AN APPROACH FOR SECURE CLOUD COMPUTING FOR FEM SIMULATION

Jörg Frochte*, Christof Kaufmann, Patrick Bouillon
Dept. of Electrical Engineering and Computer Science
Bochum University of Applied Science
42579 Bochum, Germany
**E-Mail: joerg.frochte@hs-bochum.de*

ABSTRACT

This paper deals with the challenge to make cloud computing an acceptable way for finite element method (FEM) simulations. This is of special interest for small and mid-size engineering companies (SMEs), for whom it makes no sense to provide a computation cluster for a few big simulations per year. The approach we propose makes use of the specific properties of the FEM and with these it enables the user to simulate in the cloud without risking sensitive information. The opportunity to split the simulation on different providers increases the security of the method but leads to a quite big set of parameters for the user to choose. To make the approach attractive for end-users we integrate simulation data mining based assistance systems.

KEYWORDS

Cloud Computing, Safety & Security, Simulation Data Mining, Machine Learning, Assistant systems, FEM

1. INTRODUCTION

Cloud computing has deeply changed the way how costumers use computers and as well the way companies work and communicate. However, after Edward Snowden's release of NSA material European companies began to have doubts about entrusting their important data to cloud services operated by US companies. To realize how common this problem is, one might think of the speech of Neelie Kroes, European Commission vice president, from 4 July 2013 (Kroes [2013]).

Security is essential when it comes to CAE (computer-aided engineering) data from the product development process. CAE is the typical industrial application area for Finite Element Method (FEM) simulation and it includes significant knowledge of the company's innovations. In order to make cloud computing an accepted method for industrial users in the field of simulation, this security challenge has to be solved.

It is important to enhance the acceptance because cloud computing has the potential to help resolving two problems. It promises a way to combine Green-IT – if cloud computing resources are centralized in efficient data centers where energy can be produced, e.g. with water power – with benefits concerning synergies in maintenance and need-based use of soft- and hardware. So it is an important task to make cloud computing safer by using technical approaches.

2. APPROACH FOR SECURE FEM SIMULATION

Concerning cloud computing we focus on the area of CAE, to be precisely on the simulation of large models using the finite element method (FEM) in three dimensions. The base of FEM is a mesh of elements – we consider tetrahedrons only. How fine the mesh is depends on the geometry that is to be simulated and the error tolerance for the results. For three dimensional FEM models the degrees of freedom tend to grow very

fast. A simple example is a cube with the edge length of one meter. If this is uniformly discretized with a grid spacing of 1 cm, we have 100 degrees of freedom to the power of three and so we end up with a million unknowns. If the grid must be refined uniformly, one already reaches eight million unknowns etc.

On the one hand these problems can be solved very efficiently on computer clusters using parallelization techniques from domain decomposition. On the other hand for small and mid-size companies it makes no sense to provide a computation cluster for only a few big simulations per year. So this is a perfect use case to rent soft- and/or hardware as a service.

The three primary types of cloud models, see e.g. (Borko and Armando [2010], Chapter 1), are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). A pure IaaS would not meet the need of a small or mid-size company, among others it would need too much expertise to handle it. We address for this problem a PaaS variant, in which the provided platform is accessed by client software that runs on the company computer. The source code of the client is included to make the processing transparent for the user.

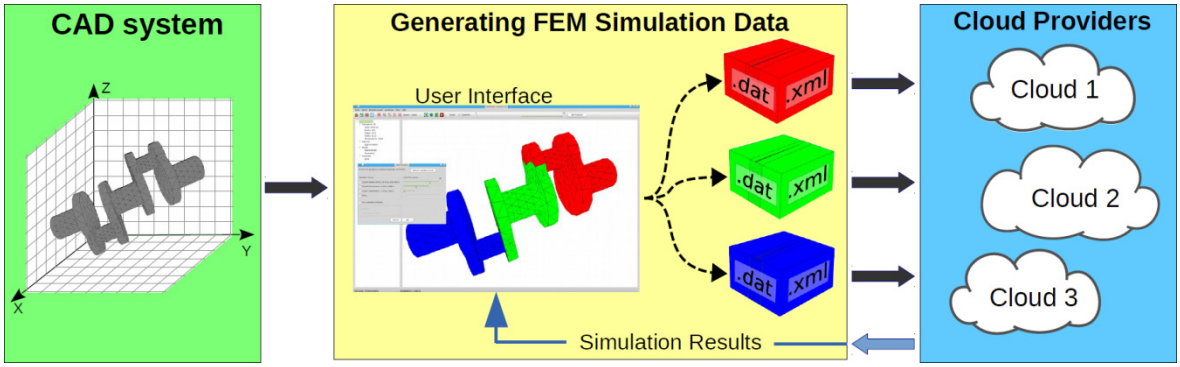
Now, with this very rough architecture we will address the basic problem, which is the fact that on the one hand the data must be protected and on the other hand it must be available for the processing on the cloud server.

Solving this problem we follow two basic ideas:

1. "Hand-off the work, not the information!"
2. "Never put all eggs in one basket!"

So the first step is to make sure that as few sensitive data as possible need to be transferred in the cloud at all; in the optimal case even none. The approach for this purpose is illustrated by the following Figure 1:

Figure 1: Sketch of application scenario



From a standard program, in which the CAD data of the model are processed, a software generates job packages. Right now we are just dealing with static problems where data files with description files turn out to be the most efficient approach. On the long run we expect that time-dependent FEM models will require some code generation. So the cloud paradigms are adapted here to the specific application environment.
The user at the beginning of the chain should work without the knowledge of the specific processing of his data. The client software calls the cloud provider for information about the hardware topology, e.g. memory, processors, operating systems, etc. which is offered and optimizes the job generation for this configuration. The produced job packages are transferred only in the form of binary form, which can connect to defined interfaces of the cloud PaaS and then get processed there. The results are returned to the company's internal client, where they are available for the user. One main aspect of this setting is that the provider of the PaaS is in general not the provider of the FEM simulation software. The user stays independent of the cloud provider as long as a standardization of the API of the provided software infrastructure could be achieved.

The user can rely on the security of the processed data because he generated it on his own host computer and is able to control what he transmits to the cloud. Storage and transmission of business-critical data is thereby avoided. The design of the software architecture requires no permanent data in the cloud. However, it

is still possible to attack the temporary data in RAM and or grab the data by an internal attack from e.g. employees of the cloud provider. To avoid this and make sure that "Hand off the work, not the information" is possible, we need to have a brief look on how FEM is performed.

A simplified description of FEM processing is as follows:

1. Generation of the FEM mesh from CAD data
2. Discretization of the equation, e.g. a linear elasticity model, by means of the mesh

For a more detailed description see e.g. (Brenner and Scott [2008]).

By discretization, in the case of a time-independent linear model as a result, a very large but sparse system of equations is obtained:

$$Ay = b$$

In the case of a time-dependent linear model we have obtained a system of ordinary differential equations by the method of lines:

$$\frac{dy}{dt} + Ay = f(y,t)$$

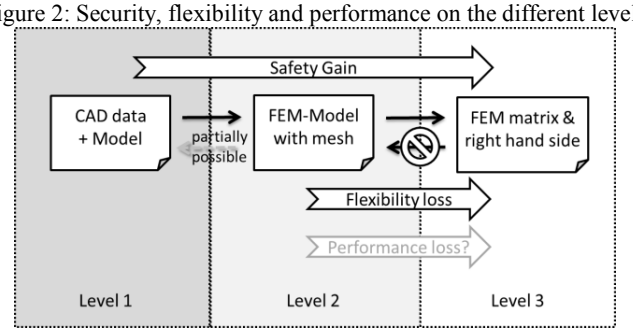
Therefore, in these cases the result is a single linear system of equations or a sequence of systems which are sparse, but might include hundreds of thousands up to several million unknowns. So we have as last step of the procedure:

3. (Repeated) solution of the system of linear equations, which represent the FEM model

Step 3 is the computationally most expensive part. By using a cloud to process this step we use the scalable resources where they are required without risking sensitive R&D data.

The entries of the above FEM matrix *A* are assembled by the integration of base functions. As a matter of fact the conversion from the FEM model - consisting of mesh, PDE, material properties etc. – to the FEM matrix is in the terms of cryptography a kind of one-way function. This means that there is no way back to the FEM model, if one just has the FEM matrix. The effect can be outlined by the following figure:

Figure 2: Security, flexibility and performance on the different levels



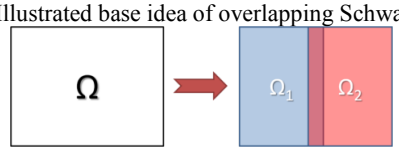
So if the full CAD data is sent to the cloud an attacker could steal all data of the design. In the step of mesh generation, all information on manufacturers and types of data is lost. An example is an approximation of a screw of a particular manufacturer with all catalog data by tetrahedrons and double values for material properties. So already at level 2 less information is transferred to the cloud and in some applications this might already be acceptable. However, at this level it cannot be completely ruled out that relevant data could be recovered by an attacker with expertise and time for a deep analysis. On the last level just the FEM matrices or the set of ordinary differential equations are transferred to the cloud, so no data is transmitted which allows an attacker to recover interesting data from the CAD model.

Of course, there are some disadvantages of the most secure level. If one just transmits the FEM matrix, the price is a loss of flexibility and possibly as well performance. Flexibility means in this context particularly the adaptive adjustment of the mesh to the desired accuracy. Such techniques require the mesh itself. For non-linear models the host would have to perform multiple transmissions and so the network

traffic might become a serious problem. Because most common CAE tools use linear problems as long as possible, e.g. linear elasticity computation, level 3 still leaves a wide area of relevant linear applications.

One way to make the second level more attractive and in some cases even improve the performance is by splitting the simulation on multiple providers. The approach is based on a method that is normally used for parallel simulation of FEM models. We use robust domain decomposition methods, see e.g. (Toselli and Widlund [2004]) for details, from the class of Schwarz methods. The underlying idea is quite simple and is illustrated by the following two-dimensional example in Figure 3:

Figure 3: Illustrated base idea of overlapping Schwarz methods



The domain Ω is divided into two subdomains Ω_1 and Ω_2 and solved separately on each domain. The computed solutions are exchanged and then the problem is solved again with this method. This iterative process may seem inefficient since the systems of equations on Ω_1 and Ω_2 must be solved repeatedly instead of just once on the domain Ω. The method is, however, used with great success in the parallel processing of partial differential equations, as a large system of equations is much more expensive with respect to CPU time than two small ones.

The theoretical background lies in the fact that solving linear equation systems with direct solvers has in general a complexity of O (n^m) with m> 1. The known Gaussian method results in an increase in the number of arithmetic operations with O (n^3).

3. SIMULATION DATA MINING BASED ASSISTANCE SYSTEMS

A critical aspect of the Schwarz method is the rate of convergence that depends on the PDE itself, which is fixed because this is the given use case, and the size as well as the position of the overlap. On the one hand we have got the fact that the wider the overlap is chosen, the faster and more robust the iteration proceeds. On the other hand increasing the overlap increases the overhead of the method significantly. For a heterogeneous application scenario with three PasS providers as displayed in Figure 4 choosing a reasonable setting is a non-trivial task, see (Bernst et al. [2014]) for details.

Figure 4: Heterogeneous application scenario with three PasS providers

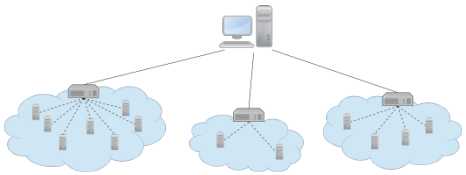
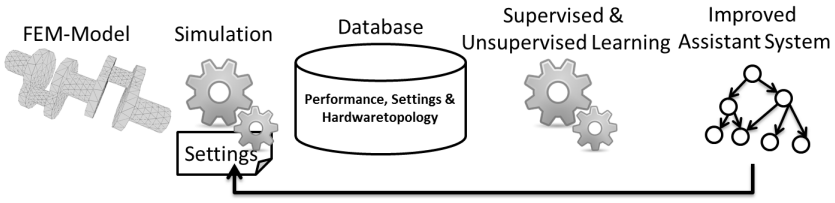


Figure 5: Simulation Data Mining Workflow



Therefore, the original set of parameters of a FEM simulation – that for professional tools is not small – is again expanded with parameters needed for the cloud simulation. So users are confronted with a parameter space of a challenging size and complexity. To address this we propose that a database of configurations should be pre-computed such that the behavior of similar cases can be used to guide decision making. A similar technique was used in (Burrows et al. [2011]) for supporting bridge design, while (Butnaru et al. 2012) focus on approaches for model reduction methods.

In particular, simulation results based on provided hardware topology, PDE model and domain partitioning are clustered to identify cases with similar behavior. This approach will make it possible to compare different settings without actually simulating them. The learned function is the basement of assistant

systems that are still under development and follow the workflow from Figure 5. One of the first papers dealing with data mining from simulation results using the term simulation data mining is (Brady and Yellig [2005]). An example how this is successfully performed is described in a collaboration paper (Burrows et al. [2013]) on an example of learning overlap optimization for domain decomposition methods.

4. CONCLUSION

In this paper we proposed a design concept for using cloud capacities for FEM simulation with a maximum of safety and security. The main insight was that a FEM simulation can be drawn out in a cloud without risking sensitive R&D data. This relies on the one-way behavior of the mathematical assembling. Therefore, we can provide an architecture that allows to hand off the computation job, which has the requirement for expensive hardware, to the cloud without transmitting information about products and R&D strategies of the user. A multi provider scenario makes it possible to increase the security in some use cases, leads to a higher performance and helps to gain independence for the user. The problem of the rising set of configuration parameters is addressed by using simulation data mining as a base of assistance systems. These assistance systems for numerical simulations are part of our future work. A key challenge in numerical simulation for end-users like engineers is the use of parameterized numerical simulation methods; see e.g. (Stein and Curatolo [1998]). These methods are often difficult to deploy for end-users. As a result, the most robust and parameter-independent methods, such as direct solvers for linear systems, are often preferred in many engineering contexts, even if they are less efficient. The key idea is that the parameters in this latter group can be learned in order to converge the ease of use towards the parameter-independent methods, particularly in aspects and use cases that involve code generation.

ACKNOWLEDGEMENT

This work is supported by the BMBF (Federal Ministry of Education and Research, Germany) under grant 03FH01812.

REFERENCES

Bernst, I., Bouillon, P., Frochte J. and Kaufmann, C., 2014. An approach for load balancing for simulation in heterogeneous distributed systems using simulation data mining, *Proceedings of the 11th International Conference Applied Computing*, Porto, Portugal (submitted)

Brady, T. F., and Yellig, E., 2005. Simulation Data Mining: A New Form of Computer Simulation Output, *Proceedings of the Thirty-Seventh Winter Simulation Conference*, Orlando, Florida, pp. 285-289.

Brenner, S.C., and Scott, L.R., 2008. *The mathematical theory of finite element method*. Springer-Verlag, New York-Berlin-Heidelberg, 3rd edition.

Borko, F., and Armando, E., 2010. *Handbook of Cloud Computing*, Springer Science & Business Media, USA.

Burrows S., Stein, B. Frochte J., Wiesner, D. and Müller, K., 2011. Simulation Data Mining for Supporting Bridge Design*, Proceedings of the Ninth Australasian Data Minig Conference*, Balarat, Australia, ACM pp. 163-170.

Burrows S., Frochte J., Völske, M., Martinez Torres, A.B. and Stein, B., 2013. Learning Overlap Optimization for Domain Decomposition Methods*, 17th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 13)*, pp. 438-449.

Butnaru, D., Peherstorfer, B., Bungartz, H., and Pfluger, D., 2012, Fast insight into high-dimensional parameterized simulation data, *Machine Learning and Applications (ICMLA), 2012 11th International Conference on*. Vol. 2. IEEE

Kroes N., 2013. *Statement by Vice President Neelie Kroes "on the consequences of living in an age of total information"* http://europa.eu/rapid/press-release_MEMO-13-654_en.htm

Stein, B. and Curatolo, D., 1998. Selection of Numerical Methods in Specific Simulation Applications, *Proceedings of the Eleventh International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems.* Castellon, Spain, 918-927

Toselli, A., and Widlund, O., 2004. *Domain Decomposition Methods – Algorithms and Theory*, Springer, Leipzig, Germany.