안전한 클라우드 컴퓨팅 환경을 위한 보안 인클레이브와 VM 마이그레이션

유시환*, 이승균, 여승현, 박재원, 남호철
단국대학교

{seehwan.yoo*, seunggyun15, seunghyun, 32151859, hcnam}@dankook.ac.kr

VM Migration with Secure Enclave for Secure Cloud Computing

Seehwan Yoo*, Seung Gyun Lee, Seunghyun Yeo, Jaewon Park, Ho-Cheol Nam
Dankook University

요 약

본 논문은 클라우드 컴퓨팅 환경의 VM 마이그레이션을 다루고 있다. 최근 안전한 클라우드 컴퓨팅 환경을 구성하기 위하여 보안 인클레이브에 대한 연구가 주목을 받고 있다. 인텔 SGX 기반의 보안 인클레이브는 사용하는 컴퓨팅 환경의 무결성을 검증하며, VM 이 실행되는 환경에서 보안 응용의 실행환경과 응용 자체의 무결성을 제공할 수 있다. 하지만, 물리적인 인클레이브 영역의 용량 제한으로 인해 보안 응용이 탑재된 VM 의 사용성이 제한된다. 한편, 클라우드 환경의 VM 마이그레이션 기술은 특정 VM 을 인클레이브의 실제 활용도가 낮은 다른 물리머신으로 이동하여 클라우드 환경에서도 보안 인클레이브 기술을 원활하게 사용할 수 있도록 한다. 본 논문에서는 보안 인클레이브를 포함한 VM 의 마이그레이션을 통한 안전한 클라우드 컴퓨팅 환경을 제안한다.

Ⅰ. 서 론

클라우드 컴퓨팅 기술의 발전에 있어 보안성은 매우 중요한 요소이다. 클라우드 컴퓨팅 환경에서 사용자는 데이터를 클라우드 데이터 센터에 보관하고, 필요에 따라 로컬머신에 다운로드 받아 사용하게 된다. 많은 클라우드 보안 공격들은 사용자의 데이터를 다루는 컴퓨팅 환경을 공격하여 멀웨어를 숨겨두거나, 실행되는 소프트웨어를 변형하여 원격에서 공격을 실행하려고 한다.

이러한 공격으로부터 컴퓨팅 환경을 보호하기 위해 하드웨어 기반 신뢰 실행 환경 (Trusted Execution Environment) 기술들이 주목받고 있다. 인텔의 SGX (software guard extension), ARM 의 TrustZone 과 같은 기술은 CPU 레지스터나 메모리와 같은 물리적인 컴퓨팅 자원을 보안/비보안 영역으로 명확히 분리하고, 보안 영역에 대한 엄격한 접근 제어와 암호화 기법을 통해 실행 환경에 대한 무결성, 기밀성을 강화한다.

클라우드 VM 환경에서 인텔 SGX 기술을 활용하기 위한 가상 SGX 기술은 2018 KVM forum[KvmForum], 2017 Xen Summit[XenSumit] 을 통해 발표되었다. 또한, SGX 를 활용할 수 있는 컨테이너 기술과 라이브러리 운영체제 기술들은 최근 연구들을 통해 발표되었다 [Haven][Scone][Graphene-sgx]. 하지만, 이러한 기술들은 SGX 가 가지고 있는 근본적인 한계에 대해 다루고 있지 않다. SGX 기술은 128MB 의 물리적으로 제한된 DRAM 내 EPC 영역에 대해서만 적용이 가능하다[IntelSGXExplained]. 따라서, 다수의 VM 들이 실행되는 하나의 물리머신에서 동시에 실행되는 모든 VM 들이 128MB 의 제한된 SGX-EPC 영역을 나누어 활용할 수 밖에 없으며, 여러 VM 이 나누어 사용하기에는 매우 부족한 용량이다.

따라서 본 논문에서는 인텔 SGX 기반의 보안 인클레이브를 포함하는 VM (가상머신, virtual machine)을 클라우드에서 활용하기 위한 기법으로 VM 마이그레이션을 제안한다. 제안하는 기법을 통해 클라우드 환경에서도 보안 응용의 실행 환경 무결성을 확인할 수 있으며, 안전한 보안 응용의 실행이 가능하다.

VM 마이그레이션 기술은 실행중인 클라우드 환경의 VM 을 다른 물리머신으로 이전하여 실행하는 기술로서 클라우드 컴퓨팅 환경이 매우 유연한 자원관리가 가능하도록 하는 핵심기술이다. 즉, 현재 VM 이 실행중인 물리머신의 가용한 자원이 부족한 경우, VM 을 보다 풍부한 물리자원을 가진 플랫폼으로 이동하여 실행할 수 있다. 예를 들어, 급격한 CPU 요구량의 증가나 메모리 사용량의 증가, GPU 활용량의 증가가 있는 경우, 보다 하드웨어 자원이 풍부한 물리머신을 활용하여 작업부하에 따른 성능저하를 최소화할 수 있다.

VM 마이그레이션 기술을 활용하는 경우, 실제 클라우드 환경의 다중 VM 을 실행하는 물리머신이 제한된 SGX-EPC 영역에 대해 보다 유연한 자원 관리를 제공할 수 있으며, 사용자는 보안 응용의 실행 환경에 대한 무결성을 검증할 수 있다.

Ⅱ. 본론

클라우드 VM 관리자는 VM 의 설정과정에서 CPU 코어 수와 메모리 용량, SGX-EPC 용량을 설정하게 된다. 즉, SGX-EPC 영역은 VM 생성 시 정적으로 할당이 이루어진다.

VM 을 구성하는 관리자 입장에서는 보안 응용 (SGX 응용)이 실제로 활용할 수 있는 SGX-EPC 영역의 최대값을 예측하여 VM 을 구성할 수 밖에 없다. 따라서 SGX-EPC 영역은 데이터 센터의 물리머신들 중에서 VM 을 실행할 물리머신을 결정하는데 중요한 요소가 된다. 즉, 데이터 센터 내 여러 대의 물리 머신 중 어떤 머신에서 VM 을 호스팅할 것인지에 대한 문제를 해결해야 한다.

자원 배분과 활용율을 고려한 최적의 VM 위치 선정 문제는 비교적 널리 알려진 문제로서 에너지나

CPU 사용량, 네트워크 사용량 등을 고려한 선형/다차원 bin-packing 의 문제로 해결할 수 있다[Energy-optimal VM placement][Optimal VM placement].

하지만 실제 SGX-EPC 영역의 활용율은 실제 정적 할당이 이루어진 용량에 비해 무척 낮다. 실제 SGX-EPC 영역은 SGX 기술을 활용하는 보안 응용을 사용하는 경우에 한해, 응용의 보안 라이브러리에서만 사용된다. 따라서 SGX-EPC 영역은 전체 VM 의 실행 시간 중 대부분은 유휴 상태가 되며, 실제로 활용되지 않는 경우에도 과대 할당으로 인해 최적의 VM 위치 선정을 방해하는 요소가 된다.

따라서, SGX-EPC 영역의 효율적인 활용을 위해서는 SGX-EPC 영역을 사용하는 경우와 그렇지 않은 경우를 구분하여 VM 의 위치 선정을 고려하는 VM 마이그레이션 기법을 다음과 같이 고려할 수 있다.

첫째, SGX 응용이 실행되지 않는 일반적인 환경에서는 기존 VM 위치 선정 알고리즘을 활용하여 최적의 VM 위치를 선정하여 실행한다. 둘째, 실제 SGX 응용이 실행되어 SGX-EPC 영역이 활용되는 경우에는 SGX-EPC 를 고려한 다중 bin-packing 문제를 통해 최적의 VM 위치를 재배치한다.

실제 SGX 응용이 실행되는 경우, VM 을 재배치하기 위해 가상 SGX 드라이버는 현재 물리머신에서 SGX 응용이 실행되고 있는지 확인한다. 만약 현재 물리머신에서 SGX 응용이 실행되지 않고 있다면, 현재 머신에서 VM 을 그대로 실행하더라도 여전히 최적이다.

만약 현재 물리머신이 SGX-EPC 영역을 사용하고 있다면, SGX-EPC 영역을 고려한 다중 bin-packing 문제를 풀어야 한다. 다중 bin-packing 문제는 선형시간에 문제를 풀기 어려운 NP 문제이므로, 런타임에 최적의 VM 위치를 선정하는 것은 상당히 어렵다[Optimal VM placement]. 따라서 다음 두 가지 조건을 이용하여 최적화를 완화한 문제를 풀도록 한다.

첫째, SGX-EPC 영역을 사용하지 않는 물리머신이 근처에 위치하는 경우, VM 을 마이그레이션하여 활용할 수 있다. 이 때, 마이그레이션을 시도하는 VM 의 CPU 활용율과 메모리 사용량 정보를 같이 전송하여, 마이그레이션 대상 물리머신 중 CPU 활용율과 메모리 사용량 조건을 만족하는 물리머신을 확인한다.

둘째, SGX-EPC 영역의 내용은 SGX 기술의 특수한 명령어(EWB, ELDB)를 이용하여 일반 DRAM 으로 내보낼 수 있다. 이 때 SGX-EPC 영역의 데이터는 암호화되어 일반 DRAM 영역에 저장되므로, 암호화에 의한 오버헤드가 고려되어야 한다.

첫번째 조건은 SGX-EPC 를 활용하는 VM 을 주변의 물리머신으로 마이그레이션함으로서 SGX-EPC 활용 조건이 없는 VM 배치 최적화 문제로 변경한다. 모든 물리머신이 SGX-EPC 를 활용하고 있거나, SGX-EPC 를 활용 가능한 물리머신의 다른 자원이 부족한 경우 최적의 VM 배치를 보장할 수 없다.

이 경우 두번째 조건을 활용한다. 두번째 조건에서는 SGX-EPC 영역 중 일부를 비 SGX 영역의 일반 DRAM 으로 추출하여 실제로 활용 가능한 SGX-EPC 영역을 최대한 확보할 수 있다. SGX-EPC 영역의 실제 활용율을 모니터링하며, DRAM 으로 추출할 필요가 없을 때는 각 VM 이 SGX-EPC 영역을 직접 사용하도록 한다. 이를 통해, 첫번째 조건을 만족하지 못하는 경우에도 SGX-EPC 를 활용할 수 있도록 한다.

SGX-EPC 영역을 확보한 클라우드 VM 은 인클레이브 실행 영역의 무결성을 원격에서 검증할 수 있으며, 해당 메모리 영역의 사용자 데이터를 암호화하여 보관하므로, 기밀성을 강화할 수 있다.

Ⅲ. 결론 및 향후 연구

본 논문에서는 VM 마이그레이션을 통해 클라우드 VM 환경에서 인텔 SGX 기술을 활용하는 방법을 제시하였다. 인텔 SGX 기술을 활용하여 클라우드 VM 환경에서 신뢰 실행 환경을 구성하는 경우, 같은 물리머신에서 실행되는 모든 VM 이 SGX-EPC 영역을 정적으로 할당받아 활용한다. 하지만 SGX-EPC 영역은 물리적으로 제한되어 있으므로, 다른 물리머신으로 게스트 VM 을 이동하거나, SGX-EPC 영역을 DRAM 영역으로 추출하여 SGX-EPC 영역을 확보해야 한다.

향후 해당 기법의 평가와 실제 구현을 통한 성능 측정을 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업 (IITP-2020-2015-0-00363)과 과학기술정보통신부의 소프트웨어중심대학 지원사업 (2017-0-00091)의 지원을 받은 연구결과로 수행되었음.

참 고 문 헌

[1] Sean Christopherson, “Intel SGX Virtualization on Linux and KVM,” KVM forum 2018, https://kvmforum2018.sched.com/event/FzuR/intel-sgx-virtualization-on-linux-and-kvm-sean-christopherson-intel.

[2] Kai Huang, "Introduction to Intel SGX and SGX Virtualization,” Xen Developer and Design Summit, 2017, https://xendeveloperanddesignsummit2017.sched.com/event/AjFF/introduction-to-intel-sgx-and-sgx-virtualization-kai-huang-intel

[3] Andrew Baumann, Marcus Peinado, and Galen Hunt, “Shielding Applications from an Untrusted Cloud with Haven,” ACM Trans. Comput. Syst. 33, 3, Article 8 (September 2015), 26 pages. DOI:https://doi.org/10.1145/2799647

[4] Sergei Arnautov, et. al., “SCONE: secure Linux containers with Intel SGX,” In Proceedings of the 12th USENIX conference on Operating Systems Design and Implementation (OSDI'16). USENIX Association, USA, 689- 703.

[5] Chia-Che Tsai, Donald E. Porter, and Mona Vij, “Graphene-SGX: a practical library OS for unmodified applications on SGX,” In Proceedings of the 2017 USENIX Conference on Usenix Annual Technical Conference (USENIX ATC '17). USENIX Association, USA, 645- 658.

[6] Intel Software Guard extension, https://software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html

[7] Y. Wang and Y. Xia, "Energy Optimal VM Placement in the Cloud," 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2016, pp. 84-91, doi: 10.1109/CLOUD.2016.0021.

[8] A. Anand, J. Lakshmi and S. K. Nandy, "Virtual Machine Placement Optimization Supporting Performance SLAs," 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, 2013, pp. 298-305, doi: 10.1109/CloudCom.2013.46.