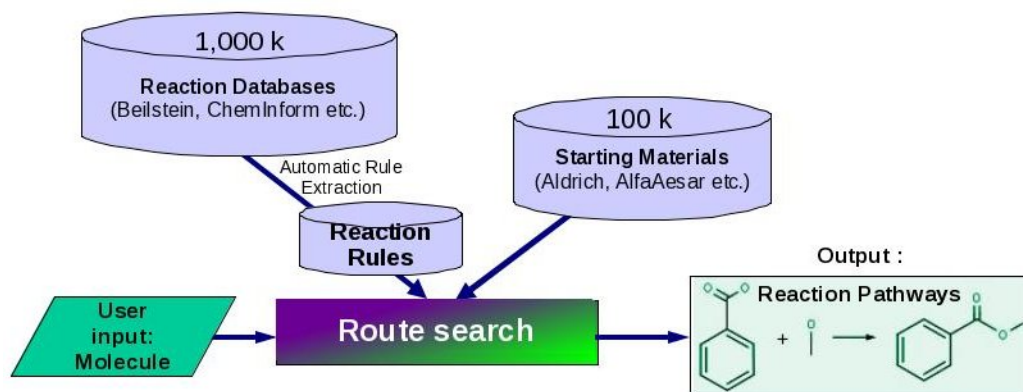


Technical Note on the Security of the On-line Version

Overview

ARChem – Route designer is a web-based retrosynthetic search engine utilizing millions of reactions abstracted from the immense amount of published work of chemists around the world from the past 100 years. The reactions databases and catalogs of starting materials are used to carry out rule-based and precedents-based search of full synthetic routes.



Over the past 12 months there has been a surge in interest among ARChem customers to use the system on-line instead of using it as an in-house installation. The on-line model is becoming increasingly compelling as a safe means to reduce operational costs, and to alleviate the complications of installing and maintaining sophisticated systems.

The benefits of on-line usage of ARChem are obvious. The installation and maintenance of this multi-component system are not trivial and require special training. Handling reactions and educts databases, editing them and keeping them up-to-date requires allocation of resources. Finally, the on-line model frees the users from having to service powerful computer-servers and database-servers in-house for this application, instead they login to a web-site, do their work, and pay their usage share of the system. The main valid concern is whether the on-line system is secure enough to protect the customers' intellectual property. This technical note attempts to address this concern.

Security Methods in ARChem

There are four ways we secure users' data in the on-line version of the ARChem system.

1. The user's input molecule is transmitted to the on-line address via secure HTTPS protocol.

HTTPS stands for **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure, and it means that the usual HTTP (**H**yper**T**ext **T**ransfer **P**rotocol) is combined with the SSL/TLS protocol to provide encryption and secure identification of the server. In the HTTPS protocol, the authenticity of the SimBioSys-owned web server is verified to the user, then the data travels via a secure channel from the user's web browser to ARChem's web server, as the data is encrypted by private key. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

2. Once the data is received and stored in the ARChem system, it can be viewed in the user interface only by the person who submitted the search, or by people from the same company if the user sends out the URL of the search to his colleagues. This way the information can be shared, which is an important feature of ARChem, but it can be shared only with authorized users within the same company and department.
3. If the user is concerned about a hypothetical possibility of accidental mistake in the company name assignment, they can request a dedicated server, where one installation is going to be exclusively assigned to just one company, and that way no other company's employees will be able to access that system. The cost of the dedicated server is a bit higher than for a shared server access, but it is still lower than that of a local installation.
4. Finally, since SimBioSys, the vendor of the system, will have root-access and other exclusive types of access to the servers, a non-disclosure agreement between the service provider and the customer is signed. The agreement guarantees that the vendor, SimBioSys, Inc., will keep the data of the user confidential, and will never use it in any manner, the data will be never used for demonstration, educational or any other purposes with any 3rd party. This is part of our standard license agreement with all customers of ARChem.

These four methods of securing users' data in ARChem are illustrated in the picture below:

