As the cloud computing is getting momentum, the need for secure software engineering has become an essential research agenda. The requirements for availability and responsiveness of cloud services virtually demand for secure seamless computing that does not require much overhead. That is, the research community has two options: either invent very efficient encryption-decryption techniques that need negligible processing overhead, or secure the system with nil or minimum encryption. The latter option is recently getting a lot of attraction. The idea is that the cloud providers as well as its servers should not know anything about the consumer’s data, although they process and store consumer’s data in their devices. The point is the cloud providers are expected to process consumers’ data without knowing the actual input and output. This objective would ensure confidentiality and privacy of consumer’s data on cloud. In order to achieve this, secure software engineering may come up with effective process and techniques that are less dependent on expensive encryption. This journal looks forward to exploring this topic further in the future.

In this issue, the first paper, by Yudis Asnar et al., presents the authors’ experience in designing security and dependability organizational patterns in an EU project. The paper uses an agent-goal-oriented modeling framework to analyze organizational settings as well as technical functionalities. Haralambos Mouratidis and Miao Kang in the second paper present their experience of designing a secure web based system. The paper is based on the principle of secure by design. The findings confirm the argument of incorporating security considerations from the early stages of the software development process, that is, secure by design.

The third paper, by Afonso Araújo Neto and Marco Vieira, proposes a methodology for detecting database security gaps based on a comprehensive list of security mechanisms which was used to perform a gap analysis of the security features of seven software packages. The main objective of the paper is to find how satisfying each software package is in order to accomplish the actual security goals that are expected from them. The fourth paper by Walid Al-Ahmad discusses the integration of XP with security activities based on the comprehensive lightweight application security process methodology. The paper argues that software developers using XP could build secure software by applying security measures in all phases and activities, thereby, minimizing the security vulnerabilities exploited by attackers.
As I noted in all previous issues, IJSSE is currently accepting new proposals for special issues on innovative areas of secure software engineering. In order to continue serve the secure software engineering community, we need more submissions. IJSSE is one of the few journals that adopt a fast review process. We do our best to finalize the review process within six-weeks. Look forward to seeing your work.

Khaled M. Khan
Editor-in-Chief
IJSSE