Construction of a Formal Software Verification System Practically Usable in Software Development

Project Leader
TAKATA, Yoshiaki, Ph.D.
Associate Professor, Information Systems Engineering

1. Objective

This project is aimed at:

Creating formal software verification systems integrated in real software development environments. Formal verification, such as model checking (a verification method based on exhaustive state-space search), is a promising approach to guarantee flawlessness of software. However, to obtain meaningful results, it requires elaboration when specifying a system model and a verification property, and therefore it has not been widely adopted in real software development projects. In this project, we try to develop a practical verification system that enables a user to conduct effective formal verification of software under development, but that does not require much learning time.

2. Project Outline

To that end, the project will consist of the following phases:

(a) Design a specification language for verification properties, which can be easily understood and used by software engineers and has sufficient expressive power for specifying verification properties useful in practical software development.
(b) Implement the verification system based on the designed specification language.
(c) Conduct experiments using the implemented system to evaluate the usefulness and feasibility of the proposed verification system.

3. Expected Performance

In this project, the successful candidate would be expected to:

(a) Work independently on a research topic.
(b) Understand the theory of model checking and other formal verification techniques.
(c) Develop an experimental system for evaluation.
(d) Collaborate with other lab members to explore new findings.

4. Required Skills and Knowledge

The successful candidate for this project will have the following knowledge and skills:

(a) Fundamental knowledge on the automata theory and the theory of computation,
(b) Mathematical capability to develop a new formal method, and
(c) Excellent programming skill in C, C++, Java, Python, and similar programming languages.

References

(1) P. Lamilla Alvarez and Y. Takata. “A Formal Verification of a Subset of Information-Based Access Control Based on Extended Weighted Pushdown System.” IEICE Trans. Information and Systems, E97-D(5), pp.1149—1159, (2014).

(2) J. Wang, Y. Takata, and H. Seki. “HBAC: A Model for History-based Access Control and Its Model

Checking.” In ESORICS 2006, LNCS 4189, pp.263—278, (2006).

See our admission guidelines:
https://www.kochi-tech.ac.jp/english/admission/ssp_aft19oct/ssp_application_guideline.html

Contact
E-mail: takata.yoshiaki@kochi-tech.ac.jp