Editorial Preface

Khaled M. Khan, Qatar University, Doha, Qatar

Outsourcing of computation is now a reality. Enterprises can outsource their computing needs, software to cloud computing. In addition to privacy and confidentiality of data, enterprises also need to ensure that their software remains confidential, meaning their algorithms and business processes should not be known even to cloud servers which execute the software owned by enterprises. This is more challenging than data confidentiality. Secure software engineering research community needs to explore how to design and develop such software that would not reveal the secret algorithms of the software to the very machine that processes the software. In other words, how to hide the actual computation from server.

This issue showcases three papers. The first paper by Oluwasefunmi and colleagues proposes an agent-based risk analysis system (ARAS) that collects threat events, probe them and correlates them using ontologies. The paper explores both quantitative and qualitative risk analysis techniques using real events data for probability predictions of threats based on security ontology. Poonam and Shailaja in the second paper presents a survey study of the security design pattern landscape. They identify shortcomings and presented future research directions related to security design pattern. The third paper by Shareeful and other researchers examines the research and practices related to risk management in cloud computing and discusses survey results on migration goals and risks.

I encourage for more submissions to IJSSE. Our review process usually takes maximum ten weeks to complete from the initial submission. We also welcome proposals for special issues on any topic related to secure software engineering. We also consider conference or workshop papers for special issues.

Khaled M. Khan
Editor-in-Chief
IJSSE