

## **An Effective Route to Control of the Safety of Accessing and Storing Data in the Cloud-Based Data Base**

**Authors :** Omid Khodabakhshi, Amir Rozdel

**Abstract :** The subject of cloud computing security research has allocated a number of challenges and competitions because the data center is comprised of complex private information and are always faced various risks of information disclosure by hacker attacks or internal enemies. Accordingly, the security of virtual machines in the cloud computing infrastructure layer is very important. So far, there are many software solutions to develop security in virtual machines. But using software alone is not enough to solve security problems. The purpose of this article is to examine the challenges and security requirements for accessing and storing data in an insecure cloud environment. In other words, in this article, a structure is proposed for the implementation of highly isolated security-sensitive codes using secure computing hardware in virtual environments. It also allows remote code validation with inputs and outputs. We provide these security features even in situations where the BIOS, the operating system, and even the super-supervisor are infected. To achieve these goals, we will use the hardware support provided by the new Intel and AMD processors, as well as the TPM security chip. In conclusion, the use of these technologies ultimately creates a root of dynamic trust and reduces TCB to security-sensitive codes.

**Keywords :** code, cloud computing, security, virtual machines

**Conference Title :** ICSE 2018 : International Conference on Continuous Software Engineering

**Conference Location :** Toronto, Canada

**Conference Dates :** July 19-20, 2018