

	dat_pkt	pkt_sum	pkt_ieee	pkt_len
	0.454645	0.69856	0.646	0.26346
	0.81641	0.987	0.16594	0.39
	0.1684	0.0326	0.1649	0.6974
	0.654	0.63164	0.64979	0.35974
➔	0.369845	0.4175	0.3684	0.14874
	0.002154	0.245584874	0.852456	0.232
	0.265	0.0365453	0.2884	0.1548764
	0.15496	0.7621101	0.5646	0.36498
	0.365994	0.4981	0.6524	0.3484
	0.2021521	0.26	0.1456786	0.151548

	dat_pkt	pkt_sum	pkt_len	pkt_rtt	LABEL
	0.454645	0.69856	0.26346	0.32226	Benign
	0.81641	0.987	0.39	0.32184	Malicious
	0.1684	0.0326	0.6974	0.3154	Benign
	0.654	0.63164	0.35974	0.187	Malicious
	0.369845	0.4175	0.14874	0.1646	Malicious
	0.002154	0.245584874	0.232	0.48	Benign
	0.265	0.0365453	0.1548764	0.564496	Benign
	0.15496	0.7621101	0.36498	0.454	Malicious
	0.365994	0.4981	0.3484	0.34694	Malicious
	0.2021521	0.26	0.151548	0.156465	Malicious

The diagram illustrates a neural network architecture for malware detection. The input is a vector of four x_0 values. The network consists of three hidden layers with 4, 4, and 2 nodes respectively. The output is a vector of two values, 0 and 1, labeled 'Benign' and 'Malicious'. A loss function $\mathcal{L}(\cdot)$ is applied to the output vector.