Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

Protecting Family Integrity from Digital Fraud: Islamic Family Law and *ITE Law* in WhatsApp Groups

Agus Munjirin Mukhotib Lathif*[1], Aliyeva Patimat Shapiulaevna[2]
[1]Institut Miftahul Huda Al Azhar Kota Banjar, Indonesia
[2]Moscow State University of Technologies and Management Moscow, Russian Federation

**Corresponding author:* Agus Munjirin Mukhotib Lathif
Email: agusmunjirin@kampusalazhar.ac.id

Article History:
Received: April 18, 2024 | Revised: June 12, 2024 | Accepted: July 22, 2024 | Published: December 30, 2024

Citation (APA Style):
Munjirin, A. M., & Shapiulaevna, A. P. (2024). Protecting family integrity from digital fraud: Islamic family law and ITE Law in WhatsApp groups. *Munakahat: Journal of Islamic Family Law, 1*(1), 46–57.

Abstract

Background: The increasing use of *WhatsApp* groups in Indonesia has transformed family communication and religious interaction, but it also exposes users to rising risks of digital fraud. Such fraud affects not only financial stability but also trust, emotional security, and family integrity. The integration between *Islamic Family Law* and Indonesia's Electronic Information and Transactions Law (*UU ITE*) in addressing these issues remains underexplored.

Methods: This study applies a qualitative normative legal approach using statutory and doctrinal analysis. Primary sources include the Qur'an, Hadith, classical *fiqh* literature, and Law No. 11/2008 as amended by Law No. 19/2016 on Electronic Information and Transactions. Data are analyzed thematically to examine legal protection mechanisms against digital fraud in *WhatsApp*-based family communication contexts.

Results: Findings show that digital fraud in *WhatsApp* groups contributes to family disputes, mistrust, and weakened social cohesion. *UU ITE* provides formal legal remedies for cyber fraud, yet its enforcement in family-centered contexts remains limited. *Islamic Family Law* offers strong moral principles for protecting family integrity but lacks operational mechanisms for digital threats.

Discussion: A normative gap exists between *Islamic Family Law* and *UU ITE* in addressing digital fraud. Both systems operate separately, resulting in fragmented protection. An integrative legal approach is needed to connect ethical-religious principles with state legal enforcement, particularly in digital family communication spaces.

Conclusion: *Islamic Family Law* must evolve by integrating its moral framework with cyber law enforcement mechanisms under *UU ITE* to ensure comprehensive protection of families in digital environments.

Novelty: This study develops an integrative framework between *Islamic Family Law* and Indonesian cyber law for addressing digital fraud in *WhatsApp* groups, contributing to emerging scholarship on digital family protection.

Keywords: Digital Fraud; *Islamic Family Law*; Cyber Law; *WhatsApp* Groups; Legal Integration

INTRODUCTION

The rapid expansion of digital communication technologies has significantly transformed patterns of human interaction, particularly through social messaging platforms such as WhatsApp groups. These platforms are widely used not only for interpersonal communication but also for family coordination, religious discussion, and community engagement in Indonesia. However, alongside these benefits, digital environments increasingly expose users to various forms of cyber-enabled fraud, including phishing, identity manipulation, smishing, and financial deception that exploit interpersonal trust within online communities (Williams et al., 2017; Ali et al., 2019; Haizam & Zulkipli, 2024; Varshney et al., 2024). Such fraudulent practices are not merely technical exploits but are embedded in social engineering strategies that rely on emotional proximity and relational trust. In this context, WhatsApp-based fraud has become a growing concern because it directly targets groups where trust functions as the primary communication foundation, including family and religious communities. This condition

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

indicates that digital fraud should be understood as a socio-legal phenomenon that threatens not only individuals but also the structural integrity of families as fundamental social institutions.

The development of digital fraud has been widely documented in contemporary cybersecurity and criminology literature. Empirical studies show that cybercriminals increasingly employ sophisticated methods such as romance fraud, hybrid investment scams, and organized cyberfraud networks to manipulate victims through digital communication platforms (Choi et al., 2024; Maras & Ives, 2024; Cretu-Adatte et al., 2024). In many cases, perpetrators combine psychological manipulation with financial exploitation, creating long-term deception cycles that are difficult to detect in early stages. Furthermore, research on online offenses highlights that cybercrime categories are increasingly blurred, as cyberattacks, fraud, and digital manipulation often overlap in practice and legal interpretation (Sarkar & Shukla, 2024). These developments are reinforced by evidence that digital fraud significantly weakens users' cognitive judgment, emotional stability, and trust-based decision-making, particularly among individuals with limited digital literacy (Esteban-Bravo et al., 2024). Accordingly, digital fraud should be conceptualized not only as an economic crime but also as a structural social threat that disrupts interpersonal relationships, including within families where trust, communication, and emotional security are essential elements of resilience.

From the perspective of Islamic legal thought, family protection constitutes a central objective of Islamic Family Law, which emphasizes justice, responsibility, and the preservation of harmony within the household. Within the framework of *maqāṣid al-sharī'ah*, the protection of family integrity (*ḥifẓ al-usrah*) represents a fundamental normative goal aimed at safeguarding moral, emotional, and socio-economic stability in family life. Contemporary Islamic legal scholarship increasingly acknowledges the need to adapt classical legal principles to modern socio-digital transformations, including the risks emerging from digital communication environments (Asman, 2020; Abubakar et al., 2023). However, despite this growing awareness, most studies in Islamic Family Law continue to focus on traditional issues such as marriage, inheritance, and child protection, while relatively limited attention has been given to digital fraud as a new form of threat to family stability (Daniela et al., 2024; Muljan et al., 2024; Setyawati et al., 2024). This gap suggests that Islamic legal discourse requires further contextual expansion to remain relevant in addressing contemporary digital vulnerabilities affecting family systems.

On the other hand, Indonesia has developed a legal framework to address digital crime through the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*, *UU ITE*), which regulates electronic communication, digital evidence, and criminal sanctions for online fraud. Recent developments in digital forensic science emphasize the importance of structured investigative procedures and electronic evidence analysis in identifying cybercrime activities across digital platforms (Reedy, 2023; Ng & James, 2024; Hanaputra et al., 2024). Comparative legal studies also indicate that legal systems globally are continuously adapting to address emerging cyber threats, particularly those involving messaging applications and social engineering techniques (Zieliński, 2024). Nevertheless, existing scholarship tends to emphasize procedural enforcement and technological solutions, while insufficient attention has been given to integrating cyber law with normative-religious legal frameworks such as Islamic Family Law. This lack of integration creates a conceptual and practical gap in understanding how dual legal systems can collaboratively strengthen family protection in digital environments.

Based on the foregoing discussion, there is a clear research gap concerning the absence of an integrative legal framework that connects Islamic Family Law and Indonesia's cyber law in addressing WhatsApp-based digital fraud. Existing studies tend to examine cybercrime, Islamic legal protection, and digital forensic enforcement as separate analytical domains without sufficiently exploring their intersection. Therefore, this study aims to analyze the impact of digital fraud occurring in WhatsApp groups on family integrity and to examine how Islamic Family Law and the Electronic Information and Transactions Law (*UU ITE*) can function in a complementary manner to provide stronger legal protection for families in the digital era. The study further seeks to develop an integrative legal framework grounded in *maqāṣid al-sharī'ah*, particularly *ḥifẓ al-usrah*, to bridge state-based cyber law and Islamic normative principles in addressing contemporary digital fraud. Through this approach, the research contributes to interdisciplinary scholarship in cyber law, Islamic legal studies, and digital ethics by offering a more holistic model of family protection in the digital society.

LITERATURE REVIEW

Recent scholarship indicates that digital fraud has evolved into a complex socio-technical phenomenon embedded within everyday communication platforms, particularly social media and messaging applications such as

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

WhatsApp. Studies on consumer-facing technology fraud emphasize that fraudsters increasingly exploit trust relationships, behavioral vulnerabilities, and platform affordances to execute scalable deception strategies (Ali et al., 2019). In parallel, digital transformation has accelerated fraud exposure due to expanded data circulation and reduced verification barriers in online environments (Abdurrahman et al., 2022). Practical reports further confirm that WhatsApp group-based scams have become a recurring public concern, where perpetrators infiltrate social groups to manipulate trust and extract financial or personal gains (Media, 2023; Popov, 2024). These developments demonstrate that digital fraud is no longer an isolated cybercrime issue but a structural risk embedded in digital social ecosystems, where users' susceptibility is shaped by both technological design and behavioral factors (Williams et al., 2017).

The literature also highlights the diversification of fraud typologies in digital environments, including phishing, smishing, romance scams, and hybrid investment fraud schemes. Research on online romance fraud reveals that perpetrators systematically construct emotional trust to exploit victims over extended periods, demonstrating high psychological sophistication (Lazarus et al., 2023; Choi et al., 2024). Similarly, hybrid investment fraud such as "pig butchering" illustrates how criminals combine social engineering with financial manipulation through digital platforms (Maras & Ives, 2024). Studies on smishing attacks further emphasize the increasing use of messaging systems as vectors for deceptive communication, particularly through mobile-based public announcement systems (Zieliński, 2024). Moreover, broader analyses of online offenses suggest the need to distinguish between cybercrime categories based on intent, structure, and impact, including cyberattacks and cyber-enabled fraud (Sarkar & Shukla, 2024). Collectively, these studies indicate that digital fraud is increasingly hybridized, adaptive, and context-sensitive, requiring interdisciplinary legal and criminological responses.

From a technological and forensic perspective, research has focused on digital evidence extraction, cybersecurity frameworks, and emerging detection systems. Digital forensic studies emphasize the importance of structured methodologies in collecting and analyzing electronic evidence from communication platforms, including WhatsApp-based transactions (Ng & James, 2024; Reedy, 2023). Empirical investigations demonstrate that digital artifacts can be systematically traced using forensic standards such as NIST SP 800-86, which supports fraud detection and evidentiary validation in legal contexts (Hanaputra et al., 2024). Additionally, advances in artificial intelligence and machine learning have been applied to detect cyber threats such as phishing, malware, and online abuse, improving early detection and prevention capabilities (Varshney et al., 2024; Ullah et al., 2024; Mishra et al., 2024). Emerging studies also highlight the role of digital identity systems and blockchain-based frameworks in enhancing trust, authentication, and fraud resistance in digital ecosystems (Jena et al., 2024; Sadhya & Sahu, 2024). These contributions collectively demonstrate that technological solutions are increasingly central to combating digital fraud, although their integration into legal and socio-cultural systems remains underdeveloped.

In the context of Islamic family law, existing studies emphasize the importance of protecting family integrity, caregiving responsibilities, and household resilience in the face of socio-digital transformation. Islamic legal scholarship highlights that family protection (*ḥifẓ al-usrah*) remains a core objective within *maqāṣid al-sharī'ah*, particularly in safeguarding moral, emotional, and economic stability (Asman, 2020). Research on household dynamics shows that role transformation within families in modern digital societies has created new legal and ethical challenges, especially concerning resilience and responsibility distribution (Abubakar et al., 2023). Other studies also examine family-related legal issues such as marriage registration, child protection, and caregiving ethics within Islamic frameworks, indicating ongoing adaptation to modern social changes (Muljan et al., 2024; Setyawati et al., 2024). Furthermore, studies on Islamic family law education highlight the importance of critical thinking and adaptive legal interpretation among scholars and practitioners in addressing contemporary challenges. However, these works largely remain doctrinal and have not fully engaged with digital fraud as an emerging threat to family integrity in digital communication environments.

Despite the growing body of literature on cyber fraud, digital forensics, and Islamic family law, there remains a significant gap in integrative legal analysis that connects these domains. Existing studies predominantly examine digital fraud from cybersecurity, criminology, or technological perspectives, while Islamic family law research focuses on normative and ethical dimensions of family protection without addressing digital vulnerabilities in communication platforms. Although some studies acknowledge the importance of legal protection in digital transformation contexts (Abdurrahman et al., 2022), there is limited scholarly effort to synthesize Indonesian cyber law (UU ITE) with Islamic legal principles in addressing family-targeted digital fraud. This gap is critical because digital fraud in WhatsApp groups directly affects family trust, economic stability, and social cohesion, requiring a dual-framework approach that combines statutory regulation and religious-ethical governance.

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

Therefore, this study contributes to the literature by developing an integrated analytical perspective that bridges cyber law enforcement and Islamic family law principles to strengthen family protection mechanisms in the digital era.

METHODOLOGY

This study employs a qualitative socio-legal research design to investigate digital fraud occurring within WhatsApp groups and its implications for family integrity under the dual framework of Indonesian cyber law (*UU ITE*) and Islamic Family Law. The socio-legal approach is adopted because digital fraud is not merely a technological violation but a socially embedded phenomenon constructed through trust exploitation, emotional manipulation, and relational engineering within digital communication environments (Varshney et al., 2024). WhatsApp groups are conceptualized as hybrid socio-digital spaces where legal norms, religious values, and technological vulnerabilities intersect, producing complex conditions for cyber-enabled deception. In such environments, fraud is not only executed through technical intrusion but also through psychological persuasion and social legitimacy built within trusted communities. Recent literature emphasizes that digital transformation reshapes legal interaction systems and requires adaptive interdisciplinary frameworks that integrate technological, legal, and socio-cultural perspectives. Accordingly, this study positions digital fraud as a socio-legal construct that must be analyzed through both normative legal reasoning and empirical social inquiry to fully understand its implications for family systems.

Primary data were collected through semi-structured interviews with individuals who had experienced digital fraud in WhatsApp group settings. Respondents were selected using purposive sampling based on three criteria: (1) direct exposure to fraud schemes within WhatsApp groups, (2) experience of financial, emotional, or familial consequences, and (3) involvement in family-related communication contexts such as academic, religious, or household networks. The interviews focused on reconstructing victim experiences, including mechanisms of deception, trust-building strategies employed by perpetrators, emotional responses following exposure, and the subsequent effects on household relationships and family cohesion. This narrative-oriented approach is essential because cyber fraud increasingly relies on social engineering and psychological manipulation rather than purely technical exploitation (Choi et al., 2024; Haizam & Zulkipli, 2024). Empirical research further shows that victims' lived experiences are central to understanding how digital deception disrupts emotional resilience, decision-making capacity, and interpersonal trust within families. Through this method, the study captures the socio-emotional dimensions of fraud that cannot be adequately explained through quantitative or purely doctrinal legal approaches.

Secondary data were obtained through doctrinal legal analysis and systematic literature review. The legal corpus includes Indonesia's Electronic Information and Transactions Law (*UU ITE*), Islamic Family Law principles, and scholarly interpretations of family protection within Islamic jurisprudence (*ḥifẓ al-usrah*). In addition, peer-reviewed literature on cybercrime typologies—such as phishing, romance scams, smishing, and organized cyberfraud networks—was analyzed to contextualize the evolving sophistication of digital fraud ecosystems (Cretu-Adatte et al., 2024). Cyber forensic studies and digital evidence frameworks were also incorporated to understand procedural challenges in investigating and prosecuting digital fraud cases. From the Islamic legal perspective, family protection is examined as a normative objective that must adapt to contemporary digital risks while preserving moral and social integrity within households. Data analysis was conducted using thematic analysis combined with doctrinal interpretation. Interview transcripts were coded to identify recurring patterns of fraud mechanisms, victim vulnerability, and family impact. These empirical themes were then triangulated with legal norms from *UU ITE* and Islamic Family Law to assess convergence, gaps, and regulatory limitations. The analytical framework follows socio-legal integration principles that emphasize combining empirical evidence with normative reasoning to understand complex cyber phenomena, supported by cybersecurity perspectives on online harm prevention and phishing mitigation strategies.

RESULTS AND DISCUSSION

Patterns of WhatsApp-Based Digital Fraud in Family-Oriented Groups

The rapid expansion of WhatsApp as a primary communication platform has transformed interpersonal interaction into highly networked, trust-based digital ecosystems, particularly within family-oriented and religious groups. These environments are characterized by immediacy, emotional closeness, and low verification thresholds, which collectively create fertile conditions for cyber-enabled fraud. Fraudsters strategically exploit these socio-digital characteristics by embedding deceptive practices within familiar communication flows, thereby bypassing technical defenses through psychological manipulation rather than system intrusion (Varshney et al., 2024). In

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

such settings, fraud is not merely an isolated cyber offense but a socially constructed process that leverages relational trust, authority perception, and emotional dependency embedded in group communication structures. This pattern reflects a broader shift in cybercrime dynamics, where attackers increasingly target human vulnerability rather than technological weakness.

Empirical findings and literature indicate that WhatsApp-based fraud commonly follows a structured escalation process involving identity infiltration, trust construction, and exploitative conversion phases. Initial contact is often initiated through impersonation of trusted figures such as group administrators, lecturers, or religious leaders, followed by gradual engagement designed to build credibility (Popov, 2024). Once trust is established, perpetrators introduce requests for sensitive information such as verification codes, financial contributions, or participation in fictitious collaborative programs. These tactics align with established models of consumer-facing technology fraud, which emphasize incremental manipulation and emotional persuasion as core operational strategies. In collectivist cultural contexts, particularly within family-oriented WhatsApp groups, such strategies are highly effective due to strong norms of social compliance and respect for perceived authority.

A key analytical finding of this study is the emergence of "social legitimacy engineering," where fraudsters construct narratives that align with morally and socially meaningful domains such as academic collaboration, religious charity, or family solidarity. This framing significantly increases victim susceptibility by activating emotional obligations and reducing critical skepticism (Williams et al., 2017; Enayati et al., 2024). For instance, fake "journal collaboration groups" or "religious donation initiatives" are frequently used as entry points before transitioning into financial exploitation or identity theft requests. These patterns are consistent with smishing-based and phishing-based manipulation techniques, where urgency and administrative legitimacy are used to extract sensitive data such as OTP codes (Haizam & Zulkipli, 2024). The hybrid nature of these scams demonstrates that modern digital fraud is increasingly relational, embedding economic exploitation within emotionally meaningful social structures (Maras & Ives, 2024).

Table 1. Patterns of WhatsApp-Based Digital Fraud in Family-Oriented Groups

Pattern Type	Modus Operandi	Psychological Target	Example in Context
Identity Impersonation	Mimicking admins or known members	Trust in authority	Fake lecturer/religious leader account
Academic Collaboration Scam	Fake journal/book cooperation requiring fees or codes	Professional ambition	"Research publication group" invitation
Religious/Charity Fraud	Fake zakat or donation requests	Moral obligation	Religious fundraising scam
Verification Code Theft	Requesting OTP or login codes	Urgency and ignorance	"Group access verification code"
Investment/Project Fraud	Fake shared investment schemes	Economic aspiration	Cooperative profit-sharing scam

Source: Author's analysis based on literature synthesis (2024).

Further analysis reveals that WhatsApp-based fraud operates through network amplification effects, where compromised individuals unintentionally facilitate further dissemination due to pre-existing trust relationships. This mechanism mirrors the virality patterns observed in misinformation diffusion, where emotional salience accelerates transmission within tightly knit groups. Limited digital literacy and weak cybersecurity awareness further intensify vulnerability, reducing users' ability to critically assess suspicious messages. Additionally, structural weaknesses in identity verification systems within messaging platforms enable repeated impersonation, allowing fraudsters to re-enter groups under alternative identities (Jena et al., 2024; Sadhya & Sahu, 2024). The absence of formal moderation in informal WhatsApp groups further exacerbates these risks, as there are no standardized mechanisms for validating membership authenticity or monitoring anomalous communication behavior (Liu et al., 2024). Collectively, these findings demonstrate that WhatsApp-based digital fraud in family-oriented groups is a multidimensional phenomenon shaped by psychological manipulation, social trust exploitation, and technological governance gaps, requiring integrated legal, educational, and digital resilience responses (Sarkar & Shukla, 2024).

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

Impacts of Digital Fraud on Family Integrity and Social Trust

Digital fraud in WhatsApp-based communication environments generates multidimensional consequences that extend far beyond financial loss, affecting emotional stability, relational trust, and the structural integrity of families. Within family-oriented and religiously framed digital groups, deception becomes particularly damaging because it occurs in spaces socially constructed as safe, intimate, and trustworthy. When fraud emerges in such contexts, the violation is not only economic but also moral and relational, leading to a profound breakdown of confidence in both digital communication systems and interpersonal relationships (Varshney et al., 2024). This condition demonstrates that cyber fraud must be conceptualized not merely as a technological offense but as a socio-relational disruption embedded within everyday family communication practices. The transformation of trust-based digital spaces into fraud channels highlights how digital crime directly destabilizes family cohesion and weakens the normative foundations of social interaction.

At the family level, the most immediate impact of digital fraud is emotional and psychological distress, often manifested through shame, anxiety, guilt, and interpersonal conflict. Victims frequently experience self-blame, especially when deception occurs within trusted WhatsApp groups involving academic, religious, or family networks. These emotional consequences are consistent with cyber-enabled fraud literature, which emphasizes that online deception produces significant psychological harm alongside financial damage (Williams et al., 2017; Lazarus et al., 2023; Choi et al., 2024). In household contexts, such emotional burdens often escalate into communication breakdowns between spouses or family members, particularly when victims struggle to disclose their experiences. This situation generates relational tension, mistrust, and in some cases prolonged emotional distancing within the family unit. Moreover, financial losses caused by fraud schemes further intensify household instability, as victims may divert personal or family resources into fraudulent transactions. This aligns with research indicating that consumer-facing fraud directly undermines household economic resilience and decision-making capacity. From an Islamic legal perspective, such losses are relevant to the principles of *ḥifẓ al-māl* (protection of wealth) and *ḥifẓ al-usrah* (protection of family), which collectively emphasize safeguarding economic and relational stability within the household system (Asman, 2020).

The impact of digital fraud also extends to broader social trust erosion, particularly within digital communities that rely on WhatsApp groups as mechanisms of coordination, communication, and collective decision-making. Trust functions as the foundational mechanism of group-based communication, and once violated, it produces long-term skepticism toward future interactions, even when communication is legitimate. This phenomenon is consistent with studies on digital influence and vulnerability, which demonstrate that repeated exposure to deception reduces individuals' capacity to trust online communication environments (Mishra et al., 2024). To summarize the multidimensional impacts observed in this study, the following classification is presented:

Table 2. Impacts of Digital Fraud on Family Integrity and Social Trust

Impact Dimension	Form of Impact	Consequence in Family Context
Emotional Impact	Shame, anxiety, stress	Internal conflict and communication breakdown
Financial Impact	Loss of money/assets	Household economic instability
Relational Impact	Broken trust	Decline in marital and kinship harmony
Social Trust Impact	Distrust in digital groups	Withdrawal from online engagement

Source: Author's analysis (2024).

Beyond individual and family-level consequences, digital fraud contributes to systemic erosion of social cohesion by weakening collective resilience in online communities. As fraud incidents increase, users develop defensive communication behaviors such as reduced participation, avoidance of group interaction, and heightened suspicion toward digital messages (Esteban-Bravo et al., 2024). This behavioral shift reduces the effectiveness of digital platforms as instruments of social coordination, particularly in contexts where WhatsApp groups function as spaces for family governance, religious communication, and community organization. Furthermore, the increasing sophistication of fraud techniques—including impersonation, social engineering, and hybrid scam models—complicates users' ability to differentiate between legitimate and fraudulent communication (Maras & Ives, 2024). The absence of robust identity verification mechanisms in informal messaging ecosystems further amplifies vulnerability, increasing the likelihood of repeated victimization. Overall, these findings indicate a cascading impact structure, where digital fraud begins at the individual level, expands into family disruption, and ultimately contributes to the deterioration of social trust within digital society, underscoring the need for integrated legal, educational, and technological interventions.

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

Legal Response under UU ITE and Its Practical Limitations

Indonesia has established a formal legal framework to address cybercrime through the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*, UU ITE), which regulates electronic communication, criminalizes online fraud, and provides legal certainty for victims of digital offenses. In principle, this law represents the state's response to the rapid expansion of digital ecosystems and the increasing sophistication of cyber-enabled fraud, including phishing, impersonation, and social engineering schemes that frequently occur within messaging platforms. However, despite its normative strength, the implementation of UU ITE in cases of WhatsApp-based family-oriented fraud remains limited in practical effectiveness. This limitation arises because the law is primarily designed to regulate digital transactions and criminal liability, rather than addressing the relational and emotional dimensions of fraud that occur within family or trust-based communication networks.

From an enforcement perspective, UU ITE focuses heavily on procedural legality, electronic evidence, and digital attribution mechanisms used in cybercrime investigations. The legal system prioritizes forensic validation of electronic data and identification of perpetrators through digital traceability frameworks (Reedy, 2023; Ng & James, 2024). However, in practice, many victims of WhatsApp-based fraud do not report incidents due to limited legal literacy, fear of social stigma, or perceived procedural complexity. This gap between normative legal availability and actual accessibility creates a structural barrier that reduces the effectiveness of law enforcement in protecting families from digital fraud. Moreover, cyber forensic processes require specialized technical expertise that is not always available at local enforcement levels, resulting in delays and reduced case resolution efficiency (Magdalene Ng & James, 2024). To summarize these limitations, the following table presents a structured overview:

Table 3. Practical Limitations of UU ITE in Handling WhatsApp-Based Digital Fraud

Legal Aspect	Practical Limitation	Impact on Victims
Legal Awareness	Low public understanding of reporting mechanisms	Underreporting of fraud cases
Procedural Complexity	Complicated forensic and legal procedures	Victims avoid formal reporting
Scope of Law	Focus on individual cybercrime, not relational harm	Family impact not legally addressed
Enforcement Capacity	Limited digital forensic expertise at local level	Delayed investigation and resolution

Source: Author's analysis (2024)

A critical limitation of UU ITE lies in its narrow legal framing, which treats digital fraud primarily as an individual cyber offense rather than a relational harm affecting family integrity and social trust. In WhatsApp-based fraud cases, deception often occurs within emotionally significant contexts such as family, academic, or religious groups, where trust is the primary mechanism of communication. This relational dimension is not fully captured within conventional cybercrime frameworks (Choi et al., 2024). As a result, the law does not adequately address secondary consequences such as emotional distress, marital conflict, and breakdown of household trust. Furthermore, digital fraud in messaging environments is increasingly hybrid in nature, combining financial deception, identity manipulation, and psychological coercion within a single scheme (Maras & Ives, 2024). This complexity exceeds the traditional scope of UU ITE, which was originally designed for more linear forms of electronic crime.

Another significant limitation is the lack of preventive orientation within UU ITE implementation. While the law provides mechanisms for punishment after fraud occurs, it does not sufficiently emphasize prevention through digital literacy, early warning systems, or community-based cyber awareness programs. Research in cybersecurity indicates that legal enforcement alone is insufficient without behavioral resilience and user education to reduce vulnerability in digital environments (Mishra et al., 2024; Esteban-Bravo et al., 2024). In WhatsApp-based ecosystems, where fraud spreads through trusted social networks, preventive approaches are particularly critical. Additionally, global studies highlight that weaknesses in digital identity verification systems and cross-platform coordination further increase susceptibility to fraud (Jena et al., 2024; Sadhya & Sahu, 2024). Overall, these findings demonstrate that although UU ITE provides an essential legal foundation for addressing cybercrime in Indonesia, its effectiveness remains constrained by procedural, structural, and socio-relational limitations. Strengthening its impact therefore requires not only legal refinement but also integration with socio-legal

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

frameworks and digital literacy strategies that recognize family integrity as a central dimension of cyber protection.

Islamic Family Law Perspective and the Gap in Digital Protection Framework

Islamic Family Law fundamentally emphasizes the preservation of family integrity, justice within household relations, and protection from harm as part of the broader objectives of *maqāṣid al-sharī'ah*. Within this normative framework, the family (*usrah*) is positioned as a core institution that must be safeguarded from all forms of physical, emotional, and financial harm. Classical and contemporary Islamic legal thought increasingly recognizes that family resilience must adapt to modern socio-digital transformations, including the rise of digital communication platforms that reshape interpersonal interactions (Asman, 2020; Alkamli & Alabduljabbar, 2024). However, while the ethical foundation of protection is well established, its translation into operational legal instruments for addressing digital fraud in messaging applications remains limited. In the context of WhatsApp-based fraud, this limitation becomes increasingly visible as digital interactions introduce new vulnerabilities that are not explicitly anticipated in traditional Islamic legal formulations.

The findings of this study indicate that Islamic Family Law provides strong normative guidance for protecting families, yet it lacks explicit juridical mechanisms to address cyber-enabled fraud. In practice, issues such as impersonation, financial deception, and psychological manipulation in digital spaces are not yet systematically integrated into Islamic legal problem-solving frameworks. Existing Islamic family law scholarship tends to focus on household governance, gender roles, caregiving responsibilities, and child protection, while relatively neglecting digital risks emerging from technological transformation (Setyawati et al., 2024; Muljan et al., 2024). From a *maqāṣid al-sharī'ah* perspective, digital fraud directly violates the principles of ḥifẓ al-māl (protection of wealth) and ḥifẓ al-usrah (protection of family), because it simultaneously disrupts economic stability and emotional harmony within households. Nevertheless, current Islamic legal interpretation has not fully extended into digital ecosystems where trust-based communication—such as WhatsApp groups—becomes a primary vulnerability exploited by fraudsters. To clarify this gap, Table 4 presents a synthesis of Islamic legal principles and their limitations in addressing digital fraud contexts.

Table 4. Islamic Legal Principles and Gaps in Digital Fraud Context

Islamic Legal Principle	Intended Objective	Observed Gap in Digital Context
Ḥifẓ al-usrah	Preserve family harmony and stability	No specific guidance on digital fraud impacts
Ḥifẓ al-māl	Protect financial resources	Limited adaptation to online financial scams
Amānah (trust)	Maintain honesty in social relations	Vulnerable to impersonation and social engineering
ʿAdl (justice)	Ensure fairness in conflict resolution	Weak integration with cyber reporting systems

Source: Author's analysis (2024)

Beyond normative gaps, Islamic Family Law also demonstrates limited integration with contemporary digital governance systems. Cybersecurity studies show that digital fraud increasingly relies on identity manipulation, social engineering, and cross-platform deception strategies, making it structurally complex and difficult to regulate without technological support systems. Moreover, fraud schemes such as romance scams, investment fraud, and hybrid "trust-building" deception are heavily dependent on emotional manipulation and long-term relational engagement (Choi et al., 2024; Maras & Ives, 2024). These characteristics are not fully addressed in classical Islamic legal procedures, which are generally oriented toward tangible transactions and direct interpersonal disputes. As a result, Islamic Family Law remains largely normative and ethical in addressing digital fraud, rather than procedural and institutional.

Furthermore, the increasing sophistication of cyberfraud networks highlights the necessity of interdisciplinary integration between Islamic legal principles and modern digital governance systems. Studies indicate that organized cyberfraud groups operate in adaptive, network-based structures across multiple platforms, making legal enforcement increasingly complex. In parallel, digital forensic research emphasizes the importance of electronic evidence, identity verification, and cross-platform data analysis in addressing cybercrime effectively (Magdalene Ng & James, 2024). However, such procedural and technological mechanisms have not yet been meaningfully incorporated into Islamic Family Law frameworks. This creates a structural gap between normative ethical principles and the operational realities of digital crime. Overall, the findings demonstrate that while Islamic

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

Family Law offers a strong moral foundation for protecting families, its current framework is not yet sufficiently equipped to address WhatsApp-based digital fraud. Strengthening its relevance in the digital era requires integrating *maqāṣid al-sharī'ah* with digital governance, cybersecurity awareness, and interdisciplinary legal mechanisms to ensure more comprehensive protection for families in contemporary society (Setyawati et al., 2024).

Integration Model of UU ITE and Islamic Family Law

The integration of the Indonesian Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik*, UU ITE) and Islamic Family Law is conceptually grounded in the need to construct a holistic protection framework that addresses both the technical-legal and socio-ethical dimensions of digital fraud affecting families. UU ITE functions as a state-based legal instrument that regulates electronic communication, digital evidence, and criminal sanctions for cyber-enabled offenses, particularly fraud, impersonation, and data manipulation in online environments. Its primary orientation is repressive and procedural, focusing on enforcement mechanisms after a violation occurs through digital forensic investigation and legal prosecution. In contrast, Islamic Family Law provides a normative-ethical framework grounded in *maqāṣid al-sharī'ah*, particularly ḥifẓ al-māl (protection of wealth) and *ḥifẓ al-usrah* (protection of family), which emphasize prevention of harm, preservation of trust, and maintenance of household stability (Asman, 2020; Ashraf et al., 2024). Therefore, integration between both systems is understood as a complementary synthesis between formal state enforcement and moral-religious safeguarding mechanisms in digital society, rather than a substitution of one system by another.

At the conceptual level, the integration model positions UU ITE as the instrumental-legal layer and Islamic Family Law as the normative-ethical layer, both operating toward the shared objective of protecting family integrity in digital communication environments. The instrumental-legal layer ensures accountability, evidence-based prosecution, and deterrence against perpetrators of WhatsApp-based fraud, which frequently employs social engineering strategies such as impersonation, phishing, and verification code theft. Meanwhile, the normative-ethical layer strengthens preventive awareness by reinforcing values of trust (*amānah*), responsibility, and digital caution within family-oriented and religious communication groups. This dual-layer structure addresses a key gap in both cybercrime literature and Islamic legal discourse, where legal enforcement exists but is not sufficiently integrated with ethical, behavioral, and familial protection mechanisms (Setyawati et al., 2024). In this sense, the integration model shifts the legal response from a purely reactive system toward a more balanced preventive–protective framework that is socially embedded in family structures. Operationally, the integration model is implemented through a three-stage framework consisting of prevention, protection, and restoration. In the prevention stage, Islamic Family Law contributes through value-based digital ethics education, encouraging users to exercise caution, verify information, and avoid blind trust in digital group interactions. In the protection stage, UU ITE provides formal mechanisms for reporting, investigating, and prosecuting digital fraud using electronic evidence and digital forensic procedures (Hanaputra et al., 2024). In the restoration stage, Islamic legal principles contribute to emotional and relational recovery through reconciliation (*iṣlāḥ*), accountability, and strengthening family resilience after fraud incidents. This integrated structure reflects the need for a hybrid legal–ethical system that does not only punish offenders but also restores trust and social harmony within families. The following table summarizes the integration framework:

Table 5. Integration Model of UU ITE and Islamic Family Law in Digital Fraud Protection

Dimension	UU ITE Contribution	Islamic Family Law Contribution	Integrated Function
Prevention	Cyber awareness and deterrence	Ethical guidance (*amānah*, trust)	Digital literacy + moral vigilance
Protection	Legal enforcement and forensic evidence	Normative obligation to prevent harm	Legal accountability + ethical responsibility
Restoration	Sanctions and reporting mechanisms	Family reconciliation (*iṣlāḥ*)	Legal justice + family healing

Source: Author's analysis (2024)

This integrative model demonstrates that addressing WhatsApp-based digital fraud requires more than isolated legal enforcement; it demands a coordinated framework that merges statutory regulation with ethical-religious values embedded in family systems. The increasing sophistication of hybrid fraud schemes—combining emotional manipulation, impersonation, and financial exploitation—requires a multidimensional response that

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

operates simultaneously at behavioral, social, and institutional levels. By aligning UU ITE with Islamic Family Law, the proposed model strengthens not only legal effectiveness but also preventive awareness and social resilience, thereby offering a more comprehensive protection architecture for families in digital communication environments.

CONCLUSION

This study concludes that WhatsApp-based digital fraud significantly affects family integrity by disrupting emotional stability, weakening financial security, and eroding social trust within family-oriented communication groups. The findings show that fraud schemes operate through systematic trust exploitation, identity impersonation, and social engineering strategies embedded in everyday digital interactions. These mechanisms are not merely technical offenses but socio-digital manipulations that transform ordinary communication spaces into channels of deception and relational harm. As a result, victims experience not only economic loss but also psychological distress, shame, and internal family conflict that may persist long after the fraud incident occurs. In this regard, digital fraud must be understood as a socio-legal phenomenon that extends beyond individual victimization and directly threatens the stability of the family as a fundamental social institution. Accordingly, the first research objective—identifying the patterns and impacts of WhatsApp-based digital fraud on family integrity—has been achieved through empirical case analysis and literature synthesis.

Furthermore, the study finds that the existing legal response under UU ITE provides an important formal mechanism for addressing digital fraud, particularly through electronic evidence collection, digital forensics, and cybercrime prosecution. However, its practical effectiveness remains constrained by limited public awareness, procedural complexity, and weak accessibility for ordinary victims. Many affected individuals do not report cases due to uncertainty about legal procedures or fear of social stigma, resulting in significant underreporting. At the same time, Islamic Family Law offers strong normative foundations for protecting family integrity through *maqāṣid al-sharī'ah*, particularly the principles of protection of wealth (*ḥifẓ al-māl*) and protection of family (*ḥifẓ al-usrah*), yet it lacks operational mechanisms to respond to cyber-enabled fraud in contemporary digital communication platforms. These findings confirm that both legal systems function in parallel but remain structurally fragmented, creating a protection gap in addressing WhatsApp-based fraud within family communication networks. In answering the second research objective, the study confirms that neither system alone is sufficient to fully address the complexity of digital fraud in family-oriented digital spaces.

The main novelty of this research lies in the development of an integrative protection model that combines UU ITE and Islamic Family Law into a three-layer framework consisting of prevention, protection, and restoration. This model bridges the technical-legal enforcement capacity of UU ITE with the ethical-preventive and restorative principles of Islamic Family Law, offering a more holistic approach to safeguarding families in digital environments. By positioning digital fraud simultaneously as a legal violation and a moral-ethical problem, the study provides a more comprehensive perspective on family protection in the digital era. Nevertheless, this research has limitations, particularly its reliance on qualitative case-based data and literature synthesis, which may limit generalization across broader populations. Future research is recommended to expand empirical coverage across different regions and to test the proposed integration model through quantitative or policy-oriented validation to strengthen its practical applicability.

REFERENCES

Abdurrahman, A., Gustomo, A., Prasetio, E. A., & Rustiadi, S. (2022). Designing an open innovation framework for digital transformation based on systematic literature review. *Journal of Information Systems Engineering and Business Intelligence, 8*(2), Article 2. https://doi.org/10.20473/jisebi.8.2.100-108

Abubakar, F., Saadah, M., & Na'mah, U. (2023). The transformation of the dilemma of role exchange in the household: Analyzed gender in family resilience discourse in national law and Islamic law. *Jurnal Ilmiah Al-Syir'ah, 21*(1), Article 1. https://doi.org/10.30984/jis.v21i1.1864

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100*, 408–427. https://doi.org/10.1016/j.future.2019.03.041

Alkamli, S., & Alabduljabbar, R. (2024). Understanding privacy concerns in ChatGPT: A data-driven approach with LDA topic modeling. *Heliyon, 10*(20), e39087. https://doi.org/10.1016/j.heliyon.2024.e39087

Ashraf, A. R., Mackey, T. K., Vida, R. G., Kulcsár, G., Schmidt, J., Balázs, O., Domián, B. M., Li, J., Csákó, I., & Fittler, A. (2024). Multifactor quality and safety analysis of semaglutide products sold by online sellers

without a prescription: Market surveillance, content analysis, and product purchase evaluation study. *Journal of Medical Internet Research, 26*. https://doi.org/10.2196/65440

Asman, A. (2020). Parental rights and obligations to children in the era of industrial revolution 4.0 (Islamic family law perspective). *Samarah: Jurnal Hukum Keluarga dan Hukum Islam, 4*(1), Article 1. https://doi.org/10.22373/sjhk.v4i1.6899

Choi, S. W., Lee, J., & Choi, Y.-J. (2024). Unveiling the patterns of romance scams in South Korea. *International Journal of Cyber Behavior, Psychology and Learning, 14*(1). https://doi.org/10.4018/IJCBPL.357152

Cretu-Adatte, C., Azi, J. W., Beaudet-Labrecque, O., Bunning, H., Brunoni, L., & Zbinden, R. (2024). Unravelling the organisation of Ivorian cyberfraudsters: Criminal networks or organised crime? *Journal of Economic Criminology, 3*, 100056. https://doi.org/10.1016/j.jeconc.2024.100056

Daniela, N. P., Hanapi, A., Husnul, M., & Fahri, M. (2024). The granting of family card for Siri marriage in Banda City: Perspective of Islamic family law. *El-Usrah: Jurnal Hukum Keluarga, 7*(1), Article 1. https://doi.org/10.22373/ujhk.v7i1.23317

Enayati, M., Arlikatti, S., & Ramesh, M. V. (2024). A qualitative analysis of rural fishermen: Potential for blockchain-enabled framework for livelihood sustainability. *Heliyon, 10*(2), e24358. https://doi.org/10.1016/j.heliyon.2024.e24358

Esteban-Bravo, M., Jiménez-Rubido, L. d. l. M., & Vidal-Sanz, J. M. (2024). Predicting the virality of fake news at the early stage of dissemination. *Expert Systems with Applications, 248*, 123390. https://doi.org/10.1016/j.eswa.2024.123390

Haizam, M. N. B., & Zulkipli, N. H. binti N. (2024). Analysing the impact of smishing attack in public announcement system on mobile phone. *Procedia Computer Science, 245*, 1165–1174. https://doi.org/10.1016/j.procs.2024.10.346

Hanaputra, R. R., Sa'adah, K., & Purwoko, R. (2024). Identifikasi digital evidence dalam transaction fraud pada WhatsApp Desktop berdasarkan NIST SP 800-86: Studi kasus bisnis properti. *JURNAL FASILKOM, 14*(2). https://doi.org/10.37859/jf.v14i2.7100

Jena, S. K., Barik, R. C., & Priyadarshini, R. (2024). A systematic state-of-art review on digital identity challenges with IoT and blockchain in healthcare. *Internet of Things, 25*, 101111. https://doi.org/10.1016/j.iot.2024.101111

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review. *Journal of Economic Criminology, 2*, 100013. https://doi.org/10.1016/j.jeconc.2023.100013

Liu, T.-H., Ma, Z., & Xia, Y. (2024). Serving on WeChat: Understanding police engagement with the public in Chinese contexts. *International Journal of Law, Crime and Justice, 77*, 100665. https://doi.org/10.1016/j.ijlcj.2024.100665

Magdalene Ng, & James, J. (2024). "What you say in the lab, stays in the lab": Digital forensic investigations challenges. *Forensic Science International: Digital Investigation, 51*, 301839. https://doi.org/10.1016/j.fsidi.2024.301839

Maras, M.-H., & Ives, E. R. (2024). Deconstructing hybrid investment fraud: Examining 'pig butchering'. *Journal of Economic Criminology, 5*, 100066. https://doi.org/10.1016/j.jeconc.2024.100066

Media, K. C. (2023, January 23). Hati-hati penipuan: Tips agar tidak dimasukkan ke grup WhatsApp sembarangan. *KOMPAS.com*. https://tekno.kompas.com/read/2023/01/23/08000027/hati-hati-penipuan-ini-tips-agar-tidak-dimasukkan-ke-grup-whatsapp-sembarangan

Mishra, A., Sinha, S., & George, C. P. (2024). Shielding against online harm: A survey on text analysis to prevent cyberbullying. *Engineering Applications of Artificial Intelligence, 133*, 108241. https://doi.org/10.1016/j.engappai.2024.108241

Muljan, M., Mustafa, M., Ilmiati, I., Rahmawati, S., & Rosita, R. (2024). Preventing child marriage in Bone District: Islamic family law perspective. *El-Usrah: Jurnal Hukum Keluarga, 7*(1). https://doi.org/10.22373/ujhk.v7i1.22482

Popov, C. (2024). Scam alert: How fraudsters exploit WhatsApp group chats. *Hot for Security*. https://www.bitdefender.com/en-us/blog/hotforsecurity/scam-alert-how-fraudsters-are-exploiting-whatsapp-group-chats-and-what-you-need-to-know-to-stay-safe

Reedy, P. (2023). Interpol review of digital evidence 2019–2022. *Forensic Science International: Synergy, 6*, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

Sadhya, D., & Sahu, T. (2024). Security and privacy aspects of Aadhaar framework. *Computers & Security, 140*, 103782. https://doi.org/10.1016/j.cose.2024.103782

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: Cybercrime frameworks. *Journal of Economic Criminology, 4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Munakahat: ***Journal of Islamic Family Law***
Vol. 1, No. 1, December 2024
DOI: https://doi.org/10.5281/zenodo.20817351

Setyawati, M. B., Parsons, A. P. J., Laing, B., Lynch, A., Habiburahman, I. L., & Izza, F. N. (2024). Family caregiving: Islamic perspective. *Heliyon, 10*(3), e25415. https://doi.org/10.1016/j.heliyon.2024.e25415

Ullah, S., Li, J., Ullah, F., Chen, J., Ali, I., Khan, S., Ahad, A., & Leung, V. C. M. (2024). Explainable AI for Android malware detection. *Internet of Things, 27*, 101320. https://doi.org/10.1016/j.iot.2024.101320

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications, 238*, 122199. https://doi.org/10.1016/j.eswa.2023.122199

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence. *Computers in Human Behavior, 72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Zieliński, S. (2024). Evolving threats, emerging laws: Poland's smishing challenge. *Computer Law & Security Review, 54*, 106013. https://doi.org/10.1016/j.clsr.2024.106013