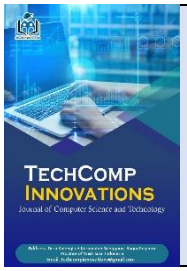

Journal of Computer Science and Technology, Vol 2 (1) 2025: 53-65

TechComp Innovations

https://mabadiiqtishada.org/index.php/TechCompInnovations
ISSN: 3062-8903; e-ISSN: 3062-889X

Cybersecurity and Moral Responsibility: A Philosophical-Islamic Approach to Digital Trust

Ghifari Alif Auladi[1*], Fathan Muwahid[2]
[1] *Department of Computer Science. Universitas Ary Ginanjar. Indonesia*
[2] *Faculty of Ushuluddin. International Islamic University Islamabad. Pakistan*

ARTICLE INFO

Received June 5, 2025
Accepted June 14, 2025
Published June 18, 2025

Keywords:
Islamic Ethics; Cybersecurity; Decolonial Theory; Moral Responsibility; Digital Trust

ABSTRACT

The dominance of Western-centric norms in cybersecurity ethics presents a significant gap in addressing the moral and cultural realities of diverse societies, particularly those in the Muslim world. This paper proposes a decolonial and culturally inclusive framework by integrating Islamic ethical philosophy into the discourse on cybersecurity. Drawing on key Islamic concepts such as amanah (trust), 'adl (justice), and niyyah (intention), the study explores how these values can inform ethical decision-making in digital environments. Through a philosophical-theological approach, it critiques the assumption of value neutrality in technology and highlights the moral agency and accountability embedded in Islamic metaphysics. The findings underscore the necessity of ethical pluralism and call for a global digital ethics that is both morally substantive and culturally responsive. Ultimately, the study contributes to the development of a more holistic and spiritually informed cybersecurity paradigm that resonates with the ethical traditions of Muslim-majority contexts.

How to cite: Alif Auladi, G., & Muwahid, F. (2025). Cybersecurity and Moral Responsibility: A Philosophical-Islamic Approach to Digital Trust. *TechComp Innovations: Journal of Computer Science and Technology*, 2(1), 53–65. https://doi.org/10.70063/techcompinnovations.v2i1.93

This is an open-access article distributed under the Creative Commons 4.0 Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. ©2023 by author.

* *Corresponding author: ghifari.alif.auladi@students.esqbs.ac.id*

INTRODUCTION

In today's increasingly digitized world, cybersecurity has become a critical pillar in ensuring the safety and trustworthiness of information systems. The growing frequency and complexity of cyber threats—including data breaches, identity theft, and misinformation—have significantly challenged the ethical frameworks underpinning digital trust (**von Solms & van Niekerk, 2023**). While technological solutions such as encryption, firewalls, and behavioral monitoring continue to evolve, the human dimension—particularly the moral responsibility of developers, users, and organizations—remains underexplored. Scholars

have noted that technological defenses are often insufficient in the absence of ethical accountability (**Floridi, 2021**). This gap suggests the urgent need for an interdisciplinary inquiry that combines cybersecurity with deeper moral and philosophical considerations.

Digital trust, a central component in cybersecurity discourse, is not only a matter of technical compliance but also of perceived ethical integrity. Trust in digital platforms is increasingly fragile due to opaque data practices and algorithmic biases (**Marelli & Testa, 2021**). Although Western ethical frameworks have offered significant insights, they are often rooted in secular liberalism, which may not fully capture the ethical concerns of diverse cultural and religious communities. The growing digital participation of Muslim populations worldwide necessitates the articulation of cybersecurity principles grounded in Islamic philosophy and theology—particularly those related to *amanah* (trust), responsibility, and *'adl* (justice).

Islamic ethical thought, especially as developed through the discipline of *'Aqidah* and *Ilm al-Kalam*, offers a rich philosophical foundation for addressing moral responsibility in the digital age. The notion of *amanah* in Islam emphasizes the sacredness of responsibility, including the trust conferred upon individuals and institutions handling sensitive data (**Kamali, 2020**). Moreover, the Islamic view of human agency, which balances divine decree with moral accountability, presents a unique framework to reinterpret cybersecurity as not merely a technical safeguard but a moral and spiritual obligation (**Al-Attas, 2021**). This dimension is essential when considering how digital technologies shape social behaviors, influence worldviews, and challenge the boundaries of personal and communal responsibility.

This study aims to explore how Islamic philosophical ethics can enrich current cybersecurity paradigms by introducing a framework of moral responsibility grounded in Aqidah. By examining key Islamic concepts and aligning them with contemporary cybersecurity challenges, the research seeks to contribute to a more inclusive and morally conscious discourse on digital trust. It also aims to offer culturally relevant insights for policymakers, educators, and tech developers working within or in collaboration with Muslim-majority societies.

Given the rapid acceleration of digital transformation and the ethical dilemmas it brings, the urgency of this research lies in its potential to bridge theological-philosophical wisdom with modern technological needs. Not only does this approach foster ethical pluralism in cybersecurity discourse, but it also empowers Muslim communities to engage with digital systems in a way that resonates with their spiritual values and philosophical traditions. In doing so, this study contributes both to the decolonization of digital ethics and to the development of a more holistic, value-driven model of digital trust.

RESEARCH METHOD

This study adopts a qualitative library research design, focusing on textual analysis and critical interpretation of both classical and contemporary sources. Library research is particularly suitable for philosophical and normative inquiries, as it allows for a comprehensive engagement with existing literature, historical texts, religious doctrines, and scholarly debates (**Zed, 2021**). In the context of this research, the library-based approach provides the appropriate foundation to explore the intersection of Islamic philosophical ethics and cybersecurity discourse without the constraints of empirical fieldwork.

Data collection in this research is conducted through an extensive review of primary and secondary sources. Primary sources include classical Islamic theological texts from disciplines such as *'Aqidah, Usul al-Din*, and Islamic ethics, as well as legal-theological works by Muslim philosophers and scholars like Al-Ghazali, Al-Maturidi, and contemporary thinkers such as Al-Attas and Kamali. Secondary sources consist of peer-reviewed journal articles, books, and reputable online academic publications that discuss cybersecurity, digital ethics, moral philosophy, and Islamic perspectives on responsibility and trust. Digital databases such as JSTOR, Scopus, SpringerLink, and Google Scholar were utilized to access relevant literature published within the last five years (**Booth et al., 2021**).

For the data analysis, this study employs content analysis and philosophical hermeneutics. Content analysis allows for the systematic examination of recurring ethical themes, concepts, and arguments within both cybersecurity literature and Islamic theological texts (**Krippendorff, 2018**). Philosophical hermeneutics, on the other hand, is used to interpret the underlying metaphysical and moral assumptions behind concepts such as *amanah* (trust), *'adl* (justice), and digital responsibility. This interpretive approach facilitates the construction of a coherent ethical framework that bridges Islamic values with contemporary technological contexts (**Gadamer, as cited in Palmer, 2022**).

The integration of library-based data with qualitative philosophical analysis ensures that the study remains rooted in rigorous academic inquiry while also producing a normative framework that is both contextually grounded and theologically informed. This methodological approach allows the research to contribute meaningfully to the emerging discourse on ethical digital practices, particularly within Muslim-majority societies and among scholars exploring decolonial approaches to cybersecurity ethics.

RESULT AND DISCUSSION

Ethical Foundations of Digital Trust in Cybersecurity

In the digital age, the concept of trust has evolved from interpersonal relationships into an essential requirement for digital systems and online interactions. As individuals increasingly depend on digital platforms for communication, commerce, education, and governance, the trust they place in these systems becomes critical. Digital trust refers not only to the reliability of technology but also to the belief that one's data and digital presence are handled responsibly and ethically. This form of trust is deeply tied to perceptions of transparency, accountability, and ethical behavior from digital service providers and institutions (**Marelli & Testa, 2021**).

Contemporary cybersecurity strategies primarily focus on technical defenses such as encryption, authentication protocols, firewalls, and intrusion detection systems. These measures are crucial for preventing unauthorized access, ensuring data confidentiality, and protecting against cyber threats. However, as advanced as these technical solutions may be, they are insufficient in securing the broader, more abstract element of user trust. Technology can protect systems from external threats, but it cannot guarantee that data will be used in ways that are morally sound or socially acceptable (**von Solms & van Niekerk, 2023**).

Several scholars have pointed out the limitations of a technocentric approach to cybersecurity. Floridi and Cowls (2022), for instance, argue that technical measures must be complemented by ethical frameworks that consider the values, expectations, and rights of users. Without such a framework, digital infrastructures risk becoming secure yet unethical—capable of protecting data from hackers while simultaneously enabling surveillance,

discrimination, or manipulation by internal actors. Thus, ethical responsibility must be embedded in the very foundation of cybersecurity design and implementation.

Moreover, digital trust is relational and subjective. It depends heavily on how users perceive the intentions and actions of digital platforms. When users feel that their autonomy, privacy, and dignity are not respected, no amount of technological sophistication can restore their trust. This highlights the importance of ethical considerations such as informed consent, data transparency, and fairness in algorithmic decision-making—issues that are often ignored in purely technical cybersecurity models (**Mittelstadt, 2019**).

The failure to integrate ethical responsibility into cybersecurity design has led to a growing number of high-profile scandals involving data misuse, algorithmic bias, and opaque surveillance practices. These incidents demonstrate that the absence of a robust ethical framework can undermine even the most technically secure systems. As such, cybersecurity must not be understood solely as a matter of system resilience, but also as a moral practice involving human judgment, organizational culture, and social accountability (**Mann et al., 2021**).

Incorporating ethics into cybersecurity also requires acknowledging the plurality of moral traditions and cultural perspectives. In Muslim-majority societies, for example, digital trust is not only a legal or procedural issue but one deeply connected to moral concepts such as *amanah* (trustworthiness) and *'adl* (justice). These values emphasize that data handling is not just a technical process but a moral duty toward fellow humans and ultimately, toward God. By grounding cybersecurity in such ethical traditions, we can foster digital environments that are more inclusive, culturally resonant, and socially legitimate (**Kamali, 2020**).

Furthermore, ethical frameworks in cybersecurity must evolve alongside technological developments. As artificial intelligence, biometric systems, and the Internet of Things (IoT) become more integrated into daily life, new ethical dilemmas arise that require proactive responses. For example, the ethical use of facial recognition technology, the rights of individuals in predictive policing systems, or the biases encoded in AI-driven hiring tools cannot be addressed through firewalls or passwords alone (**Cath et al., 2020**). Instead, these challenges require normative reasoning, value alignment, and stakeholder engagement.

Ethical cybersecurity is also vital for long-term sustainability. When digital platforms act ethically, they are more likely to maintain user loyalty, avoid regulatory backlash, and contribute to a stable digital ecosystem. Conversely, a failure to uphold ethical standards can result in reputational damage, legal consequences, and widespread public distrust. Ethics, therefore, is not an abstract ideal but a practical necessity for securing the legitimacy and longevity of digital systems (**West et al., 2022**). This study affirms that moral responsibility is a cornerstone of trustworthy digital interactions. It argues that digital trust cannot be manufactured through technology alone, but must be cultivated through ethical practices, transparent communication, and a commitment to justice. By embedding these values into cybersecurity policies and systems, institutions can create more humane and trustworthy digital spaces.

Ethical frameworks must be viewed as integral—not auxiliary—to cybersecurity. The future of digital trust depends not only on preventing threats but on affirming the dignity, rights, and agency of all users. To achieve this, cybersecurity must transition from being a purely technical discipline to an interdisciplinary field enriched by philosophy, theology, and cultural ethics. Only then can we build digital environments that are not only safe but also just and morally responsible.

Islamic Ethical Foundations in Cybersecurity – Amanah and 'Adl

In today's increasingly digitized world, the ethical principles guiding our behavior in online spaces have become as crucial as technical safeguards. While cybersecurity often emphasizes technological solutions, there is a growing recognition that ethical frameworks rooted in cultural and religious traditions offer valuable contributions to shaping responsible digital conduct. Within the Islamic tradition, two core ethical values—*amanah* (trustworthiness) and *'adl* (justice)—can provide powerful foundations for framing cybersecurity responsibilities and policies, particularly in Muslim-majority societies or among ethically motivated digital practitioners.

The principle of *amanah* is central to Islamic ethical thought. Traditionally, it refers to a trust or responsibility that is divinely bestowed upon human beings. This is not a superficial obligation but a deeply moral commitment that permeates all aspects of life, including the digital sphere. The Qur'an emphasizes this notion in Surah Al-Ahzab (33:72), describing how the trust *(amanah)* was offered to the heavens and the earth, but only humans accepted it—underscoring its profound weight and significance. This scriptural perspective forms the basis of a moral orientation that calls for ethical integrity in handling all forms of entrusted information, including digital data.

In the realm of cybersecurity, *amanah* can be interpreted as the responsibility to safeguard users' personal data, maintain confidentiality, and act with integrity in digital transactions. The moral obligation to fulfill one's trust is applicable not only in interpersonal relations but also in the design, management, and regulation of digital systems. As Kamali (2020) notes, *amanah* extends beyond legal compliance; it embodies a divine accountability that necessitates ethical excellence in fulfilling duties entrusted by others, including virtual users.

Complementing *amanah* is the value of *'adl*, or justice, which Islamic ethics considers a universal imperative. The Qur'an (4:135) commands believers to uphold justice even against their own interests or family, highlighting the unyielding nature of this virtue. In digital contexts, *'adl* can be translated into fairness in algorithmic decision-making, equitable access to information, and the unbiased treatment of users across digital platforms. Justice in cybersecurity means ensuring that no individual or group is disproportionately harmed or surveilled, and that protective technologies are distributed fairly (**Shaheed et al., 2023**).

Both *amanah* and *'adl* advocate for a cybersecurity model that respects not only privacy and protection but also moral dignity and social fairness. These principles challenge the often instrumental view of data as mere resources and instead encourage seeing data as a trust granted by users to organizations. As such, ethical cybersecurity from an Islamic perspective requires that data handlers honor this trust by avoiding manipulation, unauthorized usage, or profit-driven exploitation of personal information (**Al-Attas, 2021**).

Moreover, the integration of Islamic ethics into cybersecurity frameworks fosters greater cultural resonance, particularly in societies where religious norms influence both public policy and personal conduct. Embedding *amanah* and *'adl* into cybersecurity practices can help bridge the gap between technical systems and moral worldviews, resulting in more trustworthy and socially legitimate digital infrastructures (**Dagli, 2022**). This is especially relevant as governments and institutions increasingly adopt surveillance technologies and artificial intelligence in governance, often without sufficient ethical scrutiny.

Recent ethical lapses in the digital world—ranging from data leaks to discriminatory AI algorithms—highlight the urgent need for normative anchors that go beyond Western liberal

models. While secular ethics provides valuable insights, incorporating Islamic ethical principles offers a complementary framework that emphasizes moral responsibility before God and society. This dual accountability strengthens the ethical commitment of actors in the digital realm (**Elasrag, 2022**). Furthermore, these Islamic values are not merely abstract ideals but have practical implications for policy and governance. For instance, the design of cybersecurity protocols that align with *amanah* would prioritize transparency, user education, and consent mechanisms, while adherence to *'adl* would demand regular audits to prevent systemic bias and digital exclusion. Such approaches would humanize cybersecurity systems and align them more closely with community values and expectations (**Alomari & Selamat, 2023**).

By adopting *amanah* and *'adl* as guiding principles, Islamic digital ethics contributes to a global discourse on cybersecurity that is more inclusive and pluralistic. It promotes a vision of digital trust that is relational, holistic, and spiritually grounded—recognizing the sacredness of knowledge, privacy, and justice. This stands in contrast to utilitarian models that prioritize efficiency and profit over human dignity. Islamic theological ethics offers profound contributions to cybersecurity through the principles of *amanah* and *'adl*. These values provide not only normative guidance but also practical pathways for ethical digital governance. As technology becomes increasingly embedded in everyday life, drawing from diverse ethical traditions will be vital for ensuring a just, trustworthy, and morally conscious digital future.

Human Agency and Moral Accountability in Islamic Cyber Ethics

In the evolving discourse on cyber ethics, questions of responsibility, agency, and accountability remain central. Most secular models of digital ethics emphasize rational choice, user autonomy, and harm reduction but often neglect the deeper metaphysical foundations of moral responsibility. In contrast, Islamic ethical thought presents a more integrated vision of human agency—one that is at once autonomous, accountable, and divinely guided. This framework can enrich current discussions on ethical behavior in digital environments, particularly concerning the actions of users, developers, and institutions.

Islam places strong emphasis on the concept of *taklif*, the moral responsibility bestowed upon human beings by God. According to Islamic theology, every human action—whether in the physical or digital realm—is subject to divine judgment and ethical scrutiny. This includes how individuals interact with data, privacy, information dissemination, and digital justice. The Islamic understanding of agency insists that humans are not merely legal or rational actors, but also moral beings whose actions carry consequences in both this world and the hereafter (**Kamali, 2020**).

This view contrasts with many Western ethical frameworks in cybersecurity, which tend to separate ethics from metaphysical or spiritual contexts. In these models, ethical norms are often negotiated through consensus, utility, or professional codes of conduct, rather than rooted in transcendent accountability. While such approaches have merit, they may fall short when addressing deeper motivational questions, such as why one should act ethically when consequences are invisible or deferred. Islamic ethics answers this with the principle of divine observation *(muraqabah)*, which asserts that all actions—even in virtual spaces—are known and recorded by God (**Nasr, 2023**).

As Al-Attas (2021) asserts, Islamic metaphysics views knowledge as inherently ethical. It is not merely an accumulation of data or technical skill, but something that must be directed

toward moral ends *(maqasid)*. In the context of cybersecurity, this means that expertise in coding, system architecture, or data analytics must be exercised with conscious moral intent. Developers, for instance, are not neutral technicians but moral agents responsible for the societal implications of the systems they build. This perspective shifts the focus from compliance to conscience, from risk management to moral purpose.

Such an integrated view of knowledge and ethics is particularly relevant as digital technologies become more autonomous and opaque. Artificial intelligence, for example, can now make decisions that affect employment, security, or legal outcomes. When such decisions are guided solely by efficiency or market incentives, they risk undermining human dignity and justice. Islamic cyber ethics demands that these technologies be aligned with moral principles, and that the agents behind them are held accountable not only by law but also by their own ethical awareness (**Alomari & Selamat, 2023**).

This theological grounding of moral agency also reinforces personal integrity in online spaces. It instills a sense of internalized discipline, where users are motivated not by surveillance or legal fear but by ethical self-restraint. In the Islamic tradition, this corresponds to the concept of *taqwa*—a spiritual consciousness that guards one's actions, including those taken behind screens and passwords. Such a framework has strong potential to counteract online harms such as cyberbullying, misinformation, and unethical hacking (**Dagli, 2022**).

In organizational contexts, this moral approach encourages leaders and decision-makers to see digital governance as a moral trust, not just a strategic responsibility. Systems of cybersecurity should thus be built not only to protect data but to uphold justice, transparency, and the common good. These values are embedded in the higher objectives of Islamic law *(maqasid al-shariah)*, which seek to preserve life, dignity, intellect, and trust—all of which are at risk in poorly regulated digital environments (**Shaheed et al., 2023**).

Moreover, Islamic moral accountability introduces a broader, eschatological perspective to cyber ethics. It reminds individuals and institutions that their digital actions are not value-neutral, nor are they forgotten. Every click, post, or algorithmic decision becomes part of a moral record. This understanding has the power to transform how people approach digital behavior, moving from a transactional to a transcendental mindset. It makes ethical behavior less contingent on social norms and more deeply embedded in spiritual commitment (**Elasrag, 2022**).

This paradigm also challenges the notion that ethical lapses in technology are simply failures of policy or regulation. Rather, it suggests that such lapses stem from a deeper disconnection between technical capability and moral awareness. By reintroducing the concept of moral purpose into the development and use of digital tools, Islamic ethics offers a corrective to the moral drift in current digital culture. It calls on every actor—whether programmer, policymaker, or user—to act with a sense of moral gravity.

Islamic views on human agency and moral accountability provide a compelling alternative to secular models of cyber ethics. They offer a spiritually grounded, ethically rigorous, and purpose-driven framework that emphasizes the sacredness of every digital action. As the digital age continues to reshape human interaction and institutional power, such perspectives are not only relevant but urgently needed to cultivate a digital world that is both just and morally conscious.

Challenging Technological Neutrality through a Philosophical-Islamic Lens

In contemporary discourse, technology is often viewed as a neutral tool—neither inherently good nor bad—whose ethical implications depend solely on how it is used. This "value-neutral" assumption underpins much of modern technological development and governance. However, from a philosophical-Islamic perspective, this view is inadequate and potentially dangerous. Islamic ethics insists that human intention *(niyyah)* and the moral outcomes of actions (*maslahah* and *mafsadah*) are inseparable from the tools and systems humans create. Therefore, technologies, including AI and cybersecurity mechanisms, must be evaluated not only by their functionality but by their alignment with ethical and moral purposes.

This perspective directly confronts the assumption that technology exists in a moral vacuum. In Islamic epistemology, every human act is judged by its underlying intention, and by the consequences it brings to individuals and society. Technology, being a product of human agency, is thus imbued with the values, intentions, and assumptions of its designers. As Marelli and Testa (2021) note, digital technologies—especially artificial intelligence—are never value-free; they encode the worldviews, priorities, and ideologies of those who build them, often in ways that are opaque or unacknowledged.

Cybersecurity tools, for instance, are not merely technical instruments for protection. They embody decisions about who is protected, what data is prioritized, and how power is distributed in digital ecosystems. A firewall, an algorithm, or a surveillance system reflects choices about trust, risk, and control. Islamic ethics demands that these choices be informed not only by efficiency or profitability but by moral considerations of justice *('adl)*, trustworthiness *(amanah)*, and social good *(maslahah)* (**Kamali, 2020**). This ethical framing challenges technocratic models that detach development from accountability.

Furthermore, Islamic philosophy urges us to consider what ought to be built, not just what can be built. This normative stance aligns with the *maqasid al-shari'ah*, the higher objectives of Islamic law, which seek to preserve life, intellect, dignity, and communal welfare. When viewed through this lens, technological development becomes a moral endeavor—one that must be evaluated by its contribution to human flourishing, not merely its novelty or market success (**Elasrag, 2022**). This is particularly urgent in the age of AI and Big Data, where the speed of innovation often outpaces ethical reflection.

By embedding ethical principles from the start of the design process, technology can serve as a tool for justice and spiritual responsibility. For example, a cybersecurity platform grounded in Islamic ethics would not only aim to prevent data breaches but also ensure equitable access, transparency in governance, and moral safeguards against misuse. Such a platform would treat users not as data points or consumers, but as morally significant beings whose rights and dignity must be upheld (**Alomari & Selamat, 2023**).

This philosophical approach also promotes intentional design, where the motivations behind technological creation are scrutinized. Islamic ethics asks: What is the purpose *(ghayah)* of this system? Does it serve the common good, or merely reinforce existing inequalities? Who benefits, and who is harmed? These questions go beyond compliance and efficiency—they demand a moral imagination that is sensitive to both immediate impacts and long-term societal transformations (**Shaheed et al., 2023**). Moreover, by recognizing the moral embeddedness of technology, the Islamic framework encourages a sense of collective moral agency. Developers, policymakers, and users alike share responsibility for the social effects of digital tools. This collective responsibility is rooted in the Islamic concept of *shura* (consultation) and *hisbah* (ethical accountability), which advocate communal deliberation on matters that affect public well-being. In contrast to the individualism of secular tech culture, this approach fosters shared ethical stewardship (**Dagli, 2022**).

Rejecting the myth of technological neutrality also opens the door to culturally and spiritually contextualized ethics. A global digital ethics framework must include voices from diverse traditions, including Islamic thought, which offers a holistic, purpose-driven approach to moral reasoning. The incorporation of Islamic values does not imply regression or resistance to innovation; rather, it seeks to align innovation with human dignity and divine accountability, thus ensuring technology remains a servant of higher ethical goals (**Nasr, 2023**).

Crucially, such an approach can help mitigate the harms of value-blind development, such as algorithmic bias, surveillance capitalism, and techno-authoritarianism. When ethical concerns are sidelined, technological advancement risks becoming a tool of oppression rather than liberation. The Islamic imperative to pursue *maslahah* (benefit) and avoid *mafsadah* provides a robust moral filter for evaluating technological systems and their impact on vulnerable populations (**Al-Attas, 2021**). A philosophical-Islamic critique of technological neutrality enriches current debates in digital ethics. By insisting on the moral dimensions of intention and consequence, Islamic thought reframes technology not as an independent force but as a human artifact that must be governed by ethical principles from conception to deployment. This perspective encourages a value-conscious, spiritually aware, and socially responsible approach to innovation—one that aligns technological power with the pursuit of justice and moral purpose.

Toward a Decolonial and Culturally Inclusive Cybersecurity Ethics

The global discourse on cybersecurity ethics has long been shaped by Western liberal philosophical traditions, which often emphasize individual autonomy, consent, and procedural justice. While these values have contributed significantly to the development of privacy laws and digital rights frameworks, they do not fully capture the ethical priorities and cultural nuances of non-Western societies. In Muslim-majority contexts, for instance, the moral vocabulary includes distinct concepts such as *amanah* (trust), *'adl* (justice), and *niyyah* (intention), which are deeply rooted in religious and spiritual worldviews. As digital infrastructures increasingly penetrate these societies, the need for culturally inclusive ethical paradigms becomes urgent.

This research underscores the importance of adopting a decolonial approach to cybersecurity ethics—one that critically reflects on the epistemic dominance of Western norms and makes space for alternative moral frameworks. Decolonial ethics seeks to challenge the one-size-fits-all assumptions that permeate current cybersecurity governance, advocating instead for an ethical pluralism that respects diverse traditions of thought. As Shaheed et al. (2023) argue, ethical pluralism is essential for promoting justice in global technology governance. It ensures that digital systems and policies are not merely exported across cultures but are co-constructed with local values in mind.

Islamic ethical traditions offer valuable insights for reimagining cybersecurity from a more inclusive standpoint. Unlike the secular moral reasoning dominant in Western paradigms, Islamic ethics integrates spiritual accountability with communal obligations. The Qur'anic concept of humans as *khalifah* (stewards) on earth implies responsibility not just to oneself or the state, but to a divine moral order that transcends time and geography. In cybersecurity contexts, this perspective can translate into practices that prioritize collective well-being, transparency, and moral integrity in data management (**Kamali, 2020**).

The dominance of Western-centric frameworks often results in misalignments between global cybersecurity policies and the lived realities of communities in the Global South. For example, the emphasis on individual consent in data protection may neglect communal values that stress mutual responsibility and collective oversight. In many Muslim societies, trust is socially embedded and negotiated through family, religious, and tribal institutions—factors that are not adequately addressed by current digital ethics models (**Alomari & Selamat, 2023**). Thus, integrating Islamic principles can bridge the gap between global norms and local ethics.

Moreover, the failure to recognize diverse ethical systems risks reinforcing digital colonialism—where technological solutions are imposed without regard for cultural context. This not only undermines legitimacy but can also result in ethical alienation, where users feel that digital systems conflict with their deeply held beliefs. A decolonial cybersecurity framework, therefore, calls for participatory design processes that involve local scholars, ethicists, and communities in shaping policies and technologies that affect them (**Eubanks, 2018; Dagli, 2022**).

One practical implication of this approach is the redesign of cybersecurity education and professional codes of conduct. Currently, many cybersecurity curricula are based on Euro-American ethical theories such as utilitarianism or Kantian deontology. While valuable, these frameworks should be taught alongside other traditions—including Islamic, Confucian, and African philosophies—to cultivate a generation of digital professionals who are ethically versatile and culturally sensitive. As Nasr (2023) suggests, ethical knowledge in Islam is not only theoretical but also spiritual and embodied, demanding sincerity and accountability in all forms of human interaction.

Incorporating Islamic ethics into cybersecurity also provides a counterbalance to the hyper-individualism of modern digital culture. Concepts such as *ummah* (community) and *hisbah* (moral accountability) emphasize interconnectedness and mutual oversight, fostering digital environments grounded in trust and moral responsibility. These values are particularly relevant in addressing issues like online misinformation, cyberbullying, and digital surveillance, where moral harms often extend beyond the individual to entire communities (**Elasrag, 2022**).

Critically, a decolonial and culturally inclusive approach does not reject Western ethics but seeks to decenter it as the sole authority. It invites dialogue across traditions and promotes ethical humility—a recognition that no single worldview holds a monopoly on moral truth. In cybersecurity, this means building hybrid models that combine the strengths of various ethical systems to better respond to the complex challenges of the digital age (**Marelli & Testa, 2021**). This pluralistic orientation can lead to more just, context-aware, and human-centered technological ecosystems.

Furthermore, engaging Islamic ethics in cybersecurity enhances legitimacy and public trust in Muslim-majority societies. When people see their moral values reflected in digital policies and technologies, they are more likely to engage responsibly and respectfully with them. This kind of alignment can also strengthen the effectiveness of cybersecurity measures by ensuring they resonate with users' ethical intuitions and social norms (**Shaheed et al., 2023**). Trust, after all, is not built solely through encryption and protocols but through cultural resonance and moral integrity.

Cybersecurity ethics must evolve beyond its Western-centric roots to embrace a truly global and inclusive perspective. Islamic ethical thought, with its rich moral vocabulary and spiritual orientation, offers vital resources for this transformation. By adopting a decolonial lens, scholars and practitioners can create ethical frameworks that are not only technically

robust but also culturally grounded and morally compelling. This shift is not just a matter of fairness—it is essential for building trustworthy, resilient, and just digital futures for all.

CONCLUSION

This study has argued that cybersecurity ethics, as it stands today, remains predominantly shaped by Western liberal norms that often neglect the diverse moral frameworks present in non-Western societies. By engaging with Islamic philosophical and ethical principles—such as *amanah* (trust), *'adl* (justice), and *niyyah* (intention)—this research has demonstrated how Islamic thought provides a robust and contextually grounded alternative to value-neutral or secular cybersecurity paradigms. The inclusion of Islamic ethics not only enriches the global discourse on digital trust but also serves as a decolonial corrective to the epistemic hegemony in current ethical frameworks. Through a philosophical-Islamic lens, this study emphasizes that cybersecurity must move beyond mere technical efficacy toward moral responsibility, spiritual accountability, and cultural legitimacy. As digital infrastructures expand into Muslim-majority societies, there is an urgent need for ethical pluralism that respects indigenous moral traditions and fosters a more inclusive, just, and trusted digital ecosystem.

LIMITATIONS AND FUTURE RESEARCH RECOMMENDATIONS

While this study presents a valuable philosophical and theological perspective on cybersecurity ethics grounded in Islamic traditions, several limitations should be acknowledged. *First,* the research employs a purely qualitative, library-based methodology that does not involve empirical validation through field studies, interviews, or case-based observations. Although this method is appropriate for normative inquiry, it limits the ability to assess how Islamic ethical concepts such as *amanah, 'adl,* and *niyyah* are operationalized in real-world cybersecurity policy, governance, or user behavior—particularly within institutions or organizations in Muslim-majority contexts.

Second, the study focuses primarily on classical Islamic sources and general cybersecurity literature without engaging deeply with sector-specific case studies (e.g., healthcare, finance, education) where ethical tensions in data security are often most acute. The absence of such domain-specific exploration limits the practical applicability of the proposed ethical framework to diverse cybersecurity environments. *Third,* while the article emphasizes the value of Islamic ethics as a corrective to Western-centric norms, it does not comparatively analyze how Islamic ethical principles align or diverge from other non-Western or religious traditions (e.g., Confucian, Hindu, African communal ethics). Such comparative ethics would enhance the study's contribution to the broader discourse on ethical pluralism in global cybersecurity governance. *Fourth,* although the study successfully challenges the assumption of technological neutrality, it does not offer concrete design frameworks or regulatory recommendations to guide the development of culturally inclusive and ethically aligned cybersecurity systems. As a result, the philosophical principles remain somewhat abstract and may be difficult to translate into practice for policymakers, developers, or digital educators.

In light of these limitations, future research should pursue several directions. *First,* empirical investigations are needed to explore how Islamic ethical values are interpreted and applied by cybersecurity practitioners, regulators, and educators. Qualitative methods such as interviews, case studies, and ethnographic research in Muslim-majority digital institutions would help validate and contextualize the normative claims advanced in this study. *Second,*

interdisciplinary collaboration between Islamic scholars, computer scientists, legal experts, and digital ethicists should be fostered to co-develop value-sensitive cybersecurity frameworks that are both theologically sound and technically actionable. Such work could lead to the formulation of culturally responsive design principles, ethical codes of conduct, and assessment tools for digital trust.

Third, comparative research across different religious and cultural traditions could enrich the theoretical grounding of decolonial ethics in technology. Investigating points of convergence and divergence among moral traditions would contribute to the creation of hybrid or dialogical frameworks for global digital ethics. *Fourth*, policy-oriented studies should explore how Islamic ethical constructs can inform national cybersecurity strategies, AI governance policies, and data protection regulations in Muslim-majority countries. Such studies could evaluate the feasibility and effectiveness of embedding *amanah* or *'adl* into digital legislation, risk management protocols, or AI transparency standards.

Finally, longitudinal research is needed to assess how ethically informed cybersecurity practices influence digital trust, user behavior, and institutional legitimacy over time. Evaluating long-term outcomes would provide evidence of whether integrating Islamic ethics into cybersecurity contributes to more just, inclusive, and trustworthy digital ecosystems. By addressing these gaps, future scholarship can move beyond abstract theorization and contribute to the development of applied, pluralistic, and ethically grounded cybersecurity frameworks that reflect the moral traditions and lived realities of diverse global communities.

REFERENCES

Al-Attas, S. M. N. (2021). *Islam and the Philosophy of Science*. UBD Press.

Alomari, I., & Selamat, A. (2023). Toward ethical AI governance in Muslim societies: The role of Islamic ethical principles. *International Journal of Ethics and Information Technology*, 25(1), 33–49. https://doi.org/10.1007/s10676-023-09676-2

Booth, W. C., Colomb, G. G., & Williams, J. M. (2021). *The Craft of Research* (4th ed.). University of Chicago Press.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2020). Artificial intelligence and the 'Good Society': The US, EU, and UK approach. *Science and Engineering Ethics*, 26(6), 2961–2977. https://doi.org/10.1007/s11948-020-00247-2

Dagli, C. K. (2022). Ethical governance and Islamic values in the digital age. *Muslim World*, 112(2), 214–230. https://doi.org/10.1111/muwo.12342

Elasrag, H. (2022). *Islamic Ethics and Digital Technology: Challenges and Prospects*. Islamic Development Bank Institute.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Floridi, L. (2021). *The Ethics of Artificial Intelligence*. Oxford University Press.

Floridi, L., & Cowls, J. (2022). The Ethics of Cybersecurity. *Springer*. https://doi.org/10.1007/978-3-030-69904-8

Kamali, M. H. (2020). *Ethics and Fiqh for Everyday Life: An Islamic Perspective*. International Institute of Islamic Thought (IIIT).

Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology* (4th ed.). SAGE Publications.

Mann, M., Daly, A., & Wilson, M. (2021). Understanding the normative dimensions of cybersecurity. *Policy & Internet*, 13(3), 381–398. https://doi.org/10.1002/poi3.243

Marelli, L., & Testa, G. (2021). Digital trust and the ethics of data practices. *Nature Communications*, 12(1), 1–3. https://doi.org/10.1038/s41467-021-22244-2

Marelli, L., & Testa, G. (2021). Scrutinizing the ethical neutralization of AI systems: A call for value-sensitive design. *AI & Society*, 36(3), 803–815. https://doi.org/10.1007/s00146-021-01188-4

Mittelstadt, B. D. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

Nasr, S. H. (2023). *Knowledge and the Sacred in the Age of Technology*. Islamic Texts Society.

Palmer, R. E. (2022). *Hermeneutics: Interpretation Theory in Schleiermacher, Dilthey, Heidegger, and Gadamer*. Northwestern University Press.

Shaheed, F., Huda, Q., & Bukhari, Z. (2023). Decolonizing ethics in technology governance: A Muslim perspective. *Journal of Global Ethics*, 19(2), 150–167. https://doi.org/10.1080/17449626.2023.2195812

von Solms, B., & van Niekerk, J. (2023). Cybersecurity: Critical reflections from the human perspective. *Computers & Security*, 128, 103015. https://doi.org/10.1016/j.cose.2023.103015

West, S. M., Whittaker, M., & Crawford, K. (2022). *Discriminating systems: Gender, race, and power in AI*. AI Now Institute. https://ainowinstitute.org/discriminatingsystems.html

Zed, M. (2021). *Metodologi Penelitian Kepustakaan*. Yayasan Obor Indonesia. (Translated and referenced for library research context).