Language, Technology, and Policy: A Unified Conceptual Framework for Combating Digital Scams in Malaysia

Mohd Amirul Atan, Ahmad Azfar Abdul Hamid*, Sheik Badrul Hisham Jamil Azhar, Nuramirah Zaini, Nur Aqilah Norwahi

Akademi Pengajian Bahasa, Universiti Teknologi MARA (UiTM) Melaka, Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90900088

Received: 27 August 2025; Accepted: 02 September 2025; Published: 30 September 2025

ABSTRACT

Digital scams have become one of the most pervasive threats in the Malaysian digital ecosystem, with significant financial and psychological impacts on society. Scammers exploit the power of language to deceive, manipulate, and persuade individuals into making decisions that result in monetary loss and erosion of trust in digital platforms. While technology and law enforcement play critical roles in curbing these crimes, less attention has been given to the linguistic foundations of deception and how they interact with technology and policy. This paper proposes a unified conceptual framework to address digital scams in Malaysia by integrating linguistic analysis, digital literacy initiatives, technological detection systems, and policy reform. Drawing on recent studies in forensic linguistics, natural language processing, and cybercrime governance, the framework situates language at the centre of scam detection and prevention. The paper also discusses policy implications and challenges in implementation, emphasising the need for interdisciplinary collaboration between linguists, policymakers, educators, and technologists. By conceptualising scams as both linguistic and technological crimes, this paper contributes to the discourse on digital fraud prevention and advocates for linguistically informed policy approaches to safeguard Malaysian citizens.

Keywords: Forensic Linguistics, Digital Scams, Cybercrime Policy, Natural Language Processing (NLP)

INTRODUCTION

The rise of digital scams in Malaysia mirrors global trends, where scammers exploit the growing dependence on technologies to reach wider audiences and operate with relative anonymity. Between 2019 and 2023, Malaysia recorded over 14,000 cases of investment fraud, with total losses surpassing RM1.34 billion (Juned et al., 2024). These figures are alarming not only for their financial magnitude but also for their implications on trust in digital platforms, investor confidence, and national cybersecurity. Digital scams today are not limited to phishing emails or dubious online advertisements but have diversified into cryptocurrency frauds, illegal investment schemes, social media impersonations, and romance scams. Each of these scams employs carefully designed linguistic strategies to gain the trust of victims, manipulate their emotions, and exploit their cognitive biases.

Language is central to the operations of scams. Fraud is often described as a “language crime” because the success of the deception depends on the ability of the scammer to manipulate discourse, bend conversational norms, and persuade the victim into compliance (Momeni, 2012). In Malaysia, scammers employ multilingual strategies, reflecting the country’s sociolinguistic diversity. Messages may appear in English, Malay, Chinese, or Tamil, depending on the target demographic, and they often rely on rhetorical appeals that resonate with the cultural values of different communities. Despite the importance of language, most anti-scam strategies in Malaysia remain anchored in technological solutions such as digital surveillance, cybersecurity filters, and regulatory enforcement. These approaches, while necessary, remain incomplete without the integration of linguistic awareness and forensic insights.

The purpose of this paper is to propose a unified conceptual framework to combat digital scams in Malaysia which integrates linguistic analysis, digital literacy, AI-driven detection systems, and cyber policy governance.

This framework emphasises language not only as the medium of deception but also as the foundation for awareness, prevention, and regulation. By positioning language alongside technology and policy, the framework seeks to address the multifaceted nature of scams and provide a holistic model for digital fraud prevention.

LITERATURE REVIEW

Language and Deception in Scams

Language plays two roles in scams: it is both the weapon of the scammer and the potential defence mechanism of the victim. Forensic linguistics has long identified fraud as a form of "language crime," requiring the use of deceptive tools, the exploitation of victims' lack of knowledge, and the eventual occurrence of loss (Momeni, 2012). Scam communications often rely on discourse strategies that obscure intent, create urgency, or evoke emotional responses. Studies of cryptocurrency scams in Malaysia demonstrate scammers employ Aristotle's rhetorical appeals of ethos, pathos, and logos to establish credibility, appeal to emotions, and present seemingly logical reasoning (Hamid et al., 2023). For instance, ethos is achieved by associating scams with prominent figures or institutions, pathos is deployed through emotional testimonials and promises of financial freedom, while logos is simulated by presenting fabricated statistics or guarantees of safety and profitability.

The linguistic cues of deception extend beyond rhetorical appeals. Research on investment scams in Malaysia has shown that scammers commonly employ credibility enhancement strategies, emotive intensifiers, and framing effects to shape investor perceptions (Juned et al., 2024). Promotional materials of illegal investment schemes often construct what Sharif et al. (2024) describe as "beguiling realism," in which exaggerated promises and unverifiable claims create the illusion of authenticity and exclusivity. Deceptive cues also include unverifiable spatial and temporal information, the use of ambiguous disclaimers, and the deployment of luxurious imagery to project a sense of credibility. These findings indicate that scams thrive not merely because of technological anonymity but because of their ability to manipulate language to exploit psychological vulnerabilities.

Technological Dimensions of Scam Detection

While language provides the foundation of scams, technology facilitates their distribution and amplification. Cybercrime today is predominantly text-based, with most forms of abuse manifesting through online messages, social media posts, emails, or promotional websites (Coulthard, Grant, & Kredens, 2011). Natural language processing (NLP) and artificial intelligence (AI) have increasingly been applied to the detection of deceptive linguistic cues. Burgoon, Blair, Qin, and Nunamaker (2003) demonstrated the combinations of linguistic features such as sentence complexity, pronoun use, and affective language can distinguish between truthful and deceptive texts with measurable accuracy. More recent studies highlight the utility of sentiment analysis, stylometry, and discourse structure analysis for identifying fraudulent texts across domains (Jakupov, Longhi, & Zeddini, 2024).

Despite these advances, scam detection technologies face limitations. Scammers constantly adapt their linguistic strategies, shifting across platforms and languages to avoid detection (Hamid et al., 2023). Malaysia's linguistic diversity further complicates detection efforts, as scammers can manipulate cultural nuances and multilingual discourses to target specific communities. Automated systems trained on English datasets may struggle to detect deception in Malay, Chinese, or Tamil contexts. Thus, while AI-driven detection offers significant promise, it must be combined with linguistic expertise and locally contextualised data.

Policy and Governance

Malaysia has developed several legal and regulatory frameworks to combat scams, including the Computer Crimes Act 1997, regulations enforced by the Securities Commission Malaysia (SC), and consumer alert lists published by Bank Negara Malaysia (BNM). While these frameworks address the financial and technological dimensions of scams, they rarely incorporate forensic linguistic insights into regulatory enforcement. International models suggest the value of integrating linguistic perspectives into governance. For example, the European Union's digital security frameworks emphasise transparency in communication and the detection of misleading promotional content, while the U.S. Federal Trade Commission prosecutes deceptive advertising and misrepresentation in digital commerce.

For Malaysia, the challenge lies in aligning cybercrime governance with linguistic realities. Laws must recognise scams are not just technological crimes, but it is also discursive manipulations. Without incorporating linguistic evidence into investigations and prosecutions, many scam cases remain difficult to prove in court, thus limiting the effectiveness of existing regulations. Malaysia's challenges must be situated within global best practices. The EU criminalises misleading digital communication, while the US Federal Trade Commission prosecutes deceptive advertising language even before financial harm occurs. Singapore integrates multilingual scam awareness into public campaigns and education, supported by a "Scam Alert" portal. Globally, regulators are experimenting with AI-driven monitoring of scam language in real time.

In contrast, Malaysia faces persistent challenges; scams exploit linguistic diversity, legal recognition of language crimes remains limited, awareness campaigns are fragmented, and interventions are often reactive. Unlike the EU and US, Malaysia has not integrated linguistic deception into legal frameworks, while Singapore's multilingual campaigns are a closer model to adopt.

Dimension	Malaysia (Current)	International Best Practices
Legal Recognition	Fraud = financial misrepresentation	Fraud = discursive & financial (EU, US)
Linguistic Evidence	Rarely admissible in prosecution	Accepted as evidence (FTC, EU directives)
Awareness Campaigns	Fragmented, limited multilingual outreach	Systematic, multilingual (Singapore)
AI/NLP Use	Basic filters, English-focused	Real-time multilingual monitoring (global)
Institutional Collaboration	Agencies act separately	Cross-sector taskforces (EU, SG)

Figure 1. Comparative Policy Approaches to Scam Regulation

METHODOLOGY

Proposed Conceptual Framework

This paper advances a four-pillar conceptual framework that integrates linguistic, technological, and policy approaches to combat digital scams in Malaysia. The framework recognises that no single dimension whether language, technology, or policy can adequately address scams on its own. Instead, a cooperative approach is required.

The first pillar, Deceptive Cues, emphasises the identification of linguistic markers of deception. These include rhetorical strategies such as ethos, pathos, and logos, as well as specific cues such as unverifiable claims, exaggerated promises, and manipulative emotional appeals. By systematically documenting these cues, forensic linguists can provide investigators with linguistic fingerprints that signal fraudulent intent. Studies in Malaysia show how credibility enhancement, emotional intensifiers, and framing effects are used in promotional materials of scams to manipulate investors' decision-making (Juned et al., 2024; Sharif et al., 2024). These cues are not random but carefully crafted rhetorical devices, often exploiting ethos, pathos, and logos (Hamid et al., 2023).

The second pillar, Awareness, places digital literacy as a preventive tool. Scholars argue that many victims fall prey not because of technological weaknesses but due to limited scam awareness and susceptibility to persuasive discourse (Sharif et al., 2024; Momeni, 2012). Public education campaigns must teach citizens to recognise linguistic red flags and to resist manipulative appeals. Awareness initiatives should be taught in school curriculum, community programs, and workplace training, with particular attention to vulnerable groups such as retirees and rural communities. Given Malaysia's linguistic diversity, awareness campaigns must also be multilingual to reach across the demographic boundaries.

The third pillar, Prevention, focuses on the application of AI and NLP tools to detect scams in real time. Prior research has shown that linguistic features such as sentence complexity, pronoun use, and affective terms can be automated to identify deception with measurable accuracy (Burgoon et al., 2003; Jakupov et al., 2024). By integrating linguistic analysis with technological solutions, prevention systems can identify scam messages in emails, social media platforms, and banking communications. Stylometry and authorship profiling can be employed to trace anonymous scam messages, while early warning systems can detect scam-related keywords

and discourse structures. Notably, these technologies must be trained on Malaysian datasets to ensure cultural and linguistic relevance. These findings highlight the potential of linguistically informed AI to support scam detection in Malaysian contexts, provided the systems are adapted for multilingual data (Coulthard et al., 2011).

The final pillar, Policy, calls for the alignment of cybercrime laws with linguistic insights. Existing legal frameworks must be updated to explicitly recognize linguistic deception as evidence of fraud. Fraud is fundamentally a discursive crime, and legal frameworks must reflect this (Momeni, 2012). This includes criminalising the use of false testimonials, vague official branding, and manipulative discourse in financial promotions. Policy alignment also requires institutional collaboration among SC, BNM, the Royal Malaysia Police, and digital platforms. Current Malaysian policies address financial and technological dimensions but lack clear observations of linguistic deception, unlike EU and US models where deceptive discourse is considered prosecutable evidence (Jakupov et al., 2024). By embedding forensic linguistic expertise into regulatory and judicial processes, Malaysia can strengthen its capacity to prosecute scammers effectively.

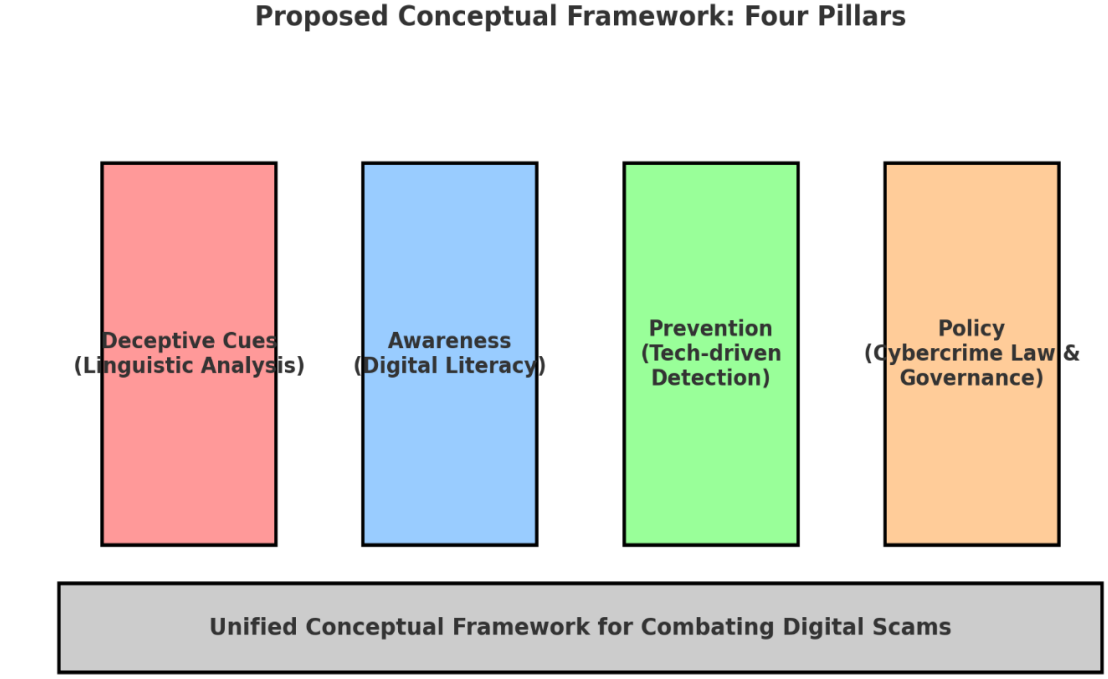

Figure 2. The Four Pillars of the Unified Conceptual Framework for Combating Digital Scams.

Illustrative Examples of Scam Messages

To demonstrate the framework in practice, three anonymised scam message examples are presented and analysed linguistically.

Cryptocurrency Investment Scam (English):

“Dear Investor, Congratulations! You have been selected to join CryptoWealth Malaysia, endorsed by top financial experts. Our platform guarantees 15% daily profit with no risk. Hundreds of Malaysians are already enjoying financial freedom. Don’t miss this once-in-a-lifetime opportunity. Only 50 slots left!” Ethos is built by referencing “top financial experts,” while pathos exploits excitement and fear of missing out. Logos is misused through a mathematically impossible “15% daily profit.” The deceptive cues include beguiling realism and framing effects.

Romance Scam (Malay)

“Hai sayang, saya baru balik dari misi di luar negara. Saya nak kongsi berita gembira, saya dapat pampasan USD200,000 daripada kontrak kerajaan. Tapi saya perlukan akaun awak untuk transfer duit ini ke Malaysia. Bila

saya balik nanti, kita boleh bina hidup baru bersama." Ethos is constructed by posing as a government contractor, while pathos manipulates intimacy ("sayang"). Logos rationalises the transfer through a plausible foreign contract. The deceptive cues include unverifiable spatial and temporal information and emotional intensifiers.

Loan Approval Scam (Bilingual)

"Selamat petang! Your loan of RM50,000 has been approved with 0% interest. Immediate disbursement available. Just pay a small processing fee of RM300 today. Jangan tunggu lagi peluang ini terhad!" Ethos is suggested through pseudo-formal language mimicking banks. Pathos is triggered by urgency, while logos fabricates logic ("0% interest" with upfront fee). The deceptive cues include dubious clarity and false credibility.

These examples illustrate how the four pillars of the framework interact; deceptive cues demonstrate linguistic manipulation, awareness training can help citizens recognise them, AI can automate detection of recurring patterns, and policy must criminalise such discourse.

Conceptual Pilot Study

To further illustrate the framework's applicability, a conceptual pilot study is proposed using a small sample of ten anonymised scam messages. Messages were coded according to four dimensions:

deceptive cues,

awareness,

prevention

policy.

From analysing the four dimensions, an illustrative finding was concluded. All messages displayed at least two deceptive cues, most often beguiling realism and emotional intensifiers. Awareness training could help ordinary readers identify around 70% of these scams by spotting red flags. Prevention through AI could detect recurring keywords like "guaranteed," "limited slots," and "processing fee." Policy implications emerged in the lack of recognition of linguistic deception as evidence. This pilot study illustrates how forensic linguistic analysis can generate actionable insights for awareness campaigns, technological detection, and policy design.

DISCUSSION

The unified conceptual framework highlights the need for interdisciplinary collaboration in combating scams. Linguists, technologists, policymakers, and educators each play a role in realising the framework. However, its implementation in Malaysia is not without challenges. One persistent issue is scammer adaptability. As Sharif et al. (2024) stated, scammers continually revise their discourse strategies, creating new narratives of legitimacy and urgency. This adaptability requires continuous research and real-time updating of linguistic databases and AI detection models.

The second challenge is linguistic diversity. Research shows that scammers exploit linguistic and cultural nuances across different communities, thereby complicating the effectiveness of monolingual detection models (Hamid et al., 2023; Coulthard et al., 2011). Malaysia's multilingual landscape means that scams may be crafted in Malay, English, Chinese, Tamil, or combinations of the languages. Detection systems trained on English-language datasets may fail to capture deception in other languages. This underscores the importance of developing localised linguistic datasets for scam detection and awareness initiatives.

The third challenge involves policy integration. While Malaysia has strong financial and technological regulations, the integration of linguistic elements into policy and legal frameworks remains limited. Scam is rarely prosecuted as a language crime in Malaysia, despite forensic linguistic evidence that deception operates primarily through discourse (Momeni, 2012; Juned et al., 2024). Policymakers must recognise that scam is not

only about financial misrepresentation but also about the deceptive use of language. This requires legal reforms that allow linguistic evidence to be admitted in courts and regulatory enforcement.

Despite these challenges, the proposed framework offers significant opportunities. Awareness campaigns grounded in forensic linguistic findings can empower citizens to resist scams. AI systems informed by linguistic insights can enhance detection capabilities. Policy alignment can strengthen prosecutions and prevention. Together, these efforts can build societal resilience against scams and contribute to Malaysia's broader digital governance goals.

Policy Implications

The framework carries several implications for Malaysian regulators and stakeholders. For regulators, the framework implies the need for forensic linguistics in investigative processes. Regulatory bodies such as the Securities Commission and Bank Negara could benefit from linguistic expertise to identify fraudulent discourse in financial promotions (Juned et al., 2024; Sharif et al., 2024). For the education sector, it underscores the importance of embedding scam awareness into digital literacy and financial literacy programs. As Hamid et al. (2023) showed, many scams succeed because persuasive rhetoric is left unchallenged. For technology providers, it calls for collaboration with linguists to develop linguistically informed AI detection tools. Previous studies confirm that stylometric and sentiment-based analysis can distinguish deceptive from truthful texts (Burgoon et al., 2003; Jakupov et al., 2024). For policymakers, it emphasises the need to update cybercrime legislation to explicitly recognise linguistic deception as prosecutable evidence. Collectively, these implications point to the necessity of an interdisciplinary approach that bridges language, technology, and governance.

To strengthen Malaysia's capacity to combat digital scams, legislative reforms should explicitly criminalise linguistic deception, such as unverifiable claims and manipulative urgency, while recognising forensic linguistic reports as admissible expert evidence in court. Regulatory agencies, particularly the Securities Commission and Bank Negara, can operationalise this approach by introducing red-flag linguistic checklists, mandating NLP based detection systems in banks, and equipping police units with basic linguistic detection training. At the societal level, nationwide multilingual awareness campaigns, the integration of scam literacy into school curricula, and the involvement of community organisations would cultivate resilience against deceptive discourse. These efforts must be complemented by the development of NLP detection tools trained on Malaysian multilingual data and supported by policies requiring digital platforms to share scam-related linguistic evidence with regulators. To ensure coordination, a National Anti-Scam Linguistics Taskforce comprising linguists, technologists, policymakers, and educators should be established, collectively repositioning Malaysia's governance from reactive financial enforcement to proactive, linguistically informed, and technologically driven prevention.

CONCLUSION

This paper has argued that scams are not only financial or technological crimes but also linguistic crimes which exploit the power of discourse to deceive and manipulate. By proposing a unified conceptual framework grounded in the four pillars of deceptive cues, awareness, prevention, and policy, the paper places language at the centre of scam prevention in Malaysia. While challenges such as scammer adaptability, linguistic diversity, and policy integration remain, the framework provides a roadmap for interdisciplinary collaboration. In due course, combating digital scams requires the convergence of language, technology, and governance. For Malaysia, adopting linguistically informed, AI-supported, and policy aligned approaches will be crucial for protecting citizens, strengthening trust in digital platforms, and ensuring resilience in the digital economy.

REFERENCES

1. Bank Negara Malaysia. (n.d.). Financial Consumer Alert List. https://www.bnm.gov.my
2. Burgoon, J. K., Blair, J. P., Qin, T., & Nunamaker, J. F. (2003). Detecting deception through linguistic analysis. Lecture Notes in Computer Science, 2665, 91–101. https://doi.org/10.1007/3-540-44853-5_7
3. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185, Budapest Convention). https://www.coe.int

4. European Union. (2016). General Data Protection Regulation (Regulation (EU) 2016/679). https://eur-lex.europa.eu
5. European Union. (2022). Digital Services Act (Regulation (EU) 2022/2065). https://eur-lex.europa.eu
6. Financial Action Task Force (FATF). (2020). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations. FATF/OECD. https://www.fatf-gafi.org
7. Hamid, A. A. A., Atan, M. A., Zaini, N., Norwahi, N. A., & Hisham, S. B. (2023). Analysis of persuasive strategies in cryptocurrency scams: A case study in Malaysia. International Journal of Academic Research in Business and Social Sciences, 13(6), 2136–2142. https://doi.org/10.6007/IJARBSS/v13-i6/17321
8. Jakupov, A., Longhi, J., & Zeddini, B. (2024). The language of deception: Applying findings on opinion spam to legal and forensic discourses. Languages, 9(1), 10. https://doi.org/10.3390/languages9010010
9. Juned, A. M., Aziz, A. A. A., Sharif, N. A. M., Shah, N. K. M., Yatim, A. I. A., & Fakhruddin, W. F. W. (2024). The language of lies: An analysis of deceptive linguistic cues on Malaysian investors' decision making. International Journal of Research and Innovation in Social Science, 8(10), 668–672. https://dx.doi.org/10.47772/IJRISS.2024.8100056
10. Malaysia. (1997). Computer Crimes Act 1997 (Act 563). Laws of Malaysia. International Law Book Services.
11. Malaysia. (1998). Communications and Multimedia Act 1998 (Act 588). Laws of Malaysia. International Law Book Services.
12. Malaysia. (2010). Personal Data Protection Act 2010 (Act 709). Laws of Malaysia. International Law Book Services.
13. Momeni, N. (2012). "Fraud in judicial system" as a language crime: Forensic linguistics approach. Theory and Practice in Language Studies, 2(6), 1263–1269. https://doi.org/10.4304/tpls.2.6.1263-1269
14. Organisation for Economic Co-operation and Development (OECD). (2016). OECD guidelines for consumer protection in e-commerce. OECD Publishing.
15. Securities Commission Malaysia. (2020). Annual Report 2020. https://www.sc.com.my
16. Securities Commission Malaysia. (2007). Capital Markets and Services Act 2007 (Act 671). https://www.sc.com.my
17. Sharif, N. A. M., Aziz, A. A. A., Juned, A. M., Yatim, A. I. A., Shah, N. K. M., & Fakhruddin, W. F. W. (2024). Unmasking deception: Linguistic cues patterns identification in promotional materials of illegal investment scams. International Journal of Research and Innovation in Social Science, 8(9), 817–823. https://doi.org/10.47772/IJRISS.2024.809070
18. United Nations. (2000). United Nations Convention against Transnational Organized Crime and the protocols thereto. United Nations Office on Drugs and Crime.