INTERNATIONAL JOURNAL OF DIGITAL RESEARCH
Conceptual Review Article

International Journal of Digital Research
www.ijdr.net
E-ISSN: 3033-179X
Volume 2; Issue 4; 2026, P.p. 31-43

Dark Web Linkages to Bank Fraud, Data Breaches, and Counterfeit Identity Trade in Sri Lanka: An Integrative Literature Review and Conceptual Framework

[1] Methmal H. K. R., [2] Geesara T. K., [3] Pabasara S.R.G.P., [4] Fernando H. Y. B., [5] Abeysekara S.S.K., [6] Wijesinghe W.V.V. & [7] Hapuarachchi H. A. D. T.

[1, 2, 4, 5, 6, 7] Applied Archaeology Department,
[3] Applied Media Technology Department,
Faculty of Humanities and Social Science, Nāgānanda International Institute for Buddhist Studies,
Manelwatta, Bollegala, Kelaniya, Sri Lanka
[1]ORCID ID: 0009-0000-4588-1241
Corresponding Author: Rusiru Methmal, E-mail: rusirumethmal0@gmail.com

https://doi.org/10.63711/ijdr.net20260402

ABSTRACT

This research paper examines possible connections between bank fraud, data breaches, and the trade in counterfeit identity documents in Sri Lanka and the broader Dark Web ecosystem. Drawing on Sri Lankan cybercrime scholarship, official institutional statements, and international Dark Web marketplace studies, it considers how stolen financial data and forged documents may circulate through anonymous online markets. Because directly verified Sri Lanka-specific marketplace evidence is limited, the analysis distinguishes documented local incidents from mechanisms inferred from international research. The article is an integrative literature review with a conceptual framework; no primary surveys, interviews, marketplace crawls, or new statistical analyses were conducted. Published research indicates that fraud-related goods are prominent within some cybercrime-oriented listings and may enable downstream fraud. The publicly disclosed 2025 Cargills Bank cybersecurity incident illustrates a local data-security risk, but does not establish any particular Dark Web transaction. Integrating routine-activity and rational-choice perspectives, the paper conceptualises data compromise, possible transnational intermediation, and downstream fraudulent reuse, and outlines priorities for prevention and future Sri Lanka-specific research.

Keywords: *Dark Web; Cybercrime; Sri Lanka; Bank fraud; Data breaches; Counterfeit identity documents; Integrative literature review; Conceptual framework*

Copyright © 2026 The Author(s). This article is licensed under CC BY 4.0.

INTRODUCTION

The Dark Web constitutes a portion of the internet that is deliberately hidden from conventional search engines and is typically accessed through anonymising networks such as Tor. Its architectural emphasis on privacy and untraceability has enabled both legitimate uses – for example, by journalists and dissidents operating under authoritarian regimes – and a parallel economy of illicit trade. Within this parallel economy, specialised marketplaces facilitate the sale of stolen financial credentials, personal data obtained from breaches, malware, and forged identity documents. International research consistently shows that these markets are resilient, adaptive, and increasingly professionalised.

Sri Lanka's rapid digitalisation of banking and public services has created new surfaces for cyber-enabled crime. Financial institutions continuously upgrade systems that handle monetary value and sensitive client information; this technological evolution simultaneously expands both opportunity and risk (Chamuddika & Ranaweera, 2021). Cybercrimes targeting the financial sector evolve in technique and impact in tandem with defensive technologies. Sri Lanka CERT reported receiving more than 12,650 complaints concerning social-media misuse and cybersecurity incidents in 2025; this figure aggregates several complaint categories and is not a count of bank fraud cases (Sri Lanka Computer Emergency Readiness Team, 2026). A January 2026 news report citing Sri Lanka Police described more than 2,000 cybercrime complaints and 318 arrests during 2025 (Daily Mirror, 2026). In March 2025, Cargills Bank disclosed a cybersecurity incident and stated that an unauthorised party had claimed to access and publish some of its data; the bank's public disclosure did not establish the volume or content of data involved or any subsequent Dark Web sales (Cargills Bank, 2025).

Despite these developments, the precise mechanisms linking Sri Lankan bank fraud, data breaches, and counterfeit identity trade to Dark Web marketplaces remain under-examined. Published Sri Lanka-specific measurements of illicit marketplace activity remain difficult to establish from the sources reviewed here. Local scholarship has concentrated primarily on the nature, techniques, and institutional responses to cybercrimes against financial institutions rather than on the anonymous marketplaces that may serve as conduits for stolen data and forged documents. This paper therefore seeks to bridge that gap by integrating selected international evidence on Dark Web markets with the Sri Lankan threat landscape and by proposing a coherent theoretical and methodological framework for future primary research.

The remainder of the paper is organised as follows. Sections 2 and 3 set out the research objectives and questions. Section 4 delineates the scope and limitations. Section 5 reviews the relevant literature. Section 6 elaborates the theoretical framework. Sections 7–9 describe the literature-based methodology, sources, and analytical approach. Section 10 discusses the evidence and its implications. Sections 11 and 12 offer conclusions, recommendations, and directions for future research, followed by the reference list.

RESEARCH OBJECTIVES

The study pursues four interrelated objectives:

1. To identify plausible mechanisms through which stolen financial data and forged identity documents associated with Sri Lankan victims or institutions might circulate within illicit online marketplaces.

© The Author(s) 2026 | Licensed under CC BY 4.0

2. To characterise the contemporary threat landscape facing Sri Lankan financial institutions and the documented patterns of bank fraud and data breaches.

3. To consider, as an agenda for future empirical testing, the motivational drivers – curiosity, privacy-seeking, and illicit acquisition – that may draw young adults (aged 18–30) into Dark Web spaces.

4. To propose an evidence-grounded theoretical framework that integrates routine activity theory and rational choice perspectives to explain the observed dynamics.

RESEARCH QUESTIONS

Corresponding to the objectives, the study addresses four research questions:

1. Through what plausible mechanisms might Sri Lankan bank fraud incidents and data breaches be connected to trading activity on Dark Web marketplaces?
2. What role do counterfeit identity documents play within this ecosystem, and how are they linked to local financial and identity fraud?
3. Which motivations identified in international research might warrant empirical examination among Sri Lankan young adults, particularly curiosity, privacy concerns, and potential interest in illicit items?
4. Which theoretical model or combination of models best explains the observed linkages between local cyber-enabled crime and international Dark Web markets?

SCOPE AND LIMITATIONS OF THE STUDY

The analytical scope of this literature-based paper is deliberately bounded. The literature synthesis draws primarily on peer-reviewed studies of Dark Web markets, stolen-data economies, and counterfeit document trade published between approximately 2016 and 2025, together with Sri Lankan criminological work on cybercrimes against financial institutions (principally Chamuddika & Ranaweera, 2021) and publicly available statements from Sri Lanka CERT, Cargills Bank, and reporting of Sri Lanka Police statistics. No structured questionnaire was finalised or administered; no interviews, direct marketplace observations, or primary survey responses were collected. The review is integrative and interpretive, not a reproducible systematic review or a statistical meta-analysis.

A central limitation must be stated with complete transparency: the sources reviewed here do not provide direct, independently verified measurements of Dark Web marketplace activity specifically attributable to Sri Lanka. Consequently, claims concerning market mechanics, product distributions, pricing, participant concentration, and ecosystem resilience are drawn from international crawls and analyses and applied to the Sri Lankan context by reasoned inference rather than by direct observation. No primary operational data from the Sri Lanka Police Cybercrime Unit or from classified intelligence holdings were available for this synthesis. Language diversity in existing marketplace studies is limited; Sinhala- and Tamil-language content, if present on Dark Web forums or markets, remains largely unexamined in the published literature. These constraints necessarily temper the strength of causal claims linking specific Sri Lankan incidents to particular Dark Web listings.

Ethical and practical considerations further shape the research design. Direct interaction with live Dark Web markets for data collection raises significant legal, safety, and ethical issues. The quantitative discussion therefore summarises previously published marketplace crawls rather than reanalysing underlying datasets or conducting new scraping. All discussion of criminal products

© The Author(s) 2026 | Licensed under CC BY 4.0

remains at a high level of abstraction; no operational guidance, vendor names, marketplace addresses, or transactional procedures are provided.

LITERATURE REVIEW

Dark Web Marketplaces: Structure and Evolution

Dark Web marketplaces are commercial platforms accessible primarily via anonymising networks such as Tor. Early markets such as Silk Road concentrated on narcotics; subsequent generations expanded product ranges to include weapons, malware, stolen credentials, and forged identity documents (ElBahrawy et al., 2020). Cryptocurrencies, including Bitcoin, are important payment mechanisms in many of the markets examined in the literature. Markets typically incorporate reputation systems, escrow services, and multi-factor authentication designed to reduce transactional risk for both buyers and sellers while simultaneously complicating external observation and law-enforcement disruption (Wang et al., 2025).

Empirical studies of marketplace dynamics reveal a pattern of resilience. When individual markets are closed – whether by law-enforcement action, exit scams, or technical failure – users migrate rapidly to coexisting platforms, often concentrating activity on the market that already commands the highest trading volume. Analysis of Bitcoin transaction networks across multiple closure episodes demonstrates that this coordinated migration restores trading volumes quickly and preserves the overall ecosystem (ElBahrawy et al., 2020). Subsequent work has identified "multihomers" – participants who operate across several markets simultaneously – as key agents of this resilience (dos Reis et al., 2024). Market closures arise from several causes, including policing and exit scams; documented migration patterns indicate adaptive capacity, although responses vary across markets and periods.

The Stolen-Data Economy and Fraud Products

Anonymous marketplaces function as a primary venue for the sale of tools and data obtained through breaches or other illicit means. Listings routinely include financial statements, credit-card details, cloned payment-card data, login credentials for banking and other services, and bulk dumps of personal records (Nazah et al., 2020; Saleem et al., 2022). A crawl-based analysis of eight marketplaces found fraud-related goods to be prominent within cybercrime product categories and reported relatively low average prices for cybercrime-related offerings; this should not be generalised to all Dark Web listings (Georgoulias et al., 2023). The low price point lowers barriers to entry for downstream offenders who may lack the technical skill to obtain the data themselves.

Stolen data enable a cascade of further crimes, including account takeover, identity fraud, extortion, and the fabrication of synthetic identities. Buyers may realise revenue through resale, although the larger economic returns typically accrue from direct fraudulent use (Holt et al., 2016). Bitcoin transaction-network research further identifies highly connected market participants whose activity is important to trading structures (dos Reis et al., 2024). These findings suggest that disruption of central actors warrants investigation, but do not by themselves quantify its effectiveness against fraud in Sri Lanka.

Counterfeit Identity Documents

Fraudulent identity documents remain a persistent feature of both open-web and Dark Web trade. Crime-script analyses of vendors advertising counterfeit documents reveal organisational practices that parallel those of other illicit online markets (Holt & Lee, 2022). A recent examination of two

© The Author(s) 2026 | Licensed under CC BY 4.0

major markets (White House Market and Empire Market) found that digital documents dominate listings; driver's licences from the United States and Australia were among the most frequently offered items, alongside broader identity packs (Devlin et al., 2024). Although the absolute volume of identity-document listings is smaller than that of narcotics or pure fraud products, the strategic value of authentic-looking identity credentials for enabling account opening, loan applications, and travel-related fraud is high.

The availability of digital identity packs is particularly relevant to jurisdictions that rely on multi-factor or points-based identity verification systems. Compromised or forged attributes may undermine identity-verification procedures, although their practical effects depend on the safeguards used. International studies underscore that the market is global; document categories and their availability can cross national boundaries, without implying that Sri Lankan documents were observed in the reviewed marketplaces.

The Sri Lankan Cybercrime Landscape

Sri Lankan scholarship on cybercrime against financial institutions remains limited but instructive. Chamuddika and Ranaweera (2021) examined trends across seven licensed commercial banks and documented the evolving nature, techniques, and institutional impacts of phishing, malware, denial-of-service, website defacement, and ransomware. The study emphasised that continuous technological upgrading in the banking sector simultaneously expands both the attack surface and the defensive repertoire required of institutions and customers.

Sri Lanka CERT reported receiving more than 12,650 complaints concerning social-media misuse and cybersecurity incidents in 2025, including reports of online scams and harassment (Sri Lanka Computer Emergency Readiness Team, 2026). This figure does not exclusively represent financial fraud and is not directly comparable with police arrest figures. Separately, a January 2026 news report citing the Sri Lanka Police stated that more than 2,000 cybercrime complaints were received in 2025 and that 318 people were arrested (Daily Mirror, 2026). Public advisories have also warned about impersonation, phishing, and other online financial fraud schemes. These data indicate continuing public concern, but differences in reporting systems preclude a simple claim of a single upward national trend.

High-profile incidents illustrate the sensitivity of banking information. In March 2025, Cargills Bank disclosed a cybersecurity incident; its subsequent notice said that an unauthorised party had claimed to access and publish some of the bank's data. The bank described measures taken to contain the incident and protect stakeholders (Cargills Bank, 2025). Reports attributing the incident to a named ransomware group or specifying a particular terabyte volume and document inventory should not be presented as independently established facts on the basis of the bank's statement. The incident demonstrates an exposure pathway, not proof that identified customer records were sold on a particular Dark Web market. Reports of cross-border scam operations involving Sri Lanka illustrate a related but distinct form of cyber-enabled crime; their connection to any particular marketplace also remains to be demonstrated.

Taken together, the literature establishes three propositions that frame the present study. First, Dark Web markets specialise in the efficient distribution of fraud-enabling products at accessible prices. Second, Sri Lankan financial institutions and their customers hold data that could have value if compromised and transferred to criminal markets. Third, the limited availability of verified local marketplace measurements constitutes both a research gap and a practical intelligence shortfall.

© The Author(s) 2026 | Licensed under CC BY 4.0

THEORETICAL FRAMEWORK

Two complementary criminological perspectives provide the conceptual scaffolding for this research: routine activity theory (Cohen & Felson, 1979) and rational choice theory (Cornish & Clarke, 1986).

Routine Activity Theory

Routine activity theory posits that crime occurs when a motivated offender converges in time and space with a suitable target in the absence of capable guardianship. Applied to the digital domain, the "space" of convergence is the online environment, including both surface-web banking portals and Dark Web marketplaces. Motivated offenders include both the initial breach actors and the secondary buyers of stolen data. Suitable targets encompass financial institutions with valuable data holdings and individual account holders whose credentials can be monetised. Guardianship may be technological (encryption, multi-factor authentication, anomaly detection), organisational (incident-response capacity, staff training), or social (public awareness and reporting norms). Regular, authorised penetration testing can complement technological guardianship by identifying exposed services and potential security weaknesses before they are exploited, thereby supporting preventive cybersecurity measures (Bibi, 2026).

Prior applications of routine activity theory to Dark Web financial markets illustrate its utility in organising patterns of fraud and scam activity (Jung et al., 2022). In the Sri Lankan context, growing reliance on digital banking may create additional opportunities if access controls, reporting, and institutional safeguards are insufficient; the relative strength of guardianship requires local measurement.

Rational Choice Perspectives

Rational choice approaches (Cornish & Clarke, 1986) emphasise the calculation of expected costs and benefits by potential offenders. In stolen-data markets, sellers and buyers weigh the probability of detection and sanction against the anticipated financial return and the relative ease of transaction. Cross-border offending is facilitated when offenders perceive that certain jurisdictions possess limited investigative tools or weak capacity for international cooperation (Smirnova & Holt, 2017). Restrictive deterrence strategies – efforts by offenders to minimise the likelihood or severity of detection – further shape market behaviour.

The low median prices observed for many fraud products (Georgoulias et al., 2023) and the documented resilience of markets after closures (ElBahrawy et al., 2020) are consistent with a rational-choice reading: the expected utility of participation remains positive for a sufficient number of actors even in the face of periodic disruption. For young adults, curiosity or privacy-seeking may be motivations for lawful exploration; neither motivation, nor the use of anonymity tools, is evidence of criminal intent. These possibilities require empirical investigation in Sri Lanka.

Integrated Framework

An integrated routine-activity and rational-choice framework is adopted here. Opportunity structures created by digitalisation and uneven guardianship generate the conditions under which motivated actors may encounter suitable targets. Within those conditions, participants evaluate perceived risks, costs, and potential gains in illicit data markets. The original conceptual contribution is a three-stage distinction between (1) local exposure or compromise of financial and identity data, (2) possible circulation by intermediaries through transnational online markets, and (3) downstream fraudulent reuse. Routine activity theory identifies opportunities and safeguards at each stage; rational

© The Author(s) 2026 | Licensed under CC BY 4.0

choice theory explains why actors may enter, leave, or move between stages. For Sri Lanka, this yields testable propositions: stronger guardianship should reduce initial compromise; perceived enforcement risk and transaction costs should influence illicit intermediation; and the availability of usable stolen credentials may facilitate downstream fraud. These are analytical propositions, not empirically tested causal findings about Sri Lanka.

RESEARCH METHODOLOGY

An integrative literature review with a conceptual synthesis was selected to address the research questions. The approach compares quantitative findings reported in published Dark Web marketplace studies with qualitative and crime-script scholarship and publicly available Sri Lankan incident information. It does not constitute an original mixed-methods empirical study: no primary questionnaire, interviews, marketplace crawl, or independently pooled statistical analysis was undertaken.

Quantitative Strand

The published quantitative evidence covers market-level findings – product-category distributions, pricing distributions, and measures of vendor concentration – drawn from published crawls of multiple Dark Web marketplaces (Georgoulias et al., 2023; Wang et al., 2025; related studies). Previously reported descriptive statistics help characterise fraud-related product offerings and prices in the sampled international markets. Previously reported network metrics, where available, inform discussion of concentration among marketplace participants; the underlying datasets were not independently reanalysed.

Qualitative Strand

The qualitative discussion draws on published studies of market content and vendor behaviour, including crime-script analyses to the procurement of counterfeit identity documents (Holt & Lee, 2022; Jung et al., 2022; Madarie, 2025). These publications describe recurrent sequences of actions, the roles of escrow and reputation systems, and strategies used by sellers; this paper did not conduct a new qualitative coding exercise.

Future Survey Research

A future survey of adults aged 18–30 in Sri Lanka could explore curiosity, privacy motivations, and potential interest in illicit acquisition, while carefully separating lawful use of anonymity tools from criminal behaviour. Relevant topics might include prior awareness of anonymity networks, reasons for exploring or avoiding Dark Web spaces, risk perceptions, and attitudes towards fraud. No questionnaire was finalised, administered, or validated for the present article, and no survey results are reported. Any subsequent instrument would require expert review, piloting, informed consent, privacy protections, and appropriate ethical approval. Thus, the young-adult dimension is a proposed direction for empirical research rather than an observed finding of this review.

DATA COLLECTION

Primary data collection from live Dark Web sources presents formidable obstacles. Marketplace administrators actively resist scraping, deploying CAPTCHAs, anti-phishing measures, multi-factor authentication, and other layered defences that both protect users and hinder external researchers

© The Author(s) 2026 | Licensed under CC BY 4.0

(ElBahrawy et al., 2020; Wang et al., 2025). Ethical guidelines and legal constraints further restrict direct interaction. Consequently, this review relies on previously published marketplace studies and related scholarship rather than original access to live markets or individual-level crime records.

For the Sri Lankan component, data sources include peer-reviewed local studies, a Sri Lanka CERT press release, Cargills Bank disclosures, and secondary reporting of police statistics. No classified or operational police data were accessed. No survey instrument was developed or fielded for this review; questionnaire design is identified only as a future research priority. Sources were assessed in an interpretive manner for relevance, provenance, and the limits of their claims, with emphasis on peer-reviewed studies and primary institutional statements. The review did not follow a preregistered or exhaustive search protocol. Reporting on police figures is explicitly identified as secondary media reporting; claims unsupported by primary documentation are treated cautiously.

EVIDENCE SYNTHESIS AND CONCEPTUAL ANALYSIS

The interpretive synthesis is organised in three stages. First, published descriptive statistics inform the discussion of marketplace product distribution and pricing. Fraud-related products are prominent within the cybercrime categories sampled, and average prices for cyber-crime offerings remain comparatively low (Georgoulias et al., 2023). Second, published thematic and crime-script research describes recurrent scam patterns, the roles of escrow systems, and the organisational features of identity-document markets (Jung et al., 2022; Holt & Lee, 2022). Third, published network analyses describe central participants and the resilience associated with user migration and multihoming (dos Reis et al., 2024; ElBahrawy et al., 2020). No original statistical analysis, content coding, or cross-study effect-size pooling was conducted.

Table 1 summarises selected analytical dimensions and findings reported in the reviewed literature:

Table 1. Summary of findings from cited studies and public reporting. International marketplace findings are not measurements of Sri Lankan market activity.

Analytical Dimension	Key Finding	Source
Product dominance	Fraud-related products prominent within cybercrime listings; relatively low average prices in sampled markets	Georgoulias et al., 2023
Seller concentration	Transaction networks include highly connected participants; estimates do not directly describe Sri Lanka	dos Reis et al., 2024
Market resilience	User migration after closures restores volume rapidly	ElBahrawy et al., 2020
Identity documents	Digital identity documents prominent in two markets studied; no Sri Lanka-specific transaction measured	Devlin et al., 2024

© The Author(s) 2026 | Licensed under CC BY 4.0

Sri Lankan exposure	CERT complaints, bank incident disclosure, and police figures reported by the media; no verified local market trace	Sri Lanka CERT, 2026; Cargills Bank, 2025; Daily Mirror, 2026; Chamuddika & Ranaweera, 2021

REVIEW FINDINGS AND DISCUSSION

Pathways Linking Local Incidents to Dark Web Markets

The reviewed international literature indicates that Dark Web marketplaces can act as channels through which stolen financial data and forged documents are offered for downstream fraud. Once credentials or identity attributes have been compromised – whether through phishing campaigns directed at bank customers, ransomware attacks on institutional systems, or other vectors – the resulting data packages acquire commercial value on anonymous markets. International evidence shows that fraud-related products are prominent within cybercrime-oriented listings and can be priced accessibly, thereby lowering the threshold for secondary offenders who may lack the technical capacity to generate the data themselves (Georgoulias et al., 2023; Nazah et al., 2020).

In the Sri Lankan setting, the 2025 Cargills Bank incident illustrates the potential sensitivity of compromised banking information. The bank publicly stated that an unauthorised actor claimed to access and publish some data and outlined mitigation steps (Cargills Bank, 2025). The specific data volume, document categories, and any subsequent sale on a Dark Web marketplace are not verified in the cited institutional notice. International research nevertheless identifies plausible pathways through which exposed credentials or identity attributes can move to criminal intermediaries and be reused in fraud. These pathways should be understood as hypotheses requiring locally sourced incident and marketplace evidence, not as proof of a transaction originating from Cargills Bank.

The Role of Counterfeit Identity Documents

Counterfeit and fraudulently obtained identity documents occupy a strategic niche within the broader ecosystem. Digital identity packs may facilitate fraudulent account opening or credit applications and may be used in attempts to evade know-your-customer controls. Studies of marketplace content confirm the persistent availability of such products and the predominance of digital formats (Devlin et al., 2024). For a jurisdiction such as Sri Lanka, where national identity cards and passports serve as foundational identity credentials, the compromise or forgery of these documents amplifies the risk of identity-enabled financial crime. The possibility of cross-border reuse is relevant, but no evidence reviewed here traces a specific Sri Lankan identity document through a particular transaction.

Motivations among Young Adults

International research and broader discussions of dark-web use distinguish curiosity, the desire for enhanced privacy, and interest in illicit items as possible motivations (Adel & Norouzifard, 2024; Raman et al., 2023). These motivations may overlap, but privacy-seeking and the use of anonymity technologies are not inherently unlawful. Young adults constitute a potentially useful population for future research because their experience with digital platforms may shape exposure and risk perception. No Sri Lankan participant data were gathered for this paper, so the prevalence of any motivation and its relationship to criminal behaviour cannot be estimated. A future questionnaire could examine these issues without presuming that exploration leads to illicit transactions.

© The Author(s) 2026 | Licensed under CC BY 4.0

Ecosystem Resilience and Implications for Disruption

A consistent finding across marketplace studies is systemic resilience. User migration after closures, the activity of multihomers, and the rapid recovery of trading volumes imply that disruption of individual platforms produces only temporary effects (ElBahrawy et al., 2020; dos Reis et al., 2024). Market closures have multiple causes, including enforcement operations and scams. Consequently, marketplace takedowns alone may not produce lasting reductions in the availability of fraud products; effectiveness depends on wider enforcement and market conditions. Targeting of elite sellers and buyers, improvement of guardianship at the point of data generation (financial institutions and individual users), and enhancement of cross-border investigative capacity emerge as complementary and potentially higher-leverage approaches.

The Local Intelligence Gap

The scarcity of directly verified Sri Lanka-specific marketplace measurements in the reviewed evidence is an important limitation. Research coverage of markets remains geographically and linguistically uneven (Marjanov & Hutchings, 2025). South Asian and Sinhala/Tamil-language activity may be under-observed, but its scale is presently unknown. Without local visibility, both academic understanding and operational intelligence remain incomplete. Closing this gap is a prerequisite for evidence-based policy and for the calibration of preventive interventions.

CONCLUSIONS AND RECOMMENDATIONS

This paper has examined the possible linkages between bank fraud, data breaches, and counterfeit identity trade in Sri Lanka and the Dark Web ecosystems that facilitate the circulation of stolen data and forged documents. The analysis rests on an integrative synthesis of international marketplace research and the available Sri Lankan evidence base. International studies show that anonymous marketplaces can facilitate the trade of fraud-enabling products. Sri Lankan institutions and individuals may face related exposure, but direct proof of particular local data-to-market pathways remains limited. The shortage of locally verified marketplace measurements is therefore both a research and an intelligence gap.

The integrated routine-activity and rational-choice framework offers a coherent lens through which to interpret these dynamics. Opportunity structures created by digitalisation and uneven guardianship intersect with rational calculations of risk and reward to suggest plausible patterns of supply, demand, and resilience. Its Sri Lanka-specific contribution is to distinguish data compromise, possible transnational intermediation, and downstream fraudulent reuse as separate stages whose opportunity conditions and offender incentives can be investigated independently. The framework remains a set of testable propositions, not a confirmed causal account.

On the basis of the synthesis, the following recommendations are advanced:

1. Enhance law-enforcement and intelligence capacity for the monitoring and analysis of financial marketplaces and stolen-data economies, with appropriate legal safeguards and ethical oversight.

2. Prioritise the development of anonymity-preserving research techniques and the recruitment of specialised analytical personnel capable of working with Dark Web data sources.

3. Strengthen cross-border collaboration with attention to mutual legal assistance, information sharing, and the balancing of investigative needs against civil-liberty protections.

© The Author(s) 2026 | Licensed under CC BY 4.0

4. Invest in public-awareness and consumer-safety programmes that reduce the suitability of individual targets and improve guardianship at the user level.

5. Encourage financial institutions to treat data-breach response and customer notification as integral components of operational resilience, and to coordinate closely with national CERT and police cyber units.

6. Support primary research that measures Sri Lanka-specific Dark Web activity, including content in local languages, and that develops and validates an appropriate motivational survey instrument for future use.

FUTURE DIRECTIONS

Several avenues for further research emerge from this study. First, primary measurement of Dark Web marketplace content and transaction patterns with a Sri Lankan focus is urgently needed. Such measurement should include systematic attention to Sinhala- and Tamil-language material and to any forums or markets that specialise in South Asian identity or financial products. Second, the psychological and social motivations that draw individuals toward illegal Dark Web activity warrant deeper investigation; findings can inform targeted prevention and intervention programmes (Raman et al., 2023). Third, the potential difference between data reportedly compromised in breaches and data actually observed for sale requires careful empirical examination (Marjanov & Hutchings, 2025). Fourth, longitudinal analysis of how key players and multihomers shape ecosystem resilience can guide the design of more durable disruption strategies (dos Reis et al., 2024). Finally, comparative research across South Asian jurisdictions would illuminate regional commonalities and differences in the pathways linking local cyber-enabled crime to global Dark Web markets.

Declaration by Authors

Ethical Approval: Not applicable

Acknowledgement: None

Source of Funding: No external funding. A one-time 100% APC waiver granted by decision of the Editorial Board of the International Journal of Digital Research.

Conflict of Interest: The authors declare no conflict of interests.

REFERENCES

Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the Dark Net: The question of detection and application. *Big Data and Cognitive Computing*, 8(8), Article 91. https://doi.org/10.3390/bdcc8080091

Bibi, I. (2026). The role of penetration testing in identifying cybersecurity vulnerabilities. *International Journal of Digital Research*, 2(3), 59–71. https://doi.org/10.63711/ijdr.net20260305

Cargills Bank. (2025, March 25). Update 2: Cyber security incident at Cargills Bank. https://www.cargillsbank.com/news/corporate/update-2-cyber-security-incident-at-cargills-bank/

© The Author(s) 2026 | Licensed under CC BY 4.0

Chamuddika, K. G. L., & Ranaweera, K. G. N. U. (2021). A criminological study on trends of cybercrimes against financial institutions in Sri Lanka. *International Journal of Information Security and Cybercrime*, 10(2), 81–88. https://doi.org/10.19107/IJISC.2021.02.08

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. https://doi.org/10.2307/2094589

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). The reasoning criminal: Rational choice perspectives on offending. *Springer-Verlag*.

Daily Mirror. (2026, January 24). 318 arrested over cybercrimes in Sri Lanka in 2025. https://www.dailymirror.lk/breaking-news/318-arrested-over-cybercrimes-in-Sri-Lanka-in-2025/108-331224

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Rossy, Q., & Morelato, M. (2024). Illuminating the dark web market of fraudulent identity documents and personal information: An international and Australian perspective. *Forensic Science International*, 363, Article 112203. https://doi.org/10.1016/j.forsciint.2024.112203

dos Reis, E. F., Teytelboym, A., ElBahrawy, A., de Loizaga, I., & Baronchelli, A. (2024). Identifying key players in dark web marketplaces through Bitcoin transaction networks. *Scientific Reports*, 14, Article 2385. https://doi.org/10.1038/s41598-023-50409-5

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific Reports*, 10, Article 18827. https://doi.org/10.1038/s41598-020-74416-y

Georgoulias, D., Yaben, R., & Vasilomanolakis, E. (2023). Cheaper than you thought? A dive into the darkweb market of cyber-crime products. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (ARES '23) (Article 106). Association for Computing Machinery. https://doi.org/10.1145/3600160.3605012

Holt, T. J., & Lee, J.-R. (2022). A crime script analysis of counterfeit identity document procurement online. *Deviant Behavior*, 43(3), 285–302. https://doi.org/10.1080/01639625.2020.1825915

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, 37(4), 353–367. https://doi.org/10.1080/01639625.2015.1026766

Jung, B.-R., Choi, K.-S., & Lee, C. S. (2022). Dynamics of dark web financial marketplaces: An exploratory study of underground fraud and scam business. *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(2), 4–24. https://doi.org/10.52306/XMHN2624

Madarie, D. R. (2025). Stolen data: Theft and trade [Doctoral dissertation, Vrije Universiteit Amsterdam]. https://doi.org/10.5463/thesis.1358

Marjanov, T., & Hutchings, A. (2025). SoK: Digging into the digital underworld of stolen data markets. In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE. https://doi.org/10.1109/SP61157.2025.00037

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: A systematic approach. *IEEE Access*, 8, 171796–171819. https://doi.org/10.1109/ACCESS.2020.3024198

© The Author(s) 2026 | Licensed under CC BY 4.0

Raman, R., Nair, V. K., Nedungadi, P., Ray, I., & Achuthan, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon*, 9(11), Article e22269. https://doi.org/10.1016/j.heliyon.2023.e22269

Saleem, J., Islam, R., & Kabir, M. A. (2022). The anonymity of the dark web: A survey. *IEEE Access*, 10, 33628–33660. https://doi.org/10.1109/ACCESS.2022.3161547

Smirnova, O., & Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist*, 61(11), 1403–1426. https://doi.org/10.1177/0002764217734270

Sri Lanka Computer Emergency Readiness Team. (2026, January 1). Sri Lanka CERT received over 12650 online incident complaints in 2025 and warns about an increase in online harassment and scams [Press release]. https://www.cert.gov.lk/wp-content/uploads/press_releases/English%20Press%20Release_01%20Jan%202026.pdf

Wang, Y., Arief, B., & Hernandez-Castro, J. (2025). Secure in the dark? An in-depth analysis of dark web markets security. *International Journal of Information Security*, 24, Article 107. https://doi.org/10.1007/s10207-025-01015-1

How to cite this article:

Methmal, H. K. R., Geesara, T. K., Pabasara, S. R. G. P., Fernando, H. Y. B., Abeysekara, S. S. K., Wijesinghe, W. V. V., & Hapuarachchi, H. A. D. T. (2026). Dark web linkages to bank fraud, data breaches, and counterfeit identity trade in Sri Lanka: An integrative literature review and conceptual framework. *International Journal of Digital Research*, 2(4), 31–43. https://doi.org/10.63711/ijdr.net20260402

*****

© The Author(s) 2026 | Licensed under CC BY 4.0