INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PROGRESSIVE EDUCATION & DEVELOPMENT

OPEN ACCESS JOURNAL

Vol 15, Issue 2, (2026) E-ISSN: 2226-6348

Internalisation of Islamic Ethics in Cybersecurity: A Systematic Literature Review

Nur Fatin Safiqa Binti Masrial, Hafizhah Zulkifli*

Faculty of Education, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Malaysia

*Corresponding Author Email: hafizhah_zulkifli@ukm.edu.my

DOI Link: http://dx.doi.org/10.6007/IJARPED/v15-i2/28245

Published Online: 21 May 2026

Abstract

The contemporary digital environment is increasingly challenged by complex cybersecurity issues that extend beyond technical threats to include concerns related to users' moral integrity. This study examines the application of Islamic ethics (akhlak) in cybersecurity and identifies factors influencing its internalisation through a Systematic Literature Review (SLR). The review was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework, analysing 15 selected journal articles retrieved from Scopus, Web of Science (WoS), and Google Scholar. Articles published between 2021 and 2025 were considered, although eligible studies were identified from 2022 onwards. Thematic analysis revealed three key domains: the application of Islamic ethics in cyberspace, extrinsic factors such as education and social interventions, and intrinsic factors related to psychospiritual strength and religious commitment. The findings indicate that effective cybersecurity practices require the integration of ethical values with technical measures. This study contributes to the development of value-based cybersecurity approaches and highlights the importance of strengthening internal ethical awareness. It further suggests the development of Islamic ethics-based educational modules to enhance digital resilience in addressing contemporary cyber challenges.

Keywords: Islamic Ethics, Cybersecurity, Internalisation, Psychospiritual Strength, Systematic Literature Review

Introduction

The nation's digital transformation agenda aims to develop a society that is not only technologically proficient but also globally competitive. However, the global digital landscape is increasingly challenged by an ethical crisis, characterized by the normalization of cyber misconduct and the erosion of digital empathy. These evolving cyber threats extend beyond technical intrusions to sophisticated forms of psychological manipulation and social engineering that exploit human trust. This critical issue is exemplified by recent high-profile transnational scams that weaponize users' psychological vulnerabilities for criminal gain (Berita Harian, 2026). In Malaysia, cybersecurity reports recorded 1,657 incidents in the first quarter of 2025 alone, largely involving email phishing and malicious attachments (CyberSecurity Malaysia, 2025a, 2025b). Theoretically, these trends suggest that cybersecurity failures are often rooted in the human factor as the "weakest link," indicating

that challenges are not solely technical but are fundamentally linked to human ethics and behaviour.

This situation is further compounded by weak self-regulation among users, which is often exacerbated by issues such as internet addiction that lead to moral decay (Ab Majid et al., 2021). Although various digital initiatives have been introduced, existing approaches tend to prioritize technological infrastructure while overlooking the development of internal ethical awareness. For instance, current national efforts such as the My Cyber Hero (MYCH) 2026 program by NACSA demonstrate a strong commitment to building technical competencies and AI-driven defence among students (NACSA, 2026). Similarly, programs like 'Pendekar Siber' have been initiated to empower youth against cyber threats through external awareness (Abdul Molok & Zulkifli, 2021). However, previous studies highlight that digital literacy or competitive technical proficiency without ethical grounding and spiritual awareness (*muraqabah*) is insufficient to address cyber misconduct effectively (Ashaari et al., 2022; Suhaime et al., 2023). As Zani et al. (2025) argue, unethical behaviour in the virtual environment is a reflection of the quality of moral values in real life, suggesting that internalized norms are the ultimate solution to behavioural-based risks.

Despite growing scholarly attention, a significant gap remains. Current studies tend to emphasize general communication ethics (Asy'ari et al., 2025) or broader educational approaches such as *Manhaj Rabbani* and emotional intelligence (Din et al., 2022; Sihombing et al., 2025), with limited focus on integrating specific Islamic ethical values—such as *Amanah* (trustworthiness) and *Hifz al-Mal* (preservation of wealth)—within cybersecurity contexts (Hutagalung et al., 2025; Abdullah et al., 2022). This indicates a lack of a comprehensive framework that connects moral development with practical cybersecurity practices. While this review synthesizes literature published between 2021 and 2025, the persistence of these challenges in 2026 underscores the urgency of this research. Therefore, this study employs a Systematic Literature Review (SLR) to examine the application of Islamic ethics in cybersecurity and to identify the key factors influencing its internalization among users. By synthesizing existing literature, this study aims to contribute towards a value-based cybersecurity framework that emphasizes the strengthening of individual moral and spiritual resilience.

Literature Review

Several studies, including systematic literature reviews (SLR), have examined the relationship between Islamic values and the digital environment. For instance, Sihombing et al. (2025) emphasise moral education grounded in emotional intelligence, while Abdullah et al. (2022) and Din et al. (2022) highlight elements of digital ethics and the Manhaj Rabbani approach. However, these studies predominantly focus on general character development and do not explicitly address cybersecurity as a distinct technical and behavioural domain. This indicates a need for a more focused synthesis that integrates ethical values within the context of contemporary cyber threats (Rahman et al., 2022).

From a theoretical perspective, Islamic ethics serves as a comprehensive value system that guides human behaviour in digital environments. Core principles such as *Siddiq* (truthfulness) and *Amanah* (trustworthiness) form the foundation of ethical digital conduct (Zani et al., 2025). Within the framework of *Maqasid Syariah* (al-Daruriyyat al-Khams), these

values support the preservation of religion, intellect, and property through concepts such as *muraqabah* (self-awareness of divine supervision) and *tabayyun* (verification of information) (Asy'ari et al., 2025; Suhaime et al., 2023). In addition, the principle of *hifz al-mal* reinforces responsible digital practices in safeguarding assets and managing cyber risks (Awais et al., 2025). Collectively, these ethical and spiritual dimensions function as an internal self-regulation mechanism that complements technical cybersecurity measures and contributes to the protection of individual well-being and dignity (Ashaari et al., 2022; Tan & Balaraman, 2023).

Methodology

This study adopts the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure a systematic, transparent, and reproducible review process (Page et al., 2021). The research questions were developed using the PICo framework (Lockwood et al., 2015), which focuses on digital users as the population, Islamic ethics as the phenomenon of interest, and cybersecurity as the contextual setting. The literature selection process was conducted through three key stages: identification, screening, and inclusion. These stages were systematically applied to filter relevant studies based on predefined criteria, as illustrated in Figure 1.

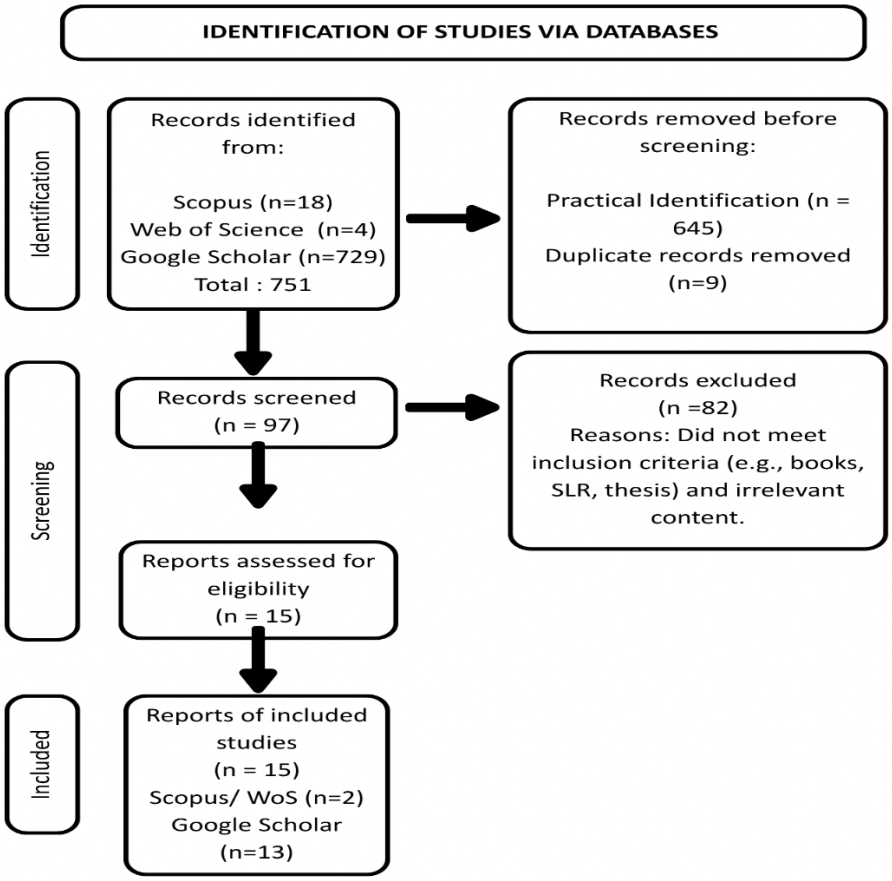

Figure 1. The article selection process based on the PRISMA 2020 guidelines
Source: Page et al. (2021)

Phase Identification: A systematic search was performed in Scopus, Web of Science (WoS), and Google Scholar databases using Boolean operators (AND/OR) and truncation symbols. This strategy produced 751 initial records.

Table 1
Search Keyword

Database	Search String	Results
Scopus	TITLE-ABS-KEY (("islamic ethic*" OR "akhlak" OR "muslim moral*" OR "shariah") AND ("cybersecurity" OR "cyber safet*" OR "digital ethic*" OR "online securit*" OR "internet ethic*"))	18 articles
Web of Science (WoS):	TS= (("islamic ethic*" OR "akhlak" OR "muslim moral*" OR "shariah") AND ("cybersecurity" OR "cyber safet*" OR "digital ethic*" OR "online securit*" OR "internet ethic*"))	4 articles
Google Scholar	Search performed using the following keywords: English: ("Islamic ethics" OR "Islamic values") AND ("cybersecurity") AND ("awareness"). Malay: ("Akhlak" OR "Etika") AND ("Keselamatan Siber" OR "Keselamatan Maklumat") site:.my	729 articles
	TOTAL	**751 articles**

Phase Screening: After removing duplicates and practical screening, 97 articles were evaluated based on inclusion and exclusion criteria. Focus was given to peer-reviewed research journal articles for the period 2021 to 2025 in Malay and English.

Table 2
Inclusion and Exclusion Criteria

CRITERIA	INCLUSION	EXCLUSION
LITERATURE TYPE	Empirical research journal articles (peer-reviewed).	Dissertations, theses, books, book chapters, concept papers, and review articles (Review paper/SLR).
LANGUAGE	Malay, English.	Languages other than these two.
TIMEFRAME	Articles published within a five-year period (2021 to 2025).	Articles published before 2021.
INDEX	Journals indexed in Scopus, Web of Science, Google Scholar.	Journals not indexed in recognized databases.
RESEARCH FOCUS	Islamic ethics in cybersecurity or digital behaviour.	Purely technical cyber aspects without elements of values/ethics.

Phase Inclusion: Based on the full-text eligibility assessment, 15 final articles were selected for synthesis analysis. This strict screening process ensures that the selected articles have a direct correlation with the study objectives.

Quality Assessment: To enhance the credibility of the findings and reduce potential bias, all 15 selected articles were assessed using the Mixed Methods Appraisal Tool (MMAT) version

2018 (Hong et al., 2018). This tool enables a systematic evaluation of qualitative, quantitative, and mixed-method studies. The assessment was conducted collaboratively to ensure consistency in judgement, and all articles were found to meet the required quality criteria for inclusion in the data synthesis.

Data Extraction and Analysis

Data from the 15 selected articles were systematically extracted, including author information, research methodology, and key findings relevant to the study objectives. To ensure consistency and minimise potential misinterpretation, the extraction process was cross-checked collaboratively among researchers.

Given that this study integrates multiple research designs, thematic analysis was employed as the primary qualitative synthesis approach. The analysis identified three main dimensions: the application of Islamic ethics (trustworthiness/adab), extrinsic factors (education and social intervention), and intrinsic factors (psychospiritual strength and religious internalisation).

The findings indicate that the literature is largely dominated by the dimension of ethical application (n=10), followed by intrinsic factors (n=9) and extrinsic factors (n=8). The presence of overlapping themes across studies suggests a strong interrelationship between external guidance and internal spiritual strength in addressing the complexity of cybersecurity challenges.

Findings

Background This section details the profile of the 15 articles, covering methodological aspects, publication trends, and geographical contexts.

Table 3
Journal Profile

No	Author (Full Name)	Journal Name	Methodology	Sample / Field Data	Context
1	Azma Alina Ali Zani, Azah Anir Norman, Norjihan Abdul Ghani and Riswan Septriayadi Sianturi (2025)	IEEE Access	Quantitative	219 social media users.	Malaysia
2	Muhamad Faisal Ashaari, Nor Faizah Ismail, Rosmawati Mohamad Rasit and Zulkefli Aini (2022)	Jurnal Komunikasi: Malaysian Journal of Communication	Fuzzy Delphi	12 media and religious experts.	Malaysia
3	Abdul Muaz bin Mustaffa and Nurbazla Ismail (2025)	Journal of Contemporary Islamic Law (JCIL)	Quantitative	60 parents.	Malaysia
4	Noorfaiz Athallah Koeswandana and Mayang Yorindafitri Yulfiatmi (2025)	Jurnal Ekonomi & Keuangan Islam	Quantitative	244 Islamic Bank respondents.	Indonesia
5	Yatiman Karsodikromo, Mohd. Razimi Hussin and	Journal of Humanities and Social Sciences	Qualitative Case Study	5 students who are victims of cyberbullying.	Malaysia

	Abdul Rahim Razali (2022)				
6	Ayu Nadhirah Mohd Suhaime, Nurul Husna Mansor, Abd. Aziz Rekan, Khairul Hamimah Mohammad Jodi and Mohd Syukri Zainal Abidin (2023)	Afkar: Jurnal Akidah & Pemikiran Islam	Qualitative (FGD)	Experts from JAKIM, IPSA, and Educators.	Malaysia
7	Ali Awais, Muhammad Umar Mehmood and Muhammad Mubeen Goraya (2025)	Contemporary Journal of Social Science Review	Exploratory Qualitative (Data Triangulation)	18 Shariah experts and cyber professionals.	UK & Pakistan
8	Nor Azah Abdul Aziz, Che Zarrina Sa'ari and Suzaily Wahab (2023)	Afkar: Jurnal Akidah & Pemikiran Islam	Qualitative	Parents (Interview).	Malaysia
9	Suhaila Zainudin, Shahrina Shahrani, Zulaiha Ali Othman, Wan Fariza Paizi@Fauzi, Khairul Akram Zainol Ariffin, Praveen a/l Kanagarajah, Siti Aishah Sahar and Nurul Hasmidar Lah (2022)	Malaysian Journal of Information and Communication Technology (MyJICT)	Quantitative	App user evaluation.	Malaysia
10	Jasmyn Tan Yu Xuan and Rani Ann Balaraman (2023)	Jurnal Psikologi Malaysia	Qualitative	12 adolescents who are victims of cyberbullying.	Malaysia
11	Muhammad Wandisyah R. Hutagalung, Saparuddin Siregar, Mhd Furqan, Ismail Pulungan and Furkan Elce (2025)	El-Qist: Journal of Islamic Economics and Business	Quantitative	384 bank customers.	Indonesia
12	Lailil Muharromah and Umar Manshur (2025)	Journal of Educational Management Research	Qualitative	Madrasah Principals and Teachers.	Indonesia
13	Azarudin Awang & Rubiah Abu Bakar (2024)	Jurnal 'Ulwan	Quantitative	258 Higher Education Institution (IPT) students.	Malaysia
14	Muhammad Haziq bin Haji Shahjahan, Adam bin Haji Jait, Anis Malik Thoha, Nurefnazahani binti Haji Durani (2024)	International Journal of ʿUmrānic Studies	Quantitative	580 university students.	Brunei
15	Ali Alqarni (2025)	Humanities & Social Sciences Communications	Quantitative	1,980 secondary school students.	Saudi Arabia

Analysis indicates a diversity of research methodologies, ranging from in-depth case studies to large-scale surveys. The credibility of the data is further strengthened by the involvement of industry experts and religious institutions such as JAKIM. In terms of publication trends, Figure 2 shows a concentration of studies in 2025 (n=7), suggesting that cyber ethics has emerged as a significant contemporary area of research.

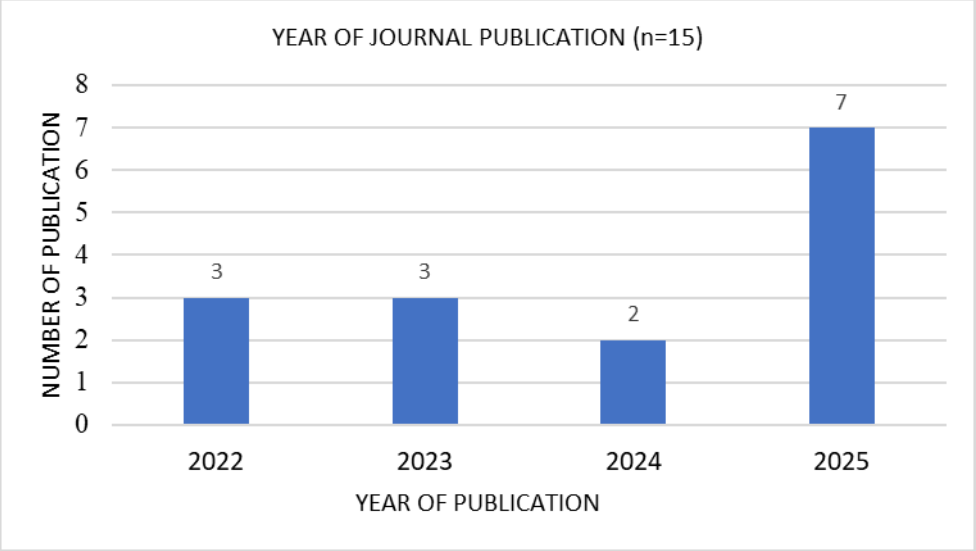

Figure 2. Number of publications by year
Source: Researcher's Analysis (2025)

Furthermore, the geographic distribution of the literature, as illustrated in Figure 3, indicates a dominance of local studies (60%), followed by regional Nusantara and Middle Eastern contexts. This distribution suggests that the findings are informed by diverse socio-cultural settings, thereby enhancing the breadth and contextual relevance of the study.

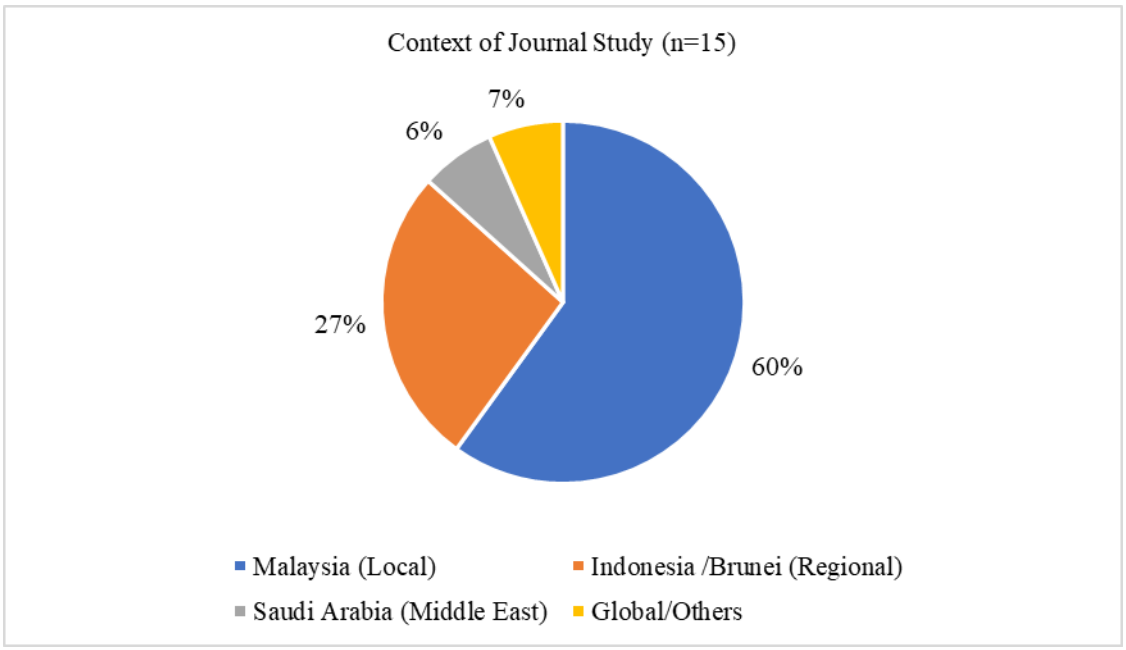

Figure 3. Distribution of Journals by Context
Source: Researcher's Analysis (2025)

Data Extraction Matrix and Gap Analysis: Based on the Xiao and Watson (2019) analysis format, data from selected articles were classified systematically to identify research gaps. Table 4 displays the mapping of theories, methodologies, and critical results that form the basis of the main themes.

Table 4
Data Extraction Matrix

No	Author (Year)	Theory / Model	Importance (I) & Main Reason (R)	Methodology	Main Research Findings	Gaps & Recommendations
1	Ashaari et al. (2022)	Ribble's Digital Citizenship Model (Islamic Adaptation).	**I:** Islamic digital citizen model. **R:** Gap in students' digital ethics.	Fuzzy Delphi (12 experts).	Digital Ethics (*Akhlak*) is the main pillar of effective cybersecurity.	Conduct quantitative tests in a large population.
2	Alqarni (2025)	Cyber Threat Perception Model.	**I:** Awareness vs. Behaviour. **R:** Cyber threats among Saudi adolescents.	SEM-AMOS (n=1,980).	Threat perception mediates the relationship between awareness and protective behaviour.	The role of parents as moderators.
3	Zani et al. (2025)	Offline Ethics Framework.	**I:** Existing ethics vs. self-disclosure. **R:** Social media privacy risks.	PLS-SEM (n=219).	Offline ethics determines user discipline in protecting personal data.	Influence of local culture on privacy.
4	Zainudin et al. (2022)	Mobile Application Development Life Cycle (MADLC).	**I:** Cyber ethics application. **R:** Need for interactive mediums.	System Development & User Evaluation.	Mobile applications significantly increase understanding of ethics and safety.	Add gamification elements.
5	Koeswandana & Yulfiatmi (2025)	Protection Motivation Theory (PMT) & Religiosity.	**I:** Bank loyalty after cyberattacks. **R:** Customer trust crisis.	PLS-SEM (n=244).	Religious internalisation maintains Islamic bank customer loyalty even if data is stolen.	Impact of compensation on image recovery.
6	Aziz et al. (2023)	Islamic Psychospiritual Perspective.	**I:** Parental monitoring. **R:** Risks of children's Home-Based	Qualitative: Interviews.	Spiritual values build internal barriers for children on the internet.	Develop practical psychospiritual modules.

			Teaching and Learning (PdPR).			
7	Suhaime et al. (2023)	Islamic Psychospiritual Approach.	**I:** Cyber addiction control. **R:** Impact of pornographic content.	Needs Analysis & Qualitative.	*Dhikr* and Repentance are critical components in restoring digital ethics.	Empirical testing of model effectiveness.
8	Hutagalung et al. (2025)	Protection Motivation Theory & Maqasid Syariah.	**I:** Reflection of *Hifz al-Mal* (Preservation of Property). **R:** Digital banking security.	PLS-SEM (n=384).	Cybersecurity is a religious demand to preserve property (*mal*).	Comparison between Islamic and conventional banks.
9	Muharromah & Manshur (2025)	Islamic Education Digital Ethics Framework.	**I:** Ethics in education. **R:** Digital content inconsistent with Islam.	Qualitative: Observation.	The main challenge is moral supervision within digital knowledge content.	Digital media literacy for religious teachers.
10	Ali et al. (2025)	Shariah Perspective (*Thiqah* & *Amanah*).	**I:** i-Fintech risks. **R:** Threats to trust.	Qualitative: Expert interviews.	Technical security is a Shariah requirement to safeguard data trust.	Shariah-compliant cyber governance framework.
11	Shahjahan et al. (2024)	Knowledge, Attitude, Practice (KAP) Model.	**I:** Student cyber literacy. **R:** Level of alertness among Brunei students.	Descriptive Quantitative.	High knowledge does not guarantee consistent alertness.	Relationship between religious background and attitude.
12	Mustaffa & Ismail (2025)	Islamic Legal Perspective & Privacy Rights.	**I:** Parental sharenting issues. **R:** Violation of child privacy.	Quantitative: Survey.	Parents are less aware of the impact of child data disclosure on privacy rights.	Comparison between civil and Shariah law.
13	Karsodikromo et al. (2022)	Psychological Impact & Mental Health Model.	**I:** Implications of cyberbullying. **R:** Victims' emotional disturbances.	Qualitative: Case Study.	Cyberbullying damages moral well-being and academic performance.	Religious-based emotional support.

14	Awang & Bakar (2024)	User Perception and Attitude Theory.	**I:** Alternative communication media. **R:** Usage without ethical boundaries.	Quantitative: Attitude Evaluation (n=258).	Attitude is influenced by the level of understanding of the risks associated with the media used.	Effectiveness of awareness campaigns in universities.
15	Tan & Balaraman (2023)	Social Behaviour Cause & Effect Framework.	**I:** Cyberbullying on Instagram. **R:** Lack of digital empathy among adolescents.	Qualitative: Interviews (n=12).	Lack of digital empathy (ethics) is a primary cause of cyberbullying.	Development of digital empathy modules.

In summary, this matrix highlights the need to move beyond technical awareness towards the development of practical modules that integrate Islamic psychospiritual values and Shariah-compliant cyber governance.

Thematic Analysis

The 15 selected articles were categorised into three primary themes to address the research questions: the application of Islamic ethics, extrinsic factors, and intrinsic factors influencing cybersecurity practices.

Application of Islamic Ethics in Cyberspace

Analysis of ten selected studies indicates that the application of Islamic ethics in cyberspace is reflected through responsible digital behaviour. Ashaari et al. (2022) and Shahjahan et al. (2024) highlight that ethical values play a central role in shaping users' self-control and vigilance against cyber threats. This role is further supported by the principle of *la darar wa la dirar*, which emphasises harm prevention, as well as the use of ethical-based digital applications to reduce potential risks.

In addition, the concepts of *thiqah* (trust) and *amanah* (trustworthiness) are associated with responsible data management and privacy protection. These ethical practices are often influenced by the integrity of offline behaviour, suggesting continuity between real-world and digital conduct. Furthermore, self-monitoring (*muraqabah*) and digital empathy are identified as important elements in reducing cyberbullying and exposure to harmful content. Overall, the literature suggests that Islamic ethics serves as a guiding framework for responsible digital engagement.

Extrinsic Factors: Education and Social Intervention

External factors play a significant role in shaping cyber ethical behaviour through the interaction of education, technology, and family environments. Alqarni (2025) and Muharromah and Manshur (2025) indicate that formal and religious education function as key socialisation agents in promoting ethical digital behaviour. This is further reinforced

through technological interventions and the development of digital citizenship models grounded in Islamic values.

At the family level, parental supervision that incorporates psychospiritual elements contributes to the development of self-regulation. However, several studies also highlight challenges, including limited parental awareness, insufficient environmental support, and peer influence, which may weaken ethical practices. These findings suggest that a holistic and coordinated support system is essential for strengthening ethical internalisation in cybersecurity contexts.

Intrinsic Factors: Psychospiritual Strength and Religious Devotion

Intrinsic factor**,** particularly psychospiritual strength and religious commitment, function as internal control mechanisms in managing digital risks. These factors are linked to an individual's awareness of moral responsibility, including the concepts of reward and sin, as well as the application of Maqasid Syariah principles such as *hifz al-mal*.

Psychospiritual practices and ethical consistency in offline life are associated with improved digital well-being and behavioural discipline. However, the literature also suggests that knowledge alone is insufficient without corresponding emotional and spiritual resilience. Individuals with high awareness but limited self-control remain vulnerable to cyber risks and psychological distress. Overall, these findings indicate that internal strength plays a crucial role in shaping sustainable cybersecurity behaviour.

Discussion

This section synthesises the literature findings in relation to the two research questions.

Regarding the application of Islamic ethics in cybersecurity (RQ1), the findings suggest that ethical values function as practical control mechanisms within the digital environment. Core principles such as *amanah* and *thiqah* are closely associated with responsible data management and privacy protection, contributing to risk mitigation in digital interactions (Ali et al., 2025; Muharromah & Manshur, 2025). In addition, the integration of digital citizenship models with the principle of *la darar wa la dirar* highlights the role of security literacy as part of ethical responsibility (Ashaari et al., 2022; Shahjahan et al., 2024; Zainudin et al., 2022). These ethical orientations are also linked to reduced exposure to cyber risks, including cyberbullying and harmful content (Suhaila et al., 2022; Tan & Balaraman, 2023). Furthermore, self-regulation through *muraqabah* is identified as an internal mechanism that shapes users' awareness and restraint in digital behaviour (Hutagalung et al., 2025; Suhaime et al., 2023; Zani et al., 2025). Collectively, these findings indicate that ethical values play a significant role in strengthening cybersecurity beyond purely technical measures.

In relation to factors influencing the internalisation of Islamic ethics (RQ2), the literature highlights the interaction between extrinsic and intrinsic dimensions. External factors, including formal education, family influence, and technological interventions, contribute to shaping ethical awareness and behaviour. Studies emphasise the role of educational and religious institutions as key agents in promoting ethical digital conduct, supported by digital citizenship frameworks grounded in Islamic values (Alqarni, 2025; Muharromah & Manshur, 2025; Ashaari et al., 2022; Zainudin et al., 2022). At the family level, parental guidance that incorporates psychospiritual elements is associated with the

development of self-control (Aziz et al., 2023). However, challenges such as limited parental awareness, insufficient environmental support, and peer influence may weaken ethical internalisation (Mustaffa & Ismail, 2025; Awang & Bakar, 2024; Shahjahan et al., 2024).

At the same time, intrinsic factors, particularly psychospiritual strength and religious commitment, appear to play a more fundamental role in sustaining ethical behaviour. These internal dimensions are linked to moral awareness, including the understanding of reward and sin, as well as the application of Maqasid Syariah principles such as *hifz al-mal* (Hutagalung et al., 2025; Alqarni, 2025). Spiritual practices and consistency in offline ethical conduct are associated with improved digital well-being and behavioural discipline (Suhaime et al., 2023; Zani et al., 2025; Aziz et al., 2023). Nevertheless, the findings also suggest that knowledge alone is insufficient without corresponding emotional and spiritual resilience, as individuals may remain vulnerable to cyber risks despite having high levels of awareness (Shahjahan et al., 2024; Karsodikromo et al., 2022). Overall, the interaction between external support and internal strength highlights the importance of a holistic approach to cybersecurity that integrates both technical and ethical dimensions.

Conclusion

This study synthesises the integration of Islamic ethics within the cybersecurity framework through a systematic literature review approach. The findings highlight that the application of Islamic ethics is reflected through values such as *amanah* and *muraqabah*, shaped by both extrinsic factors, including education and social intervention, and intrinsic factors related to psychospiritual strength and religious internalisation. These results underscore the importance of integrating ethical values with technical measures in strengthening cybersecurity practices.

Despite these contributions, several limitations should be acknowledged. The study is restricted to selected databases and includes only publications in Malay and English, excluding potentially relevant works in other languages such as Arabic and Indonesian.

Overall, this study contributes to the growing body of knowledge on value-based digital ethics by offering a holistic perspective that integrates spiritual and behavioural dimensions. It further highlights the need for future research to develop practical intervention modules based on Islamic ethical principles to enhance digital resilience in addressing contemporary cyber challenges.

Acknowledgement: Thank you to all parties who have provided academic and technical support throughout this research until the article was ready for publication.

Conflicts of Interest: The authors declare that there are no conflicts of interest in the production of this research.

References

Abdullah, M. H., Jaes, L., Rahman, R., & Johar, S. S. (2022). Elemen pengukuhan etika digital berdasarkan analisis tinjauan literatur sistematik. *Advances in Humanities and Contemporary Studies, 3*(2), 9–19. https://doi.org/10.30880/ahcs.2022.03.02.002

Ali, A., Mehmood, M. U., & Goraya, M. M. (2025). Managing cyber security risks in Islamic fintech: A Shariah perspective. *Contemporary Journal of Social Science Review, 3*(4), 1674–1688.

Alqarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviours among Saudi secondary school students: The mediating role of cyber threat perception and the moderating role of internet usage duration. *Humanities and Social Sciences Communications, 12*, 1–11. https://doi.org/10.1057/s41599-025-06122-x

Asy'ari, D. A., Ramadhan, Z. L., Gibran, D., Pratama, N., Satria, Y. P. B., & Setyaningrum, R. P. (2025). Analisis etika komunikasi digital di era media sosial (suatu kajian literatur). *Jurnal Inovasi dan Kolaborasi Nusantara, 6*(2). https://ejurnals.com/ojs/index.php/jikn/article/view/2091

Ashaari, M. F., Ismail, N. F., Rasit, R. M., & Aini, Z. (2022). Pembangunan model kewarganegaraan digital Islami berdasarkan metode Fuzzy Delphi. *Jurnal Komunikasi: Malaysian Journal of Communication, 38*(4), 97–117. https://doi.org/10.17576/JKMJC-2022-3804-06

Awang, A., & Bakar, R. A. (2024). Menilai pengetahuan, persepsi, dan sikap pelajar terhadap penggunaan media komunikasi alternatif. *Jurnal 'Ulwan, 9*(2), 151–169. https://unimel.edu.my/journal/index.php/JULWAN/article/view/1790

Aziz, N. A. A., Sa'ari, C. Z., & Wahab, S. (2023). Cyber security for children: Parental monitoring from a technological, child psychology and Islamic psychospiritual perspective during the Covid-19 pandemic. *Afkār: Jurnal Akidah & Pemikiran Islam, 25*(1), 73–98. https://doi.org/10.22452/afkar.vol25no1.3

Berita Harian. (2026, January 8). Dalang penipuan dalam talian ditahan di Kemboja, diekstradisi ke China. https://www.bharian.com.my/dunia/asean/2026/01/1493966/dalang-penipuan-dalam-talian-ditahan-di-kemboja-diekstradisi-ke-china

CyberSecurity Malaysia. (2025a). SR-030.062025: MyCERT report - Cyber incident quarterly summary report - Q1 2025. https://www.cybersecurity.my/portal-main/advisories-details/93c2ce07-468d-11f0-a5d3-0050568c1b65

CyberSecurity Malaysia. (2025b). Advisory: Technical vulnerabilities and mitigation strategies for digital infrastructure. https://www.cybersecurity.my/portal-main/advisories-details/dc8402e8-b9f7-11f0-b161-0050568ccc16

Din @ Mohamad Nasirudin, N., Majid, M. A., Husin, H., & Rahman, K. A. A. (2022). Elemen pendidikan Manhaj Rabbani menggunakan analisis kajian literatur bersistematik (SLR). *Jurnal Sultan Alauddin Sulaiman Shah, 9*(1), 16–31. https://jsass.uis.edu.my/index.php/jsass/article/view/180/149

Edwards, P., Clarke, M., DiGuiseppi, C., Pratap, S., Roberts, I., & Wentz, R. (2009). Identification of randomized controlled trials in systematic reviews: Accuracy and reliability of screening records. *Journal of Information Science, 35*(1), 13–24.

Flemming, K., Booth, A., Garside, R., Tunçalp, Ö., & Noyes, J. (2018). Qualitative evidence synthesis: Where are we at? *International Journal of Qualitative Methods, 17*(1), 1–13.

Hong, Q. N., Fàbregues, S., Bartlett, G., Boardman, F., Cargo, M., Dumont, P., Vedel, I., & Pluye, P. (2018). The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers. *Education for Information, 34*(4), 285–291.

Hutagalung, M. W. R., Siregar, S., Furqan, M., Pulungan, I., & Elce, F. (2025). Cybersecurity behaviour as a reflection of Ḥifẓ al-Māl in Islamic banking: A behavioural model based on protection motivation theory. *El-Qist: Journal of Islamic Economics and Business, 15*(2), 127–153. https://doi.org/10.15642/elqist.2025.15.2.127-153

Karsodikromo, Y., Hussin, M. R., & Razali, A. R. (2022). Implikasi buli siber, kemurungan, kebimbangan dan tekanan terhadap pencapaian akademik murid. *Journal of Humanities and Social Sciences, 4*(3), 129–139.

Koeswandana, N. A., & Yulfiatmi, M. Y. (2025). Do cyberattacks and religiosity impact customers' loyalty? Study on Bank Syariah Indonesia. *Jurnal Ekonomi & Keuangan Islam, 11*(2), 179–195. https://doi.org/10.20885/JEKI.vol11.iss2.art2

Muharromah, L., & Manshur, U. (2025). Digital ethics in the perspective of Islamic education: Cultivating religious awareness in cyberspace. *Journal of Educational Management Research, 4*(6), 2484–2497. https://doi.org/10.61987/jemr.v4i6.1397

Mustaffa, A. M., & Ismail, N. (2025). Tahap pengetahuan ibu bapa terhadap kesan trend sharenting kepada kanak-kanak di Lembah Klang, Malaysia. *Journal of Contemporary Islamic Law, 10*(2), 62–70. https://doi.org/10.26475/jcil.2025.10.2.07

National Cyber Security Agency (NACSA). (2026). *My Cyber Hero (MYCH) 2026*. Retrieved from https://www.nacsa.gov.my/my-cyberHero.php

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology, 134*, 178–189.

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The titans of bibliographic information in today's academic world. *Publications, 9*(1), 12. https://doi.org/10.3390/publications9010012

Rahman, S. M. H. S. A., Ramli, M. A., Sa'ari, C. Z., Norman, A. A., Mamat, M. A., & Azhar, M. H. M. (2022). Pengidentifikasian kajian-kajian berkaitan isu penyalahgunaan media sosial dalam interaksi sosial berasaskan systematic literature review. *International Journal of Law, Government and Communication, 7*(28), 166–191.

Shahjahan, M. H. H., Jait, A. H., Thoha, A. M., & Durani, N. H. (2024). Pengetahuan dan sikap pelajar institusi pengajian tinggi di Negara Brunei Darussalam terhadap aspek keselamatan siber: Perisian aplikasi. *International Journal of 'Umranic Studies, 7*(1), 37–51.

Sihombing, D. A. H., Husaini, F. H., Irfandi, M., & Atikah, S. (2025). Systematic literature review: Model pendidikan akhlak berbasis emotional intelligence di era digital. *Sindoro: Cendikia Pendidikan, 18*(1), 1–17. https://doi.org/10.9644/sindoro.v3i9.252

Suhaime, A. N. M., Mansor, N. H., Rekan, A. A., Jodi, K. H. M., & Abidin, M. S. Z. (2023). Pembangunan model intervensi kawalan ketagihan pornografi berasaskan pendekatan psikospiritual Islam: Satu analisis keperluan. *Afkār, 25*(1), 253–290. https://doi.org/10.22452/afkar.vol25no1.9

Tan, J. Y., & Balaraman, R. A. (2023). Instagram dan buli siber dalam kalangan remaja di Malaysia. *Jurnal Pengajian Media Malaysia, 25*(1), 35–47. https://doi.org/10.22452/jpmm.vol25no1.4

Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. *Journal of Advanced Nursing, 52*(5), 546–553. https://doi.org/10.1111/j.1365-2648.2005.03621.x

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112.

Zani, A. A. A., Norman, A. A., Ghani, N. A., & Sianturi, R. S. (2025). Navigating social media: How offline ethics, online etiquette, and protection behaviour shape self-disclosure. *IEEE Access, 13*, 70597–70619. https://doi.org/10.1109/ACCESS.2025.3555548

Zainudin, S., Shahrani, S., Othman, Z. A., Fauzi, W. F. P., Ariffin, K. A. Z., Kanagarajah, P., ... Lah, N. H. (2022). Pembangunan dan penilaian pengguna untuk aplikasi kesedaran etika siber. *Malaysian Journal of Information and Communication Technology, 7*(1), 54–68. https://doi.org/10.53840/myjict7-1-9