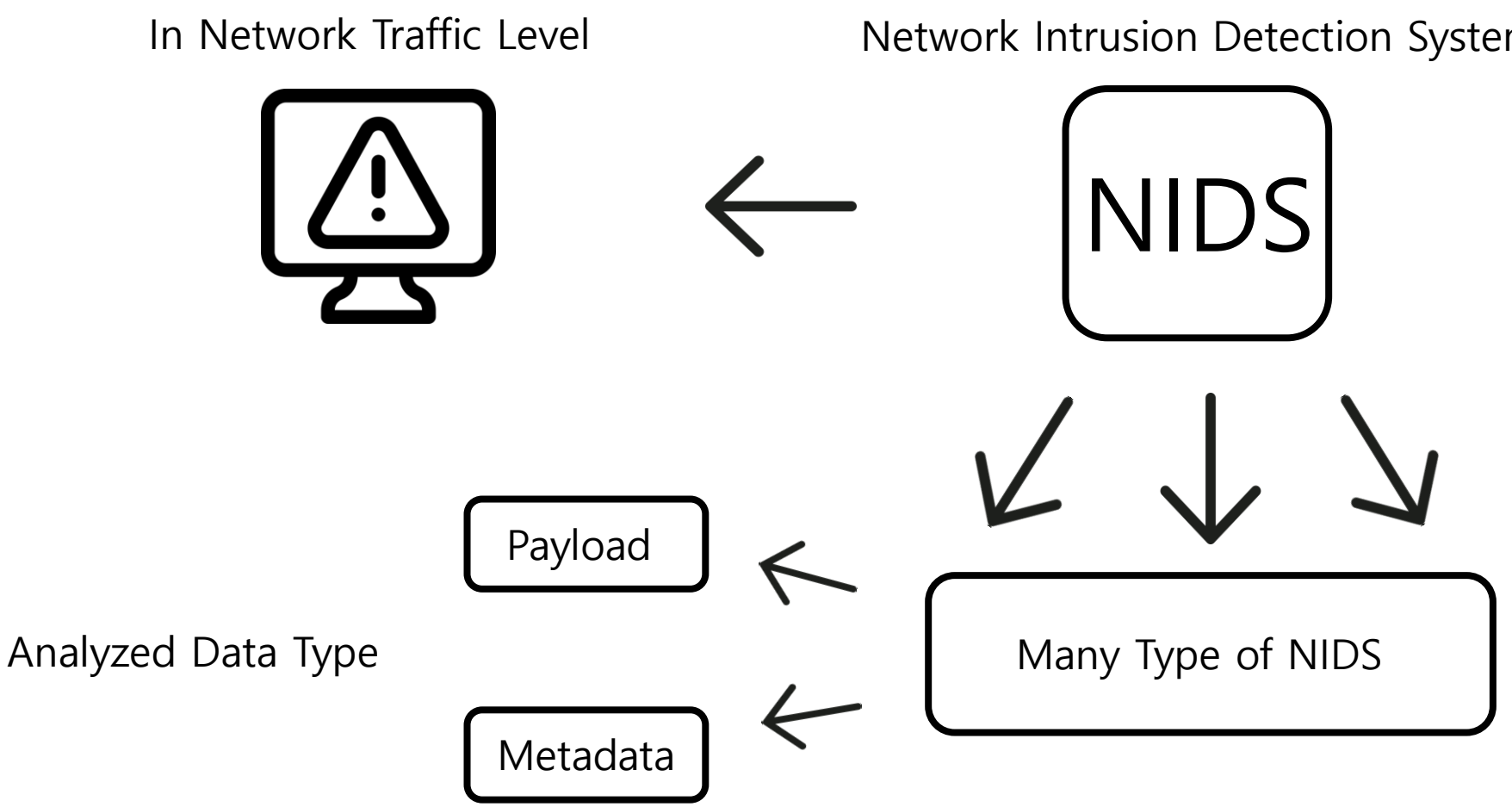
# Intrusion Detection System

Practically Impossible

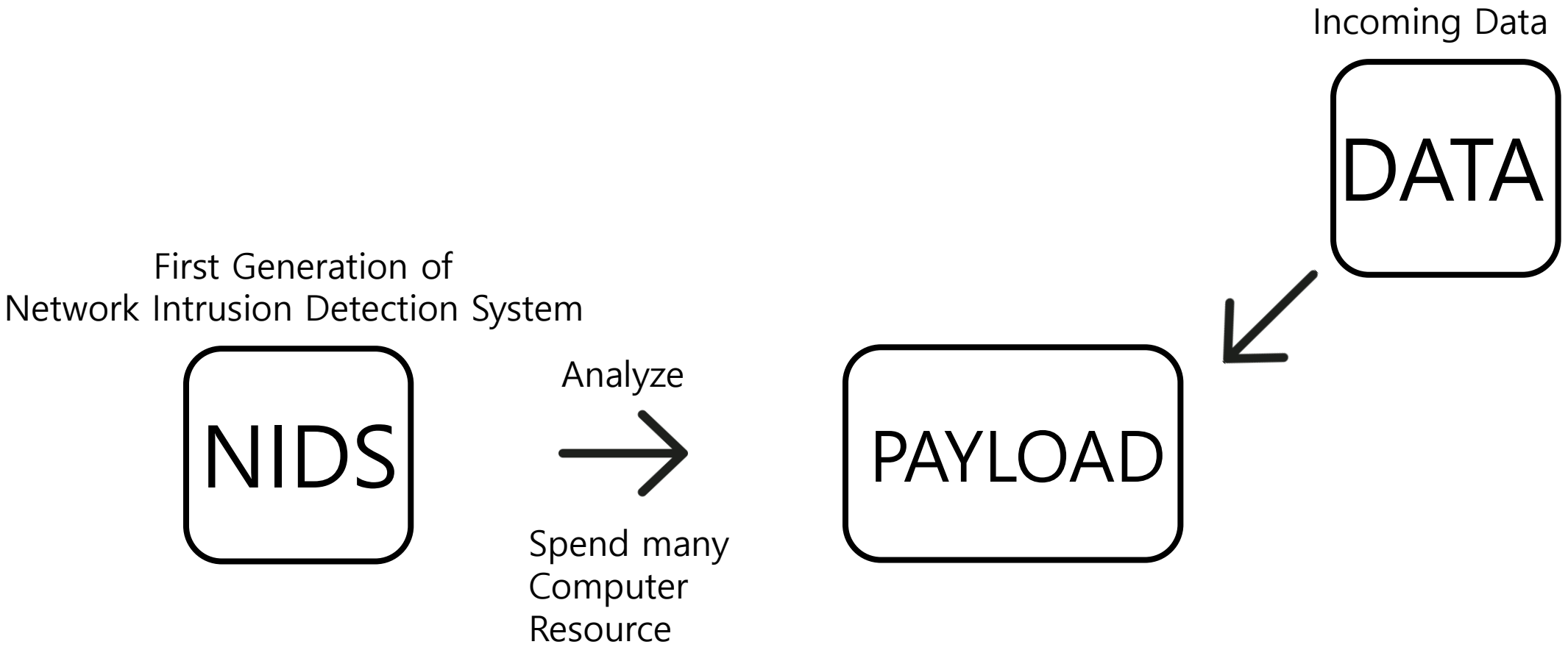
# Intrusion Detection System

Intrusion Detection System

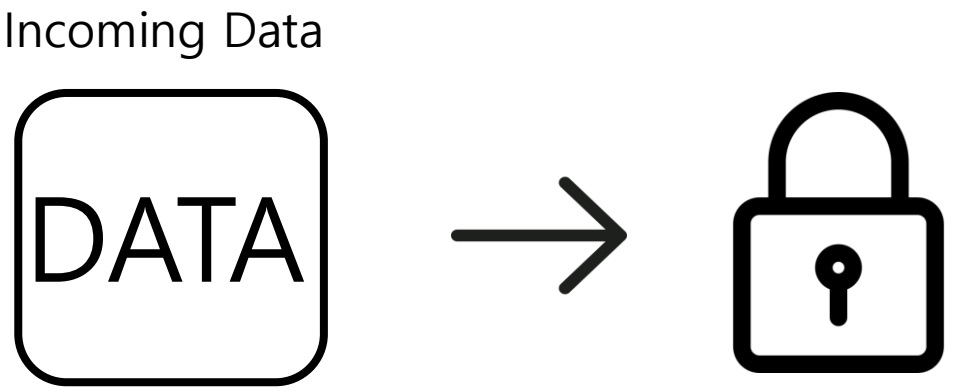
NIDS


In Network Traffic Level
Network Intrusion Detection System
NIDS
Payload
Analyzed Data Type
Many Type of NIDS
Metadata

# 1st Generation of NIDS

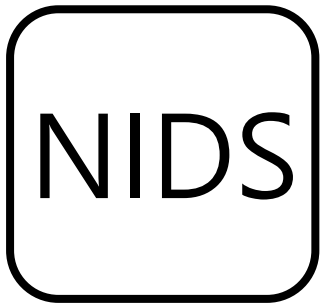


# 1st Generation of NIDS

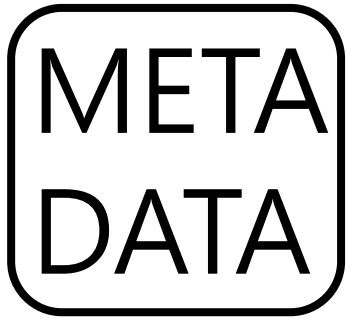


# Next Generation of NIDS

Next Generation of
Network Intrusion Detection System




Metadata
Ex) Networkflow



# Next Generation of NIDS

Computationally
store and analyze

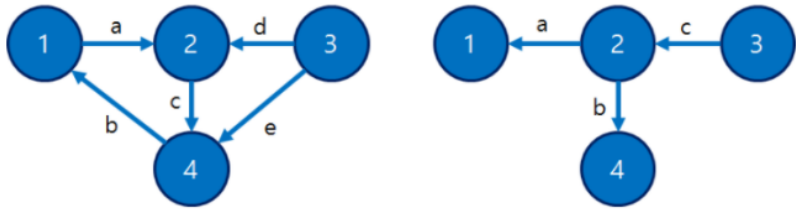
Not present
Privacy concerns

Network Intrusion Detection System

NIDS

Analyze

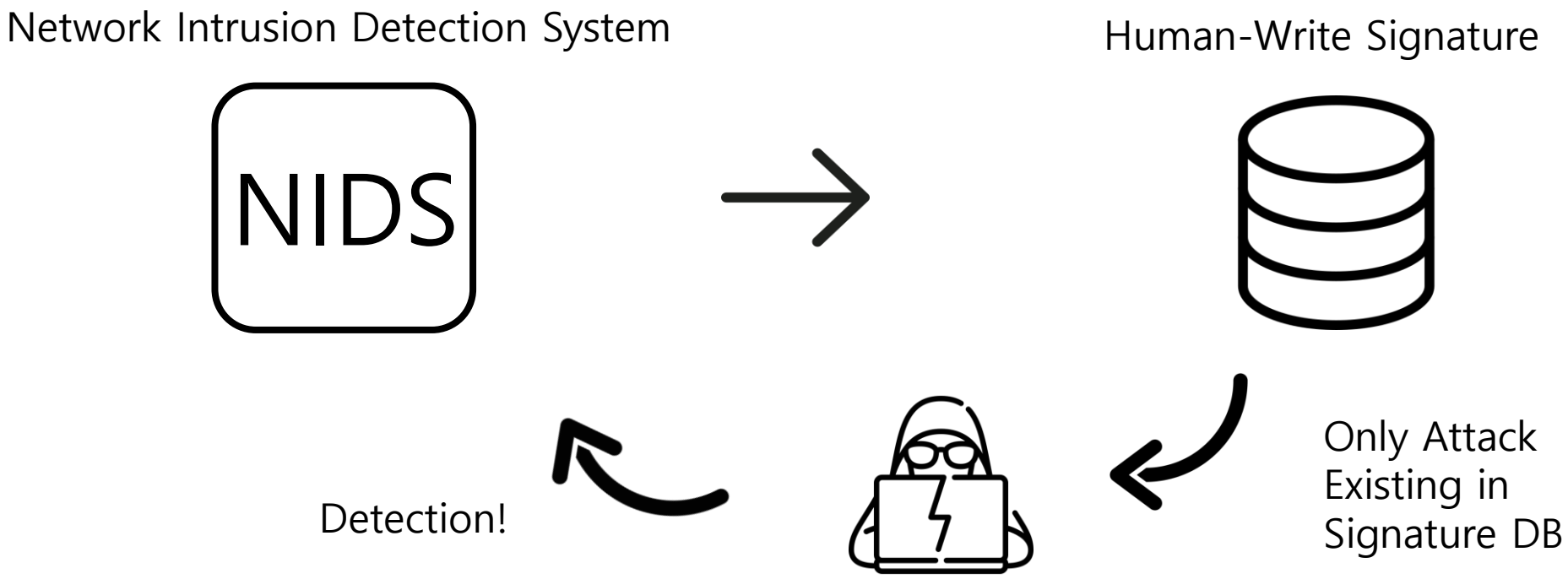
Network Metrics




$$\begin{bmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Ex) Session Duration
Amount of Exchanged Byte

# Signature based Detection



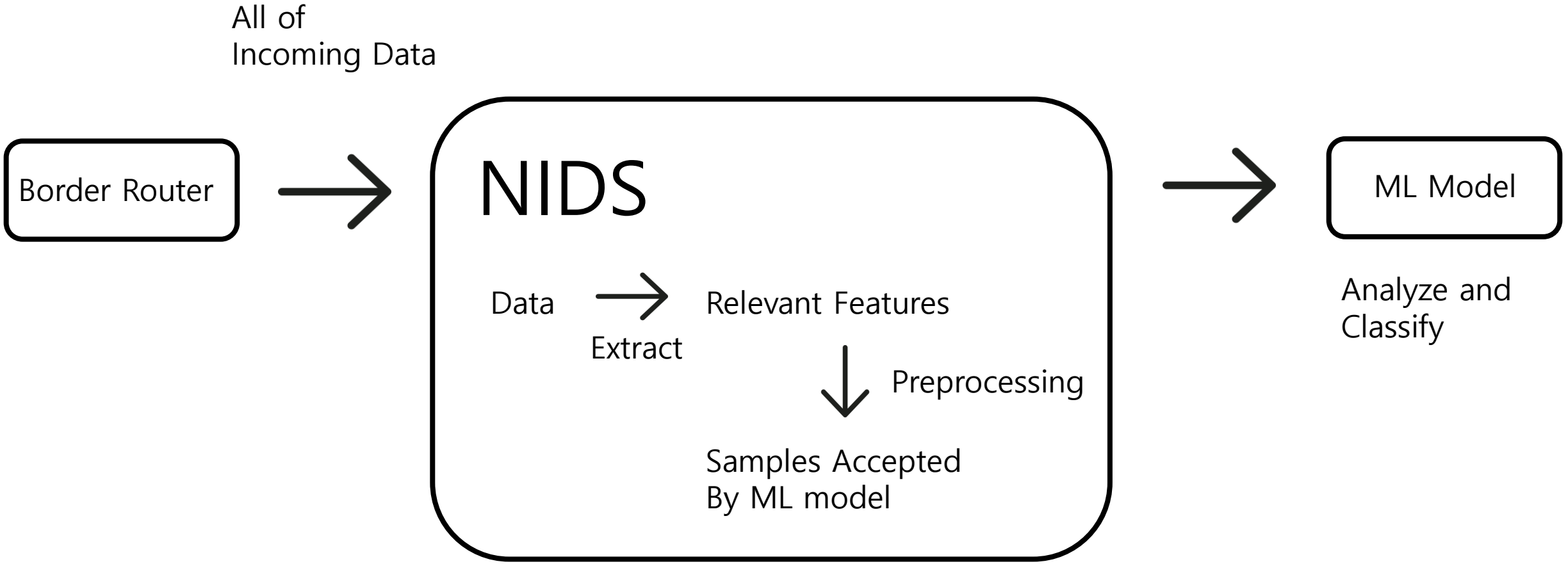
# Next Generation of NIDS

Maching-Learning based
Network Intrusion Detection System

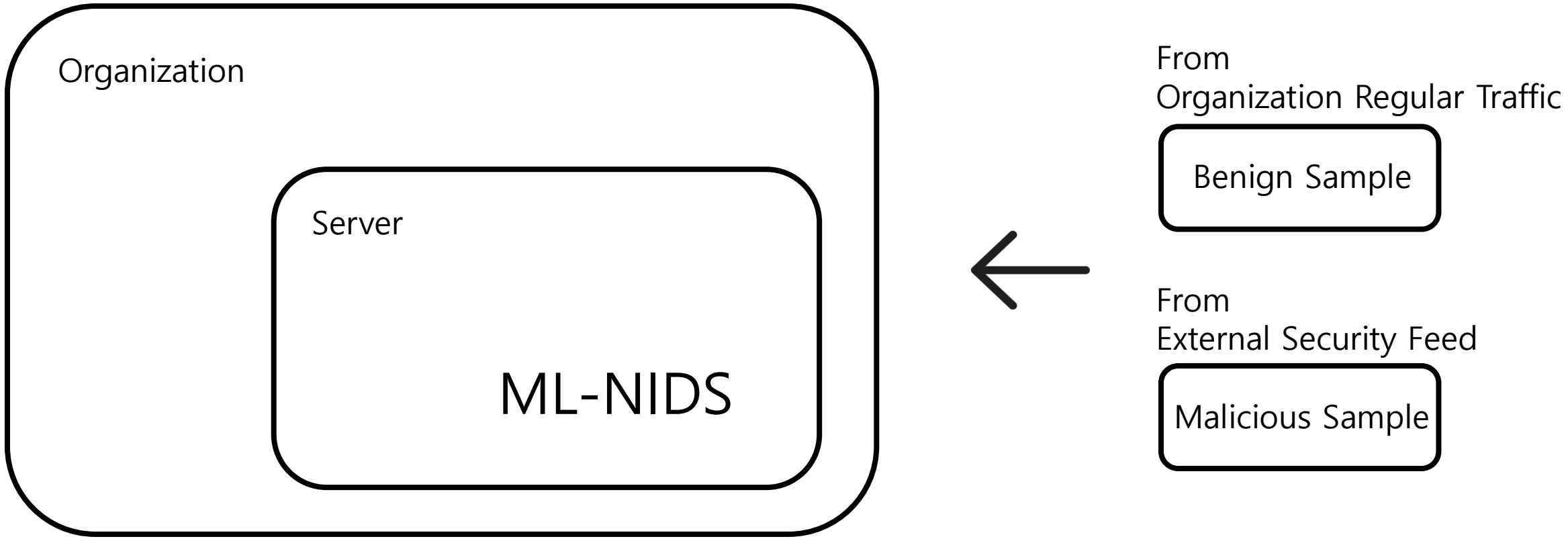
ML-NIDS

1. Can detects even attacks that evade 'signature' based detection method
2. No Human-Intervention
3. Can be used in both 'PAYLOAD analysis' and 'METADATA' analysis

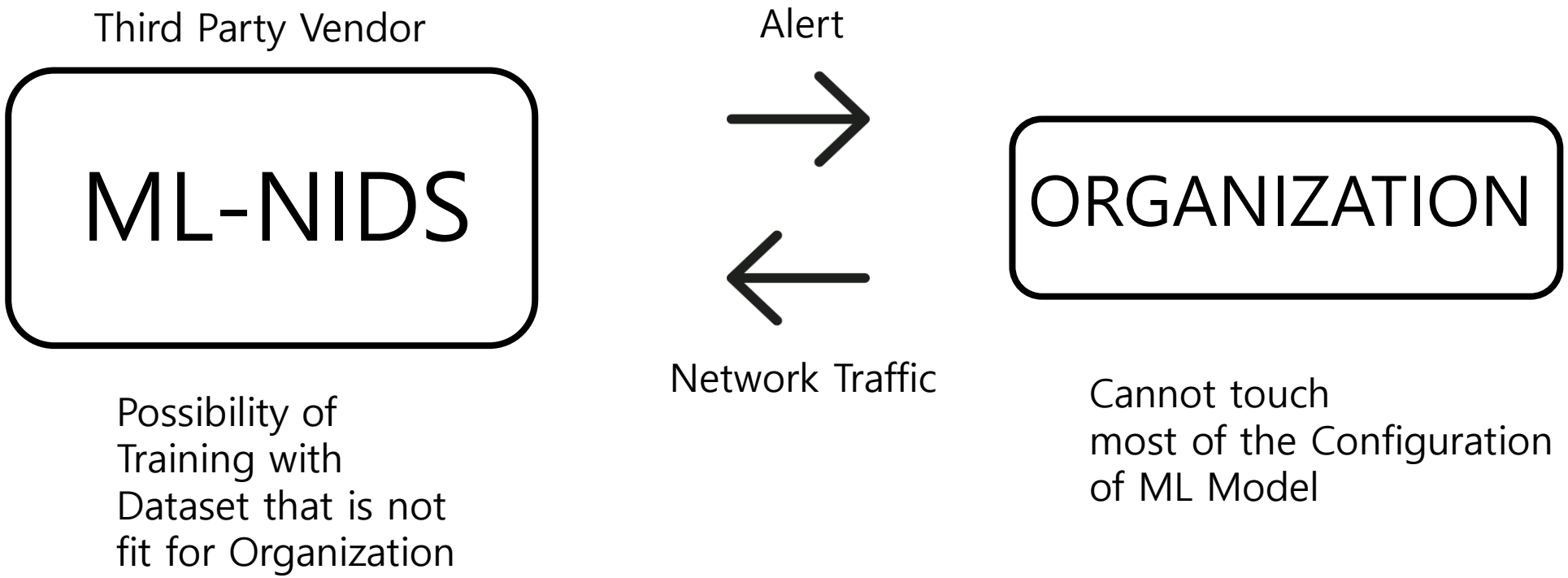
Typical Deployment of NIDS



Solution of ML-NIDS
1st. ML-NIDS on premise



Solution of ML-NIDS
2nd. ML-NIDS from Third Party Vendor



# Weekly Review and Plan

1. Reverse Engineering 스터디 : 뒤로 가면서 내용이 어려워져, 우선 선행 없이 진도를 따라갈 예정
2. 논문 리뷰 : 지금 읽고있는 논문 3주 내로 마무리(공격 배경지식 + 공격 모델링 + 성능과 결론)
3. 앱 크롤러 제작 : 배경지식 공부 완료, 오늘부터 개발 돌입