# The Next Frontier



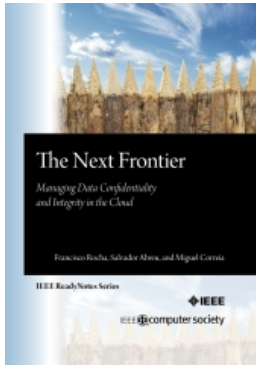**List Price: $19.00**

**Add to Cart**

IEEE Computer Society news and membership information

## Managing Data Confidentiality and Integrity in the Cloud
**Authored by Francisco Rocha, Salvador Abreu, Miguel Correia**

Many companies have embraced the benefits of cloud computing because of its pay-per-use cost model and the elasticity of resources that it provides. But from a data confidentiality and integrity viewpoint, moving a company's IT systems to a public cloud poses some challenges. System protection is often based on perimeter security, but in the cloud, the company's systems run on the cloud provider's hardware and coexist with software from both the provider and other cloud service consumers. Simply put, the cloud blurs the formerly clear separation between the trusted inside and the untrusted outside.

Malicious insiders represent a particularly significant concern for security in the cloud, as cloud operators and system administrators are unseen, unknown, and not onsite. Confidential data such as passwords, cryptographic keys, or files are just a few commands away from access by a malicious or incompetent system administrator.

This ReadyNote addresses the threat of malicious insiders in the context of clouds that provide the infrastructure as a service (IaaS) model, in the sense of clouds where consumers can run virtual machines. The text is complementary to several guidelines and reports on cloud security that have been published by organizations like the National Institute of Standards and Technology (NIST), the European Network and Information Security Agency (ENISA), and the Cloud Security Alliance.

**About the author:**

Francisco Rocha is a second-year PhD student with the School of Computing Science at Newcastle University, UK. His research interests include systems security, software security, and security architectures. His latest work focuses on developing prevention techniques that guarantee memory confidentiality and integrity for cloud consumers in the presence of malicious insiders in cloud computing. Francisco holds an MSc in Information Technology – Information Security (MSIT-IS) from the Information Networking Institute at Carnegie Mellon University.

Salvador Abreu is associate professor in the Department of Computer Science at the University of Évora and member of CENTRIA, the AI research center of the New University of Lisbon and University of Évora. He has participated in or coordinated research projects on logic and constraint programming, parallelism, and applications of declarative paradigms. His research interests include declarative programming language design and application to hard combinatorial search problems, including intrusion detection as well as parallel and distributed computing models.

Miguel Correia is associate professor in the Instituto Superior Técnico at the Technical University of Lisbon and researcher in the Distributed Systems Group at INESC-ID. He has a PhD from Faculdade de Ciências, University of Lisbon. He has been involved in several international and national research projects related to cloud computing, intrusion tolerance, and security. He has more than 100 publications, and his research interests include security, intrusion tolerance, distributed systems, cloud computing, and critical infrastructure protection.