IJASAT

International Journal on Islamic Applications in Computer Science and Technology

Peer-reviewed journal

Volume 14 *Issue 1*

March 2026

International Journal on Islamic Applications in Computer Science And Technology

Volume 14, Issue 1, March 2026

EDITED BY

Prof. Dr. Mohammed Zeki Khedher

ISSN (Online): 2289-4012

International Journal on Islamic Applications in Computer Science and Technology is published both in traditional paper form and in Internet. This journal is published at the website http://sign-ific-ance.co.uk, maintained by Design for Scientific Renaissance, Malaysia.

Design for Scientific Renaissance

Malaysia

Typesetting: Camera-ready by author

TABLE OF CONTENTS

FOREWORD

By the grace of Allah, it is a great pleasure to introduce this issue of: **The International Journal on Islamic Applications in Computer Science and Technology**

During the 13th year of the publication of this Journal, this issue is the 52nd of this journal. We thank Allah for enabling us to continue all through these years. With the wide specialization of this Journal, it attracted contributions from researchers from all over the world. We pray to Allah to put his "Baraka" in the contents of the Journal and spread the fruits of its contents in the future.

This issue contains three papers. The first one is entitled:

An Intelligent Model for Analyzing the (I'rāb) Syntax Parsing of the First Three Parts (Juz') of the Holy Quran

This paper focuses on unintentional employees' behaviors that have impacts on organizational information security, rather than unintentional behaviors in general IT practices. It explores unintentional information security behavior based on the perspective of the Qur'an and Hadith. Moreover, it provides some recommendations based on academic studies and Sharia teachings to overcome unintentional information security behavior. This paper starts with the discussion on information security behavior, human intentions based on the Sharia, and unintentional behavior under Islamic perspective. Finally, the significance of the study relies on the recommendation to reduce unintentional security threats based on information security studies and Sharia teachings by proposing a model to understand unintentional information security behavior and the factors that affect them.

The second paper is entitled:

Cyber Laws and Islamic Perspectives on Digital Ethics

This paper examines the intersection between cyber laws and Islamic perspectives on digital ethics. It analyzes how global and regional legal frameworks address digital threats while incorporating Shariah-based principles such as privacy, harm prevention, and public interest. By reviewing cyber regulations in countries such as Malaysia and Indonesia, alongside Islamic jurisprudential responses to issues like cyber-sectarian conflict and online exploitation of women, the study identifies key areas of convergence and gaps. Core Islamic concepts—including *maqasid al-shari'ah*, *ijtihad*, and *amanah*—are applied to emerging technologies such as artificial intelligence and social media platforms. Case studies from Muslim-majority contexts illustrate practical implementations, while challenges such as enforcement limitations and cultural differences are also discussed. The findings support a balanced approach to digital governance that integrates Islamic ethical accountability with effective legal mechanisms to promote trust and justice in cyberspace.

The third paper is entitled:

Explainable Privacy-Budget Governance for Multi-Service Educational AI Systems

This paper introduces a governance-oriented reformulation of existing differential privacy budget-allocation approaches for multi-service educational AI systems. Rather than proposing a new differential privacy mechanism, the approach embeds institutional policy constraints, fairness considerations, and interpretable decision rules directly into the privacy-budget allocation process. Each educational AI service is assigned a local privacy budget within a constrained global privacy limit ($\bar{\varepsilon}$), determined according to its pedagogical relevance, sensitivity to fairness disparities across student groups, and governance-defined explainability requirements.

The allocation process is formulated as a constrained multi-objective decision framework, where trade-offs among pedagogical utility, fairness sensitivity, and governance transparency are resolved through rule-based policies rather than black-box optimization strategies. An explainability layer produces auditable allocation justifications, counterfactual policy analyses, and governance logs designed to support institutional oversight. A structured comparative analysis compares the proposed approach with uniform, utility-only, and non-explainable allocation strategies using governance-relevant criteria such as policy traceability, fairness awareness, and auditability. The results demonstrate that the proposed framework provides stronger governance alignment and transparency, thereby bridging the gap between high-level AI governance principles and operational privacy management in educational AI systems