# Lab 8 - Data Security & Privacy

## Jonathan Chacko – 133659243

## A1G 150

## Introduction:

In today's increasingly data-driven world, ensuring the security and privacy of information is not only a technical challenge but also a critical business imperative. As organizations embrace machine learning (ML) to drive innovation and gain insights, they also face new vulnerabilities and ethical dilemmas associated with managing large, diverse datasets. This lab focuses on identifying and applying the most appropriate security tools to protect data throughout the ML lifecycle, from data collection and preprocessing to model training and deployment.

Machine learning activities inherently involve handling sensitive and personal data, which raises significant privacy concerns and potential ethical issues. Protecting this data requires a thorough understanding of both the security mechanisms available and the broader implications of data misuse. In this lab, we explore key ML activities and align them with effective security tools, while also addressing privacy implications and ethical considerations. By evaluating various security strategies and their corresponding privacy safeguards, this report aims to provide a comprehensive guide on mitigating risks and ensuring ethical data practices in machine learning projects.

## Key Machine Learning Activities:

1. Data Lifecycle Management - The process of managing data throughout its lifecycle.
2. Data Collection - The process of gathering data from various sources.
3. Data Processing - The process of cleaning, transforming, and preparing data for analysis.
4. Data Storage - The process of storing data in a secure and accessible manner.
5. Data Usage - The process of using data to train machine learning models.
6. Data Archiving - The process of storing data for future reference.
7. Data Destruction - The process of securely deleting data that is no longer needed.
8. Model Lifecycle Management - The process of training machine learning models on data.
9. Model Training - The process of training machine learning models on data.
10. Model Evaluation - The process of evaluating the performance of machine learning models.
11. Model Deployment - The process of deploying machine learning models into production.
12. Model Monitoring & Maintenance - Continuously tracking model performance and updating as necessary.

## Table 1 – Tools Used in ML Activities & what Protection they Offer.

|  |  |  |
| --- | --- | --- |
| **ML Activity** | **Tool** | **What protection it offers?** |
| *Data Collection* | VPN | Encrypts data in transit to protect against eavesdropping. |
| *Data Processing* | Data Masking | Replaces sensitive data with fake data to protect privacy. |
| *Data Storage* | Encryption | Encrypts data at rest to protect against unauthorized access. |
| *Data Usage* | Access Control | Restricts access to data to authorized users only. |
| *Data Archiving* | Data Backup | Creates copies of data to prevent data loss. |
| *Data Destruction* | Data Erasure | Securely deletes data to prevent data recovery. |
| *Model Training* | Differential Privacy | Adds noise to data to protect individual privacy. |
| *Model Evaluation* | Model Explainability | Provides insights into how models make decisions. |
| *Model Deployment* | Model Versioning | Tracks changes to models over time. |
| *Model Monitoring & Maintenance* | Model Performance Monitoring | Tracks model performance metrics over time. |

## Table 2 – Possible Issues in ML Activities & How to mitigate.

|  |  |  |
| --- | --- | --- |
| **ML Activity** | **Tool** | **What protection it offers?** |
| *Data Collection* | Data Breach | Use encryption to protect data in transit. |
| *Data Processing* | Data Leakage | Use data masking to protect sensitive data. |
| *Data Storage* | Data Loss | Use encryption to protect data at rest. |
| *Data Usage* | Unauthorized Access | Use access control to restrict access to data. |
| *Data Archiving* | Data Corruption | Use data backup to create copies of data. |
| *Data Destruction* | Data Recovery | Use data erasure to securely delete data. |
| *Model Training* | Model Bias | Use differential privacy to protect individual privacy. |
| *Model Evaluation* | Model Explainability | Use model explainability to understand model decisions. |
| *Model Deployment* | Model Drift | Use model versioning to track changes to models. |
| *Model Monitoring & Maintenance* | Model Performance Degradation | Use model performance monitoring to track model performance metrics. |