Tampere University

Split Without a Leak: Reducing Privacy Leakage in Split Learning

Khoa Nguyen, Tanveer Khan and Antonis Michalas

Tanveer Khan

PhD Researcher,

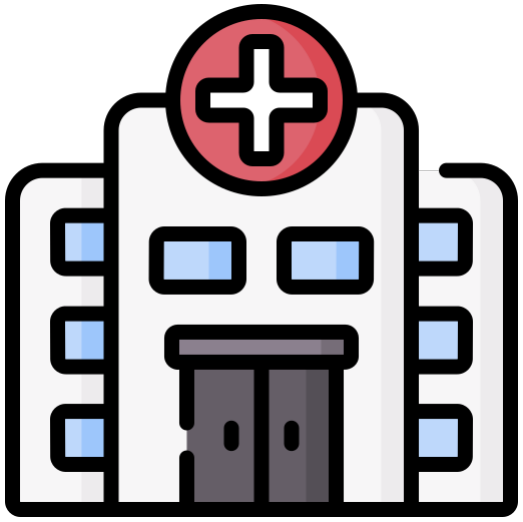
Network and Information Security Group (NISEC),

Tampere University,

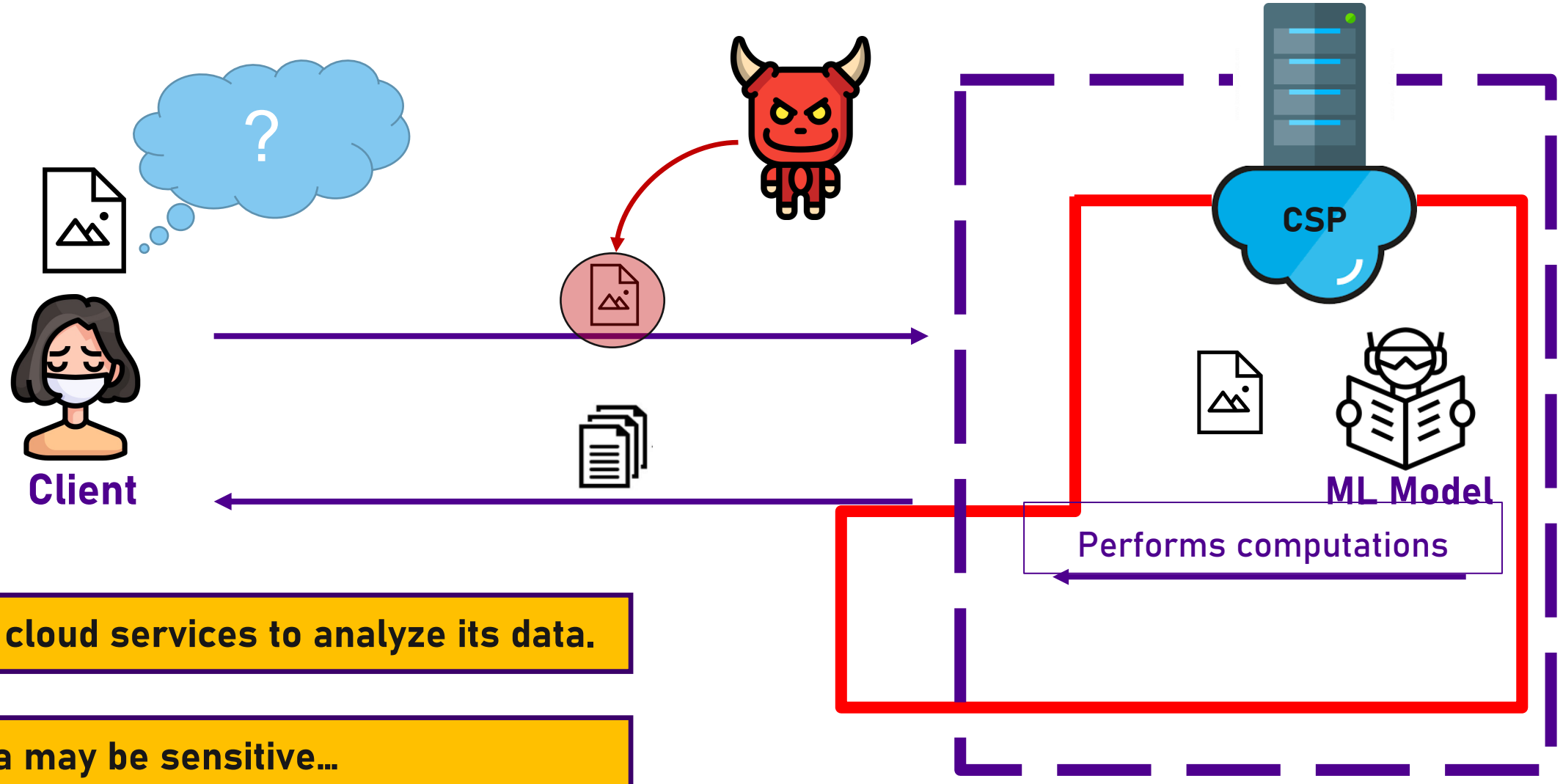
Tampere, Finland

tanveer.khan@tuni.fi

The Big Dream

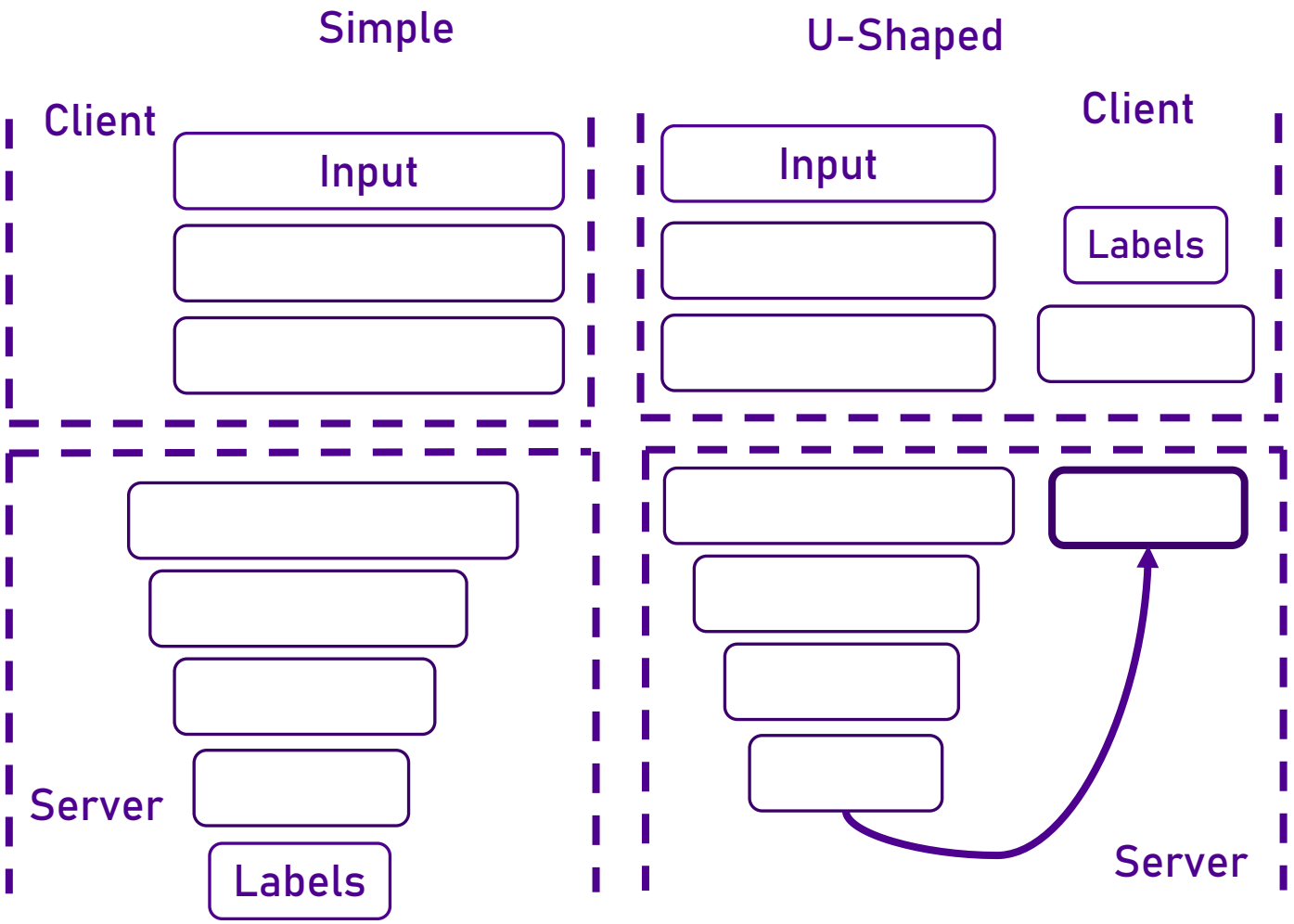


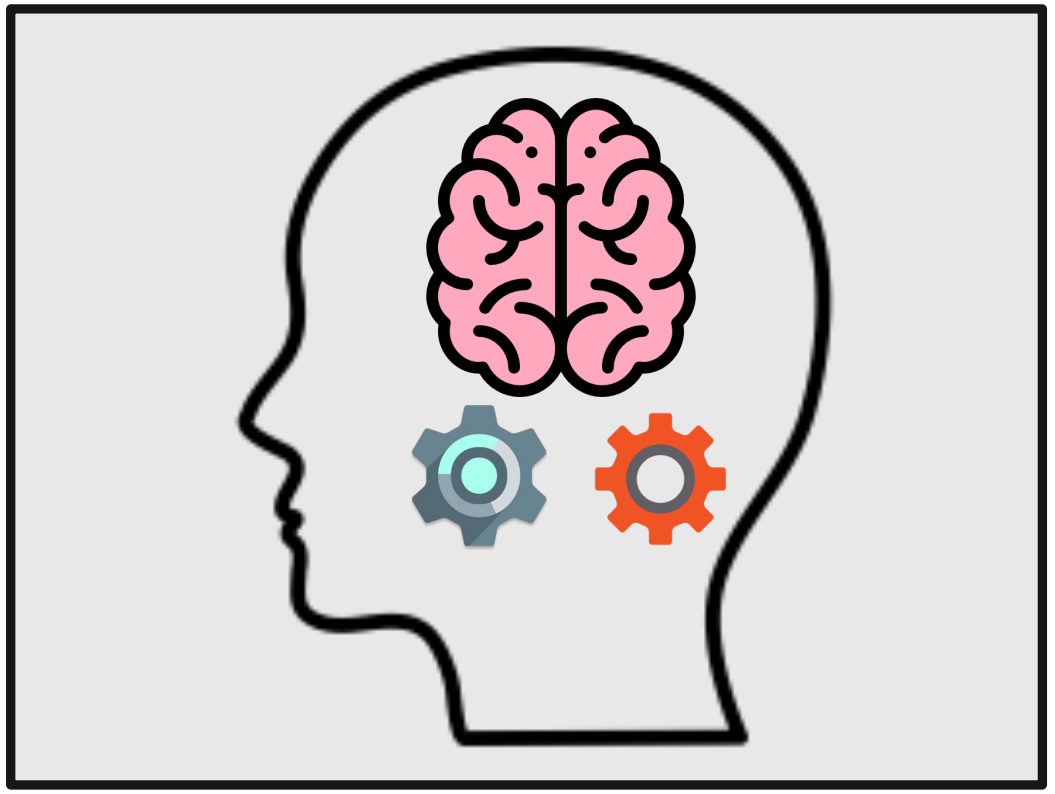
Machine Learning as a Service (MLaaS)



- Client uses cloud services to analyze its data.
- Client's data may be sensitive…

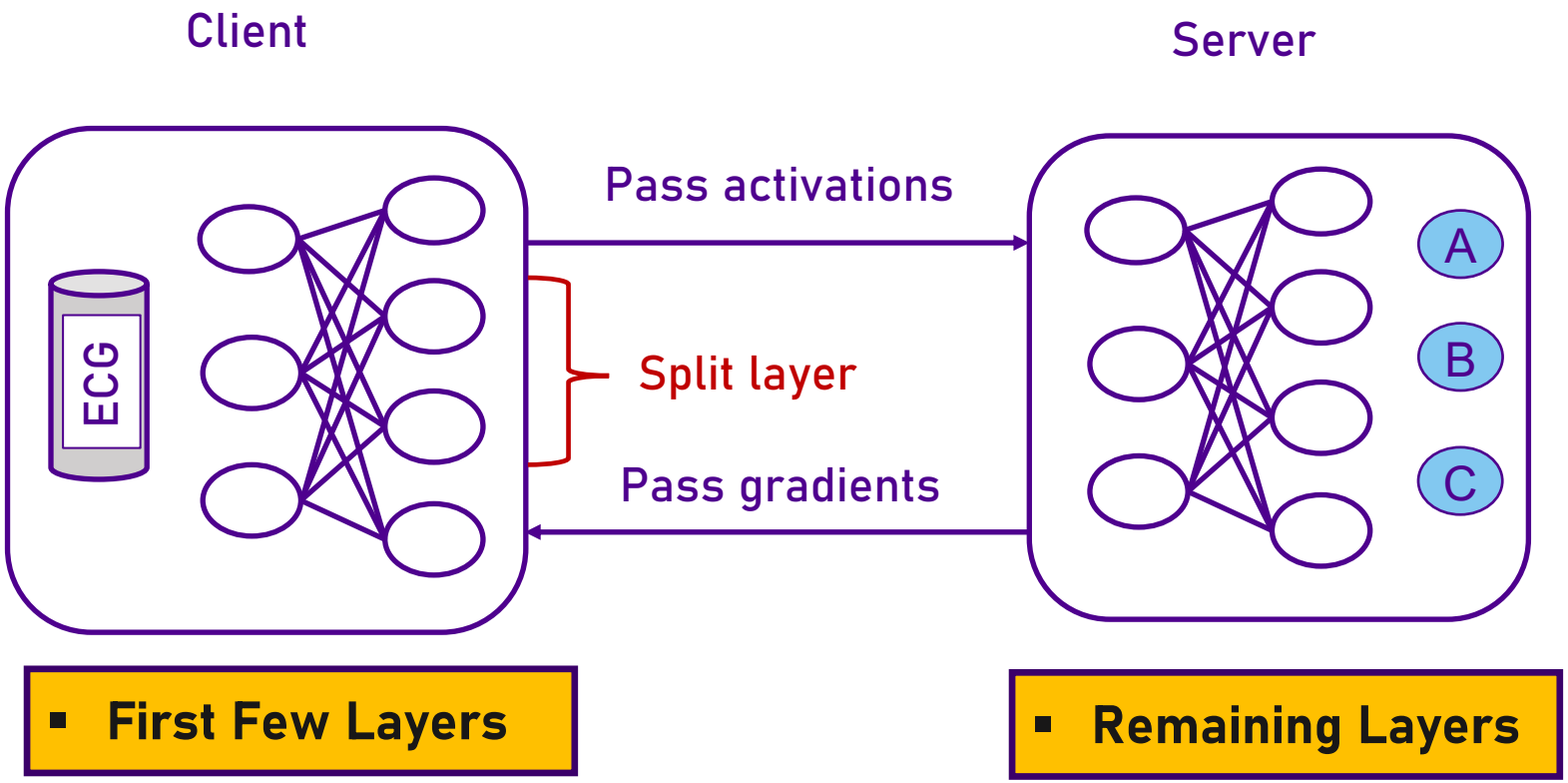
Split learning





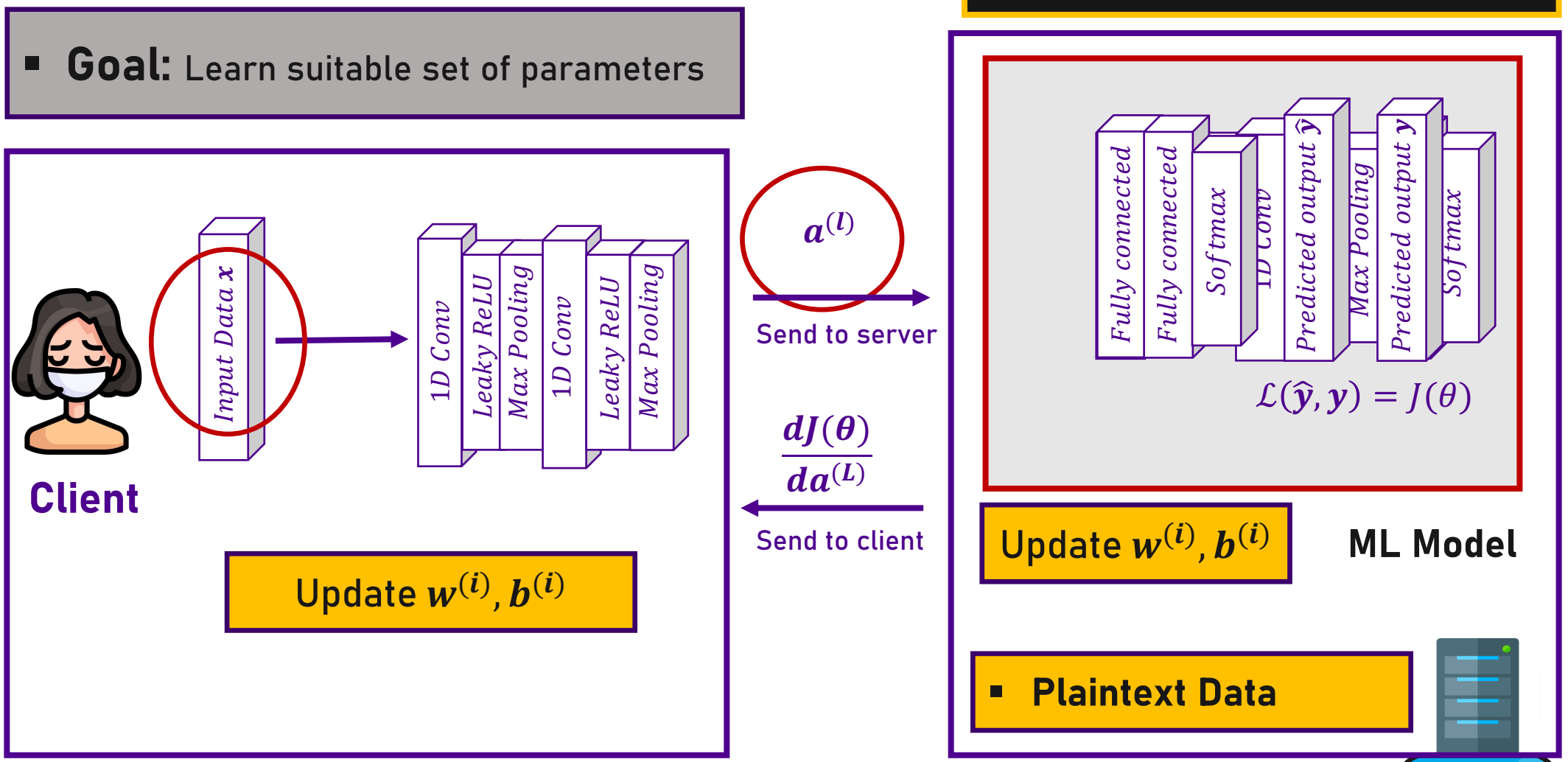
- Take a model (NN) split into multiple parts client part (data lives) send one part to server.

Split Learning Overview



Split Learning (Base Paper)

- **Goal:** Learn suitable set of parameters

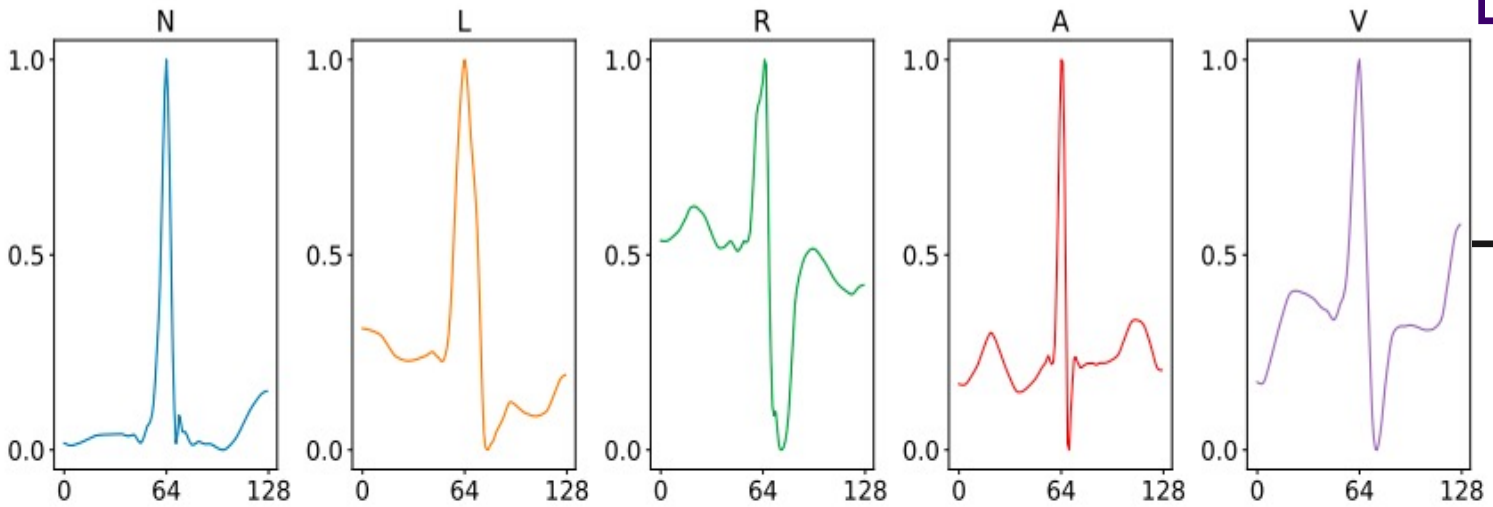


Abuadbba, Sharif, Kyuyeon Kim, Minki Kim, Chandra Thapa, Seyit A. Camtepe, Yansong Gao, Hyoungshick Kim, and Surya Nepal. "*Can we use split learning on 1d cnn models for privacy preserving training?*" In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, pp. 305-318. 2020.

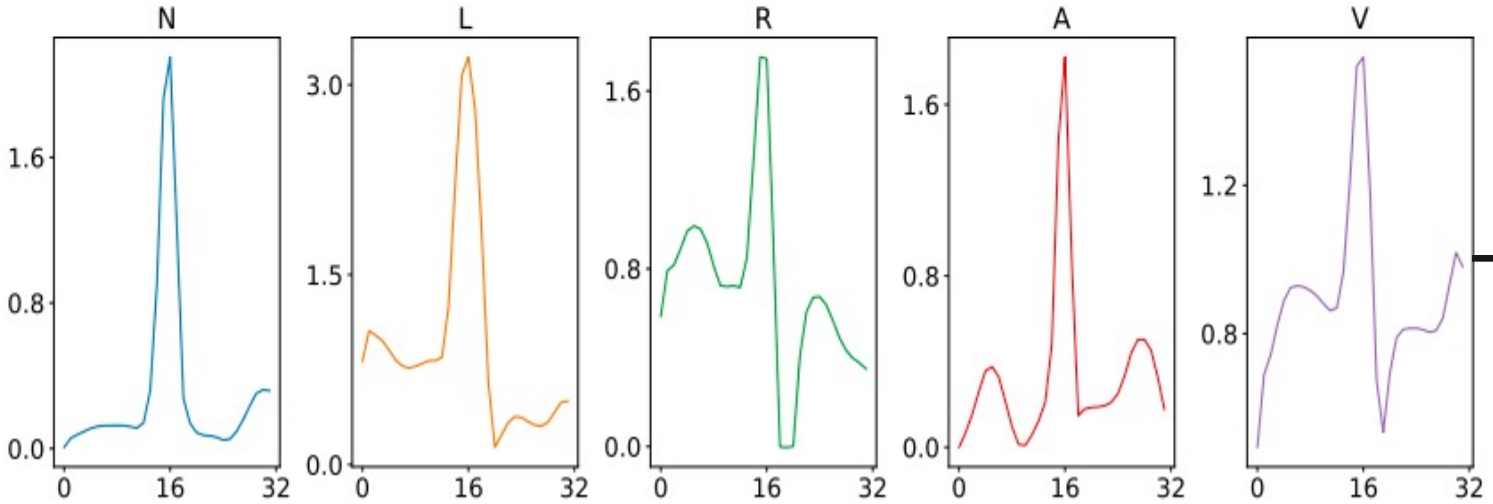
Visual Invertibility

- **Mitigate shortcomings**

1. Add more layers before splitting;
2. Apply differential privacy on split layer activation before send them to the server.

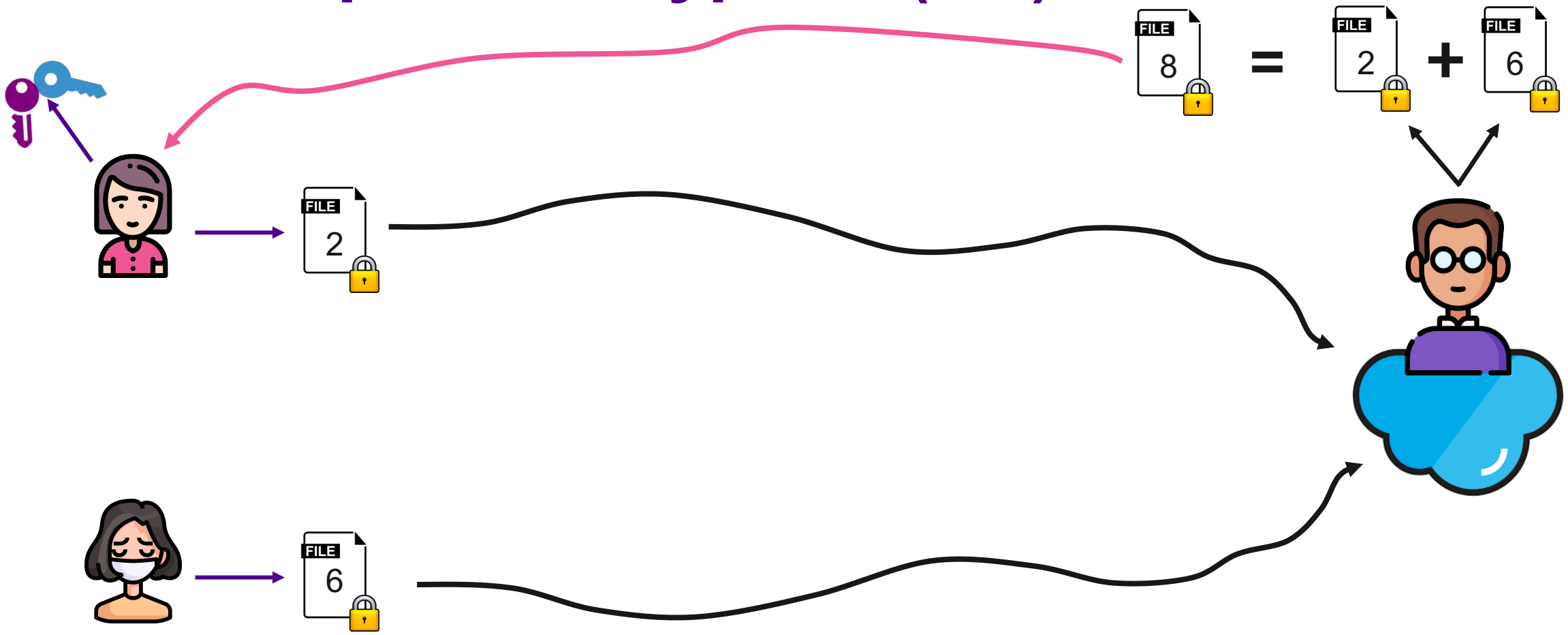


- **Original ECG samples**

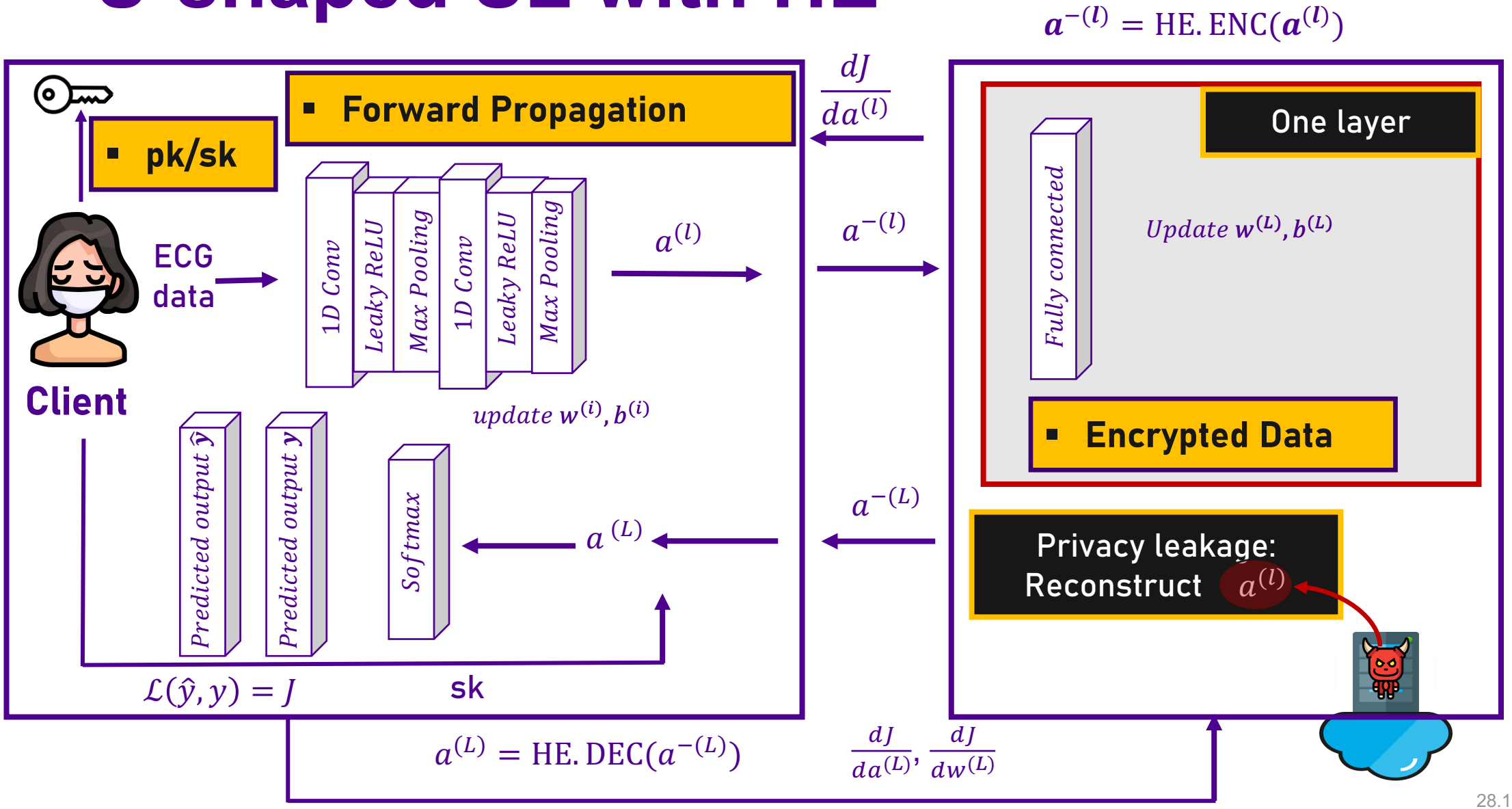


- **Reconstructed samples**

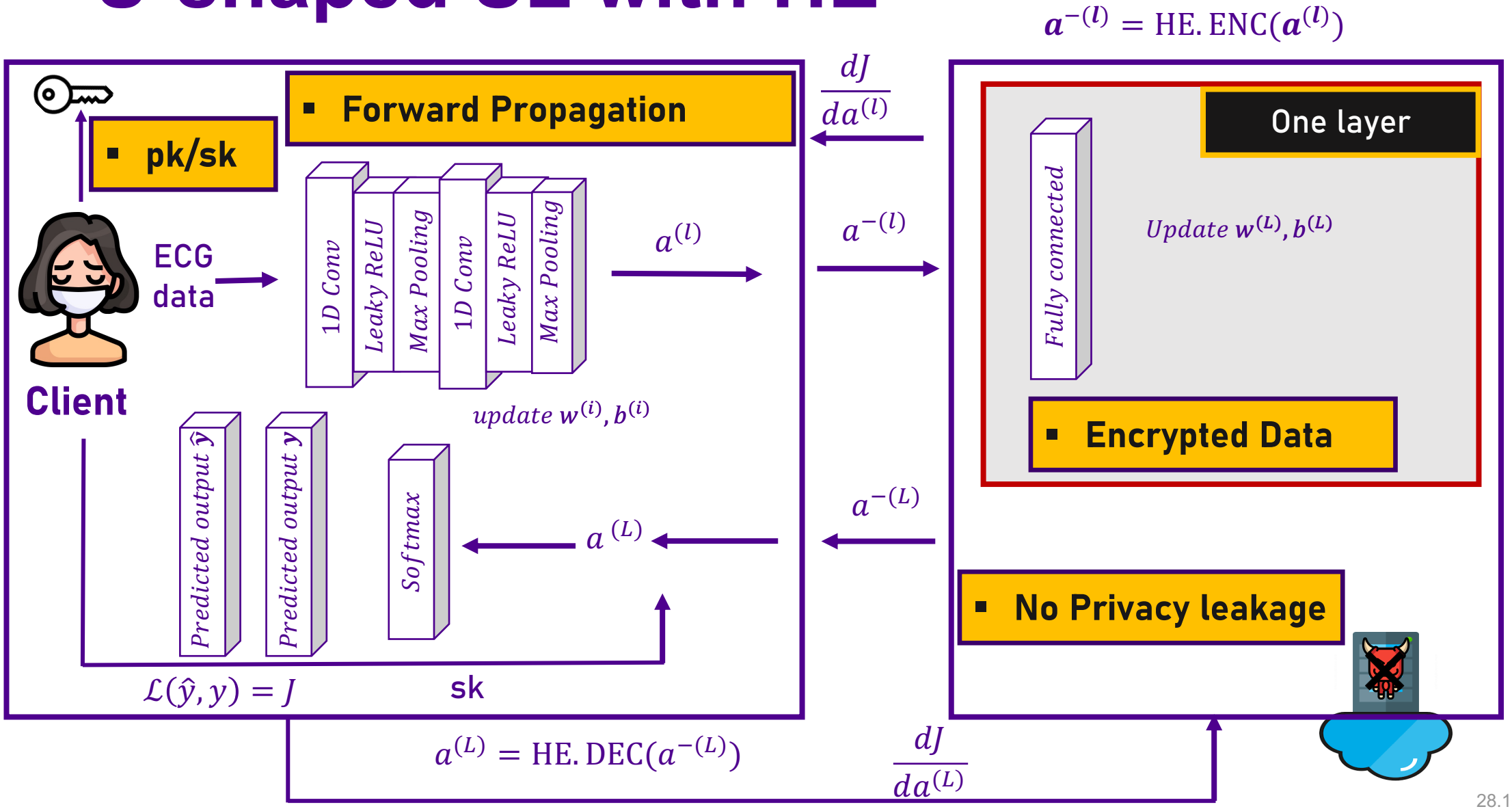
Homomorphic Encryption (HE)



U-shaped SL with HE



U-shaped SL with HE



Experimental Results

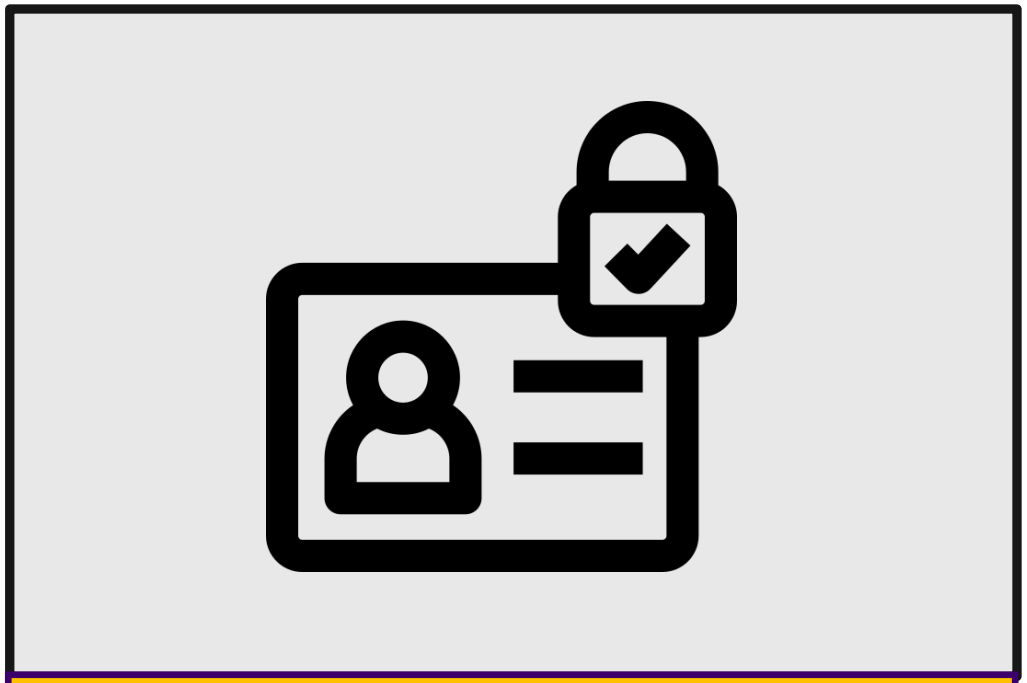
Dataset	HE param set	Batch Size	Accuracy (%)	Training Time (s)	Communication (Gb)
MIT-BIH	S1	4	83.49	8100.60	239.53
		8	78.01	4780.73	121.57
		16	74.77	2855.29	62.58
		32	73.79	1658.73	33.09
		64	62.08	987.42	18.35
	S2	4	83.09	19746.85	471.57
		8	67.94	10378.92	239.33
		16	70.33	5358.59	123.20
		32	72.47	3152.82	65.14
		64	64.42	1913.11	36.11
PTB-XL	S1	4	58.71	100060.60	2624.85
		8	58.95	49334.95	1315.38
		16	57.10	22501.79	660.65
		32	59.36	12370.38	333.23
		64	56.45	5702.29	169.60

Experimental Results

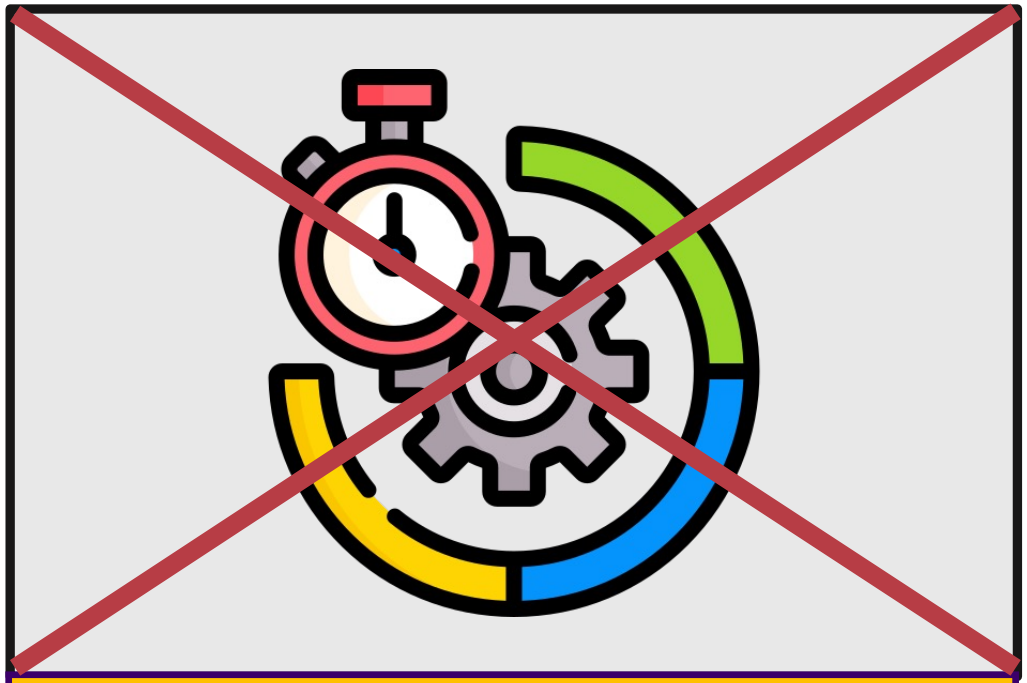
Dataset	Framework	Batch Size	Accuracy (%)	Training Time (s)	Communication (Gb)
MIT-BIH	HESplit	4	83.49	8100.60	239.53
	Split Ways [23]	4	85.31	50318	37840
	Plaintext	4	88.06	8.56	0.033
PTB-XL	HESplit	4	58.71	100060.60	2624.85
	Split Ways [23]	4	65.42	72534	115640
	Plaintext	4	67.68	15.55	0.317

Conclusion

- Our protocol…



- Better Data Privacy



- Efficiency

Tampere University

Thanks!

https://research.tuni.fi/nisec/

Antonis Michalas,

Associate Professor,

Network and Information Security Group (NISEC),

Tampere University,

Tampere, Finland

www.amichalas.com

antonios.michalas@tuni.fi