Of course, bro! Here is a comprehensive breakdown of the data you provided, presented in a clear and human-friendly format.

Overall Performance Metrics

This table provides a high-level overview of how each model performed under two different adversarial attack scenarios: Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD).

Model	Attack Scenario	Overall Accuracy	Overall F1 Macro	Overall AUC OVR	Adversarial Prediction Rate	Natural Data Accuracy	Natural Data F1 Macro
Decision Tree	FGSM	0.756	0.770	0.905	0.581	0.932	0.932
	PGD	0.827	0.831	0.943	0.721	0.932	0.932
Logistic Regression	FGSM	0.682	0.684	0.760	0.499	0.864	0.882
	PGD	0.677	0.681	0.745	0.490	0.864	0.882
DL-FTTransformer	FGSM	0.723	0.727	0.892	0.514	0.932	0.933
	PGD	0.763	0.777	0.936	0.595	0.932	0.933
Calibrated Linear SVC	FGSM	0.475	0.448	0.620	0.074	0.876	0.888

	PGD	0.474	0.447	0.619	0.072	0.876	0.888
XGBoost	FGSM	0.874	0.872	0.965	0.811	0.936	0.936
	PGD	0.887	0.884	0.967	0.837	0.936	0.936
Random Forest	FGSM	0.750	0.764	0.945	0.565	0.934	0.934
	PGD	0.828	0.833	0.958	0.723	0.934	0.934
AdaBoost	FGSM	0.691	0.693	0.903	0.558	0.824	0.858
	PGD	0.845	0.830	0.941	0.865	0.824	0.858
Gaussian Naive Bayes	FGSM	0.365	0.324	0.735	0.000	0.730	0.709
	PGD	0.365	0.329	0.745	0.000	0.730	0.709
LightGBM	FGSM	0.833	0.837	0.954	0.729	0.936	0.937
	PGD	0.860	0.862	0.959	0.783	0.936	0.937
DL-MLP	FGSM	0.933	0.924	0.990	0.933	0.934	0.934
	PGD	0.962	0.951	0.994	0.990	0.934	0.934

Confusion Matrices

The following tables show the confusion matrices for each model under both FGSM and PGD attacks. The labels are:

- **0:** Natural Data (Class 0)
- **1:** Natural Data (Class 1)
- **2:** Adversarial Data

Decision Tree

Attack	True 0	True 1	True 2
FGSM	232305, 17354, 143	16257, 233652, 289	17303, 192345, 290352
PGD	232305, 17354, 143	16257, 233652, 289	8566, 130861, 360573

Logistic Regression

Attack	True 0	True 1	True 2
FGSM	230541, 17342, 1919	29592, 201681, 18925	135403, 115229, 249368
PGD	230541, 17342, 1919	29592, 201681, 18925	159223, 95988, 244789

DL-FTTransformer

Attack	True 0	True 1	True 2
FGSM	231458, 18056, 288	15238, 234539, 421	141903, 101061, 257036
PGD	231458, 18056, 288	15238, 234539, 421	11991, 190658, 297351

Calibrated LinearSVC

Attack	True 0	True 1	True 2
FGSM	229522, 20039, 241	27687, 208678, 13833	250392, 212382, 37226
PGD	229522, 20039, 241	27687, 208678, 13833	250392, 213632, 35976

XGBoost

Attack	True 0	True 1	True 2
FGSM	233691, 16098, 13	15610, 234350, 238	6918, 87424, 405658
PGD	233691, 16098, 13	15610, 234350, 238	86, 81403, 418511

Random Forest

Attack	True 0	True 1	True 2
FGSM	232148, 17644, 10	15001, 234969, 228	18695, 198859, 282446
PGD	232148, 17644, 10	15001, 234969, 228	8938, 129782, 361280

AdaBoost

Attack	True 0	True 1	True 2
FGSM	231232, 18570, 0	26043, 180786, 43369	76473, 144662, 278865
PGD	231232, 18570, 0	26043, 180786, 43369	30772, 36710, 432518

Gaussian Naive Bayes

Attack	True 0	True 1	True 2
FGSM	249778, 10, 14	135129, 115050, 19	115557, 384408, 35
PGD	249778, 10, 14	135129, 115050, 19	91168, 408797, 35

LightGBM

Attack	True 0	True 1	True 2
FGSM	233784, 15996, 22	15485, 234414, 299	5992, 129677, 364331
PGD	233784, 15996, 22	15485, 234414, 299	226, 108192, 391582

DL-MLP

Attack	True 0	True 1	True 2
FGSM	232188, 17590, 24	15331, 234815, 52	14346, 19382, 466272
PGD	232188, 17590, 24	15331, 234815, 52	116, 4941, 494943

Summary of Findings

This analysis evaluates the performance of ten different machine learning models against adversarial attacks. The key takeaways are:

- **Top Performer:** The **DL-MLP** model is the clear winner, demonstrating exceptional resilience to both FGSM and PGD attacks. It achieves the highest overall accuracy, F1 scores, and adversarial prediction rates.
- **Strong Contenders: XGBoost** and **LightGBM** also show strong performance, with high accuracy and good adversarial detection rates, making them reliable choices.
- **Worst Performers: Gaussian Naive Bayes** and **Calibrated LinearSVC** are the most vulnerable models. They have very low accuracy and struggle significantly to identify adversarial samples.
- **PGD is a Stronger Attack:** In most cases, the PGD attack is more effective at fooling the models than the FGSM attack. This is evident from the lower overall accuracy and adversarial prediction rates when models are subjected to PGD.

- **Natural Data Performance:** Most models perform well on natural data, with accuracy scores typically above 93%. This indicates that the models are well-trained for normal conditions but vary greatly in their robustness to attacks.

Model-by-Model Description

Here's a detailed breakdown of each model's performance:

Decision Tree

The Decision Tree model performs moderately well. It has a decent accuracy of around 75-82% and is fairly good at detecting adversarial samples. However, it is more vulnerable to FGSM attacks compared to PGD.

Logistic Regression

This model is not very resilient to adversarial attacks. It has a low accuracy of around 68% and struggles to correctly classify adversarial data, with a prediction rate of just under 50%. It is one of the weaker models in this comparison.

DL-FTTransformer

This deep learning model shows promise but is not as robust as the DL-MLP. Its performance is moderate, with an accuracy of 72-76%. While it outperforms some of the simpler models, it is still significantly impacted by adversarial attacks.

Calibrated LinearSVC

This is one of the worst-performing models. It has an accuracy below 50% and a very low adversarial prediction rate (around 7%). This model is highly susceptible to being fooled by adversarial examples.

XGBoost

XGBoost is a top-tier performer. It boasts an accuracy of over 87% and is very effective at identifying adversarial inputs, with a detection rate of over 81%. This makes it a very reliable model in adversarial environments.

Random Forest

Similar to the Decision Tree, the Random Forest model offers moderate performance. Its accuracy is in the range of 75-82%, and it has a reasonable ability to detect adversarial samples. It is a solid, if not spectacular, choice.

AdaBoost

AdaBoost's performance is a mixed bag. It struggles against FGSM attacks but shows a surprising resilience to PGD, with its accuracy jumping from 69% to 84%. This suggests its robustness is highly dependent on the type of attack.

Gaussian Naive Bayes

This model performs very poorly. It has the lowest accuracy of all the models (around 36%) and completely fails to detect adversarial samples (0% prediction rate). It is not a suitable choice for environments where adversarial attacks are a concern.

LightGBM

LightGBM is another strong performer, rivaling XGBoost. It achieves high accuracy (83-86%) and a good adversarial detection rate (72-78%). It is a robust and reliable model.

DL-MLP

The DL-MLP is the standout model. It achieves over 93% accuracy against FGSM and over 96% against PGD. Its ability to detect adversarial samples is exceptional, with a prediction rate of over 93% for both attack types. This model is highly resilient and the best choice for this task.