Plan Overview

A Data Management Plan created using DMPTuuli

Title: Securing and Encryption of Students Private Data

Creator: Meysam Abedi

Principal Investigator: Meysam Abedi Javazm

Project Administrator: Meysam Abedi Javazm

Affiliation: University of Eastern Finland

Funder: The Research Council of Finland (former The Academy of Finland)

Template: General Finnish DMP template

ORCID iD: 2207925

Project abstract:

Researches and the findings of scientific strives are extremely important for entrepreneurial concept-holders, university students, startups, and data security sectors. They can be proficiently alive only upon the advantages of their acquired knowledge. Then the attributed security and encryption matter for them. Accordingly, the present study is about to discover a series of algorithmic solutions for a secure and encrypted procedure of critical data-driven privacy.

ID: 20708

Start date: 01-04-2023

End date: 01-04-2025

Last modified: 12-02-2023

Copyright information:

Securing and Encryption of Students Private Data

1. General description of the data

1.1 What kinds of data is your research based on? What data will be collected, produced or reused? What file formats will the data be in? Additionally, give a rough estimate of the size of the data produced/collected.

Abstract
Researches and the findings of scientific strives are extremely important for entrepreneurial concept-holders, university students, startups, and data security sectors. They can be proficiently alive only upon the advantages of their acquired knowledge. Then the attributed security and encryption matter for them. Accordingly, the present study is about to discover a series of algorithmic solutions for a secure and encrypted procedure of critical data-driven privacy.
We have two types of data:
1- Physical data: which is often in written form.
2- System data: in the form of a database.
This data is analyzed in a unified manner, then stored as a unique file.

data	Is the data collected, produced, or reused	File format	File size	Sensitive data (Y/N)	What part of the data can be made openly available	Who owns the data/planned licenss
1- Student's personal information	collected	frm,myd,MYI (My SQL)	More than 100 Gb	Yes	None	Universities and schools
2- The student's academic record	collected	frm,myd,MYI	About 100 Gb	Yes	None	Universities and schools
3- The student's elective courses	collected	frm,myd,MYI	About 100 Gb	Yes	None	Universities and schools

1.2 How will the consistency and quality of data be controlled?

Compare data in different databases.

2. Ethical and legal compliance

2.1 What legal issues are related to your data management? (For example, GDPR and other legislation affecting data processing.)

The most important ethical issue related to my data, and its management, relate to personal information of students.
All information is encrypted in various ways and the possibility of leakage of information is almost impossible.

2.2 How will you manage the rights of the data you use, produce and share?

The ownership of the data of each school and university is its own and there are no restrictions or rights of third parties regarding background or background.
Agreements about sharing and publishing data will be formalized.

3. Documentation and metadata

3.1 How will you document your data in order to make it findable, accessible, interoperable and re-usable for you and others? What kind of metadata standards, README files or other documentation will you use to help others to understand and use your data?

The data to be shared will be made available after research. The data will be available for subsequent reuse by other researchers by restoring it to the FSD archive. No time limits will be set for the reuse of the data. At FSD, the data will be given an ID number, and it will also be identifiable with the study title.
At FSD, the metadata will be stored into XML files using the frm,myd,MYI specification. Structured XML is suited for long-term preservation, and various documents can be created based on it.

4. Storage and backup during the research project

4.1 Where will your data be stored, and how will the data be backed up?

During the research project, the data will be stored in electronic formats with a password and will be only for the use of the researchers of the project.
During the research process, the data that is in electronic format will be stored on the computers of the team members, with each team member responsible for the data produced by themselves.

4.2 Who will be responsible for controlling access to your data, and how will secured access be controlled?

I myself personally control access to the data, and then it will be available to the administrators. The team members will be responsible for the backup and recovery of the data produced by them. However, regards the data that will be jointly used with collaborators, we will agree in each case on how
to store and back it up and ensure safe transfer between us. In any case, we will avoid storing or sharing unencrypted personal or sensitive data with them.

5. Opening, publishing and archiving the data after the research project

5.1 What part of the data can be made openly available or published? Where and when will the data, or its metadata, be made available?

All data, which is not defined as confidential, will be made available after research. And the databases and personal information of students will never be made available to the public and will remain confidential.

5.2 Where will data with long-term value be preserved, and for how long?

No time limit will be set for the storage and reuse of the data. Valuable data will be stored in the servers of universities and schools for a long time.

6. Data management responsibilities and resources

6.1 Who (for example role, position, and institution) will be responsible for data management?

I am the responsible data manager for the duration of the study. After the studies, The host will be responsible for the data afterward.

6.2 What resources will be required for your data management procedures to ensure that the data can be opened and preserved according to FAIR principles (Findable, Accessible, Interoperable, Re-usable)?

Due to the fact that important and sensitive data are encrypted and remained on the server for a long time, the data should be findable for re-use. For this, proper keywords, and classifications will be used when data is uploaded. Accessibility means that a standardized communication protocol is used to retrieve the data or metadata.