Al-Mau'izhoh: Jurnal Pendidikan Agama Islam E-ISSN: 2684-9410
Volume 7, Number 2, 2025, pp 180-185
DOI: https://doi.org/10.31949/am.v7i2.16844

Development of a Conceptual Islamic Cyber-Ethical Model (ICEM) for Cybersecurity Professionals Based on Digital Islamic Education Values

Asruddin[1], Muhammad Immawan Aulia[2], Oman Fathurohman Sw[3]
[1]Faculty of Industrial Technology, Department of Informatics, Ahmad Dahlan University, Yogyakarta, Indonesia
[2] Faculty of Industrial Technology, Department of Informatics, Ahmad Dahlan University, Yogyakarta, Indonesia
[3]Faculty of Islamic Studies, Ahmad Dahlan University, Yogyakarta, Indonesia

Article Info

Article history:

Received 09 12, 2025
Revised 12 12, 2025
Accepted 30 12, 2025

Keywords:

Islamic cyber ethics
Cybersecurity professionals
Digital Islamic Education
Conceptual model
Ethical hacking

ABSTRACT

Cybersecurity threats have become increasingly complex, requiring not only advanced technical competencies but also strong ethical foundations to guide responsible digital behavior. Current cybersecurity education often emphasizes technical skills but still lacks a comprehensive moral framework that integrates spiritual and ethical reasoning. This conceptual study develops the Islamic Cyber-Ethical Model (ICEM), a normative ethical framework derived from Islamic ethical principles and integrated into the paradigm of Digital Islamic Education. Using a library research method, this study synthesizes key Islamic ethical values amanah (trust), maslahah (public benefit), adab al-'ilm (ethics of knowledge), anti-fasad (prevention of harm), and moral responsibility with global cybersecurity ethics principles such as confidentiality, responsible disclosure, risk minimization, and prevention of misuse. The resulting model consists of five components: Niyyah Checkpoint, Amanah Assessment, Maslahah Justification, Anti-Fasad Filter, and the Responsible Disclosure Protocol. ICEM provides a structured ethical reference for decision-making in cybersecurity practices, vulnerability handling, and digital responsibility. This model contributes theoretically to Islamic cyber ethics and offers a conceptual foundation for future empirical validation, curriculum development, and training programs for cybersecurity professionals.

INTRODUCTION

Cybersecurity issues such as data theft, system intrusion, privacy violations, and vulnerability exploitation continue to escalate in frequency and complexity. These challenges demand cybersecurity professionals who not only possess advanced technical competencies but also demonstrate strong ethical judgment in handling sensitive systems and data. However, most cybersecurity education and professional training programs still prioritize technical skills, while ethical, moral, and spiritual dimensions receive comparatively limited attention, despite their critical role in shaping responsible digital behavior.

Recent studies consistently highlight human factors as a major source of cybersecurity vulnerability, where users' knowledge, attitudes, and behaviors significantly influence security outcomes. Empirical research conducted among Indonesian students indicates that cybersecurity awareness and behavioral factors strongly affect how individuals protect personal data and interact in digital environments (Chasanah & Candiwan, 2020). These findings reinforce the importance of integrating ethical awareness into cybersecurity education, beyond purely technical safeguards.

Alongside this, emerging literature on Islamic-based digital ethics has begun to explore how Islamic values can guide responsible behavior in digital contexts. Studies by (Saputra, Fasa, & Ambarwati, 2022) demonstrate that Islamic principles such as amanah (trust) and maslahah (public benefit) can be systematically applied to issues of online consumer data security, positioning Islamic ethics as a relevant moral framework for digital decision-making. Similarly, (Komaruddin, Utama, Sudarmanto, & Sugiono, 2023) show a strong alignment between Islamic teachings on trust, secrecy, and public interest and contemporary expectations regarding data protection, confidentiality, and responsible information handling in cyberspace.

Despite these developments, existing studies remain fragmented across different domains, including cybersecurity awareness, digital citizenship, and Islamic digital ethics. Most works address ethical issues at a general user or consumer level, without offering a unified conceptual framework specifically designed for cybersecurity professionals who routinely face complex operational dilemmas such as vulnerability assessment, penetration testing, and responsible disclosure. Furthermore, studies on Digital Islamic Education and digital citizenship have not yet been systematically linked to the professional practices and ethical decision-making processes within cybersecurity operations.

Based on these limitations, this study seeks to construct a conceptual Islamic Cyber-Ethical Model (ICEM) that integrates Islamic ethical principles, cybersecurity ethics, and the paradigm of Digital Islamic Education into a single coherent framework. The study aims to identify Islamic ethical values relevant to cybersecurity, analyze ethical challenges

Corresponding Author:
Asruddin
Email: 2537083018@webmail.uad.ac.id

encountered by cybersecurity professionals, and develop a structured conceptual model that can guide ethical decision-making in professional cybersecurity practice. The novelty of this research lies in proposing ICEM as the first structured Islamic ethical framework tailored specifically for cybersecurity professionals, establishing a new theoretical intersection between Islamic ethics, cybersecurity ethics, and Digital Islamic Education, and providing a conceptual foundation for curriculum development and professional training in Islamic cybersecurity ethics.

METHODS

This study uses a library research method and a conceptual model development approach. The research does not involve empirical data collection but relies on systematic analysis and synthesis of existing literature.

Study Design

The study adopts a descriptive–analytical design that synthesizes three major bodies of literature:

a. Islamic ethical literature (classical and contemporary) discussing amanah, maslahah, adab al-'ilm, anti-fasad, and moral responsibility.
b. Cybersecurity and digital ethics literature, focusing on professional responsibility, vulnerability disclosure, and ethical use of security tools.
c. Digital Islamic Education and digital citizenship literature, particularly studies on how Islamic education contributes to ethical digital behavior and responsible digital citizenship.

Data Sources

Relevant literature was obtained from:

a. Scopus-indexed and SINTA-indexed journals in cybersecurity, ethics, and Islamic education.
b. Peer-reviewed articles on Islamic ethics and Islamic moral philosophy applied to digital contexts.
c. Empirical studies on cybersecurity awareness, digital citizenship, and Islamic-based digital ethics published between 2020 and 2025.

By emphasizing recent peer-reviewed journals, the study ensures that the conceptual model reflects current discussions in both cybersecurity and Islamic studies.

Procedure and Data Analysis

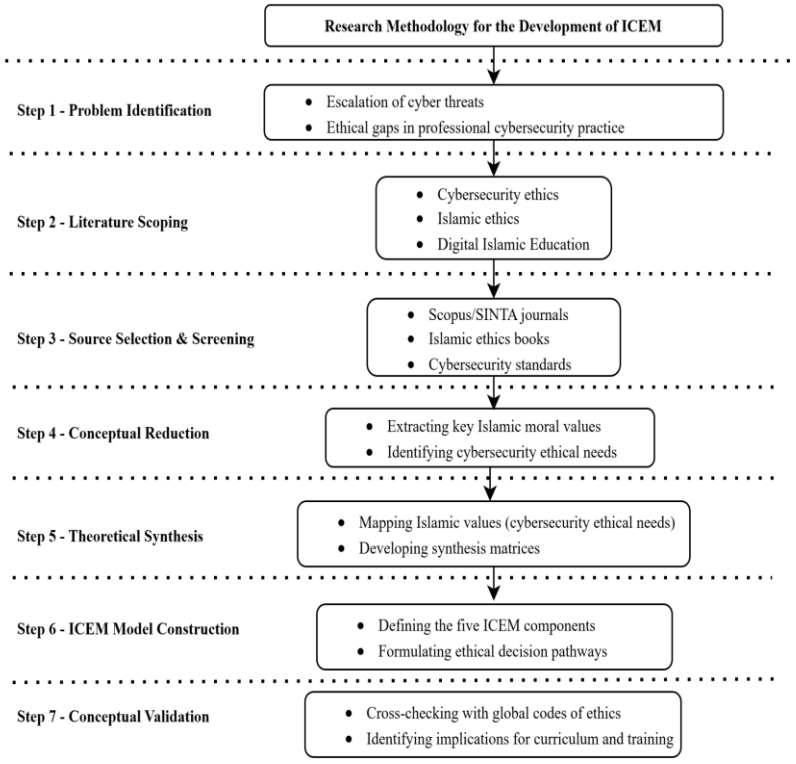

Figure 1. Research Methodology for the Development of ICEM

The conceptual development process followed several structured stages (represented as a flow in Figure 1 in the full paper layout):

a. Problem clarification - identifying ethical challenges in cybersecurity practice that are not adequately addressed by existing curricula and codes.
b. Literature mapping - classifying relevant works into three clusters: cybersecurity ethics, Islamic ethics, and Digital Islamic Education.
c. Conceptual reduction - selecting core Islamic ethical values and key cybersecurity ethical needs that are most directly related to professional practice.

d. Theoretical synthesis - aligning Islamic ethical concepts with concrete cybersecurity dilemmas (e.g., penetration testing, vulnerability disclosure, dual-use tools).
e. Model structuring - formulating ICEM's components (Niyyah Checkpoint, Amanah Assessment, Maslahah Justification, Anti-Fasad Filter, Responsible Disclosure Protocol).
f. Internal consistency review - checking the logical coherence of the model and its compatibility with both Islamic moral reasoning and cybersecurity practice.
g. Implication mapping - identifying potential applications in curriculum development, training design, and organizational policy.

This procedure ensures theoretical clarity while keeping the model directly linked to practical needs in cybersecurity.

RESULTS AND DISCUSSION

Overview of the Islamic Cyber-Ethical Model (ICEM)

The main result of this conceptual study is the formulation of the Islamic Cyber-Ethical Model (ICEM), which structures Islamic ethical principles into a decision-making framework for cybersecurity professionals. ICEM is designed as a normative guide that can be applied when professionals face ethical dilemmas in activities such as penetration testing, vulnerability assessment, incident response, and threat intelligence operations.

ICEM consists of five core components:

a. Niyyah Checkpoint - examination of intention before engaging in any cybersecurity action.
b. Amanah Assessment - evaluation of trust, confidentiality, and accountability obligations.
c. Maslahah Justification - justification of actions based on the public benefit and harm minimization.
d. Anti-Fasad Filter - screening to prevent corruption, misuse, and destructive consequences of technical capabilities.
e. Responsible Disclosure Protocol - guidance on ethically reporting and handling vulnerabilities.

These components are grounded in Islamic values and aligned with widely accepted expectations of responsible professional conduct in cybersecurity.

Table 1. Synthesis of Islamic Ethical Values and Cybersecurity Ethical Needs

Islamic Value	Core Meaning	Cybersecurity Ethical Need	ICEM Component Mapping
Amanah	Safeguarding trust and entrusted resources	Confidentiality, accountability	Amanah Assessment
Maslahah	Promoting public benefit and preventing harm	Risk reduction, secure-by-design	Maslahah Justification
Adab al-'ilm	Ethical use, seeking, and sharing of knowledge	Ethical hacking, lawful authorization	Niyyah Checkpoint
Anti-fasad	Avoiding corruption, damage, and unjust harm	Misuse prevention, abuse control	Anti-Fasad Filter
Moral responsibility	Accountability before God and society	Responsible disclosure, transparency	Responsible Disclosure Protocol

The table 1. shows how core Islamic values can be systematically mapped onto cybersecurity ethical needs. Instead of merely adding religious terminology to existing ethics, ICEM reinterprets cybersecurity activities through an Islamic moral lens and translates values into operational checkpoints.

Overview Conceptual Structure of the Islamic Cyber-Ethical Model (ICEM)

At the foundational level, Digital Islamic Education (PAI Digital) nurtures the internalization of Islamic ethical values, including amanah, maslahah, adab al-ilm, anti-fasad, and moral responsibility. These values feed into the five ICEM components - Niyyah Checkpoint, Amanah Assessment, Maslahah Justification, Anti-Fasad Filter, and Responsible Disclosure Protocol which subsequently guide professional cybersecurity practices such as secure system design, ethical penetration testing, vulnerability management, and incident response.

In practice, ICEM can be visualized as a layered model:

a. Layer 1 – Islamic Ethical Values (PAI Digital Context):
   Consists of core Islamic values such as amanah, maslahah, adab al-'ilm, anti-fasad, and moral responsibility. These values form the ethical foundation that informs all subsequent reasoning and actions in cybersecurity.
b. Layer 2 – Five Core Components of ICEM:

Includes Niyyah Checkpoint, Amanah Assessment, Maslahah Justification, Anti-Fasad Filter, and the Responsible Disclosure Protocol. These components serve as ethical checkpoints embedded within cybersecurity workflows.

c. Layer 3 – Ethical Decision-Making in Cybersecurity:
Represents the real-world application of the ICEM components in professional contexts, including vulnerability handling and ethical hacking, incident response and disclosure, and the daily digital responsibilities of cybersecurity practitioners.

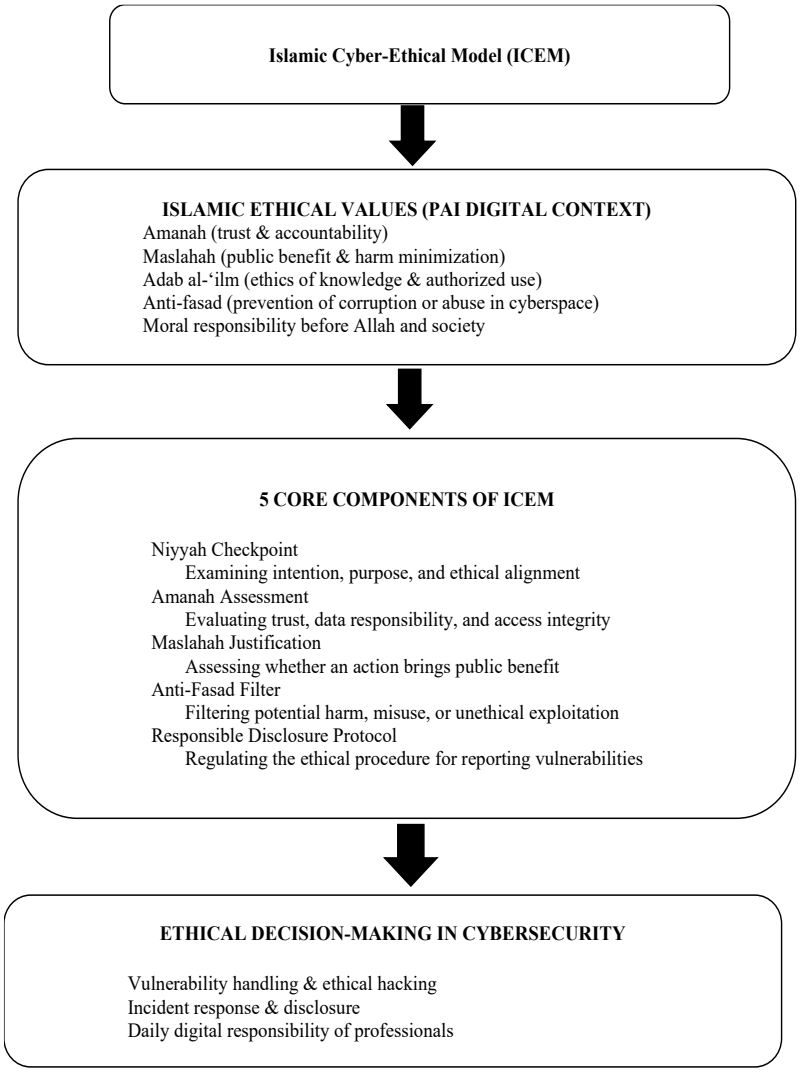

Figure 2. Conceptual Structure of the Islamic Cyber-Ethical Model (ICEM)

Niyyah Checkpoint: Intention in Cybersecurity Practice

The Niyyah Checkpoint ensures that every cybersecurity action begins with a clear and ethically sound intention. Before running a penetration test, scanning a network, or analyzing user logs, professionals are encouraged to reflect on whether their intention is genuinely oriented toward system protection, risk reduction, and organizational benefit - rather than personal curiosity, prestige, or economic gain.

Operationally, this component can be integrated as a pre-action checklist:

a. Is the activity fully authorized?
b. Is the objective aligned with organizational security goals?
c. Could the action drift into unnecessary data exposure or privacy violation?

By formalizing intention as a checkpoint, ICEM translates a core Islamic principle into a practical control in security operations.

Amanah Assessment: Trust, Confidentiality, and Accountability

In cybersecurity, professionals are frequently entrusted with privileged access to systems, data, and sensitive configurations. The Amanah Assessment requires professionals to evaluate:

a. What assets (data, systems, credentials) are being entrusted to them.
b. How their actions might impact confidentiality, integrity, and availability.
c. What accountability mechanisms (logging, supervision, reporting) are in place.

This component reinforces the idea that access rights, encryption keys, and administrative privileges are forms of amanah that must not be exploited - even when misuse is technically possible and difficult to detect. It encourages organizations to design policies where every high-privilege action is both technically controlled and ethically framed as a trust.

Maslahah Justification: Public Benefit and Harm Minimization

Maslahah Justification focuses on assessing whether a planned action will lead to greater benefit or risk. In cybersecurity operations, professionals often face trade-offs-for example, conducting aggressive testing in a production environment might reveal critical weaknesses but also risk disrupting services.

ICEM encourages professionals to:

a. Evaluate potential harms and benefits in both technical and social terms.
b. Prefer methods that minimize disruption while still achieving security goals.
c. Document the justification of high-risk actions, including alternatives that were considered but rejected.

This aligns Islamic legal reasoning on maslahah with established practices of risk assessment and change management in cybersecurity work.

Anti-Fasad Filter: Preventing Misuse and Corruption

The Anti-Fasad Filter operates as a safeguard against the misuse of technical skills and tools. It raises questions such as:

a. Can a specific tool, exploit, or script be easily diverted for malicious use inside or outside the organization?
b. Are there adequate controls to prevent the leakage of sensitive knowledge, proof-of-concept exploits, or configuration details?
c. Does a planned action indirectly support harmful activities (for example, sharing too-detailed vulnerability information with untrusted parties)?

By integrating anti-fasad into operational decision-making, ICEM directly addresses the dual-use dilemma that is common in cybersecurity: tools and skills that can be used for protection can also be deployed for harm.

Responsible Disclosure Protocol: Ethical Vulnerability Reporting

The Responsible Disclosure Protocol provides ethical guidance on how vulnerabilities should be communicated and remediated. It promotes:

a. Coordinated disclosure to affected stakeholders within reasonable and agreed time frames.
b. Avoiding premature public disclosure that would significantly increase risk before mitigation is in place.
c. Maintaining clear documentation of findings, communication, and remediation steps.

This component mirrors industry practices of responsible disclosure but frames them within the Islamic notions of nasihah (sincere advice) and moral responsibility toward both system owners and end-users whose data and services are at stake. Conceptually, it extends discussions on Islamic digital ethics from consumer data protection into the operational life cycle of cybersecurity work (Saputra, Fasa, & Ambarwati, 2022).

CONCLUSION

This study has developed the Islamic Cyber-Ethical Model (ICEM) as a conceptual framework for guiding cybersecurity professionals based on Islamic ethical values and the paradigm of Digital Islamic Education. The model translates core Islamic principles-niyyah, amanah, maslahah, anti-fasad, and moral responsibility-into five structured ethical components: the Niyyah Checkpoint, Amanah Assessment, Maslahah Justification, Anti-Fasad Filter, and Responsible Disclosure Protocol. Collectively, these components provide a normative guide for ethical decision-making in cybersecurity practices such as vulnerability assessment, ethical hacking, incident response, and disclosure management.

From a theoretical perspective, ICEM contributes to the emerging field of Islamic cyber ethics by systematically linking Islamic moral reasoning with contemporary cybersecurity ethics and professional expectations. Practically, the model offers a conceptual foundation for designing curricula, training modules, and organizational guidelines for cybersecurity professionals, particularly in contexts where Islamic ethics are considered an integral part of professional identity and digital responsibility. By embedding ethical checkpoints into cybersecurity workflows, ICEM extends discussions on Islamic digital ethics beyond general digital behavior toward concrete professional practices.

Nevertheless, this study is limited by its purely conceptual nature. The ICEM framework is derived from literature synthesis and normative analysis rather than empirical observation or experimental validation. As such, its effectiveness in influencing professional behavior and ethical decision-making has not yet been empirically tested. Future research is therefore encouraged to validate the model through empirical studies in cybersecurity education and professional training contexts, to develop and evaluate instructional modules and case-based learning materials grounded in ICEM, and to examine the impact of integrating ICEM into organizational policies and codes of conduct on ethical culture and decision-making within cybersecurity teams.

ACKNOWLEDGMENT

The author would like to thank colleagues and institutions that provided constructive feedback on the development of this conceptual model, as well as the academic community whose works on Islamic ethics, cybersecurity, and digital education formed the foundation of this study.

REFERENCES

Abu, A., Alhabsyi, F., & Ruslin, S. H. (2015). Digital Islamic Education Learning in Secondary Schools: Educational Quality and Student Engagement. *Jurnal Pendidikan Islam*, 133-148.

Al-Aidaros, A.-H., Shamsudin, F. M., & Idris, K. M. (Ethics and Ethical Theories from an Islamic Perspective). 2023. *An Islamic perspective. Journal of Moral Education*, 1-13. doi:https://doi.org/10.24035/ijit.4.2013.001

Al-Hamad, A. &.-H. (2023). Exploring ethical digital behaviour among Gulf youth: An Islamic perspective. *Journal of Moral Education*, 195–214.

Alqaralleh, B., & Alsmadi, I. (2022). Ethical decision-making in cybersecurity: A conceptual review. *Journal of Cybersecurity*.

Alshaikh, M. (2020). Developing cybersecurity culture: A behavioural framework for organisational change. *Computers & Security*.

Chasanah, B. R., & Candiwan. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia. *SISFORMA: Journal of Information Systems*.

Hilman, C. (2025). Digital-based Islamic religious education: Enhancing student engagement and spiritual understanding. *Jurnal Pendidikan Islam*.

Ibrahim, R. M. (2021). Cybersecurity awareness and behaviour among university students: A systematic review. Education and Information Technologies.

Juhaidi, A., Fitria, A., Hidayati, N., & al., e. (2023). Digital citizenship of Generation Z in Indonesia: Does Islamic higher education matter? Journal of Higher Education Theory and Practice. *Journal of Higher Education Theory and Practice*, 165–181. doi:https://doi.org/10.33423/jhetp.v23i13.6325

Khan, M. A., & Azhar, A. (2024). Islamic perspectives on AI and digital ethics: Principles for responsible technology development. *Journal of Islamic Thought and Civilization*, 99–118.

Komaruddin, K., Utama, A. S., Sudarmanto, E., & Sugiono. (2023). Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications. *West Science Law and Human Rights*, 166-172. doi:https://doi.org/10.58812/wslhr.v1i04.323

Kumar, A., & Somani, A. (2022). Cybersecurity challenges in the digital era: A review. *Journal of Cybersecurity and Privacy*, 610-628.

Mubiarto, A. N. (2024). Challenges and opportunities for Islamic education in the era of digital literacy. *Journal of Islamic Education Studies. 233–245. doi:https://doi.org/10.70963/jm.v1i2.166

Muharromah, L., & Manshur, U. (2025). Digital Ethics in the Perspective of Islamic Education: Cultivating Religious Awareness in Cyberspace. *Journal of Educational Management Research* , 2484-2497. doi:https://doi.org/10.61987/jemr.v4i3.1397

Pabbajah, T., Abdullah, I., & Salik, M. (2021). From the scriptural to the virtual: Indonesian engineering students' responses to the digitalization of Islamic education. *Teaching Theology & Religion*, 212–223.

Putra, A., & Nasution, R. (2022). Understanding digital responsibility and online ethics among Indonesian university students. *Journal of Applied Information Science*, 122–134.

Rahman, M., & Yusuf, F. (2022). Islamic ethical reasoning in the digital age: A framework for Muslim digital behaviour. *Journal of Islamic Ethics*, 45–63.

Saputra, A. A., Fasa, M. I., & Ambarwati, D. (2022). Islamic-Based Digital Ethics: The Phenomenon of Online Consumer Data Security. *Share: Jurnal Ekonomi dan Keuangan Islam*.

Yusoff, S., & Ahmad, K. (2021). Digital citizenship among Muslim youth: Integrating Islamic values in digital engagement. *Journal of Information and Communication Technology*, 565–584.