Security & Privacy: Federated Kaplan-Meier

Date	Authors	Description	version
16-05-2024	F.C. Martin, A.J. van Gestel	Initial version	0.1
17-06-2024	F.C. Martin	Updated privacy guards	0.2
10-09-204	A.J. van Gestel, F.C. Martin	Updated privacy guards threshold	0.3

Introduction

This document is intended to assess the risk of using the Federated Kaplan-Meier algorithm. The document is modelled after the guidelines for describing risks for a federated learning algorithm as described in the vantage6 Security & Privacy document **[1]**.

The first section explains how the algorithm works and which data is shared between the parties. Note that we only discuss data that originates from the privacy sensitive database and not the data that is used by the vantage6 infrastructure. In the second part, we discuss which known federated learning vulnerabilities apply to this algorithm . Finally, we discuss how these vulnerabilities may be mitigated.

Algorithm description

The Kaplan-Meier algorithm is a non-parametric statistic used to estimate the survival function from lifetime data. In medical research, it is often used to measure the fraction of patients living for a certain amount of time after treatment **[2]**.

There are four types of parties involved in the algorithm; (1) The aggregator, (2) the data stations, (3) the client and (4) the vantage6 server **[1]**. Figure 1 presents a flow diagram which explains the different steps of the algorithm, which are then explained in the remainder of this section. Note that the server is not displayed as it merely acts as a communication hub between data station, aggregator and researcher.

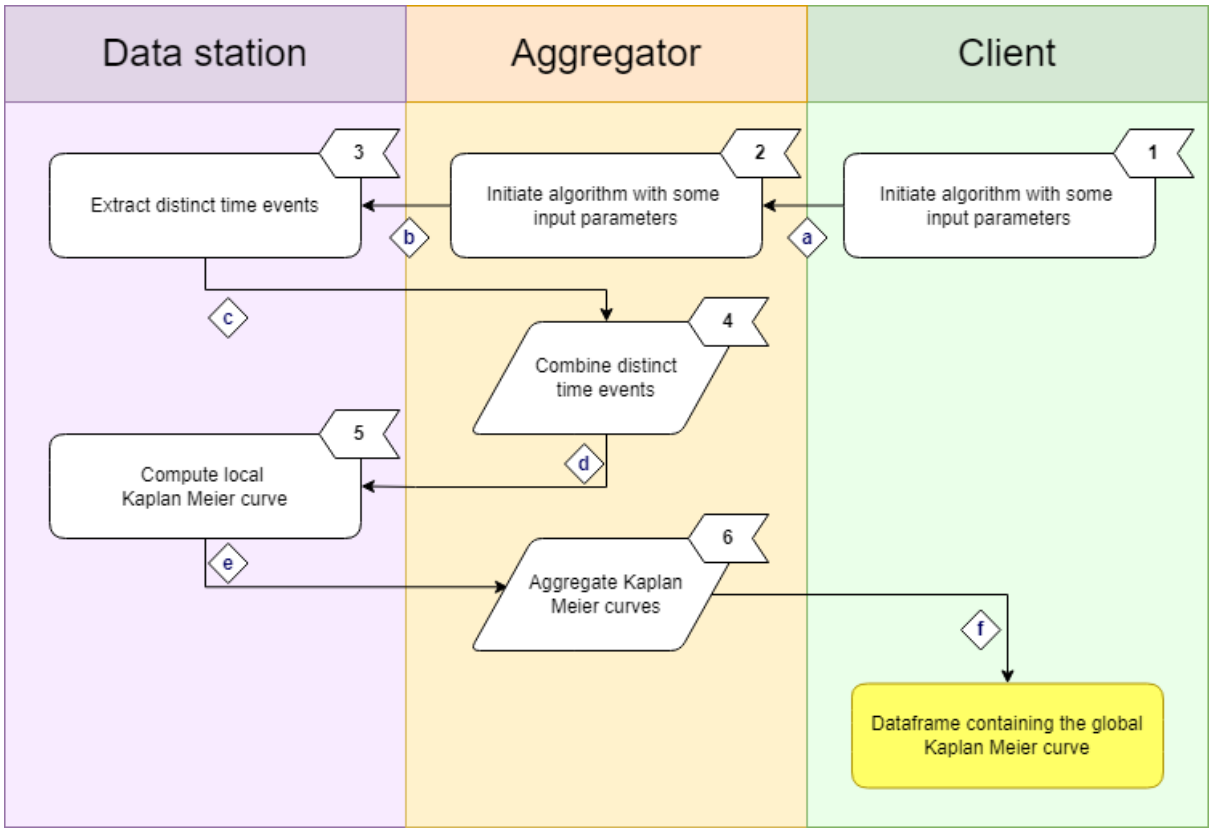

Figure 1 Schematic of the Kaplan-Meier algorithm. For a full description of the steps, see section 'Algorithm steps'. Note that all communication between these parties goes via the Central Server.

Algorithm steps

The different steps of the algorithm are shown in Figure 1.

1. User initiates the federated analysis.
2. The aggregator requests the unique event times from all the data stations.
3. Each data stations computes their unique event times in their dataset. Before it computes these it will add (Poisson or Gaussian) noise to the event times or the event times can be binned.
4. The aggregator combines the local unique event times to global unique event times.
5. Each data station computes their local Kaplan Meier curve with the global unique event times.
6. The local Kaplan Meier curves are summed to a global Kaplan Meier curve.

Data in transit

*Table 1 – A description of data transfers between vantage6 components. Note that all data transfers are mediated by the vantage6 server. The risk level comes from the original paper on Security and Privacy **[1]**.*

Description	Labels	Source	Destination	Risk
Input parameters	a	Client	Aggregator	Low
Input parameters	b	Aggregator	Data station(s)	Low
Distinct event times	c	Data station(s)	Aggregator	Medium
Global distinct event times	d	Aggregator	Data station(s)	Medium
Local Kaplan Meier curve	e	Data station(s)	Aggregator	Medium
Kaplan Meier curve	f	Aggregator	Client	Medium

As is indicated in the table above, the transferred data types that are potentially most sensitive are the *distinct event times* and the *Kaplan-Meier curves*. However, whether these are sensitive in practice depends on how sensitive it is to share (noised) unique event times.

Risks

In this section we will look at the types of attack and other kind of risks that the algorithm will be vulnerable to. Not all types of attack are relevant to this algorithm. Please refer back to the Security and Privacy document **[1]** for the various types of attack definitions. It is important to note that the risk analysis is by all means not exhaustive and malicious parties will know more creative techniques.

Attack name	Risk analysis
Reconstruction	It is possible to reconstruct the distinct event times in case the attacker has access to the distinct event times of N-1 parties, where N is the total number of participating parties.
Differencing	This potentially is possible through the preprocessing steps but not from this algorithm itself.
Deep Leakage from Gradients (DLG)	Not applicable.
Generative Adversarial Networks (GAN)	Not applicable.
Model Inversion	Not applicable.
Watermark attacks	Not applicable.

Privacy Guards / Mitigation

The aggregator will stop executing when less than three organization are selected for the analysis. Furthermore, there are several settings that can be modified to the needs of the project:

1. **Minimum number of records**
   The algorithm will only share information if there are at least *n* records present in the local dataset.

   This can be set using the variable `KAPLAN_MEIER_MINIMUM_NUMBER_OF_RECORDS`.

   Default: 3

2. **Add noise to event times**
   In order to protect the individual event times noise can be added to this column. The column is user defined, see "Fixed event time column" section.

   The type of noise can be set through `KAPLAN_MEIER_TYPE_NOISE`. This can be one of the following:

   - NONE – no noise will be added to the time event columns
   - GAUSSIAN – Gaussian noise will be added, the amount of noise can be controlled to a signal to noise ratio: `KAPLAN_MEIER_PRIVACY_SNR_EVENT_TIME`. The SNR is defined as the amount of noise compared to the standard deviation of the original signal [3].
   - POISSON – Poisson noise will be applied [4].

   Default: `POISSON`

3. **Fixed event time column**
   In order to limit the options the user has for selecting the event time column the `KAPLAN_MEIER_ALLOWED_EVENT_TIME_COLUMNS_REGEX` can be set to a comma separated list. Each element in the list can be a regex pattern.

   Default: `.*`

4. **Minimum number of organizations**
   In order to minimize the risk of reconstruction the number of organizations should be at least 3. The value of this threshold can be changed by setting `KAPLAN_MEIER_MINIMUM_ORGANIZATIONS`. Note that this threshold can be set by the *aggregator* party only!

   Default: 3

References

[1] Martin, F., van Gestel. A., van Swieten, M., Knoors D., van Beusekom, B., Geleijnse, G., 2023. 'Security and Privacy using vantage6 for Privacy Enhancing Analysis'.

[2] https://en.wikipedia.org/wiki/Kaplan%E2%80%93Meier_estimator

[3] Mivule, K. 'Utilizing Noise Addition for Data Privacy, an Overview'

[4] https://numpy.org/doc/stable/reference/random/generated/numpy.random.poisson.html