M. Tichy, E. Bodden, M. Kuhrmann, S. Wagner, J.-P. Steghöfer (Hrsg.): SE 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 59

Optimized Cloud Deployment of Multi-tenant Software Considering Data Protection Concerns – Abridged Version

Zoltán Ádám Mann[1] and Andreas Metzger [1]

Abstract: To ensure that a cloud tenant's data cannot be accessed by malicious code from another tenant, critical software components of different tenants are traditionally deployed on separate physical machines, leading to inefficient resource usage. In this paper, we show how secure hardware enclaves can be employed to address data protection concerns of cloud tenants, while optimizing hardware utilization. We provide a model, formalization and experimental evaluation of an efficient algorithmic approach to compute an optimized deployment of software components and virtual machines, taking into account data protection concerns and the availability of secure hardware enclaves.

Keywords: Cloud computing; data protection; privacy; resource optimization; secure enclave

1 Introduction

Ensuring the protection of sensitive data is key for the adoption of cloud services [SMM17]. Data protection concerns may especially arise in a multi-tenant setting, in which the confidentiality of a tenant's data may be breached by malicious code from another tenant. Even if different tenants' code and data are deployed in different virtual machines (VMs), if these separate VMs are deployed on the same physical machine (PM), malicious code in one VM may still breach the confidentiality of data in another VM. To address such security risks, the traditional solution is to physically separate critical code and data of one tenant from the code and data of other tenants by deploying each on different PMs. However, physical separation reduces the opportunity for sharing resources, thus leading to limited hardware utilization and increased costs [Ma15a, Ma15b].

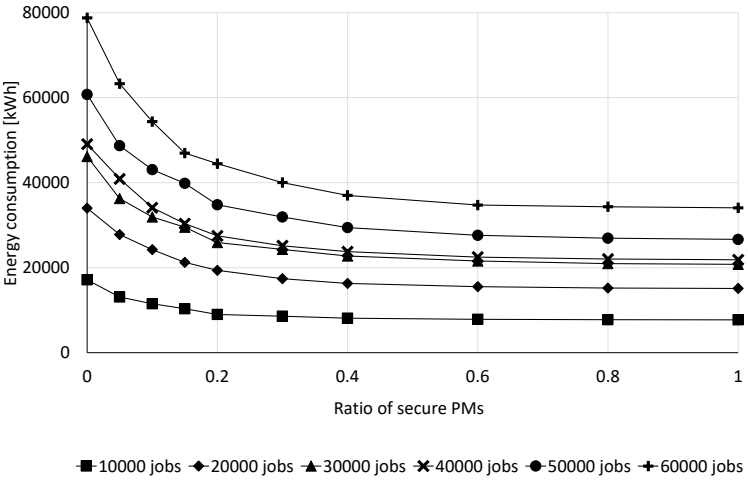
Secure enclaves (such as offered by Intel's SGX technology[2]) provide hardware mechanisms to protect critical code and data, maintaining confidentiality even when an attacker has physical control of the hardware platform and can conduct direct attacks on memory. Secure enclaves thereby make it possible to protect code and data within a PM, thus offering an alternative to physical separation. Since PMs offering secure enclaves are likely to remain a scarce resource in data centers in the near future, a combination of secure hardware and physical separation on traditional hardware appears to be a good compromise to achieve data protection goals while aiming to optimize resource usage.

[1] paluno – The Ruhr Institute for Software Technology, University of Duisburg-Essen, Essen, Germany. {zoltan.mann, andreas.metzger}@paluno.uni-due.de

[2] Software Guard Extensions, see `https://software.intel.com/en-us/sgx`

2 Approach and results

In our original paper [MM17], we defined and formalized a cloud deployment model considering data protection concerns. We introduced efficient heuristic algorithms to compute an optimized cloud deployment for tenant components (i.e., code and data) and VMs, taking into account data protection concerns and capacity constraints. By means of a comprehensive empiric evaluation with real workload data, we analyzed how cost savings depend on data security properties. In particular, we found that even if only 20% of the PMs offer secure hardware enclaves, savings of energy consumption (which is a major cost driver) may be as high as 47.5%. This is also exemplified by the following figure.



Acknowledgement. This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant no. 731678 (RestAssured).

References

[Ma15a] Mann, Zoltán Ádám: Approximability of virtual machine allocation: much harder than bin packing. In: Proceedings of the 9th Hungarian-Japanese Symposium on Discrete Mathematics and Its Applications. pp. 21–30, 2015.

[Ma15b] Mann, Zoltán Ádám: Modeling the virtual machine allocation problem. In: Proceedings of the International Conference on Mathematical Methods, Mathematical Models and Simulation in Science and Engineering. pp. 102–106, 2015.

[MM17] Mann, Zoltán Ádám; Metzger, Andreas: Optimized Cloud Deployment of Multi-tenant Software Considering Data Protection Concerns. In: Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. pp. 609–618, 2017.

[SMM17] Schoenen, Stefan; Mann, Zoltán Ádám; Metzger, Andreas: Using Risk Patterns to Identify Violations of Data Protection Policies in Cloud Services. In: 13th International Workshop on Engineering Service-Oriented Applications and Cloud Services. 2017.