CS 6301.0U1 Project Name: Vibha Belavadi Netid: vxb141530

Project on: Differential Privacy based Access control

This project is an implementation of Differential Privacy based access control taken from the book: On the Move to Meaningful Internet Systems: OTM 2016 Conferences.

In this project based on the privacy clearance of the user (low risk, medium risk, medium-high risk and high risk), the data access is provided with or without noise addition.

A low risk user, typically the admin/owner of the database can view either the complete table or the aggregated values, aggregation being based on education and income levels and values being the number of records for the given education income value.

As the user privacy clearance decreases (goes from medium risk to high risk), the randomness added to the data increases and error from the actual value of records also increases. This deviation is measured by the normalized error rate.

The following use cases were implemented, as adapted from the paper:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Role | Operation | Risk | Utility |
| 1 | HR Manager | HR view (internal) | Low Risk | Full access |
| 2 | HR Manager | HR view (external) | Medium Risk | Aggregated |
| 3 | HR Developer | Testing data | Medium-High Risk | Anonymized |
| 4 | HR Benchmarking | Benchmark | High Risk | Anonymized |

The parameter used:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Role | Operation | Risk | Privacy Clearance |
| 1 | HR Manager | HR view (internal) | Low Risk | T > 1 |
| 2 | HR Manager | HR view (external) | Medium Risk | T ]0.1, 1] |
| 3 | HR Developer | Testing data | Medium-High Risk | T ]0.05, 0.1] |
| 4 | HR Benchmarking | Benchmark | High Risk | T |

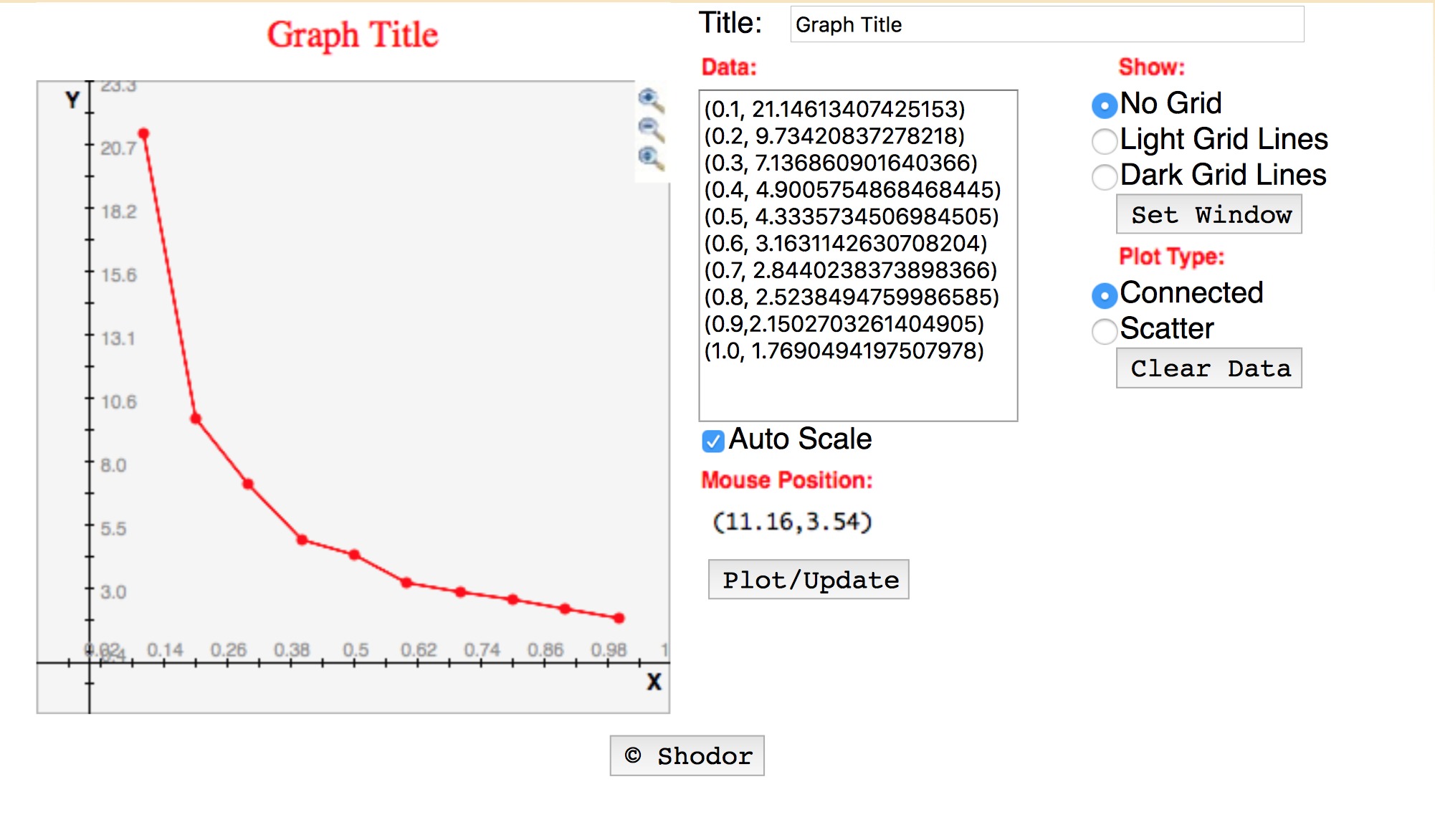
Here T if data sanitization is required. The dataset used is adult.csv file

The user is required to log into his role and operation. Upon doing so, the program automatically picks up risk level of the user and grants him access accordingly.

The following use cases were tested:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Role | Operation | User | Password | T or used |
| 1 | HR Manager | HR view (internal) | lr | xxxxxx | ~ |
| 2 | HR Manager | HR view (external) | mr | xxxxxx | 0.4 |
| 3 | HR Developer | Testing data | mhr | xxxxxx | 0.07 |
| 4 | HR Benchmarking | Benchmark | hr | xxxxxx | 0.02 |

The following shows correlation between and Normalized error:



Since this project tries to create a privacy preserving system, this project falls in the realm of projects that can be presented in this course.

Difficulties faced:

For differential privacy implementation, Laplace mechanism is used with parameters varying from . The main problem was figuring out the implementation of Laplace mechanism for noise addition. That was done using the Exponential Generator available from uncommons-maths.jar file and using a difference of the exponential values to get Laplacian noise. Also there was NaN error popping up initially when noise addition