International Secure Platform for Export-controlled Computing Tools

Timothy E. Valentine
Radiation Safety Information Computational Center (RSICC)
Oak Ridge National Laboratory
One Bethel Valley Road, Oak Ridge, Tennessee, USA 37831
E-mail: valentinete@ornl.gov

Abstract:

The Radiation Safety Information Computational Center (RSICC) at Oak Ridge National Laboratory is an information analysis center that collects, archives, evaluates, synthesizes and distributes information, data, and codes used in various nuclear technology applications. RSICC retains more than 2,000 software packages provided by code developers from various federal and international agencies. RSICC's customers (scientists, engineers, and students from around the world) obtain access to such computing codes (source and/or executable versions) and data to promote ongoing research, to help ensure nuclear and radiological safety, and to advance nuclear technology. However, in light of nonproliferation and national security concerns, it is prudent to explore alternatives to distribution of certain codes and data that pose a greater risk of diversion from their intended purposes or that could be utilized for nefarious activities. The international secure platform for export-controlled computing tools addresses the concern of providing access to export-controlled modeling and simulation (M&S) tools while also providing an avenue to foster cooperation among existing and new-entrant nuclear countries. This presentation provides a general overview of the secure cloud computing system, along with the access requirements and protocols established to permit use of certain export-controlled M&S tools and data.

Keywords: modeling, simulation, export, control, cloud, computing

1. Introduction

For the past five decades, the Radiation Safety Information Computational Center (RSICC) has served as the official repository for nuclear modeling and simulation (M&S) and data for the Department of Energy (DOE) and its predecessors and has collected and disseminated related information worldwide under specific distribution restrictions and guidelines set forth by the US government. RSICC maintains collaborations with other similar international organizations to foster cooperation and exchange of M&S tools and data to benefit to our customers. RSICC houses nearly 2,000 software packages provided by code developers supported from various research institutes and universities in the US, as well as international agencies and research centers. Many of these codes have a broad range of applications and uses.

One revolutionary challenge that RSICC has faced is the ever-expanding capability of computing technology accompanied by growing reliance on the need for M&S tools. In some part, the demand and reliance on M&S tools is a consequence of the increasing cost associated with operation of experimental nuclear facilities and the reduced availability of such facilities. Therefore, being able to provide quality-controlled software and data that can be utilized across a diverse set of computing environments is an important aspect of ongoing research and development at RSICC.
technologies is of growing importance, yet it is no easy task. Fortunately, RSICC has had the support of sponsors and code and data developers, along with access to a variety of computing resources to ensure that the packages that we supply to the user community span the breadth of resources for our users and address the range of the applications for which such software is needed.

RSICC’s distribution of M&S tools and data helps to promote international cooperation in nuclear safety, ensures the safe development and deployment of nuclear technology, and provides those countries possessing or pursuing nuclear technology access to state-of-the-art software. However, in the light of nonproliferation and national security concerns, alternatives to distribution of certain codes and data that pose a greater risk of diversion from the intended purposes or that could be utilized for nefarious activities have been explored. Some of the most modern and versatile codes pose the greatest risk of diversion and/or theft. To help to resolve the dilemma between the open sharing of nuclear technology and the need to minimize the potential use of nuclear technology for nefarious purposes, RSICC developed, deployed, and implemented a system to provide access to modern software and data for which access would otherwise be limited or restricted. The deployment of this system also has additional benefit because some new entrant countries may lack access to sufficient computing infrastructure to effectively utilize modern M&S tools. In addition, the development and deployment of a secure computing architecture allows the user to access M&S tools installed under a controlled quality assurance process, thereby ensuring that the M&S tools function as designed. This paper describes the growing demand for M&S tools, along with a general description of the secure cloud system, as well as the protocols for accessing the system. Through its implementation, the system will help foster international cooperation in the peaceful uses of nuclear technology while minimizing the diversion of M&S software for other purposes.

2. Software Demand

The demand for state-of-the-art M&S tools has nearly doubled over the past 5 years, as shown in Figure 1. Over the past 4 years, RSICC has distributed over 4,000 software and data packages annually to customers and has seen a substantial growth in the number of packages delivered to customers who are not US citizens (shown in the figure as “foreign”). At the same time, RSICC has seen substantial growth in the number of requests from US universities at which a growing number of students are not US citizens.

![Figure 1. RSICC’s annual software package distribution](image)

Along with the growth in the demand for M&S tools and data, RSICC’s customer base has expanded to include over 100 countries (Figure 2) and over 20,000 registered individuals. The greatest number of our customers is in the US, but RSICC has seen additional growth over the past 5 years in countries pursuing development and deployment of nuclear technology. Over 16,000 active customers from the US have requested or received software from RSICC since 2005. Outside the US, most of RSICC’s clients reside in Canada, France, the United Kingdom, China, South Korea, and Germany.
As reliance on advanced M&S tools and data grows, RSICC anticipates further growth in the demand for its services.

The use of M&S tools spans a range of applications. The M&S software and data distributed by RSICC are being used for designing advanced reactor concepts, computing radiation source terms, designing and developing fusion devices, ensuring nuclear criticality safety, designing accelerators, implementing nuclear medicine applications, and implementing nuclear security applications. The Los Alamos Monte Carlo code MCNP [1] and the Oak Ridge National Laboratory SCALE system [2] can be applied across all of these areas and are in the most demand by our customers. These codes can also be used for other purposes when there are concerns regarding diversion, theft, or proliferation of the codes. Given these concerns, a balance between open sharing of advanced M&S tools and mitigation of improper code was sought through development and deployment of a secure cloud computing system. As previously stated, the primary purpose of this system would be to minimize national security concerns while allowing access to state-of-the-art M&S software and data for peaceful purposes.

3. System Description and Access Protocols

3.1. System Description

The general specifications of RSICC’s secure cloud computing system are provided in Table 1. This is a capacity system capable of supporting 50 to 100 intermittent users. The system is comprised of 10 compute servers with 4 compute nodes per server and 2 processors per node. The system is built on “Abu Dhabi” Opteron eight core servers. The theoretical peak performance of the cluster is approximately 12 teraflops (TFlops). The system has 5,120 gigabytes (GB) of total memory, with more than 12 terabytes (TB) of disc space. The system is accessed through a log-in node using an RSA SecurID service for two-factor authentication as shown in Figure 3. The system is also segregated from other computing systems at Oak Ridge National Laboratory (ORNL) for network security purposes.

<table>
<thead>
<tr>
<th>Secure cluster</th>
<th>Each node</th>
<th>Each server</th>
<th>Total cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 compute servers/cluster</td>
<td>1</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>4 compute nodes/server</td>
<td>2</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>2 processors/node</td>
<td>2</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>16 cores/processor</td>
<td>32</td>
<td>128</td>
<td>1280</td>
</tr>
<tr>
<td>Memory</td>
<td>128 GB</td>
<td>512 GB</td>
<td>5,120 GB</td>
</tr>
<tr>
<td>Peak theoretical performance</td>
<td>0.307 TFlops</td>
<td>1.23 TFlops</td>
<td>12.3 TFlops</td>
</tr>
</tbody>
</table>

Table 1. RSICC’s secure cloud computing system description.
3.2. Access Protocols

As previously stated, individuals who otherwise cannot be provided access to certain M&S software will now be able to use state-of-the art M&S software on the secure cloud system. Currently, targeted users include foreign nationals collaborating or working at US national laboratories and universities. Additional users are likely to include individuals identified by the US Department of Energy for whom the use of the system is deemed to be in the interest of the US government.

The access process requires that the user register with RSICC by providing their contact information, including their physical address and their email address. After registering with RSICC, individuals can request software from our extensive collection. When foreign nationals who meet the selection criteria request MCNP, SCALE, and RELAP from RSICC, [3] they will be evaluated for access to the secure server, and instructions for access will be provided on approval. Approved users with access to the secure cloud system will be provided with instructions for using the system and will be provided with RSA SecurID tokens that are usable for a 5-year period. The RSA SecurID token will be mailed to the address the user provided during registration.

Each user will have a unique identifier and password associated with his or her account. The user will only be able to access the system remotely through a secure shell (ssh) using both the password and RSA SecurID token. The user will be permitted to upload and download ASCII text files and to send and/or retrieve input and output files. Each uploaded file will be scanned for viruses, and uploading of non-ASCII files will not be permitted. Users attempting to upload non-ASCII files will have his or her account suspended. Furthermore, a user will only have access to his or her personal area on the hard drive, and any attempt to access other areas of the system will result in the suspension of the user’s account. Scripts have been written to execute MCNP, SCALE, and/or RELAP. The installed versions of these codes will be the production versions and will be updated as warranted. Beta versions of the codes will not be available on the secure cloud computing system.
4. Summary

Development and deployment of a secure cloud computing system at RSICC allows for controlled access to state-of-the-art M&S tools and data with extensive applications while simultaneously addressing concerns with diversion, theft, or nefarious uses of the codes. System deployment will also provide some users with computing infrastructure that may not be easily accessible in their own organizations. In addition, the system has been built to support 50 to 100 intermittent users at one time and can be accessed remotely using a unique customer identifier along with a secure token. Approved users will be able to use the production releases of MCNP, SCALE, and RELAP that currently reside at RSICC. Additional codes may be added to the secure cloud system as warranted.

The benefits of this system are notable. Individuals who otherwise would not be allowed access to these modern programs will now be able to use them on a rigorously tested and verified computing platform. System users will be able to focus on addressing scientific problems without being concerned with software installation or quality control. Individuals from some participant countries lacking modern computing infrastructure will now have access to a high-capacity computing system. Successful deployment of this system will permit sharing of state-of-the-art M&S tools and data to facilitate the safe application of nuclear technology while also fully addressing and mitigating proliferation concerns.

5. Acknowledgements

The author would like to acknowledge the support of the US Department of Energy Office of Nuclear Energy, the National Nuclear Security Administration, and the Office of Nonproliferation and Arms Control for development and deployment of the secure cloud computing system. The author would like to thank Mark Baird, Matt Disney, Ken Barker, and Brian Zachary of ORNL for their efforts to install, test, and validate the system’s operation, as well as for their development of the network security protocols that enabled the system to be deployed.

6. References

