ID	Name	Goal of the Attack	Tactics	Techniques	Possible Attacks	Mitigations
D001	Attack in data collection	Resulting in some bias or altering the output.	AML.TA0003 - Resource Development	AML.T0019 - Publish Poisoned Datasets, AML.T0020 - Poison Training Data	Adversarial Example in the Physical domain	AML.M0001- Limit Model Artifact Release, AML.M0005 - Control Access to ML Models and Data at Rest, AML.M0007 - Sanitize Training Data
			AML.TA0004 - Initial Access	AML.T0010.002 - ML Supply Chain Compromise: Data		
			AML.TA0006 - Persistence	AML.T0020 - Poison Training Data		
D002	Attack to data storage	The attacker can aim to obtain some data or alter the data to change the output	TA0040 - Impact	T1485 - Data Destruction, T1486 - Data Encrypted for Impact, T1565 - Data Manipulation,	Perturbation attacks, Poisoning attacks, Data Leak,	M1041 - Encrypt Sensitive Information, M1041 - Encrypt Sensitive Information, M1029 - Remote Data Storage, M1022 - Restrict File and Directory Permissions
D003	Attack through training	The attacker aims gaining access to model architecture to perturbate model outputs or gain access to filesystem.	AML.TA0002 - Reconnaissance	AML.T0000 - Search for Victim's Publicly Available Research Materials	The adversary can use this information to identify targets for attack, or to tailor an existing attack to make it more effective	AML.M0000 - Limit Release of Public Information
			AML.TA0004 - Initial Access	AML.T0010.003 - ML Supply Chain Compromise: Model	Model poisoning, input manipulation, availability attacks (Gradient and GAN-based)	AML.M0007 - Sanitize Training Data, AML.M0005 - Control Access to ML Models and Data at Rest
			AML.TA0001 - ML Attack Staging	AML.T0018 - Backdoor ML Model	Introduce a backdoor by training the model poisoned data, or by interfering with its training process.	AML.M0007 - Sanitize Training Data, AML.M0005 - Control Access to ML Models and Data at Rest, AML.M0008 - Validate ML Model
			AML.TA0000 - ML Model Access	AML.T0044 - Full ML Model Access	Gaining full white-box access to	AML.M0017 - Model Distribution Methods
D004	Attack through testing	Testing is a part of training process, so all the tactics and techniques are valid for this AP. But, we included this attack point for additional attacks.	AML.TA0000 - ML Model Access	AML.T0044 - Full ML Model Access	Incomplete Testing in Realistic conditions	Bias and fairness checks, Benefiting AI Governance methods
D005	Attack on trained model storage	Degrading the performace or reverse engineering.	TA0040 - Impact	T1485 - Data Destruction, T1486 - Data Encrypted for Impact, T1565 - Data Manipulation,	Perturbation attacks, Poisoning attacks, Data Leak,	M1041 - Encrypt Sensitive Information, M1041 - Encrypt Sensitive Information, M1029 - Remote Data Storage, M1022 - Restrict File and Directory Permissions
			AML.TA0011 - Impact	AML.T0031 - Erode ML Model Integrity	Model stealing, Reprogramming deep neural nets, ML Supply Chain Attack, Model inversion, Membership Inference attack, Distributional shifts	AML.M003 - Model Hardening, AML.M0006 - Use Ensemble Methods, AML.M0010 - Input Restoration, AML.M0015 - Adversarial Input Detection
D006	Attack through inference	They misuse the system, run expensive queries, or exfiltrate private information via ML Model Inference API Access.	AML.TA0010 - Exfiltration	AML.T0024 - Exfiltration via ML Inference API	Inferring Training Data Membership, Inverting ML Model	AML.M0002 - Passive ML Output Obfuscation, AML.M0004 - Restrict Number of ML Model Queries,
			AML.TA0011 - Impact	AML.T0034 - Cost Harvesting, AML.T0045 - ML Intellectual Property Theft, AML.T0048 - System Misuse for External Effect	Prompt crafting	AML.M0004 - Restrict Number of ML Model Queries, AML.M0005 - Control Access to ML Models and Data at Rest