

Results for A FRAMEWORK F... >

A Framework for Secure Software Engineering in Hybrid Agile Software Dev...



Full text at publisher

Export

Add To Marked List

< 1 of 1 >

A Framework for Secure Software Engineering in Hybrid Agile Software Development

By [Abu Bakar, NSA](#) (Abu Bakar, Normi Sham Awang) ^[1]; [Yahya, N](#) (Yahya, Norzariyah) ^[1]; [Maidin, SS](#) (Maidin, Siti Sarah) ^[2]
[Are you this author?](#)

Source [PERTANIKA JOURNAL OF SCIENCE AND TECHNOLOGY](#)

[← View Journal Impact](#)

Volume: 34 Issue: 4 Page: 2255-2273
DOI: 10.47836/pjst.34.4.14

Published [AUG 2026](#)

Indexed [2026-08-27](#)

Document Type [Article](#)

Abstract This study examines how Secure Software Engineering (SSE) practices can be applied while developing with Hybrid Agile methods. The Hybrid Agile approach combines disciplined

planning and extensive documentation, which are the hallmarks of traditional software development, with flexibility, incremental delivery and quick adoption for changing requirements contributed by Agile practices. Generally, existing secure software engineering frameworks only support either classical or Agile methods. As a result, Hybrid Agile implementations rarely provide enough guidance to integrate security throughout the full development life cycle. The purpose of this research is to investigate the current utilisation of secure software engineering practices in Hybrid Agile to identify and introduce security-focused coding elements designed for those environments. In line with the qualitative research approach being used, we evaluate current secure software practices in Hybrid Agile project implementation. In this study, interviews with professional programmers in diverse business sectors were conducted. It is evident that there is a lack of standardised security practices and that it is crucial for managers and project managers to encourage and support these. In addition, it is important that this study highlights the importance of automation tools in secure software engineering practices. With these findings in mind, this paper provides a structured approach for these organisations seeking to integrate security into Hybrid Agile projects and for improving the reliability and integrity of their software applications. The shift towards proactive environments in hybrid software applications requires an assessment of their software development life cycle to deal with security weaknesses and build tools for detecting possible threats in their applications.

Keywords

Author Keywords: [software engineering](#); [Software Development Lifecycle \(SDLC\)](#); [software security framework](#)

Author Information

Corresponding Address: Abu Bakar, Normi Sham (corresponding author)
Awang
Int Islamic Univ Malaysia, Fac ICT, Dept Comp Sci, Gombak 53100, Kuala Lumpur, Malaysia
E-mail Addresses : nsham@iium.edu.my
Addresses :
¹ Int Islamic Univ Malaysia, Fac ICT, Dept Comp Sci, Gombak 53100, Kuala Lumpur, Malaysia
▼ ² INTI Int Univ, Fac Data Sci & Informat Technol, Nilai 71800, Negeri Sembilan, Malaysia

E-mail Addresses :

nsham@iium.edu.my; norzariyah@iium.edu.my;
sitisarah.maidin@newinti.edu.my

**Categories/
Classification**

Research Areas: Science & Technology - Other Topics

**Web of Science
Categories**

[Multidisciplinary Sciences](#)

Funding

✓ [View funding text](#)

Funding agency	Grant number
Fundamental Research Grant Scheme	FRGS/1/2019/ICT01/UIAM/03/2

+ [See more data fields](#)

Journal information

[PERTANIKA JOURNAL OF SCIENCE AND TECHNOLOGY](#)

← [View Journal Impact](#)

ISSN 0128-7680

**Current
Publisher** UNIV PUTRA MALAYSIA PRESS, SERDANG,
SELANGOR 00000, MALAYSIA

**Research
Areas** Science & Technology - Other Topics

**Web of
Science
Categories** [Multidisciplinary Sciences](#)

0.16

Journal
Citation
Indicator™
(2025)

