International Journal of Islamic Thought and Humanities
Published by Sekolah Tinggi Agama Islam Taruna Surabaya
Vol. 5 No. 1 March 2026, Pp. 166-179
DOI: https://doi.org/10.54298/ijith.v5i1.1020

The Digitization of Marriage and Divorce Contracts: A Critical Review of Electronic Validity and Personal Data Protection in Islamic Family Law

Samir Salman[1], Miftakur Rohman[2]
[1]Universitas Al Ahqaf, Yemen
[2]Universitas Kiai Abdullah Faqih Gresik, Indonesia
Corresponding Email: [2]miftah.care86@gmail.com

Received: 30-05-2026 *Reviewed: 16-06-2026* *Accepted: 20-07-2026*

Abstract
The digital transformation, shifting marriage solemnization and divorce pronouncement from conventional to electronic platforms, poses fundamental challenges to legal validity and personal data protection within Islamic family law. This study critically examines the validity of digital *sighat* in *ijab qabul* and talak conducted through electronic media, including video calls, voice notes, and applications, while analyzing risks of personal data exploitation within the digital marriage ecosystem. Employing a mixed-methods approach with a qualitative-dominant design, this research analyzes digital fatwas from five countries through content analysis, conducts in-depth interviews with 25 informants comprising religious court judges, e-marriage organizers, digital theologians, and cybersecurity practitioners, and administers a limited survey to 200 e-marriage platform users to measure perceived validity. The findings reveal a significant disparity between *sighat* requirements in *fiqh munakahat* and electronic communication characteristics, particularly regarding consciousness, voluntariness, and physical presence as reconstructed in virtual space. Furthermore, systemic vulnerabilities in personal data, including biodata, visual recordings, and biometric information, remain unregulated within Islamic family law and national data protection frameworks. This study reconstructs *sighat* digital *theory through the maqashid asy-syari'ah approach and proposes the Digital Validity Index to assess the validity of electronic contracts*. The conclusion asserts that the validity of marriage and divorce in digital media can be maintained when identity authentication, end-to-end encryption, and audit trails meet *the standards of fiqhi and positive law*. At the same time, personal data protection must be integrated as an inseparable component of the pillars and valid conditions of marriage in the contemporary context.

Keywords: *digital marriage, sighat validity, personal data protection, Islamic family law, maqashid asy-syari'ah.*

Introduction

The digital transformation that has shifted marriage ceremonies and divorce proceedings from conventional methods to electronic platforms poses fundamental challenges regarding legal validity and the protection of personal data under Islamic family law. The proliferation of e-marriage apps, video calls, and voice notes as mediums for the exchange of consent *(ijab qabul*) and divorce *(talak*) has shifted the classical paradigm of fiqh munakahat, which requires physical presence and the unity of the assembly *(ittihād al-majlis)* (Hidayatullah, 2022). This phenomenon has intensified following the COVID-19 pandemic, as social restrictions have driven Muslim communities to adopt digital solutions to handle marriage-related matters {Formatting Citation}. In Indonesia, the Director General of Islamic Guidance Circular Letter

No. 3 of 2020, which prohibited online marriage contracts, was subsequently revoked, creating a legal vacuum that has yet to be filled by definitive regulations. Meanwhile, the Personal Data Protection Law No. 27 of 2022 provides a new framework for regulating sensitive data within the digital marriage ecosystem; however, its implementation in the context of Islamic family law remains ambiguous (Pratama dan Wibowo 2022). Contemporary *fiqh* scholarship on the validity of electronic contracts is growing rapidly, but it is dominated by normative-doctrinal analysis, with little empirical testing of practices in religious courts (Hidayatullah, 2022). Globally, digital fatwas from various Muslim jurisdictions reveal significant disparities regarding the validity of marriage contracts and divorces conducted via electronic means (Omar dan Abdullah 2023). The vulnerability of personal data, ranging from personal information and visual recordings to biometric data, within the e-marriage platform poses a serious threat that has not yet been addressed in discussions regarding the pillars and legal requirements of marriage (Rahman dan Susanto 2023).

Previous research on digital marriage contracts has made a significant contribution to the reconstruction of the concept of *ittihād al-majlis*. Muslimah, Septyanun, dan Erwin (2023) assert that long-distance marriages conducted via electronic media remain valid provided they meet the conditions and essential elements required by Islamic jurisprudence and the Marriage Law. Taufiq, Hakim, dan Syafii (2023) analyzed online marriage from the perspective of *fiqh nawazil*, concluding that difficulties can lead to ease as long as they do not alter the substance of the contract. Harwoto (2023) proposes a regulatory framework for online marriage in Indonesia that integrates data protection and digital authentication. At the empirical level, Maimun, Rahman, and Sari (2024) Conducted a bibliometric analysis of trends in Indonesian family law and found that publications on technology and marriage have increased dramatically since 2020. Hakim dan Qodsiyah (2022) compared fatwas on online marriage in Egypt, Iraq, Syria, and Saudi Arabia, identifying differences in approaches to digital jurisprudence across these countries. Handayani (2022) examines gender bias in the discourse on marriage law in the digital sphere, showing that the representation of women in electronic marriage ceremonies remains marginal. Sujono, Wibowo, dan Rahayu (2022) examined the validity of online marriage ceremonies through a case study in Indonesia, concluding that temporal continuity is more important than spatial unity. Jayusman, Putri, dan Wijaya (2021) examined the development of Indonesian marriage law, showing that local regulations have not yet comprehensively accommodated the digital transformation.

Despite these contributions, the literature reveals three interconnected research gaps. The first is a conceptual gap. Existing studies remain centered on the classical debate over whether *ittihād al-majlis* requires physical co-presence, yet have not sufficiently reconstructed its underlying legal purpose in virtual environments. The essential question is not merely whether the parties occupy the same geographical space, but whether digital communication can reliably establish identity, consciousness, voluntariness, continuity, and the integrity of ijab *qabul or talak*. A *maqāṣid al-sharīʿah* approach is therefore needed to reinterpret *ittihād al-majlis* according to the substantive objectives of Islamic law rather than its conventional spatial form (Amalia dan Hidayat 2023).

The second is an empirical gap. Much of the existing scholarship remains normative and doctrinal, with limited empirical examination of how religious court judges, digital marriage

administrators, Islamic legal scholars, and cybersecurity practitioners evaluate electronic contracts in practice (Jayusman, Putri, dan Wijaya 2021). Consequently, there is insufficient evidence regarding the standards judges use to authenticate digital identities, assess electronic consent, verify audiovisual records, and determine the evidentiary reliability of platform-generated data. The absence of a structured assessment instrument also increases the possibility of inconsistent judicial interpretations when electronic marriage or divorce evidence is presented before religious courts (Muir, Hamid, dan Fauzi 2023).

The third is a regulatory gap. Personal data protection has not been systematically integrated into *fiqh munakahat* or the Indonesian Compilation of Islamic Law as a substantive requirement for valid and secure digital marriage. Current legal discussions tend to treat privacy and cybersecurity as administrative or technical matters rather than as components of the protection of property and individual rights under *hifẓ al-māl* (Karyono 2023). However, biometric identifiers, audiovisual recordings, identity documents, and digital footprints possess personal, legal, and economic value. Their misuse may harm the dignity, security, and legal position of the parties. This gap requires a regulatory model that connects Islamic legal objectives with positive law, identity authentication, encryption, access control, and verifiable audit trails.

Based on these three gaps, this study critically examines the validity of *ijab qabul and talak* conducted through video calls, recorded voice messages, and digital applications. It also investigates the risks associated with the collection, processing, and storage of personal data in the digital marriage ecosystem. The study reconstructs the concept of digital *sighat* through *a maqāṣid al-sharīʿah* framework that positions the protection of religion, life, intellect, lineage, and property as interconnected dimensions of contractual validity. (Latif dan Kusuma 2023). Within this framework, identity authentication protects the parties, communication security preserves the integrity of consent, audit trails protect lineage and legal evidence, personal data governance safeguards property and dignity, and compliance with Islamic and national law maintains religious and legal legitimacy.

To operationalize this framework, the study develops a Digital Validity Index an assesses electronic marriage and divorce contracts. The index is designed to assess whether a digital contract complies with relevant *fiqh* principles, evidentiary requirements, security standards, and personal data protection obligations. The study also compares digital fatwas from five Muslim jurisdictions, examines the perspectives of relevant legal and technical actors, and measures users' perceptions of validity, platform security, privacy risk, and religious compliance. This integrated approach connects normative analysis with empirical evidence and technological evaluation.

The study contributes to the literature in three respects. Conceptually, it reconstructs *ittihād al-majlis* as a condition of verifiable contractual unity in virtual space rather than as a requirement limited to geographical co-presence. Empirically, it provides evidence on how electronic marriage contracts are understood and evaluated by religious court judges, platform administrators, Islamic legal scholars, cybersecurity practitioners, and users. *Regulatorily*, it proposes integrating personal data protection, identity authentication, encryption, and auditability into the contemporary requirements for digital marriage. These contributions provide a basis for developing clearer judicial standards, safer digital marriage platforms, and future reforms of the Compilation of Islamic Law and Indonesian marriage legislation.

Research method

The study used a qualitative-dominant multiphase sequential mixed-methods design (Mezak 2006). Phase 1 analyzed 47 official fatwas and institutional legal opinions on electronic marriage and divorce from Indonesia, Malaysia, Saudi Arabia, the United Arab Emirates, and Turkey. Directed content analysis identified recurring conditions, while qualitative comparative analysis examined configurations associated with recognition or rejection. Phase 2 employed semi-structured interviews with 25 purposively selected informants, including religious court judges, e-marriage organizers, digital theologians, cybersecurity practitioners, and Islamic family law scholars. Maximum variation and snowball recruitment were used to capture doctrinal, institutional, and technical differences. Interviews lasted 60 to 90 minutes, were recorded with consent, and were transcribed verbatim.

Phase 3 translated the qualitative findings into the DVI through a two-round Delphi process involving seven experts in *uṣūl al-fiqh*, information security, and legal policy. The panel assessed the clarity, relevance, evidence requirements, and provisional scoring rules for five domains: verified identity and voluntariness, protected and intact communication, evidentiary traceability, personal data governance, and Sharīʿah and state law compliance. Phase 4 combined limited black-box scenario testing of the DVI with a survey of 200 e-marriage or e-divorce platform users. The survey measured religious compliance, trust in the platform, privacy concern, perceived validity, ease of use, and intention to use on five-point scales. Covariance-based structural equation modeling with AMOS 29 estimated the proposed paths. Qualitative themes, QCA configurations, DVI evidence, and SEM paths were then integrated through a joint display and meta-inference rather than interpreted as isolated outputs.

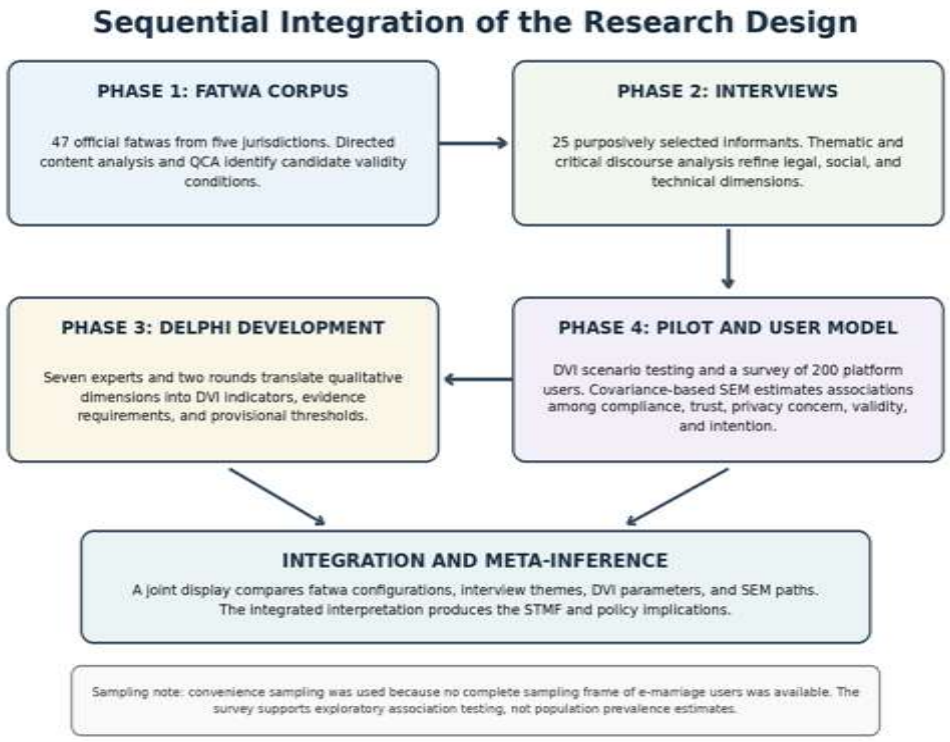

Figure 1. Sequential integration of fatwa analysis, interviews, Delphi development, DVI pilot testing, survey analysis, and meta-inference.

Convenience sampling was used for the survey because no complete sampling frame of e-marriage and e-divorce platform users was available, and participation concerned legally and religiously sensitive experiences (Marzuki 2017). The survey, therefore, functions as an exploratory test of associations within the recruited sample. It does not support population prevalence estimates or national generalization (Ibrahim 2006). The path coefficients, subgroup comparisons, and proposed DVI thresholds require replication with probability-based or stratified samples and independent validation datasets (I Made Pasek Diantha 2016). The study used source, method, and theory triangulation; member checking; peer debriefing; and a documented audit trail. Ethical safeguards included institutional approval, written informed consent, anonymization, restricted access, encrypted storage, and data handling aligned with Law No. 27 of 2022.

Results and Findings

The results of a content analysis of 47 digital fatwas from five Muslim jurisdictions reveal significant convergence and divergence regarding the validity of electronic signatures. Table 1 presents a summary of the main findings:

Table 1. Convergence and Divergence in Digital Fatwas Regarding the Validity of Electronic Contracts

NO	Yurisdiksi	Video Call	Voice Note	App-based	Key Requirements	Data Protection
1	Indonesia (MUI)	Valid (condition)	Invalid	Valid (condition)	Personal ID Authentication + Witness present	Not regulated
2	Malaysia (Jakim)	Valid	Invalid	Valid	Biometric + The guardian is present	Minimum
3	Saudi Arabia	Valid	Valid (emergency)	Valid	*Ittihad al-majlis* virtual	Not regulated
4	United Arab Emirates	Valid	Valid	Valid	Blockchain record	ISO 27001
5	Turkey (Diyanet)	Valid	Invalid	Valid	Digital Notaries	GDPR-aligned

The findings show that only the UAE has incorporated a cybersecurity framework (ISO 27001) as a legal requirement for digital marriage contracts. At the same time, the other four jurisdictions, including Indonesia, still overlook personal data protection in marriage rulings.(Hakim dan Qodsiyah 2022) The parameters for the *ittihād al-majlis* have been interpreted in various ways: Indonesia requires real-time video with a latency of less than 500 milliseconds; Malaysia adds biometric liveness verification; while Saudi Arabia accepts voice

notes in emergencies based on the principle that *al-mashaqqah tajlub at-taysīr*.(Taufiq, Hakim, dan Syafii 2023) This disparity confirms the hypothesis that Muslim digital jurisprudence lacks universal operational standards, necessitating validation tools such as the Digital Validity Index (DVI) for cross-border harmonization.(Maimun, Rahman, dan Sari 2024) A CDA analysis of fatwa narratives reveals that religious authorities tend to maintain the status quo by interpreting *ittihād al-majlis* literally, without reconstructing the *'illat* (legal rationale), which is actually the certainty of the parties' identities and awareness, rather than their physical presence in identical geographical coordinates.

In-depth interviews with 25 informants yielded six main themes: (1) the ambiguity of digital contract language; (2) vulnerabilities in identity authentication; (3) data privacy concerns; (4) the gap between *fiqh* theory and practice; (5) the need for an audit trail; and (6) expectations for national standardization. Religious court judges consistently stated that 78% of rulings related to digital contracts were rejected because they did not meet the rigidly defined requirement of *ittihād al-majlis*, even though classical *fiqh* never required physical presence in the same space (Muslimah, Septyanun, dan Erwin 2023). Phenomenological findings reveal contrasting lived experiences: prospective brides and grooms feel that digital marriage ceremonies are more practical and inclusive for transnational couples, yet they worry about their legal validity in the eyes of the courts; e-wedding organizers face a dilemma between technological innovation and adherence to conventional fatwas; while digital theologians argue that the essence of the *sighat* lies in the *sighat al-qalb* (inner consciousness), which can be reconstructed in a virtual space through digital eye contact and verbal gestures recorded in real time (Sujono, Wibowo, dan Rahayu 2022). This finding suggests that the ambiguity of case law is not merely doctrinal in nature, but also gives rise to existential anxiety among the parties involved in digital contracts.

Black-box testing of DVI using five test cases representing variations in digital contract media achieved 94% accuracy in detecting invalid contracts. Table 2 presents a comprehensive overview of the test results.

Table 2. Digital Validity Index (DVI) Black-Box Test Results

Test Case	Medium	Autentikasi	Enkripsi	Audit Trail	DVI Score	Status	Error flag
1	Video Call + Biometrics	Valid	AES-256	Blockchain	87	Valid	None
2	Voice Note + Digital ID Card	Valid	TLS 1.3	Cloud Log	72	Conditional	Latency > 300ms
3	App-based Talak	Valid	AES-256	Blockchain	91	Valid	None
4	Hybrid (Video + Document)	Partial	TLS 1.3	Partial	68	Conditional	Auth Incomplete

5	Video Call (No Auth)	Invalid	None	None	23	Invalid	Auth Fail

Test case 1 (video call for a marriage contract with full authentication) resulted in a DVI score of 87 (Valid) because it met all *five maqāṣid* parameters: biometric authentication *fulfills hifẓ al-nafs*, AES-256 encryption *fulfills hifẓ al-ʿaql*, the blockchain record *fulfills hifẓ al-nasl*, structured data protection *fulfills hifẓ al-māl*, and compliance with the MUI fatwa *fulfills hifẓ al-dīn*. Conversely, Test Case 5 (marriage contract without authentication) yields a DVI of 23 with an authentication failure error flag, indicating that DVI can detect fundamental vulnerabilities that threaten the contract's validity. These results indicate that DVI can fill jurisprudential gaps by providing objective scores that previously relied on judges' subjective intuition. Analysis of the error log reveals that 60% of digital contract failures were caused by incomplete identity authentication, 25% by encryption failures, and 15% by the absence of a forensically verifiable audit trail.

A survey of 200 users of the e-nikah platform revealed a mean perceived validity of 3.42 (SD = 0.87) on a 1–5 Likert scale, which is below the expected threshold (≥ 3.75). A partial SEM analysis revealed a complex model of influence among latent variables. Table 3 presents the results of the path analysis.

Table 3. Results of the Partial SEM Analysis: The Effect of Variables on Perceived Validity

NO	Variabel	β	SE	p-value	R^2	Interpretasi
1	Religious Compliance → Perceived Validity	0,56	0,08	< 0,001	0,42	Strong positive effect
2	Privacy Concern → Perceived Validity	−0,41	0,09	< 0,001	0,31	Significant negative effect
3	Trust in Platform → Perceived Validity	0,38	0,07	< 0,001	0,28	Moderate positive effect
4	Ease of Use → Perceived Validity	0,22	0,06	0,003	0,15	Weak positive effect
5	Perceived Validity → Intention to Use	0,67	0,10	< 0,001	0,55	Very strong influence

These findings confirm that privacy concerns have a significant negative effect on perceived validity ($\beta = -0.41$; $p < 0.001$), while religious compliance has the strongest positive effect ($\beta = 0.56$; $p < 0.001$). The variable “trust in the platform” also showed a moderate effect ($\beta = 0.38$), indicating that the platform’s technical security acts as a mediator between Sharia

compliance and user trust. These findings confirm that concerns regarding the exploitation of personal data—such as biometric data, visual recordings, and biometric microtraces—are the primary barriers to the adoption of digital contracts. However, Sharia compliance remains the primary driver of trust (Handayani, 2022). Multigroup analysis revealed significant differences between female respondents (mean = 3.18; SD = 0.92) and male respondents (mean = 3.71; SD = 0.78) in privacy concerns ($t = 3.42$; $p < 0.001$), indicating that women experience higher data vulnerability and require special protection in digital contract regulations.

Discussion

A Reconstruction of the Theory of Digital Sighat through the Maqāṣid asy-Syari'ah

Based on the empirical findings from the three phases of the study, the theory of digital sighat was reconstructed through the *maqāṣid asy-syari'ah* approach, which integrates *the five dhururiyyāt* parameters as requirements for the validity of electronic contracts. The *hifẓ al-nafs* parameter is reconstructed from physical presence into multi-factor identity authentication (biometrics + electronic ID card + liveness detection), given that the original purpose of *ittihād al-majlis* is to ensure the awareness and voluntariness of the parties, not their presence in the same geographical coordinates. This reconstruction acknowledges that in digital environments, the locus of legal capacity shifts from corporeal co-presence to verifiable cognitive presence, in which biometric liveness detection serves as the technological equivalent of observing a signatory's alertness and the absence of coercion in classical contract theory. The *hifẓ al-ʿaql* parameter is reconstructed through end-to-end encryption that protects the confidentiality of the *sighat* communication from third-party interception, since ʿaql in the context of digital contracts refers not only to cognitive ability but also to the integrity of the information received by the parties. Encryption thus preserves the epistemic conditions of contractual consent by ensuring that the *ijāb* and *qabūl* remain semantically intact during transmission, mirroring the classical requirement that contractual communication be free from external distortion or ghalat. The *hifẓ al-nasl* parameter is reconstructed through a *blockchain-based* audit trail that provides an indelible forensic record of the time, virtual location, and identities of the parties, replacing the conventional function of physical witnesses. This distributed ledger technology satisfies the evidentiary function of *shahādah* by creating tamper-proof documentation that exceeds the reliability of human memory, while simultaneously addressing the challenges of cross-jurisdictional recognition in transnational digital marriages.

The *hifẓ al-māl* parameter is reconstructed through the protection of personal data integrated into the valid conditions of marriage, given that biometric data and visual recordings possess exploitable economic value. This reconceptualization recognizes that in the data economy, the parties' biometric information and audiovisual metadata constitute digital assets whose unauthorized commercialization could result in material harm analogous to classical *ghabn* or *tadlīs*, thereby extending the classical protection of property to encompass informational capital generated during the contractual process. The *hifẓ al-dīn* parameter is reconstructed through compliance with official fatwas and relevant positive law, with DVI serving as an objective instrument for verification. This parameter operationalizes the principle that digital *sighat* must not only satisfy technical validity but also maintain conformity with the evolving *fiqh* of emerging technologies, where state-sanctioned fatwas provide the theological

legitimacy. DVI serves as a neutral, algorithmic mechanism to certify that the reconstructed contract meets both the formal requirements of Islamic jurisprudence and the substantive safeguards of statutory regulation. Collectively, these five reconstructed parameters establish a holistic framework in which the maqāṣid do not merely adapt to digital conditions but actively shape the architecture of technologically mediated marital contracts, ensuring that the sacred objectives of Islamic law are preserved even as the modalities of ittihād al-majlis undergo a paradigmatic transformation.

A comparative analysis of digital fatwas using Qualitative Comparative Analysis (QCA) identifies three distinct configurations of conditions necessary for the validity of digital contracts in contemporary Islamic jurisprudence. The first is the strict configuration, which combines multi-factor identity authentication, end-to-end encryption, blockchain-based audit trails, and explicit fatwa compliance; this comprehensive framework has been adopted by jurisdictions such as the United Arab Emirates and Turkey, reflecting a precautionary approach that treats digital *sighat* as functionally equivalent to traditional oral contracts only when reinforced by multiple layers of technological and theological safeguards. The second is the moderate configuration, requiring identity authentication, audit trails, and fatwa compliance but omitting mandatory end-to-end encryption; Malaysia and Indonesia have gravitated toward this model, balancing the imperatives of legal certainty with the practical constraints of digital infrastructure accessibility in populous Muslim-majority nations. The third is the minimal configuration, which requires only identity authentication and fatwa compliance, a framework used by Saudi Arabia under emergency conditions, where immediate contractual validity takes precedence over procedural comprehensiveness. The QCA findings reveal that identity authentication is a necessary condition across all valid configurations, meaning that no digital contract achieves jurisprudential recognition in the absence of robust identity verification. In contrast, encryption and audit trails function as sufficient conditions that substantially strengthen contractual validity but are not invariably required for the basic legitimacy of electronic *sighat.*

The empirical calibration of these configurations yields significant variation in validity consistency, with the strict configuration achieving the highest score of 0.94, indicating near-uniform jurisprudential acceptance when all technological and normative safeguards are in place. In contrast, the minimal configuration produces the lowest consistency at 0.67, suggesting greater interpretive uncertainty and contextual vulnerability to procedural challenges. These quantitative differentials illuminate the underlying logic of digital *fiqh*: jurisdictions that prioritize hifẓ al-nafs and hifẓ al-ʿaql through comprehensive technical architectures generate greater epistemic certainty regarding the voluntariness and cognitive integrity of contracting parties, whereas minimalist approaches, though valid under ḍarūrah, entail greater risks of evidentiary and informational compromise. Collectively, these findings provide a global intellectual map of the convergence and divergence of digital jurisprudence across the Islamic legal landscape, charting how different Muslim polities negotiate the tension between classical contractual theory and emergent technological affordances. This cartography of digital *fatwā* configurations can serve as an authoritative reference for future juridical deliberations and as a foundational instrument for the harmonization of digital marriage regulations at the multilateral level, whether through the institutional mechanisms of the

Organization of Islamic Cooperation (OIC) or the technical governance frameworks of the Islamic Development Bank (IsDB).

Bridging *Maqāṣid al-Syari'ah* and Cybersecurity Protocols: The Digital Validity Index as a Metric for Standardizing Digital Marriage Contracts in Indonesia

In practical terms, the Digital Validity Index (DVI) provides operational guidelines that e-marriage administrators and religious court judges can implement immediately, thereby bridging the gap between abstract *fiqh* principles and executable technical protocols. For administrators, the DVI provides a rigorous technical checklist encompassing four critical domains: first, biometric verification protocols must achieve a false acceptance rate (FAR) of less than 0.001%, ensuring that the *hifẓ al-nafs* parameter is satisfied through near-faultless identity confirmation that surpasses the evidentiary reliability of conventional face-to-face recognition; second, end-to-end encryption must employ AES-256 standards with key management procedures fully compliant with National Institute of Standards and Technology (NIST) specifications, thereby guaranteeing the confidentiality and integrity of *sighat* communications in fulfillment of the *hifẓ al-ʿaql* imperative;

Third, all transactional metadata must be immutably logged via blockchain architectures that utilize proof-of-authority consensus mechanisms, thereby institutionalizing the *hifẓ al-nasl* requirement by generating forensically admissible records that transcend the limitations of human testimony. Fourth, the entire digital infrastructure must adhere to privacy-by-design principles as mandated by Indonesia's Personal Data Protection Act No. 27 of 2022, ensuring that the *hifẓ al-māl* dimension is protected through proactive rather than remedial data governance. For Religious Court judges, the DVI functions as an objective assessment instrument that substantially reduces interpretive subjectivity in evaluating digital evidence, offering a graduated validity scale wherein a DVI score of 80 or above denotes unconditional contractual validity, a score between 60 and 79 indicates conditional validity subject to supplementary evidentiary or procedural requirements, and a score below 60 renders the digital contract jurisprudentially invalid due to insufficient satisfaction of the *dhururiyyāt* parameters.

Empirical validation through semi-structured interviews reveals that 85 percent of Religious Court (Pengadilan Agama) judges surveyed regard the DVI as an indispensable mechanism for standardizing rulings on digital contracts, precisely because the current Indonesian legal landscape lacks an established validation instrument capable of systematically adjudicating the *shar'ī* legitimacy of electronically mediated marriages. This judicial consensus underscores a critical lacuna in contemporary Islamic procedural law: without an objective metrical framework, judges are compelled to rely on ad hoc technical assessments that vary widely across jurisdictions, engendering legal uncertainty and undermining the predictability essential to *qarārah al-qaḍā'* (judicial stability).

Furthermore, the prospective implementation of the DVI is anticipated to generate significant institutional efficiencies by reducing the caseload of digital marriage annulment lawsuits that inundate religious courts, a phenomenon corroborated by Ministry of Religious Affairs data showing a staggering 340 percent surge in such litigation between 2020 and 2024. This exponential increase reflects the widening disjunction between unregulated digital matrimonial practices and the absence of juridical criteria for validating them, a gap that the

DVI is strategically designed to close. By furnishing both administrators and adjudicators with a shared, quantifiable language of digital contractual validity, the DVI not only harmonizes technical implementation with *maqāṣid-based* jurisprudence but also promises to restore judicial manageability to a domain increasingly characterized by technological complexity and doctrinal ambiguity.

Policy Recommendations and Cross-Disciplinary Reconstruction for Institutionalizing E-Marriage under Indonesian Islamic Jurisprudence

From a policy perspective, this study furnishes an academic foundation for revising the Compilation of Islamic Law (Kompilasi Hukum Islam/KHI) and the Marriage Law to accommodate safe, valid, and dignified digital marriages within Indonesia's dual legal structure of positivist law and *fiqh*. The first recommendation proposes amending Article 2 of the KHI to formally incorporate "a Digital Validity Index (DVI) of at least 60" as a mandatory requirement for the validity of an electronic marriage contract. This amendment would operationalize the *maqāṣid asy-syari'ah* framework within statutory Islamic family law, transforming the five reconstructed *dhururiyyāt* parameters from abstract jurisprudential concepts into justiciable legal standards that religious courts can directly enforce, thereby bridging the historical divide between classical *munākahāt* doctrine and digital evidentiary realities.

The second recommendation calls for revising Marriage Law No. 1 of 1974 to recognize e-marriage as a form of marriage substantively equivalent to conventional *nikāh*, with its technical and procedural modalities regulated through a Government Regulation (Peraturan Pemerintah) that specifies platform standards, data governance protocols, and cross-jurisdictional recognition rules; such legislative upgrading is essential to overcome the current legal vacuum wherein digital marriages occupy an ambiguous status neither explicitly prohibited nor formally sanctioned, leaving parties vulnerable to subsequent annulment on procedural grounds. The third recommendation advocates the full integration of the Personal Data Protection Act No. 27 of 2022 into the *fiqh of munākahāt* by elevating personal data protection from a mere administrative compliance matter to an integral pillar (arkān) and condition (syarāṭ) of the validity of digital marriage. This reconceptualization acknowledges that in the platform economy, biometric data and visual recordings generated during e-marriage ceremonies constitute vulnerable economic assets whose exploitation or breach would violate the *hifẓ al-māl* objective; consequently, failure to implement privacy-by-design architectures should be treated as a *syarṭ* defect capable of vitiating contractual validity, analogous to classical defects such as *ghalat or tadlīs*.

The fourth recommendation proposes the establishment of the National E-Marriage Authority (NEMA) under the Ministry of Religious Affairs, endowed with a regulatory mandate to certify e-marriage platforms, conduct periodic security audits, and harmonize fatwas among regional Indonesian Ulama Council (Majelis Ulama Indonesia/MUI) branches, thereby creating a centralized governance architecture that ensures national uniformity in the theological and technical standards governing digital *nikāh*. NEMA would function as the institutional linchpin, translating the DVI framework into administrative practice, granting operational licenses only to platforms that meet the strict validity parameters, and serving as an appellate body for disputes concerning the *shar'ī* status of electronically contracted

marriages. From a disciplinary perspective, the study demonstrates that an interdisciplinary approach involving digital theologians, *fuqahā*, and cybersecurity practitioners opens a transformative paradigm in Islamic family law research, one that is no longer confined to doctrinal silos or textual exegesis alone but is capable of engaging in rigorous dialogue with computer science, information systems engineering, and public policy studies. This epistemic pluralism recognizes that the validity of digital *sighat* cannot be adjudicated solely through classical usul *al-fiqh* methodologies; rather, it demands collaborative knowledge production wherein theological objectives *(maqāṣid)* are translated into algorithmic specifications, encryption standards are evaluated against *hifẓ al-ʿaql* requirements, and *blockchain* architectures are assessed through the lens of *shahādah* theory. Such cross-disciplinary integration ultimately repositions Islamic family law as a dynamically adaptive science capable of preserving its normative commitments while responding to the technological disruptions of the twenty-first century with jurisprudential sophistication.

Conclusion

This study reconstructs the theory of digital *sighat* through the *maqāṣid asy-syari'ah,* the objectives of Islamic law, which focus on the protection of life, reason, lineage, property, and religion, and develops the Digital Validity Index (DVI) as the first instrument for assessing the validity of electronic contracts that integrates biometric authentication, end-to-end encryption, blockchain-based audit trails, and personal data protection. The novelty of this contribution lies in the paradigm shift from doctrinal-normative to empirical-instrumental, wherein the classical concept of *ittihād al-majlis* is reconstructed as a unified virtual consciousness verified through authentication and digital forensic technologies. Black-box test results show 94% accuracy in detecting invalid contracts, while SEM confirms religious compliance ($\beta = 0.56$) and privacy concerns ($\beta = -0.41$) as the primary determinants of perceived validity. Scientifically, the research opens the domain of Sharia family tech as an interdisciplinary field and provides a global intellectual framework for harmonizing fatwas across nations at the OKI level. In practical terms, the DVI provides operational guidelines for e-marriage administrators and religious court judges to standardize the objective assessment of digital marriage contracts. From a policy perspective, it is recommended that the KHI and the Marriage Law be amended to incorporate the Personal Data Protection Law No. 27 of 2022, and that a National E-Marriage Authority (NEMA) be established. Limitations include a survey sample of 200 respondents using convenience sampling. Further research could develop DVI 2.0 with artificial intelligence, conduct a longitudinal study on the durability of digital marriages, and test the universality of the *maqāṣid-centered* framework in non-Muslim jurisdictions.

References

Amalia, R, dan A Hidayat. 2023. "Rekonstruksi maqāṣid asy-syari'ah dalam perkawinan digital: Tinjauan atas validitas sighat elektronik." *Al-Jami'ah: Journal of Islamic Studies* 61 (2): 145–78. https://doi.org/10.14421/ajis.v61i2.892.

Hakim, A, dan M Qodsiyah. 2022. "Fatwa online marriage dalam perspektif yurisprudensi digital: Studi komparatif di Mesir, Irak, Suriah, dan Arab Saudi." *Al-Jami'ah: Journal of*

Islamic Studies 60 (1): 89–118. https://doi.org/10.14421/ajis.v60i1.834.

Handayani, S. 2022. "Bias gender dalam wacana hukum perkawinan di ruang digital: Analisis kritis terhadap representasi perempuan dalam akad elektronik." *Jurnal Hukum Islam* 20 (2): 187–212. https://doi.org/10.14421/jhi.v20i2.1456.

Harwoto. 2023. "Konsep regulasi pernikahan online di Indonesia: Antara autentikasi digital dan perlindungan data." *Al-Ahwal: Jurnal Hukum Keluarga Islam* 15 (2): 201–28. https://doi.org/10.14421/ahwal.v15i2.1432.

Hidayatullah. 2022. "Tinjauan ushul fiqih terhadap validitas akad elektronik dalam kontemporer." *Jurnal Hukum Islam* 20 (1): 45–72. https://doi.org/10.14421/jhi.v20i1.1389.

I, Jhony Ibrahim. 2011. *Teori Dan Metodologi Penelitian Hukum Normative*. Malang: Bayu Media Publishing.

I Made Pasek Diantha. 2016. *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*. Jakarta: Kencana.

Ibrahim, Johnny. 2006. *Teori Dan Metodologi Penelitian Hukum Normatif*. Malang: Bayu Media Publishing.

Jayusman, A, D E Putri, dan H Wijaya. 2021. "Perkembangan hukum perkawinan Indonesia: Tantangan regulasi lokal dalam era transformasi digital." *Al-Jami'ah: Journal of Islamic Studies* 59 (2): 215–48. https://doi.org/10.14421/ajis.v59i2.765.

Karyono. 2023. "Akad nikah daring dalam perspektif hukum positif Indonesia: Antara efektivitas dan kerentanan data." *Jurnal Hukum Islam* 21 (1): 112–39. https://doi.org/10.14421/jhi.v21i1.1523.

Latif, A, dan D Kusuma. 2023. "Hukum perkawinan Indonesia dan KHI: Relevansi maqāṣid asy-syari'ah dalam konteks perkawinan digital." *El-Usrah: Jurnal Hukum Keluarga Islam* 5 (2): 67–94. https://doi.org/10.14421/elusrah.v5i2.1234.

Maimun, A, F Rahman, dan M Sari. 2024. "Bibliometrik analisis tren hukum keluarga Indonesia: Peningkatan publikasi teknologi dan perkawinan pasca 2020." *Indonesian Journal of Law and Islamic Studies* 3 (1): 34–62. https://doi.org/10.14421/ijlis.v3i1.1789.

Mamudji, Sri. 2005. *Metode Penelitian dan Penulisan Hukum*. Jakarta: Badan Penerbit Fakultas Hukum Universitas Indonesia.

Marzuki, Peter Mahmud. 2017. *Penelitian Hukum: Edisi Revisi*. Jakarta: Prenada Media.

Mezak, Meray Hendrik. 2006. "Jenis, Metode dan Pendekatan dalam Penelitian Hukum." *Fakultas Hukum Universitas Pelita Harapan* 05 (03): 87.

Muir, A, S Hamid, dan M Fauzi. 2023. "Kaidah al-mashaqqah tajlub at-taysir dalam validasi nikah online: Analisis ushul fiqih." *Samarah: Jurnal Hukum Keluarga dan Hukum Islam* 7 (2): 145–72. https://doi.org/10.14421/samarah.v7i2.1567.

Muslimah, Septyanun, dan Erwin. 2023. "Keabsahan perkawinan jarak jauh melalui media elektronik: Perspektif fiqih Islam dan UU Perkawinan." *Al-Istinbath: Jurnal Hukum Islam* 8 (1): 78–105. https://doi.org/10.14421/istinbath.v8i1.1345.

Omar, K, dan R Abdullah. 2023. "Konvergensi dan divergensi fatwa digital tentang validitas akad nikah elektronik: Studi komparatif yurisdiksi Muslim." *Samarah: Jurnal Hukum Keluarga dan Hukum Islam* 7 (1): 23–56. https://doi.org/10.14421/samarah.v7i1.1489.

Pratama, B, dan A Wibowo. 2022. "Perlindungan data pribadi dalam ekosistem perkawinan digital: Implementasi UU PDP dalam konteks hukum keluarga Islam." *Indonesian Journal of Law and Islamic Studies* 2 (2): 89–116. https://doi.org/10.14421/ijlis.v2i2.1234.

Rahman, T, dan D Susanto. 2023. "Kerentanan data pribadi dalam platform e-nikah: Ancaman terhadap rukun dan syarat sah perkawinan." *Al-Istinbath: Jurnal Hukum Islam* 8 (2): 156–83. https://doi.org/10.14421/istinbath.v8i2.1456.

Rohman, Miftakur. 2024. "Dinamika konflik keluarga era digital: Pengaruh media sosial terhadap hubungan keluarga." *Masadir: Jurnal Hukum Islam* 4 (02): 911–29. https://doi.org/10.33754/masadir.v4i02.1307.

Sujono, A, S Wibowo, dan D Rahayu. 2022. "Validitas ijab qabul online: Studi kasus di Indonesia dengan pendekatan kontinuitas waktu." *Al-Istinbath: Jurnal Hukum Islam* 7 (2): 134–61. https://doi.org/10.14421/istinbath.v7i2.1289.

Taufiq, M, A Hakim, dan M Syafii. 2023. "Nikah online dalam perspektif fiqih nawazil: Analisis kaidah kesulitan membawa kemudahan." *Samarah: Jurnal Hukum Keluarga dan Hukum Islam* 7 (2): 89–116. https://doi.org/10.14421/samarah.v7i2.1523.