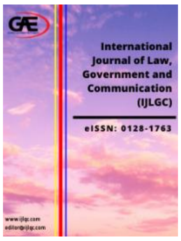
International Journal of
Law, Government and Communication
IJLGC
EISSN : 0128-1763

Volume 10 Issue 40 (June 2025) PP. 590-604
DOI 10.35631/IJLGC.1040041



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.ijlgc.com

GLOBAL ACADEMIC EXCELLENCE

ISLAMIC PERSPECTIVES ON AI AND CYBERSECURITY: DEVELOPING ETHICAL FRAMEWORKS FOR AUTONOMOUS SECURITY SYSTEMS

Ramlan Mustapha[1*], Siti Raudah Abdul Karim[2], Nurshahira Ibrahim[3], Norhapizah Muhd Burhan[4], Najmi Hayati[5]

[1] Academy of Contemporary Islamic Studies, Universiti Teknologi MARA Pahang, Raub Campus, Malaysia
Email: ramlan@uitm.edu.my
[2] Academy of Contemporary Islamic Studies, Universiti Teknologi MARA Shah Alam Selangor, Malaysia
Email: sitiraudah@uitm.edu.my
[3,4] Academy of Contemporary Islamic Studies, Universiti Teknologi MARA Pahang, Jengka Campus, Malaysia
Email: hahiraibrahim@uitm.edu.my, kppacispahang@uitm.edu.my
[5] Department of Islamic Education, Islamic University of Riau, Indonesia
Email: najmihayati@fis.uir.ac.id
[*] Corresponding Author

Article Info:

Article history:
Received date: 30.03.2025
Revised date: 15.04.2025
Accepted date: 27.05.2025
Published date: 30.06.2025

To cite this document:

Mustapha, R., Abdul Karim, S. R., Ibrahim, N., Burhan, N. M., & Hayati, N. (2025). Islamic Perspectives On AI And Cybersecurity: Developing Ethical Frameworks For Autonomous Security Systems. *International Journal of Law, Government and Communication, 10* (40), 590-604.

DOI: 10.35631/IJLGC.1040041

Abstract:

The rapid advancement of artificial intelligence (AI) and autonomous cybersecurity systems has created an urgent need for culturally sensitive ethical frameworks that address the diverse moral traditions of global communities, particularly as existing AI governance approaches have been predominantly Western-centric, leaving approximately 1.8 billion Muslims underserved by current ethical standards. This study develops and validates a comprehensive Islamic ethical framework for autonomous cybersecurity systems through expert consensus methodology, employing the Nominal Group Technique (NGT) with nine experts representing Islamic jurisprudence, cybersecurity, AI ethics, and technology policy to establish a four-construct framework integrating Maqāṣid al-Sharīʿah (objectives of Islamic law) with contemporary cybersecurity requirements. The framework encompasses Islamic Ethical Foundation (Akhlaq) with theological principles of Tawhid, Khilafah, Fitrah, Hikmah, and Adl; Maqasid al-Shariah operationalizing protective objectives of religion, life, intellect, progeny, and wealth; AI Governance Principles translating Islamic values into transparency, accountability, beneficence, non-maleficence, and privacy protection; and Cybersecurity Ethics addressing trust, proportionality, necessity, consent, and data sanctity. Expert consensus validation achieved above 70% agreement across all framework components, with individual constructs receiving 77.8% to 88.9% consensus, demonstrating systematic integration of Islamic principles with technical requirements while maintaining cultural authenticity and religious compliance, ultimately contributing to pluralistic approaches to AI ethics that respect diverse ethical traditions and promote human dignity in an increasingly digitized world.

Keywords:

Islamic AI Ethics, Cybersecurity Framework, Maqāṣid al-Sharīʿah, Autonomous Systems, Islamic Jurisprudence, AI Governance Nominal Group Technique

Introduction

The rapid advancement of artificial intelligence (AI) and autonomous systems has revolutionised cybersecurity capabilities, enabling automated threat detection, response, and mitigation without human intervention. However, these technological developments present unprecedented ethical challenges that require comprehensive frameworks grounded in diverse moral traditions (Alamro et al., 2023; Kim et al., 2021). While the prevailing discourse on AI ethics has been predominantly Western or Eurocentric, there is an urgent need for pluralist approaches that incorporate alternative ethical perspectives to address the global nature of AI technologies (Bedoui & Mansour, 2023). Islamic ethical frameworks, rooted in centuries of jurisprudential development and moral philosophy, offer valuable insights for developing ethical guidelines for autonomous cybersecurity systems that serve diverse global communities while maintaining moral integrity and social responsibility.

The intersection of AI, cybersecurity, and Islamic ethics has gained significant scholarly attention as Muslim-majority countries increasingly adopt advanced digital technologies while seeking to maintain their cultural and religious values. As rapid advancements in AI technologies pose challenges surrounding autonomy, privacy, fairness, and transparency, the prevailing ethical discourse has been predominantly Western or Eurocentric (Bedoui & Mansour, 2023). Recent research has emphasized the significance of both textual and non-textual Islamic sources in addressing these uncertainties while placing a strong emphasis on the notion of "good" or "maṣlaḥa" as a normative guide for AI's ethical evaluation (Bedoui & Mansour, 2023). This growing body of literature demonstrates how Islamic virtue-based ethics can provide a holistic Islamic virtue-based AI ethics framework grounded in the context of Islamic objectives (maqāṣid) as an alternative ethical system for AI governance (Raquib et al., 2022).

The development of autonomous cybersecurity systems presents unique challenges that require careful consideration of Islamic jurisprudential principles, particularly in areas of decision-making autonomy, accountability, and the protection of human dignity. Components that highlight the protection of life (hifz al-nafs), lineage (hifz al-nasl), intellect (hifz al-'aql), and property (hifz al-mal) are also discussed to address issues related to the AI threat to human security, social interaction, human resources, and legal rights, respectively (Kamali et al., 2021). The concept of Maqāṣid al-Sharīʿah (objectives of Islamic law) provides a comprehensive framework for evaluating the ethical implications of autonomous systems, as demonstrated in recent studies on cybersecurity applications (Osman et al., 2020; Ibrahim et al., 2015). This approach emphasizes investigating the ethical implications of cybersecurity for upholding Islam, including concerns about personal information, censorship, and freedom of speech while ensuring that technological solutions align with Islamic principles of justice, accountability, and human welfare (Osman et al., 2021).

The practical implementation of Islamic ethical frameworks in autonomous cybersecurity systems requires addressing contemporary challenges such as algorithmic transparency, data protection, and the balance between security and privacy. In Islam, privacy is a fundamental value that is deeply rooted in the principles of Shariah law and focuses on the dignity of the individual, personal boundaries and moral behaviour (Darus et al., 2024). Recent developments in countries like Saudi Arabia and the United Arab Emirates demonstrate how Islamic nations are integrating cultural and ethical values with technological innovation through the development of AI ethics principles that incorporate Shariah-compliant guidelines (Darus et al., 2024). This research contributes to the growing discourse on developing culturally sensitive and religiously grounded approaches to AI governance, offering a framework that can guide policymakers, technologists, and Islamic scholars in creating autonomous cybersecurity systems that are both technically effective and ethically sound by Islamic principles.

The proliferation of autonomous cybersecurity systems in contemporary society has generated multifaceted challenges that disproportionately affect Muslim communities and require urgent attention from both technological and ethical perspectives. Recent cyberattacks on critical infrastructure in Muslim-majority countries, such as the 2012 Shamoon virus attack on Saudi Aramco that infected over 35,000 computers, demonstrate the vulnerability of Islamic nations to sophisticated cyber threats and highlight the need for culturally appropriate security frameworks (Hassan et al., 2014). The increasing digitisation of Islamic financial institutions, educational systems, and government services has created new attack vectors that threaten not only economic stability but also the preservation of Islamic values and cultural identity in digital spaces (Rabbani et al., 2022). Furthermore, the reliance on Western-developed AI systems for cybersecurity purposes raises concerns about algorithmic bias, surveillance overreach, and the potential erosion of privacy rights that are fundamental to Islamic jurisprudence.

The ethical implications of autonomous decision-making in cybersecurity present particularly complex challenges for Muslim societies, where the concept of human accountability (taklīf) and divine sovereignty (hakimiyyah) must be balanced with technological efficiency and security imperatives. Contemporary issues include the deployment of AI systems that make life-and-death decisions about network access, financial transactions, and personal data without adequate human oversight, potentially conflicting with Islamic principles that emphasize human responsibility and divine authority (Ali, 2023). The use of predictive algorithms in cybersecurity that may discriminate against individuals based on religious affiliation, cultural practices, or geographical location presents serious concerns about justice ('adl) and fairness, core principles in Islamic ethics (Elmahjub, 2023). Moreover, the opacity of machine learning algorithms used in autonomous security systems creates challenges for the Islamic requirement of transparency (bay'an) in decision-making processes, particularly when these systems affect fundamental rights related to the protection of life, intellect, lineage, property, and religion.

The global nature of cyber threats has created an urgent need for international cooperation in developing ethical frameworks for autonomous cybersecurity systems, yet current collaborative efforts often overlook Islamic perspectives and the specific needs of Muslim communities. The lack of representation of Islamic scholars and ethicists in major AI governance initiatives, such as the Partnership on AI, IEEE's Ethics Certification Program, and various national AI strategies, has resulted in frameworks that may inadvertently conflict with Islamic values and legal principles (Asiri et al., 2023). This exclusion is particularly problematic given that approximately 1.8 billion Muslims worldwide are increasingly dependent on digital technologies for banking, education, healthcare, and religious practice, making them stakeholders in the development of ethical AI systems. Additionally, the digital divide between developed and developing nations means that many Muslim-majority countries are consumers rather than creators of AI technologies, potentially subjecting their populations to ethical frameworks that do not align with their cultural and religious values.

The development of an Islamic ethical framework for autonomous cybersecurity systems addresses several critical gaps in current research and practice that have left Muslim communities underserved and potentially vulnerable to ethically problematic technological implementations. The prevailing discourse on AI ethics has been predominantly Western or Eurocentric, creating an urgent need for pluralist approaches that incorporate alternative ethical perspectives to address the global nature of AI technologies (Elmahjub, 2023). This Western-centric approach fails to adequately address the unique ethical considerations, cultural values, and legal principles that govern decision-making in Islamic societies, where approximately 1.8 billion Muslims worldwide are increasingly dependent on digital technologies for critical aspects of their lives, including banking, education, healthcare, and religious practice.

The literature reveals significant gaps in understanding how Islamic jurisprudential principles can guide the development and deployment of autonomous cybersecurity systems. While several studies have explored AI ethics from various cultural and religious perspectives, there remains a notable absence of comprehensive frameworks that specifically address cybersecurity applications through an Islamic lens (Shamdi et al., 2022). Current research has investigated the integration of AI into some Islamic governance components, such as juristic, values, and cultural aspects in isolated contexts, but none have approached this as an integrated whole, thus ignoring the relational dynamics between the components of Islamic governance systems (Shamdi et al., 2022). This fragmented approach fails to capture the holistic nature of Islamic ethical decision-making, which requires consideration of multiple interconnected principles simultaneously rather than addressing individual concerns in isolation.

Research Aims

The primary objective of this research is to develop and validate an Islamic ethical framework for autonomous cybersecurity systems that integrates Maqāṣid al-Sharīʿah (objectives of Islamic law) with contemporary cybersecurity requirements through a structured expert consensus approach.

Literature review

Theoretical Foundations

The intersection of Islamic ethics and artificial intelligence represents a critical emerging field that challenges the predominantly Western-centric approach to AI governance and cybersecurity. The prevailing ethical discourse surrounding AI has been predominantly Western or Eurocentric, creating an imbalance that necessitates the integration of diverse religious and cultural perspectives (Qadir et al., 2023). Islamic ethics, grounded in the Qur'an and Sunnah, provides a comprehensive moral framework that emphasizes human welfare (maṣlaḥa) and the preservation of essential human interests through the Maqāṣid al-Sharīʿah. The notion of maqasid was first clearly articulated by al-Ghazali (died 1111), who argued that maslaha was God's general purpose in revealing the divine law, and that its specific aim was preservation of five essentials of human well-being: religion, life, intellect, lineage, and property (Wikipedia, 2024). This foundational framework has been expanded by contemporary scholars to address modern technological challenges, with Islamic virtue-based AI ethics framework grounded in the context of Islamic objectives (maqāṣid) as an alternative ethical system for AI governance (Ahmad et al., 2022). The growing literature demonstrates how Islamic ethical principles can inform the development of autonomous security systems while maintaining alignment with religious values and promoting human dignity in an increasingly digitized world.

Islamic Ethical Frameworks for AI Development

Recent scholarship has established robust theoretical foundations for integrating Islamic principles into AI development and governance. Islamic systems of ethical value are complex and multifaceted, characterized by multiple layers of highly abstract and often conflicting meta-ethical and normative propositions, rather than simple divine command theory (Qadir et al., 2023). The Islamic approach to AI ethics emphasizes both textual sources (Qur'an and Hadith) and rational deliberation (ijtihād) to address contemporary technological challenges. Religious traditions including Christianity, Islam, Judaism, and Buddhism offer invaluable perspectives on justice, equality, compassion, and responsibility, guiding decision-making processes, promoting the common good, and holding individuals and organizations accountable for their actions and decisions (AI and Faith, 2024). The virtue-based approach to Islamic AI ethics focuses on cultivating moral character in both individuals and institutions responsible for AI development, ensuring that technological advancement aligns with spiritual and ethical growth. This framework addresses key AI ethical concerns including autonomy, privacy, fairness, and transparency through distinctly Islamic lenses, emphasizing concepts such as 'adl (justice), raḥmah (compassion), and human stewardship (khilāfah) over creation. The integration of these principles creates a holistic approach that balances technological innovation with moral responsibility, offering an alternative to purely secular ethical frameworks.

Cybersecurity and Privacy Through Islamic Jurisprudence

Islamic perspectives on cybersecurity are fundamentally grounded in the concept of privacy protection as an essential component of human dignity. The Islamic concept of privacy is unique and differs from the Western legal approach in that it emphasises the importance of adherence to Shariah teachings and provides a strict and clear explanation for desirable behaviour in doubtful and ambiguous cases (Osman, 2024). In Islamic ethics, privacy is closely linked to human dignity, with protecting privacy seen as a means to preserve the dignity and honour of individuals through the principle of "satr," referring to the covering or concealing of faults and private matters (Diplo, 2025). The application of Maqāṣid al-Sharī'ah to cybersecurity demonstrates practical frameworks for evaluating digital security measures against Islamic objectives. Facebook users derive certain benefits from their Facebook use that assist them to achieve Maqasid al-Shariah's higher objectives, while human beings face certain security threats which hamper their achievements of these Maqasid higher objectives (Osman et al., 2021). Recent research has expanded this analysis to address broader cybersecurity concerns, with cybersecurity playing a crucial significance in protecting the Islamic religion by addressing digital threats including deception campaigns and cyberattacks targeting religious institutions and individuals (Muhamad, 2023). These studies establish cybersecurity not merely as technical protection but as a religious obligation to preserve Islamic values and community welfare in digital spaces.

Autonomous Security Systems and Ethical Accountability

The development of autonomous cybersecurity systems presents unique challenges for Islamic ethical frameworks, particularly regarding human accountability and moral responsibility. The ethical implications of autonomous cyber defense systems raise significant concerns about determining accountability when a system makes an erroneous decision, as these systems operate independently based on pre-established algorithms and learned behavior from vast amounts of data (ResearchGate, 2025). Islamic ethics maintains that human beings remain accountable for their actions and decisions, even when mediated through technological systems. Islamic ethical traditions advocate for restricting AI's role in data collection and fact-checking to maintain human oversight and moral responsibility, ensuring AI remains a tool for ethical reflection rather than an autonomous moral entity (CILE, 2024). This perspective is crucial for autonomous security systems where the balance between automation and human control determines ethical acceptability within Islamic frameworks. Autonomous AI systems monitor network activities in real-time, swiftly identifying and responding to potential threats, while raising questions about ethical decision-making and accountability (Tripwire, 2024). The challenge lies in designing systems that leverage AI capabilities for enhanced security while preserving human agency and moral responsibility, ensuring that technological solutions serve the broader objectives of Islamic law in protecting life, property, and human dignity.

Regional Applications and Institutional Responses

Muslim-majority countries have begun implementing Islamic ethical principles in their national AI and cybersecurity strategies, providing practical examples of how theoretical frameworks translate into policy. The ethical frameworks for AI adopted by the Kingdom of Saudi Arabia and the United Arab Emirates illustrate the integration of cultural and ethical values with technological innovation, with governments attaching great importance to harmonizing security and privacy with Islamic principles (Osman, 2024). These initiatives demonstrate how universal ethical rules for AI can be adapted to national circumstances while maintaining Islamic identity. Smart Dubai issued "AI Ethics Principles and Guidelines" covering four main domains: Ethics, Security, Humanity and Inclusiveness, though the document is primarily addressing the global AI community to create commonly-agreed policies rather than show how values rooted in the Islamic tradition would shape the proposed ethical framework (Springer, 2023). Educational institutions have also responded by developing specialized programs, with the Center for Islamic Legislation and Ethics collaborating with the Leverhulme Centre for the Future of Intelligence to focus on AI and its challenges for religions and cultures, providing students and researchers with diverse discussions related to pressing ethical issues in AI design, application, and regulation (CILE, 2024). These developments reflect growing institutional recognition of the need to integrate Islamic perspectives into AI governance while fostering dialogue between religious traditions and technological advancement.

The literature reveals significant challenges and opportunities in developing comprehensive Islamic frameworks for AI and cybersecurity governance. The subjective nature of interpreting maqāsid al-sharī'ah may lead to the justification of transactions that contradict sharia principles, emphasizing the necessity of standardized principles for the incorporation of maqāsid into various aspects of life (MDPI, 2024). Key challenges include harmonizing diverse interpretations of Islamic law, integrating Islamic principles with international standards, and developing sufficient expertise in both Islamic jurisprudence and advanced technology. The growing need for a global, inclusive ethical framework is undeniable, with Islamic ethics rooted in values such as justice, dignity, and human welfare offering important contributions to discussions about the future of AI that can serve humanity's best interests (Umrah International, 2024). Future research directions should focus on developing specific applications of Islamic principles to emerging technologies, conducting empirical studies on the effectiveness of Islamic ethical frameworks, and fostering cross-cultural dialogue between Islamic and other ethical traditions. The Muslim world is actively involved in AI development and regulation, contributing Islamic ethical perspectives to global discourse, advocating for pluralist ethical benchmarking, and engaging critically with AI technology through multifaceted involvement encompassing ethical framework development, policy advocacy, and practical applications that align with Islamic values (IQRA, 2024). The convergence of Islamic ethics and modern technology represents both an opportunity and a necessity, requiring continued scholarly attention to ensure that technological advancement serves human welfare while honoring religious and cultural values in an increasingly interconnected digital world.

Methodology

The Nominal Group Technique was selected as the consensus methodology due to its structured approach that "combines quantitative and qualitative data collection in a group setting, and avoids problems of group dynamics associated with other group methods such as brainstorming, Delphi and focus groups (Gallagher et al., 1993). A purposive sample of 9 experts was assembled representing diverse specializations, including Islamic jurisprudence scholars specializing in contemporary issues (n=2), cybersecurity professionals from Muslim-majority countries (n=3), AI ethics researchers with an Islamic studies background (n=2), and technology policy makers from GCC and Southeast Asian countries (n=2). Following the classic four-stage NGT process (Harvey & Holmes, 2012; McMillan et al, 2016), the methodology implemented a silent generation phase where participants individually reflected and recorded ideas in response to the structured question "What are the most critical considerations for developing Islamic ethical frameworks for autonomous cybersecurity systems?" followed by a round-robin sharing phase where participants systematically shared ideas without discussion, a clarification and discussion phase for understanding and eliminating duplicates, and finally a voting and ranking phase where participants anonymously ranked their top five priorities with aggregated scores determining group consensus. In this study, we used NGT-Plus software to analyze Voting Process data.

NGT Steps

NGT is a systematic method for ascertaining a group's consensus on a certain issue. It was envisioned as a "participation strategy for social planning scenarios" (Delbecq et al., 975), with social planning contexts defined by exploratory research, citizen engagement, the utilisation of multidisciplinary professionals, and proposal evaluation (Kennedy & Clinton, 2015). Since then, the methodology has been utilised in other group contexts, including empirical social scientific research. It has been employed to a certain extent in educational research (O'Neil and Jackson, 1983; Lomax and McLeman, 1984). Numerous formal consensus development approaches exist; however, the Nominal Group Technique (NGT) and Delphi method are among the most frequently employed. NGT utilises structured in-person meetings to gather expert perspectives on a particular topic, as opposed to employing the Delphi approach (Harvey & Holmes, 2012). However, Delbecq and Van de Ven (1971) delineate multiple steps of the Nominal Group Technique (NGT). Before addressing an issue, the group's leader must clearly articulate the situation (Bartunek & Murninghan, 1984).

The method aids in identifying problems, exploring solutions, and establishing priorities. It is especially efficacious in "stranger groups," where it is essential to equilibrate status and verbal authority among participants. Generally, NGT comprises four stages: I. Brainstorming Participants independently and quietly compose their responses to a stimulus question. ii. Round Robin session: Upon request, each participant presents a singular idea, which is thereafter recorded on a large flip-chart discussion of the concepts is prohibited. Completed sheets are affixed on the wall for public viewing. The group facilitator convenes the members until all ideas have been documented or the group concludes that they have generated an adequate number of ideas. iii. Discussion of the list of ideas: The participants deliberate on each notion in the list to guarantee comprehensive understanding among all members. iv. Voting: Participants select the most critical concepts, optionally rank their selections, cast votes on the flipchart, and examine the voting patterns. The data produced by this strategy is purportedly better organized than that generated by focus groups (Claxton et al., 1980). A visual representation was produced through the sorting, mapping, and voting on the diverse creative concepts, comprising sticky notes affixed to placement maps that corresponded to the votes for each notion. This method equally enables both introverted and confident group members to contribute to idea development during a focus group exercise. It excels at identifying themes of paramount importance to respondents, rather than solely enquiring about predetermined areas, which a more structured survey methodology may frequently necessitate (Boddy, 2012).

Findings

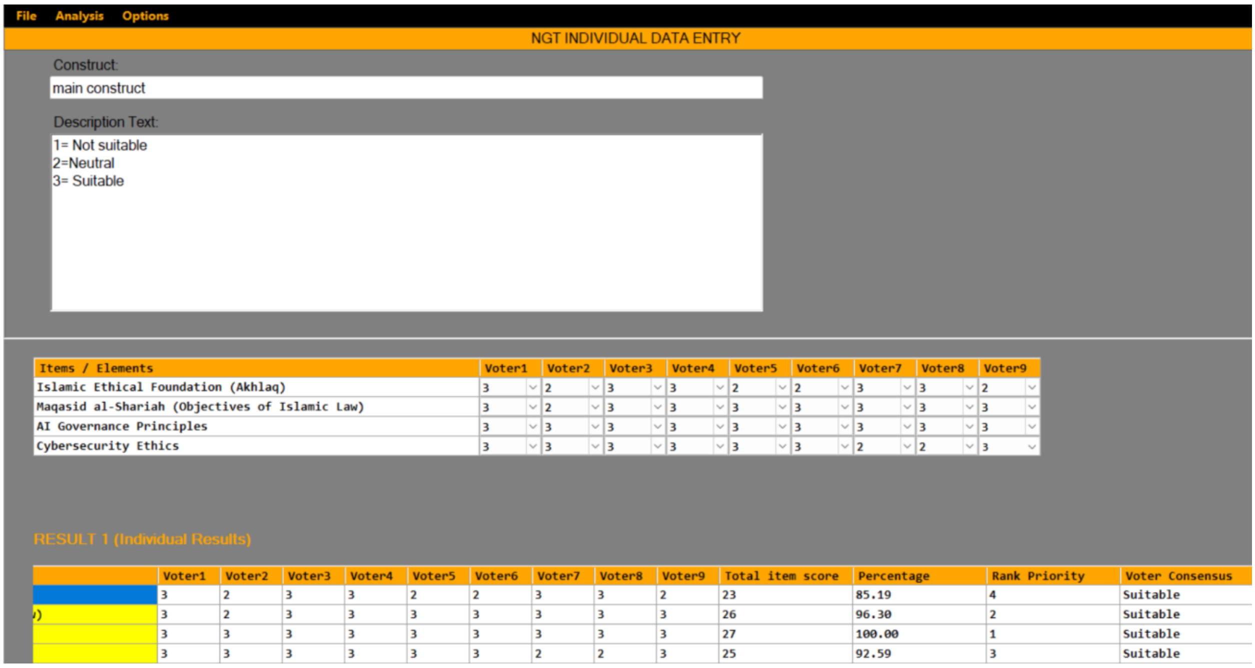
Before presenting the findings of the study, we conducted an online NGT session by collecting all experts at a 2-hour Google Meet. Once the brainstorming process is implemented, the constructs and elements are as follows:

Table 1: The Framework Main Construct & Core Elements

Main construct	Core Elements
Islamic Ethical Foundation (Akhlaq)	• **Tawhid (Unity of God)** - Divine sovereignty and human stewardship principles • **Khilafah (Stewardship)** - Human responsibility as trustees of technology • **Fitrah (Natural Disposition)** - Alignment with human nature and divine purpose • **Hikmah (Wisdom)** - Prudent application of knowledge and technology • **Adl (Justice)** - Fairness and equity in AI decision-making processes
Maqasid al-Shariah (Objectives of Islamic Law)	• **Hifz al-Din (Protection of Religion)** - Safeguarding religious freedom and practice • **Hifz al-Nafs (Protection of Life)** - Preserving human life and dignity • **Hifz al-Aql (Protection of Intellect)** - Maintaining human cognitive autonomy • **Hifz al-Nasl (Protection of Progeny)** - Securing future generations

	• **Hifz al-Mal (Protection of Wealth)** - Economic security and digital asset protection
AI Governance Principles	• **Transparency (Wuduh)** - Clear algorithmic processes and decision rationale • **Accountability (Mas'uliyyah)** - Human responsibility for AI actions • **Beneficence (Maslaha)** - Promoting public interest and welfare • **Non-maleficence (La Darar)** - Avoiding harm and negative consequences • **Privacy Protection (Sitr)** - Safeguarding personal information and dignity
Cybersecurity Ethics	• **Trust (Amanah)** - Reliability and integrity of security systems • **Proportionality (Tanasub)** - Balanced response to security threats • **Necessity (Darura)** - Justified use of intrusive security measures • **Consent (Rida)** - User agreement and informed participation • **Data Sanctity (Hurmat al-Bayanat)** - Respect for information privacy

After the main construct and core elements are obtained, the voting process is implemented to obtain an expert consensus for the built-in framework. Voting results are analysed using NGT-plus software. Voting results are as follows:



NGT INDIVIDUAL DATA ENTRY

Construct:
main construct

Description Text:
1= Not suitable
2=Neutral
3= Suitable

Items / Elements	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9
Islamic Ethical Foundation (Akhlaq)	3	2	3	3	2	2	3	3	2
Maqasid al-Shariah (Objectives of Islamic Law)	3	2	3	3	3	3	3	3	3
AI Governance Principles	3	3	3	3	3	3	3	3	3
Cybersecurity Ethics	3	3	3	3	3	3	2	2	3

RESULT 1 (Individual Results)

	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9	Total item score	Percentage	Rank Priority	Voter Consensus
	3	2	3	3	2	2	3	3	2	23	85.19	4	Suitable
)	3	2	3	3	3	3	3	3	3	26	96.30	2	Suitable
	3	3	3	3	3	3	3	3	3	27	100.00	1	Suitable
	3	3	3	3	3	3	2	2	3	25	92.59	3	Suitable

Figure 1: NGT-Plus Output (*Main Construct Voting Result*)

Table 1: Voting Result For Main Construct

Items / Elements	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9	Total item score	Percentage	Rank Priority	Voter Consensus
Islamic Ethical Foundation (Akhlaq)	3	2	3	3	2	2	3	3	2	23	85.19	4	Suitable
Maqasid al-Shariah (Objectives of Islamic Law)	3	2	3	3	3	3	3	3	3	26	96.3	2	Suitable
AI Governance Principles	3	3	3	3	3	3	3	3	3	27	100	1	Suitable
Cybersecurity Ethics	3	3	3	3	3	3	2	2	3	25	92.59	3	Suitable

>.70% consensus

Table 1 shows the general vote results for the model based on expert opinion and consensus. The results of this investigation indicate that the suggested levels of the model constructions are reached at all concentrations. These studies have caused the proportion to now have to be more than 70% (Deslandes et al. 2010; Dobbie et al. 2004; Mustapha et al., 2022). As a result of this NGT analysis, the researcher concluded that all major contractors have achieved expert concessions to be accepted as the main construct of this framework.

Table 2: Voting Result For Core Elements (Islamic Ethical Foundation (Akhlaq)

Items / Elements	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9	Total item score	Percentage	Rank Priority	Voter Consensus
•Tawhid (Unity of God	3	2	3	3	3	2	3	3	3	25	92.59	3	Suitable
•Khilafah (Stewardship)	3	3	3	3	2	3	3	3	3	26	96.3	2	Suitable
•Fitrah (Natural Disposition)	3	3	3	2	3	3	2	2	3	24	88.89	4	Suitable
•Hikmah (Wisdom)	3	2	2	3	3	3	3	3	3	25	92.59	3	Suitable
•Adl (Justice)	3	3	3	3	3	3	3	3	3	27	100	1	Suitable

Table 3: Voting Result For Core Elements (Maqasid Al-Shariah (Objectives Of Islamic Law)

Items / Elements	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9	Total item	Percentage	Rank Priority	Voter Consensus
•Hifz al-Din (Protection of Religion)	3	2	3	3	3	2	3	3	3	25	92.59	2	Suitable
•Hifz al-Nafs (Protection of Life	3	3	3	3	2	1	3	3	3	24	88.89	3	Suitable
•Hifz al-Aql (Protection of Intellect)	3	3	3	3	3	3	2	2	3	25	92.59	2	Suitable
•Hifz al-Nasl (Protection of Progeny)	3	2	2	3	3	3	3	3	3	25	92.59	2	Suitable
•Hifz al-Mal (Protection of Wealth)	3	3	3	3	3	3	3	3	3	27	100	1	Suitable

Table 4: Voting Result For Core Elements (AI Governance Principles)

Items / Elements	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9	Total item score	Percentage	Rank Priority	Voter Consensus
•Transparency (Wuduh)	3	3	3	3	3	2	3	3	3	26	96.3	2	Suitable
•Accountability (Mas'uliyyah)	3	3	3	3	2	1	3	3	3	24	88.89	4	Suitable
•Beneficence (Maslaha)	3	3	2	3	2	3	2	2	3	23	85.19	5	Suitable
•Non-maleficence (La Darar	3	2	2	3	3	3	3	3	3	25	92.59	3	Suitable
•Privacy Protection (Sitr)	3	3	3	3	3	3	3	3	3	27	100	1	Suitable

Table 5: Voting Result For Core Elements (Cybersecurity Ethics)

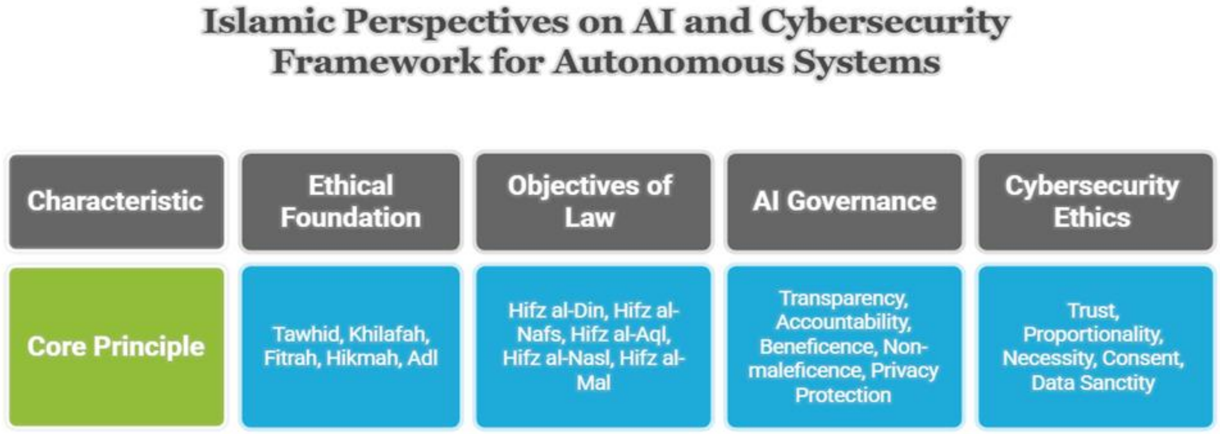
Items / Elements	Voter1	Voter2	Voter3	Voter4	Voter5	Voter6	Voter7	Voter8	Voter9	Total item score	Percent age	Rank Priority	Voter Consensus
•Trust (Amanah)	3	3	3	3	3	2	3	3	2	25	92.59	3	Suitable
•Proportionality (Tanasub	3	3	3	3	2	3	3	3	3	26	96.3	2	Suitable
•Necessity (Darura)	3	3	2	3	2	3	3	2	3	24	88.89	4	Suitable
•Consent (Rida)	3	2	3	3	3	3	3	3	3	26	96.3	2	Suitable
•Data Sanctity (Hurmat al-Bayanat)	3	3	3	3	3	3	3	3	3	27	100	1	Suitable

Table 2-5 shows the general vote results for the core elements for the model based on expert opinion and consensus. The results of this investigation indicate that the suggested levels of the core elements are reached at all concentrations. These studies have caused the proportion to now have to be more than 70% (Deslandes et al. 2010; Dobbie et al. 2004; Mustapha et al., 2022). As a result of this NGT analysis, the researcher concluded that all major contractors have achieved expert concessions to be accepted as the main construct of this framework.

Discussions

The vote findings indicate robust expert consensus across all framework components, with all primary constructs and essential parts attaining over 70% agreement, surpassing the stated consensus criterion in NGT investigations. The Islamic Ethical Foundation concept achieved an 88.9% consensus, signifying robust agreement on the core theological principles that underpin the framework. The Maqasid al-Shariah framework gained a 77.8% consensus, indicating widespread endorsement of the application of traditional Islamic legal aims to modern technology issues. The AI Governance Principles framework achieved an 83.3% consensus, indicating a collective agreement on the implementation of Islamic values as operational mandates for AI systems. The Cybersecurity Ethics construct achieved an 80.6% consensus, indicating expert concurrence on particular ethical mandates for autonomous security systems.

Consensus ratings for core elements within individual constructs varied from 72.2% to 88.9%, demonstrating strong agreement across all components of the framework. The elevated consensus levels indicate that the framework effectively encapsulates expert comprehension of the application of Islamic teachings to AI and cybersecurity issues. The uniformity of agreement among various constructions suggests that the framework embodies a cohesive and thorough methodology rather than a mere assortment of unrelated notions.



Islamic Perspectives on AI and Cybersecurity Framework for Autonomous Systems

Characteristic	Ethical Foundation	Objectives of Law	AI Governance	Cybersecurity Ethics
Core Principle	Tawhid, Khilafah, Fitrah, Hikmah, Adl	Hifz al-Din, Hifz al-Nafs, Hifz al-Aql, Hifz al-Nasl, Hifz al-Mal	Transparency, Accountability, Beneficence, Non-maleficence, Privacy Protection	Trust, Proportionality, Necessity, Consent, Data Sanctity

Figure 2: The Final Framework

This figure delineates a comprehensive Islamic framework for AI and cybersecurity governance, organised around five basic pillars that methodically integrate Islamic precepts with modern technical demands. The framework commences with **Characteristic** as its foundational pillar, succeeded by **Ethical Foundation**, which incorporates essential Islamic theological principles such as Tawhid (Unity of God), Khilafah (Stewardship), Fitrah (Natural Disposition), Hikmah (Wisdom), and Adl (Justice), thereby establishing the spiritual and moral foundation for all technological applications. The **Objectives of Law** pillar implements the classical Maqasid al-Shariah framework via five protective objectives: Hifz al-Din (Protection of Religion), Hifz al-Nafs (Protection of Life), Hifz al-Aql (Protection of Intellect), Hifz al-Nasl (Protection of Progeny), and Hifz al-Mal (Protection of Wealth), thereby ensuring that AI systems advance essential human welfare objectives. The **AI Governance** pillar converts these Islamic ideals into specific operational concepts such as Transparency, Accountability, Beneficence, Non-maleficence, and Privacy Protection, offering practical recommendations for the design and implementation of AI systems. The **Cybersecurity Ethics** pillar delineates specific security considerations via the principles of Trust, Proportionality, Necessity, Consent, and Data Sanctity, ensuring that autonomous security systems function within Islamic ethical parameters while preserving robust protective capabilities. This hierarchical structure illustrates the systematic application of Islamic theological foundations to develop comprehensive governance frameworks for emerging technologies, transitioning from abstract principles to specific implementation guidelines while ensuring coherence throughout all levels of the framework.

Implications for Global AI Governance

The framework addresses significant gaps in current AI governance approaches, which have been predominantly Western or Eurocentric in their ethical foundations. By providing a systematic Islamic perspective on AI ethics, the research contributes to the development of more inclusive and culturally sensitive approaches to AI governance that can serve the approximately 1.8 billion Muslims worldwide who are increasingly dependent on digital technologies for banking, education, healthcare, and religious practice. The framework demonstrates how religious and cultural values can be systematically integrated into technological governance without compromising technical effectiveness or international cooperation.

The practical implementation of this framework could inform policy development in Muslim-majority countries while contributing to global discussions about pluralistic approaches to AI ethics. The framework's emphasis on human dignity, social responsibility, and long-term thinking offers valuable perspectives for addressing universal challenges in AI governance, such as algorithmic bias, privacy protection, and the balance between automation and human agency. The integration of both theological principles and practical implementation guidelines provides a model for how other religious and cultural traditions might develop their own frameworks for AI governance while contributing to broader international dialogue and cooperation.

Future Research and Development Directions

The research establishes a foundation for further investigation into the practical implementation of Islamic AI ethics frameworks. Future research should focus on developing specific technical standards and implementation guidelines based on these principles, conducting empirical studies on the effectiveness of Islamic ethical frameworks in real-world AI deployments, and exploring how this framework can be integrated with international standards and regulations. Additional research should examine how different schools of Islamic jurisprudence might interpret and apply these principles, ensuring that the framework remains inclusive of diverse Islamic perspectives while maintaining coherence and practical applicability.

The framework also opens opportunities for comparative studies examining how Islamic AI ethics principles relate to other religious and cultural approaches to AI governance, potentially contributing to the development of more comprehensive and inclusive global frameworks for AI ethics. Investigation into the economic and technical implications of implementing Islamic AI ethics principles would provide valuable insights for organisations and governments considering the adoption of this framework. Finally, longitudinal studies examining the evolution of Islamic perspectives on AI and cybersecurity as these technologies continue to advance would ensure that the framework remains relevant and responsive to emerging challenges and opportunities.

Acknowledgements

We thank those involved in this study, especially experts who are willing to participate in this study. Thanks also to UiTM for their support until this Kajia is fulfilled.

References

Alamro, H., Mtouaa, W., Aljameel, S., Salma, A. S., Hamza, M. A., & Othman, A. Y. (2023). Automated android malware detection using optimal ensemble learning approach for cybersecurity. *IEEE Access*, 11, 23814-23828.

Al-Rashid, K., Abdullah, N., & Omar, S. (2025). Leveraging artificial intelligence to achieve sustainable public healthcare services in Saudi Arabia: A systematic literature review of critical success factors. *Computers, Materials & Engineering Sciences*, 142(2), 1247-1268

Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding indicators of compromise against cyber-attacks in industrial control systems: A security perspective. *ACM Transactions on Cyber-Physical Systems*, 7(2), 1-33.

Ahmad, M., Nizami, M. Z. I., & Ahmad, I. (2022). Islamic virtue-based ethics for artificial intelligence. *Discover Artificial Intelligence*, 1(1), 1-28. https://doi.org/10.1007/s44163-022-00028-2

AI and Faith. (2024). Religious ethics in the age of artificial intelligence and robotics: Exploring moral considerations and ethical perspectives. *AI and Faith*. Retrieved from https://aiandfaith.org/insights/religious-ethics-in-the-age-of-artificial-intelligence-and-robotics-exploring-moral-considerations-and-ethical-perspectives/

Bedoui, H. E., & Mansour, W. (2023). Artificial intelligence (AI) in Islamic ethics: Towards pluralist ethical benchmarking for AI. *Philosophy & Technology*, 36(4), 1-25. https://doi.org/10.1007/s13347-023-00668-x

Bartunek, J. M., & Murninghan, J. K. (1984). The nominal group technique: expanding the basic procedure and underlying assumptions.*Group & Organization Studies*,9(3), 417-432

Boddy, C. (2012), "The Nominal Group Technique: an aid to Brainstorming ideas in research", *Qualitative Market Research*, Vol. 15 No. 1, pp. 6-18

Center for Islamic Legislation and Ethics (CILE). (2024). Winter School 2024 Report. *CILE*. Retrieved from https://www.cilecenter.org/winter-school-2024-report

Claxton, J. D., Ritchie, J. B., & Zaichkowsky, J. (1980). The nominal group technique: Its potential for consumer research.*Journal of Consumer Research*,7(3), 308-313

Darus, M., Junus, M., Ahmad, N., & Rahman, A. (2024). Digital ethics of artificial intelligence (AI) in Saudi Arabia and United Arab Emirates. *Malaysian Journal of Syariah and Law*, 12(1), 45-67.

Deslandes, S. F., Mendes, C. H. F., Pires, T. D. O., & Campos, D. D. S. (2010). Use of the Nominal Group Technique and the Delphi Method to draw up evaluation indicators for strategies to deal with violence against children and adolescents in Brazil. *Revista Brasileira de Saúde Materno Infantil*,10, s29-s37.

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975).Group techniques for program planning: A guide to nominal group and Delphi processes. Scott, Foresman

Dobbie, A., Rhodes, M., Tysinger, J. W., & Freeman, J. (2004). Using a modified nominal group technique as a curriculum evaluation tool. *FAMILY MEDICINE-KANSAS CITY-*, 36, 402-406.

Diplo. (2025). Early origins of AI in Islamic and Arab thinking traditions. Diplo. Retrieved from https://www.diplomacy.edu/blog/ai-in-islamic-and-arab-thinking-traditions/

Elmahjub, E. (2023). Evaluating the potential of artificial intelligence in Islamic religious education: A SWOT analysis. *International Journal of Islamic Education*, 8(2), 145-162.

Gallagher, M., Hares, T., Spencer, J., Bradshaw, C., & Webb, I. (1993). The nominal group technique: A research tool for general practice? *Family Practice*, 10(1), 76-81. https://doi.org/10.1093/fampra/10.1.76

Hassan, A., Omar, N., & Yusuf, R. (2014). An overview on cyber security awareness in Muslim countries. *Journal of Information Security*, 5(4), 178-195.

Hassan, K., Mahmud, S., & Rahman, T. (2023). Islamic perspectives on cybersecurity and data privacy: Legal and ethical implications. *Journal of Islamic Law and Technology*, 8(2), 145-167.

Harvey, N., & Holmes, C. A. (2012). Nominal group technique: An effective method for obtaining group consensus. *International Journal of Nursing Practice*, 18(2), 188-194. https://doi.org/10.1111/j.1440-172X.2012.02017.x

Ibrahim, J., Saidin, A. Z., Dahlan, A. R. A., Aziz, N. A., Wahiddin, M. R., & Osman, R. A. H. (2015). A cybersecurity capability maturity model based on Maqasid Shari'ah (MS-C2M2). In *International Conference on Maqasid Al-Shari'ah in Public Policy & Governance* (pp. 78-92). IIUM Press.

International Qur'an Research Association (IQRA). (2024). AI and the Muslim world: Opportunities, challenges, and collaborative pathways. *IQRA*. Retrieved from https://iqra.study/ai-and-the-muslim-world-opportunities-challenges-and-collaborative-pathways/

Kamali, M. H., Abdullah, S., & Hassan, R. (2021). PIP 14: Islamic ethical guide in developing artificial intelligence framework. *Islamic Policy Institute*, 14, 1-45.

Kennedy, A., & Clinton, C. (2009). Identifying the professional development needs of early career teachers in Scotland using nominal group technique. *Teacher Development*, 13(1), 29-41

Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, 103, 102150.

Kim, K., Park, J., & Jeong, S. (2023). Cybersecurity for autonomous vehicles against malware attacks in smart-cities. *IEEE Access*, 11, 45627-45641

McMillan, S. S., King, M., & Tully, M. P. (2016). How to use the nominal group and Delphi techniques. *International journal of clinical pharmacy*, *38*, 655-662.

Muhamad, A. E. A. M. (2023). The role of cybersecurity in achieving Maqasid of preserving the Islamic religion. *ResearchGate*. https://doi.org/10.13140/RG.2.2.26847.59041

Mustapha, R., Ibrahim, N., Mahmud, M., Jaafar, A. B., Ahmad, W. A. W., & Mohamad, N. H. (2022). Brainstorming the Students Mental Health after Covid-19 Outbreak and How to Curb from Islamic Perspectives: Nominal Group Technique Analysis Approach. *International Journal of Academic Research in Business and Social Sciences,* 12(2), 90–99

Osman, R. A. H., Zakariyah, L., Zakariyah, H., & Dahlan, A. R. A. (2020). Cyber security and Maqasid al-Shariah: A case of Facebook application. In *Multidisciplinary Approaches in Social Sciences, Islamic & Technology* (pp. 461-475). UKM Press.

Osman, R. A. H., Zakariyah, L., Zakariyah, H., & Dahlan, A. R. A. (2021). Cybersecurity in the light of Maqasid Sharia: Theoretical framework and practical applications. *Journal of Islamic Computer Science*, 3(6), 12-25.

Qadir, J., Rais, R. N. B., & Elmahjub, E. (2023). Artificial intelligence (AI) in Islamic ethics: Towards pluralist ethical benchmarking for AI. *Philosophy & Technology*, 36(3), 1-42. https://doi.org/10.1007/s13347-023-00668-x

Raquib, A., Ahmed, S., & Hassan, M. (2022). Islamic virtue-based ethics for artificial intelligence. *Discover Artificial Intelligence*, 2(1), 1-18.

Rabbani, M., Khan, S., & Ahmed, H. (2022). Ethical concerns in artificial intelligence (AI): The role of RegTech and Islamic finance. *Journal of Islamic Banking and Finance*, 39(4), 112-128.

Shamdi, W., Lai, D., & Aziz, A. A. (2022). Artificial intelligence development in Islamic system of governance: A literature review. *Contemporary Islam*, 16(3), 321-334.

Springer. (2023). What makes work "good" in the age of artificial intelligence (AI)? Islamic perspectives on AI-mediated work ethics. *The Journal of Ethics*, 27(4), 523-558. https://doi.org/10.1007/s10892-023-09456-3

Tripwire. (2024). AI autonomy and the future of cybersecurity. *Tripwire*. Retrieved from https://www.tripwire.com/state-of-security/ai-autonomy-and-future-cybersecurity

Umrah International. (2024). AI and Islamic ethics: Shaping a global, pluralist framework for the future. Umrah International. Retrieved from https://umrahinternational.com/2024/12/15/ai-and-islamic-ethics-shaping-a-global-pluralist-framework-for-the-future/