Security & Privacy: Federated t-test

Date	Authors	Description	version
14-02-2025	V. Ramella	Initial version	0.1

Introduction

This document is intended to assess the risk of using the Federated t-test 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 t-test, also known as Student's t-test, is a parametric statistical test used to determine whether the mean of a population significantly differs from a reference value or to compare the means of two groups. The main types of t-tests include:

- One-sample t-test, which compares the mean of a sample to a known value.
- Independent (two-sample) t-test, which compares the means of two independent groups.
- Paired t-test, which compares two related measurements from the same subjects (e.g., before and after an intervention) **[2]**.

Currently, the algorithm implements the independent t-test.

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.

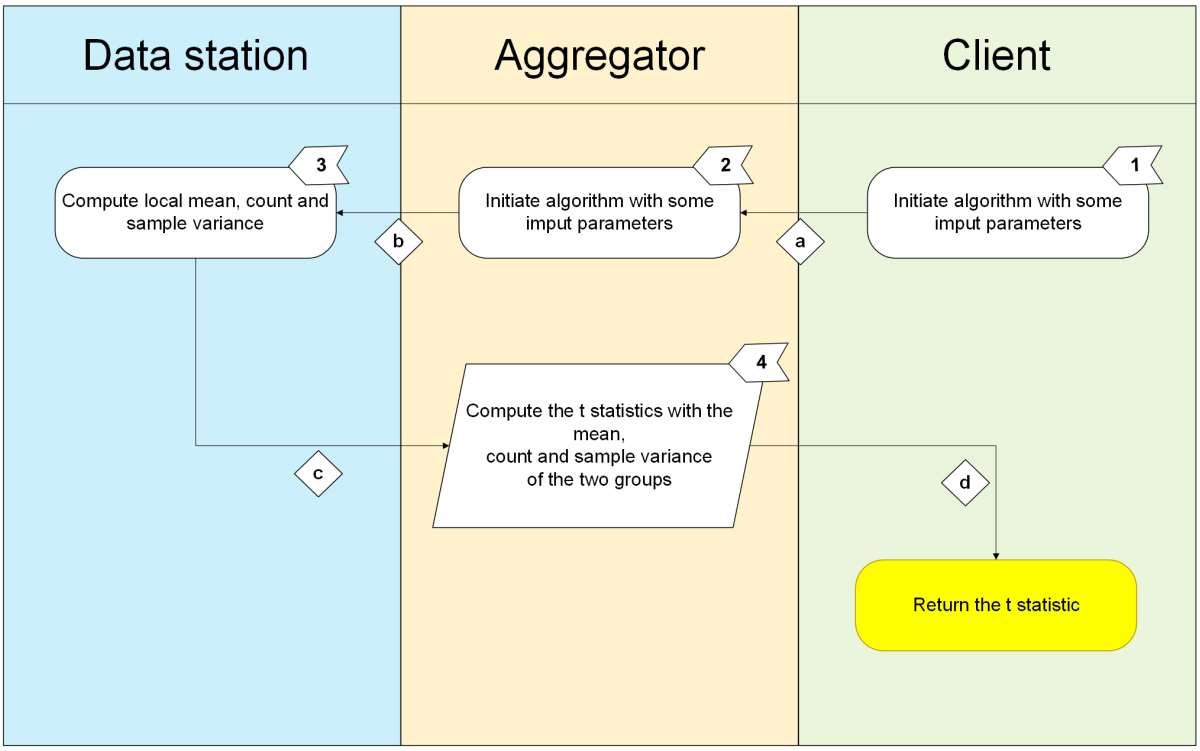

Figure 1 Schematic of the t-test algorithm. For a full description of the steps, see section 'Algorithm steps'. Note that all communication between these parties goes via the Central Server.

Algorithm steps

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

1. User initiates the federated analysis.
2. The aggregator requests the mean, the count of observations and the sample variance of a column from all the data stations.
3. Each data stations computes their local mean, total count and sample variance in their dataset.
4. The aggregator combines the local statistics to compute the *t* value for the independent-samples t-test.

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
Local mean, count and sample variance	c	Data station(s)	Aggregator	Medium
T value	d	Aggregator	Client	Medium

As is indicated in the table above, the transferred data types that are potentially most sensitive are the *local mean, count, sample variance* and the *t value*. However, whether these are sensitive in practice depends on the privacy settings in place.

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	Not applicable.
Differencing	It is potentially possible to single out a patient by selecting subgroups of patients.
Deep Leakage from Gradients (DLG)	Not applicable.
Generative Adversarial Networks (GAN)	Not applicable.
Model Inversion	Not applicable.
Watermark attacks	Not applicable.

Privacy Guards / Mitigation

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 `T_TEST_MINIMUM_NUMBER_OF_RECORDS`.

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/Student%27s_t-test