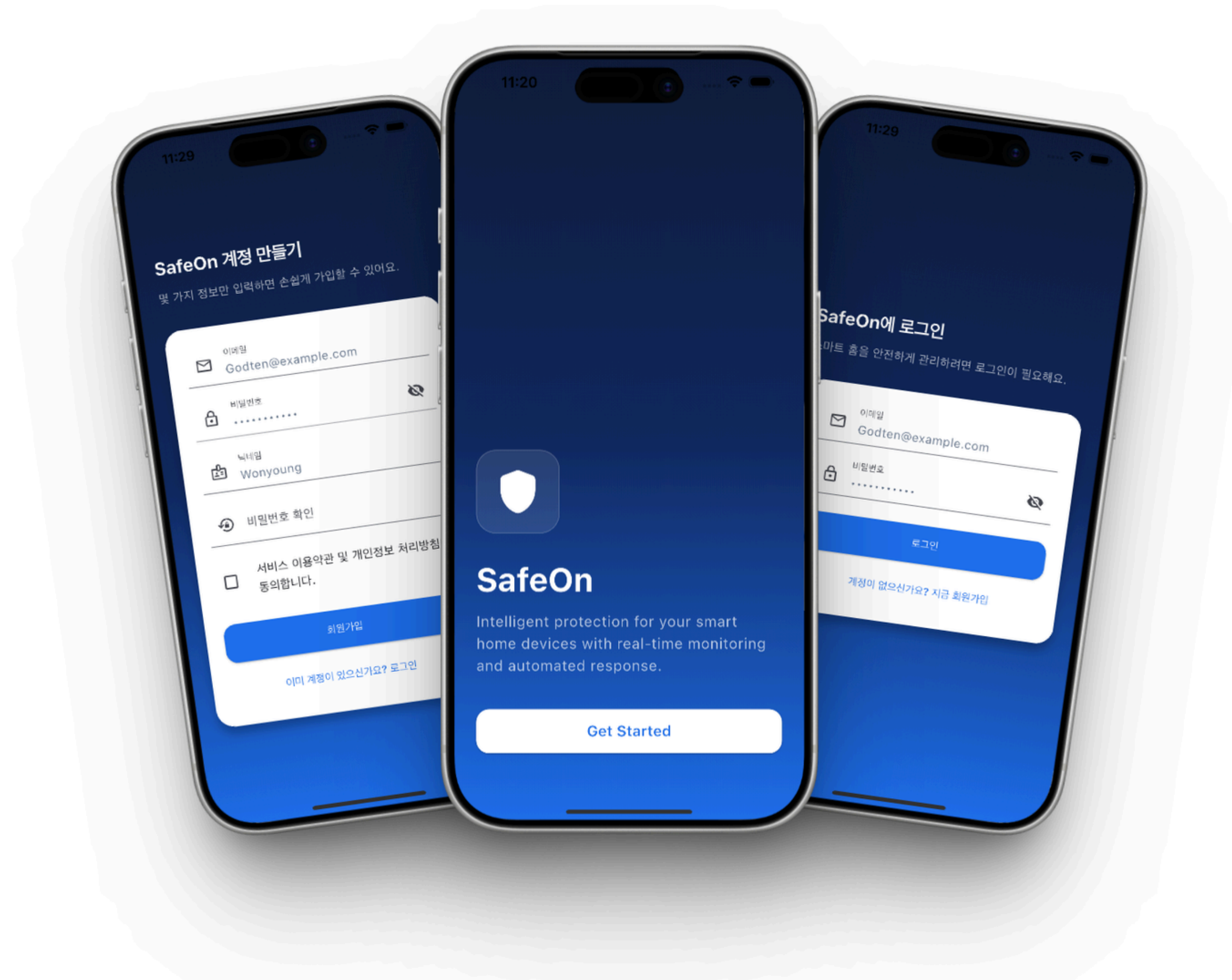


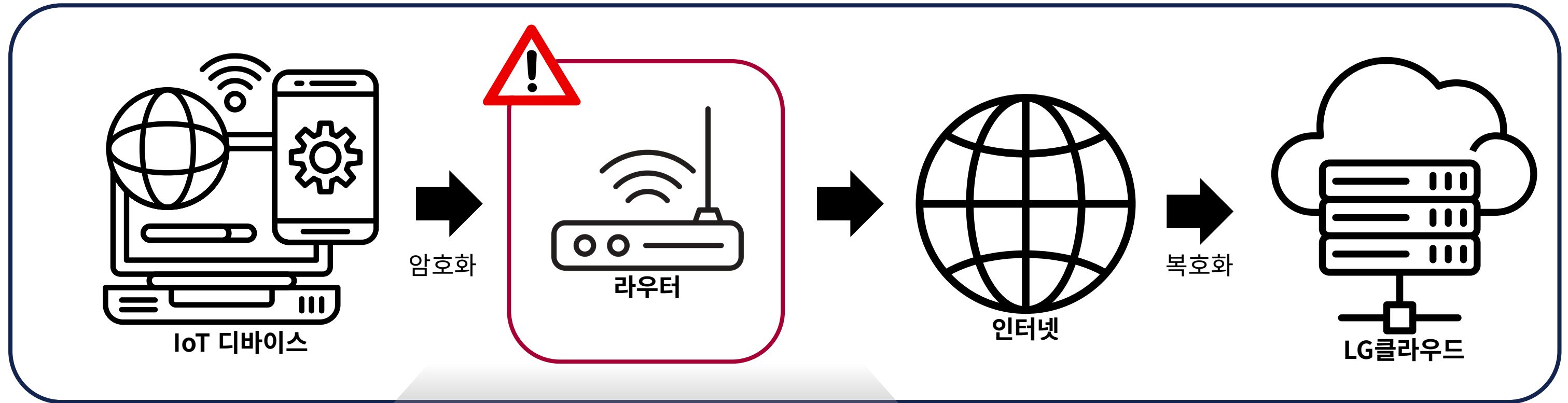


# SafeOn

가정용 IoT를 위한  
엔드포인트 탐지 및 대응 시스템



Current  
System



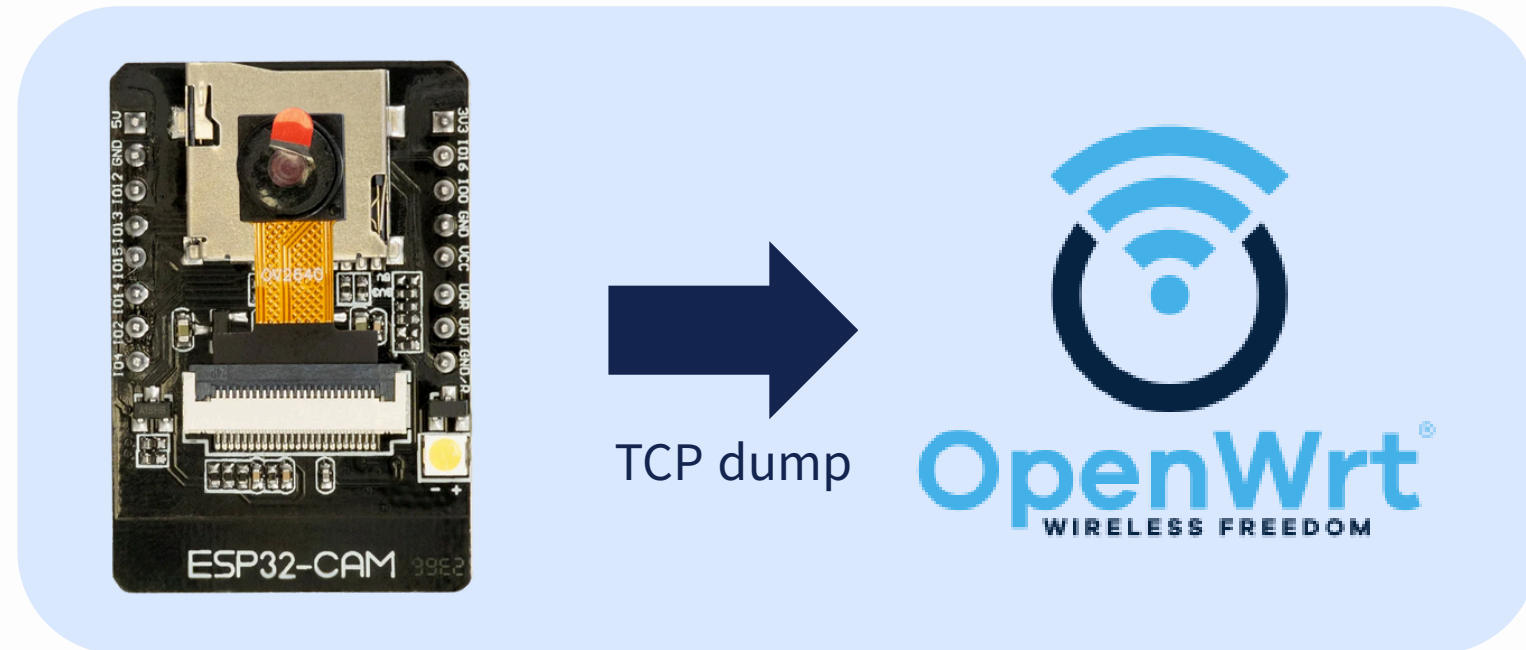
## <문제점>

완전한 암호화  
→ 패킷 내용 분석 불가  
즉, 이상이 발생해도 정상처럼 위장



“보안 사각지대”

# 데이터셋 & 이상치 탐지 방법



	A	B	C	E	F	G	H	I	J	K	L	M	N
1	src_ip	dst_ip	src_port	proto	time	start_time	end_time	duration	packet_count	byte_count	pps	bps	label
2	192.168.0.10	192.168.10.1	34694	6	0	2025-12-0	2025-12-0	0.215693	2	128	9.27239727	593.4334255	0
3	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	1.69277	2	124	118149.4084	7325263.323	0
4	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	1e-06	1	62	1000000	62000000	0
5	192.168.0.10	192.168.10.1	34678	6	0	2025-12-0	2025-12-0	8.821487	2	108	226719.1351	12242833.29	0
6	192.168.0.10	192.168.10.1	34690	6	0	2025-12-0	2025-12-0	1e-06	1	54	1000000	54000000	0
7	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	1e-06	1	62	1000000	62000000	0
8	192.168.0.10	192.168.10.1	34692	6	0	2025-12-0	2025-12-0	1e-06	1	54	1000000	54000000	0
9	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	1e-06	1	62	1000000	62000000	0
10	192.168.0.10	192.168.10.1	34710	6	0	2025-12-0	2025-12-0	0.619527	9	905	14.52720950	1460.791622	0
11	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	0.540084	6	4706	11.10938044	8713.457393	0
12	192.168.0.10	192.168.10.1	34712	6	0	2025-12-0	2025-12-0	0.524655	2	128	3.811998654	243.9679139	0
13	192.168.0.10	192.168.10.1	34720	6	0	2025-12-0	2025-12-0	0.3207	2	128	6.236999200	399.1679488	0
14	192.168.0.10	192.168.10.1	34728	6	0	2025-12-0	2025-12-0	0.430546	2	128	4.645253607	297.2962308	0
15	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	1e-06	1	62	1000000	62000000	0
16	192.168.10.1	192.168.0.10	80	6	0	2025-12-0	2025-12-0	1e-06	1	62	1000000	62000000	0
17	192.168.0.10	192.168.10.1	34730	6	0	2025-12-0	2025-12-0	0.225566	2	128	8.866578655	567.4610339	0

**attacker.csv: 10503 rows**  
**dataset.csv: 28286 rows**

## 하이브리드 탐지 아키텍처

비지도(이상탐지)와 지도(공격 분류) 결합 모델

### 입력 플로우 데이터 (Input)

MinMax 스케일링 전처리



### 비지도 학습

#### Isolation Forest

정상 패턴 학습 & 이상치 탐지

contamination = 0.05  
random\_state = 42

입력: 정상데이터 (Label 0)  
출력: 이상 점수 (0~1)



### 지도 학습

#### Random Forest

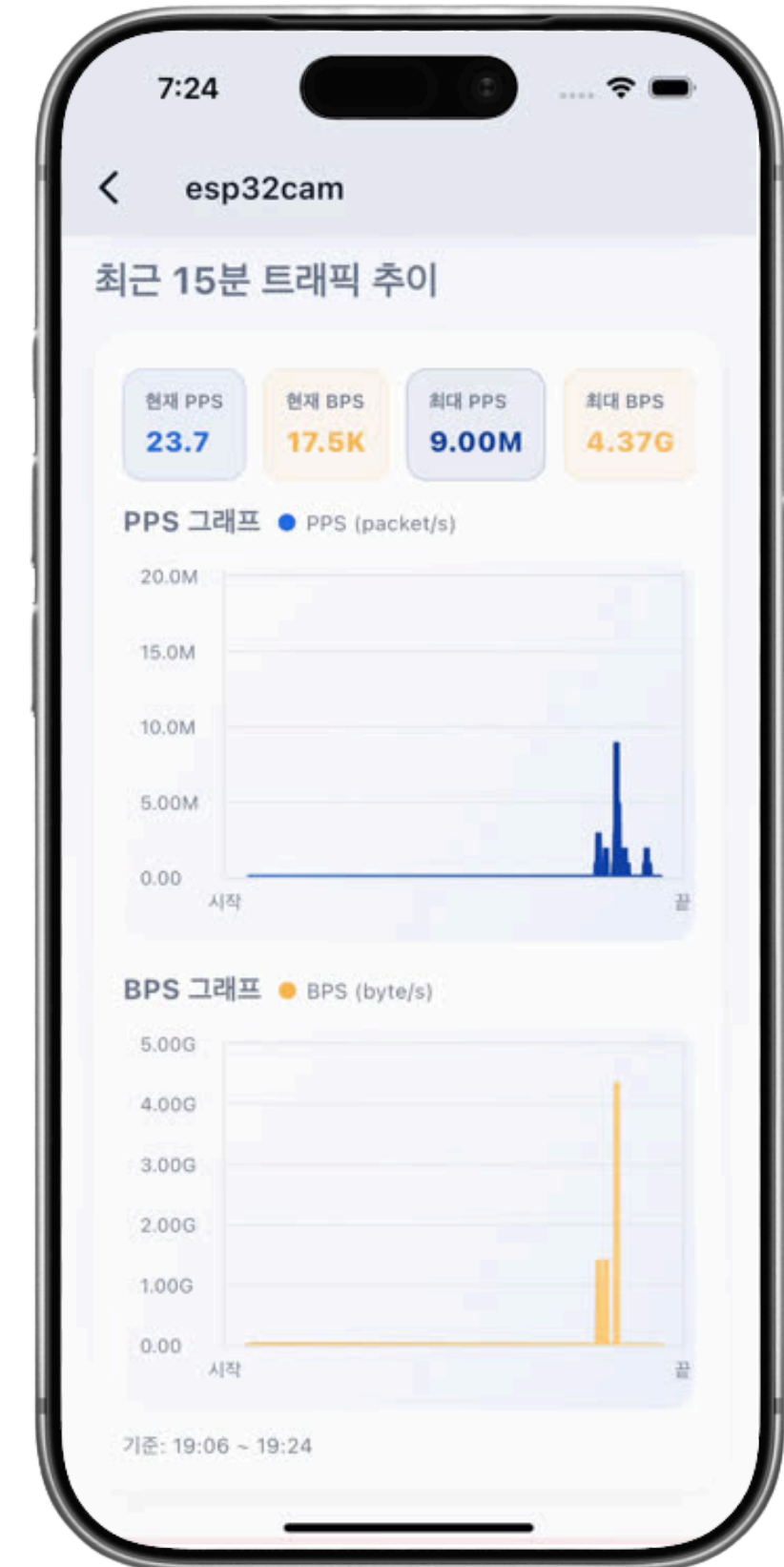
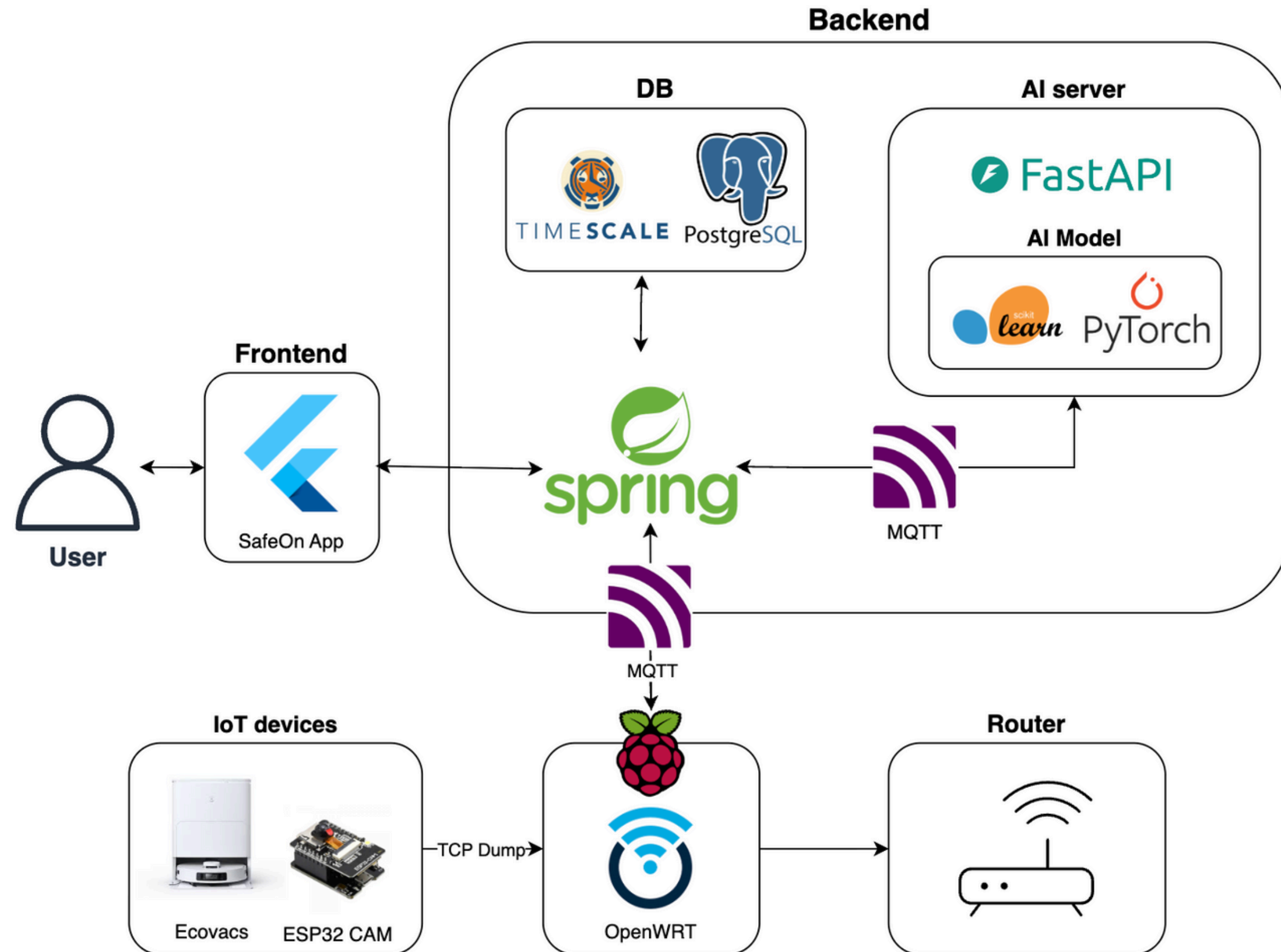
공격 여부 확률 예측

n\_estimators = 0.05  
class\_weight = balanced

입력: 전체데이터 (Label 0/1)  
출력: 공격 확률 (0~1)



# 아키텍처 & 트래픽 추이





**이상 징후 발생**

IoT 디바이스 고장  
또는 해킹 시도



**비정상 패턴 감지**

평소와 다른  
Wi-Fi 사용 패턴



**네트워크 관점 탐지**

패킷 내용을 보지 않고  
**프라이버시 침해 없이**  
정상 / 비정상 판단



**“이상 패턴을 감지하는 순간, SafeOn이 LG 가전을 보호합니다.”**