# Security & Privacy: GLM

| Date | Authors | Description | version |
|---|---|---|---|
| 01-01-2025 | B. van Beusekom, H. Alradhi, F. Martin | Initial version | 0.1 |

## Introduction

This document is intended to assess the risk of using the Generalized Linear Models 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 General Linear Model (GLM) is a statistical framework used to understand the relationship between multiple predictor variables and a continuous outcome variable by fitting a linear equation to the observed data. The following sections give a high level overview of algorithm, for more (mathematical) details please refer to **[1]**.

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 **[2]**. 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.

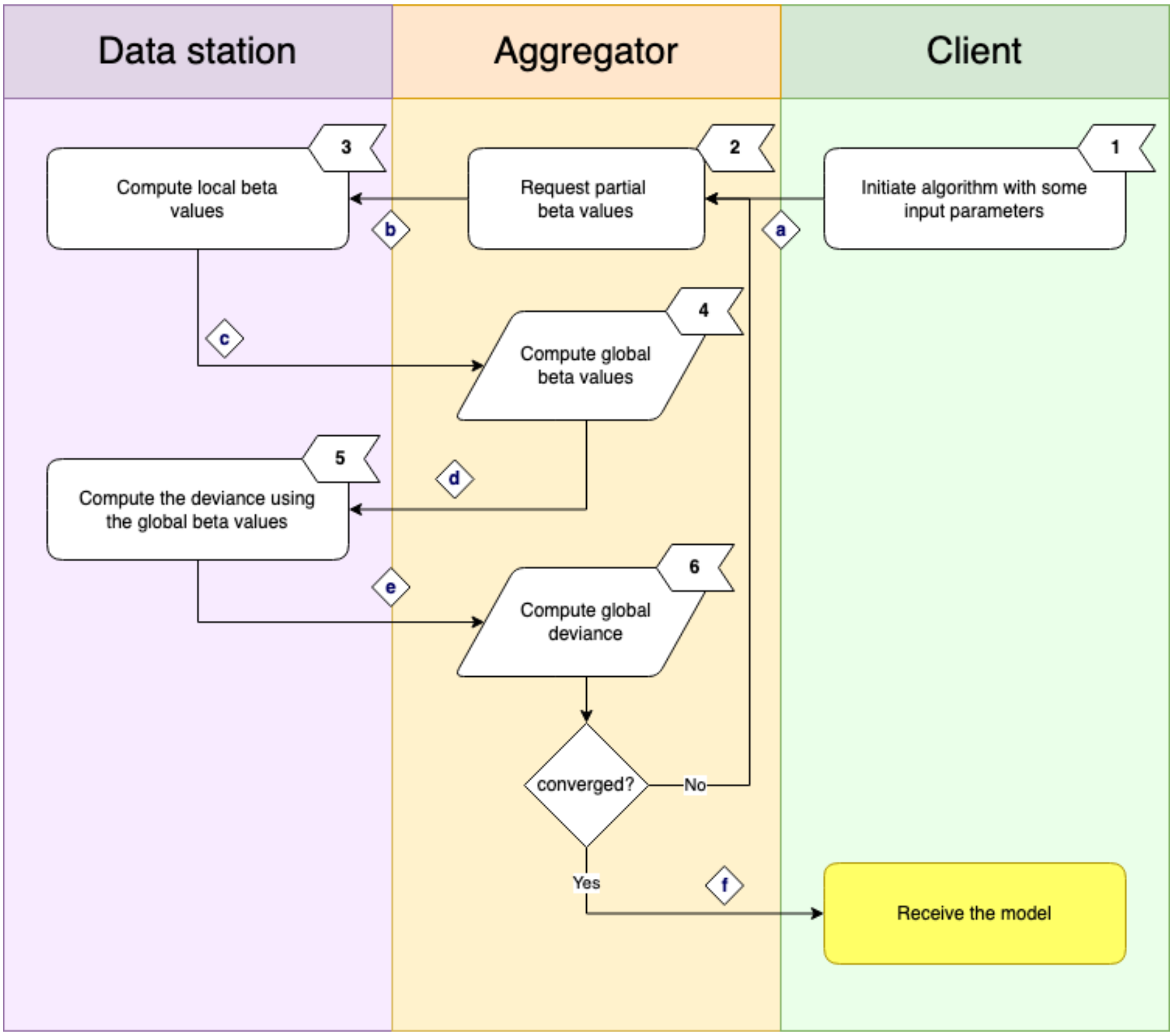
Data station
Aggregator
Client
1
Initiate algorithm with some input parameters
a
2
Request partial beta values
b
3
Compute local beta values
c
4
Compute global beta values
d
5
Compute the deviance using the global beta values
e
6
Compute global deviance
converged?
No
Yes
f
Receive the model

*Figure 1 Schematic of the GLM 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 GLM analysis.
2. The aggregator requests the local beta values from all the data stations.
3. An iterative process computes the local partial beta values.
4. The aggregator combines the local partial beta values to global beta values.
5. Each data station compute the local deviance using the global beta values from the current iteration.
6. The aggregator combines the local deviance to a global deviance and checks wether the model has converged. In case the model converged, the results are returned to the client. In

case it did not converge, the algorithm continues from step 2 with the updated beta values as starting point.

## 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 beta values | c | Data station(s) | Aggregator | Medium |
| Global (intermediate) beta values | d | Aggregator | Data station(s) | Low |
| Local deviance | e | Data station(s) | Aggregator | Low |
| GLM model | f | Aggregator | Client | Low |

As is indicated in the table above, the transferred data types that are potentially most sensitive are the *local beta values*. However, when using appropriate privacy guards these risks can be minimized.

## 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 | It is possible to reconstruct a patient vector when a malicious user computes the model based on N and N-1 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

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 data rows to participate**
   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 `GLM_MINIMUM_ROWS`.

   *Default:* `3`

2. **Minimum number of organizations to participate**
   The minimum number of organizations to participate in a GLM computation is set to 3. This is to prevent that a single organization can try to infer the data of only one other organization involved in the computation.

   This can be set using the variable `GLM_MINIMUM_ORGANIZATIONS`.

   *Default:* `POISSON`

3. **Check parameters vs observations ratio**
   If the number of parameters is high compared to the number of observations, the computation will not be allowed. This is to prevent that data may be inferred from an overfitted model. The maximum ratio of parameters vs observations is set to 10%.

   This can be set using the variable `ENVVAR_MAX_PCT_PARAMS_OVER_OBS`.

   *Default:* `10`

4. **Setting the allowed columns**
   The node administrator can set on which columns they want to allow or disallow computation.

   These can be set using the `GLM_ALLOWED_COLUMNS` and `GLM_DISALLOWED_COLUMNS`.

   *Default:* `*` (all columns allowed)

## References

[1] Cellamare, M., van Gestel, A.J, Alradhi, H., Martin F.C., Moncada-Torres A. 2022 'A Federated Generalized Linear Model for Privacy-Preserving Analysis'

[2] 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'.