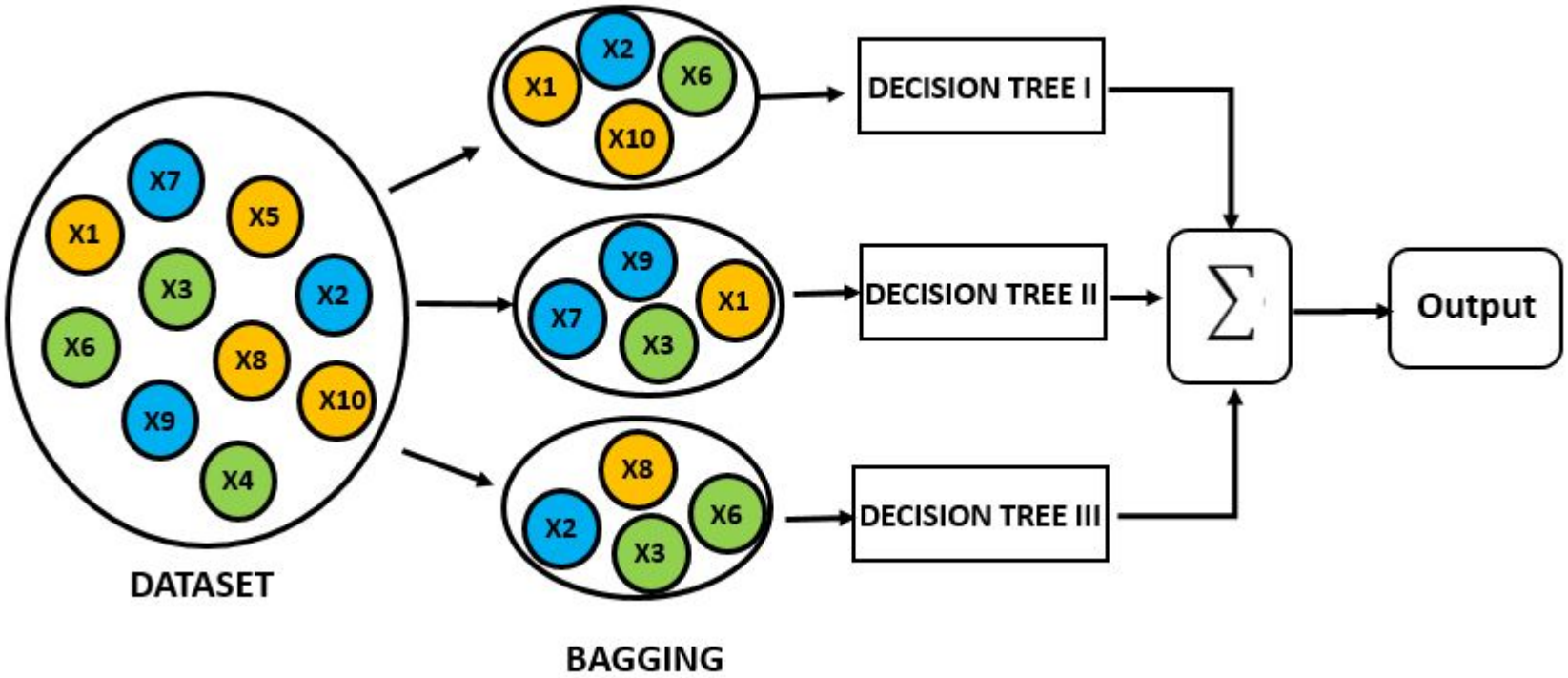
특수보안연구
방화벽로그분석

M2021522 문성현
M2021520 곽상열

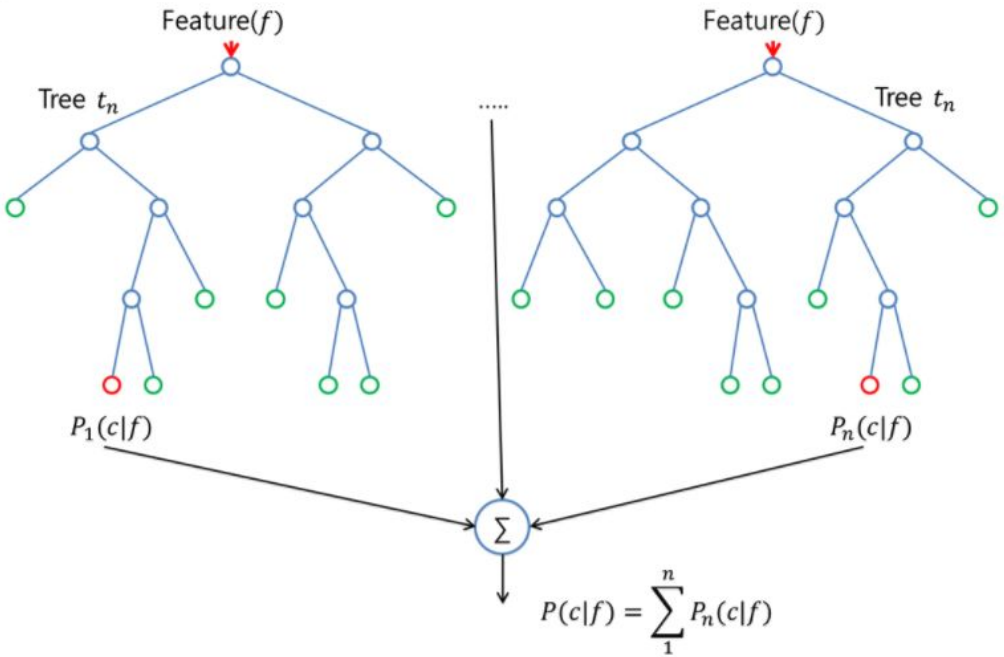
Anomaly Detection Techniques

- Isolation Forest, Random Forest
- One-Class SVM
- Autoencoder
- etc.

Random Forest



Random Forest

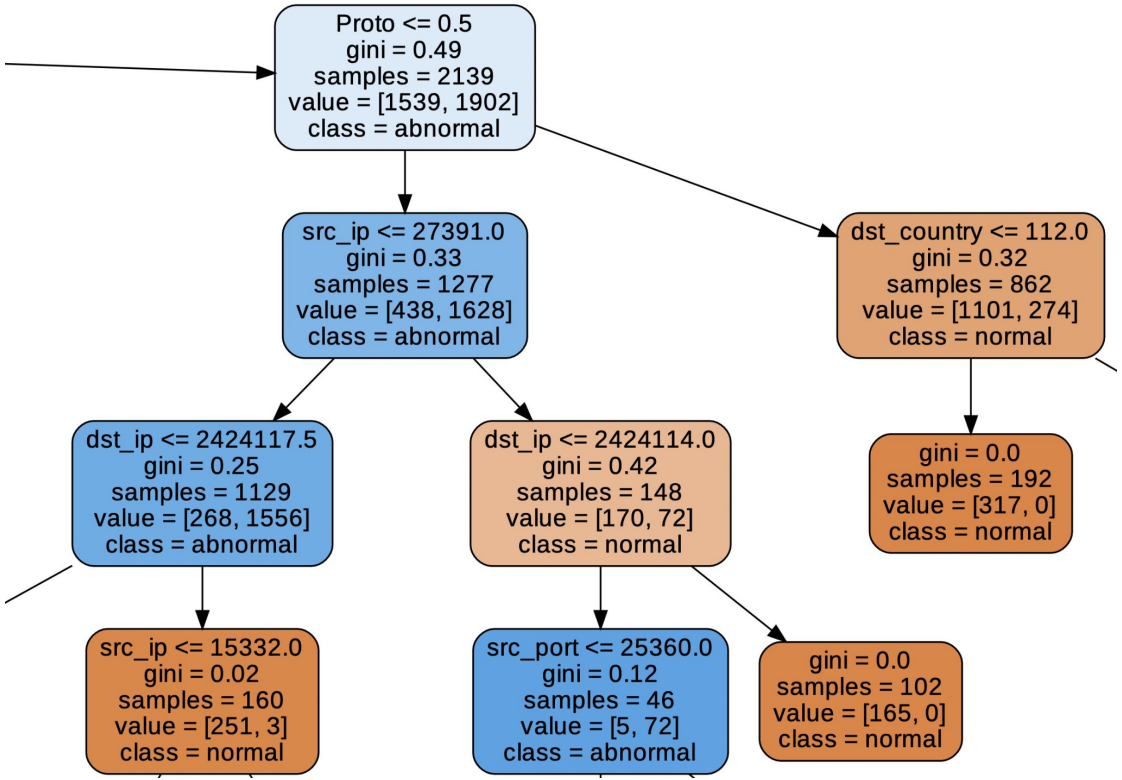


Dataset

	Rdate	src_ip	dst_ip	Proto	src_port	dst_port	Action	src_country	dst_country
0	20210410000018.641	154.58.159.102	103.177.12.42	6	52897	445	2	None	US
1	20210410000018.641	154.58.159.20	125.66.92.196	6	60579	445	2	None	DE
2	20210410000018.641	154.58.159.164	117.121.178.223	6	63831	445	2	None	US
3	20210410000018.641	154.58.159.165	205.34.95.97	6	55241	445	2	None	US
4	20210410000018.641	154.58.159.102	93.56.164.131	6	52898	445	2	None	US

	Rdate	src_ip	dst_ip	Proto	src_port	dst_port	Action	src_country	dst_country
0	2	7607	67542	0	48256	189	1	121	224
1	2	7619	330078	0	55938	189	1	121	54
2	2	7612	225498	0	59190	189	1	121	224
3	2	7613	1282597	0	50600	189	1	121	224
4	2	7607	2674297	0	48257	189	1	121	224

Decision Tree



Score

```
Training results:

Accuracy Score: 0.999977

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00   1915187
           1       1.00      1.00      1.00   2431177

    accuracy                           1.00   4346364
   macro avg       1.00      1.00      1.00   4346364
weighted avg       1.00      1.00      1.00   4346364


Confusion Matrix:
[[1915115      72]
 [     26 2431151]]

Average Accuracy:       0.9996

Standard Deviation:     0.0001
```

```
Test results:

Accuracy Score:0.9995

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00    628409
           1       1.00      1.00      1.00    820380

    accuracy                           1.00   1448789
   macro avg       1.00      1.00      1.00   1448789
weighted avg       1.00      1.00      1.00   1448789


Confusion Matrix:
[[628151    258]
 [   512 819868]]
```

Result

Rdate	src_ip	dst_ip	Proto	src_port	dst_port	src_country	dst_country	predict	Action
18350	7613	504224	0	45737	189	121	165	1	1
18350	7613	1734848	0	45738	189	121	108	1	1
18350	7607	500682	0	48164	189	121	224	1	1
18350	7619	2069083	0	56909	189	121	224	1	1
18350	7613	1910369	0	45751	189	121	41	1	1
18350	7613	2252597	0	45752	189	121	224	1	1
18350	7613	110957	0	45755	189	121	224	1	1
18350	7607	2563130	0	48168	189	121	46	1	1
18350	7612	671170	0	53895	189	121	46	1	1
18350	7612	999107	0	53894	189	121	100	1	1
18350	7607	2190985	0	48167	189	121	37	1	1
18350	3628	2098203	0	54273	5383	33	116	1	1
18350	18167	2423287	0	33443	7165	164	116	1	1
18350	24795	2423164	1	33154	225	164	116	1	1
18350	7619	329418	0	56916	189	121	73	1	1
18350	7612	52976	0	53900	189	121	224	1	1
18350	7607	508360	0	48173	189	121	116	1	1
18350	7607	1105047	0	48176	189	121	30	1	1
18350	7613	1932801	0	45758	189	121	159	1	1
18350	7619	2408087	0	56920	189	121	224	1	1
18350	7613	110328	0	45763	189	121	30	1	1
18350	23989	1659245	0	51941	187	85	90	1	1
18350	3065	555399	0	51407	189	121	100	1	1
18350	7619	788877	0	56923	189	121	224	1	1
18350	7612	273814	0	53905	189	121	108	1	1
18350	27034	2098161	0	49275	187	85	116	1	1
18350	19899	2098205	0	42478	21450	117	116	1	1
18350	7607	2647346	0	48183	189	121	224	1	1
18350	7607	1235288	0	48186	189	121	71	1	1
18350	7619	634795	0	56930	189	121	191	1	1

감사합니다.