International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 10 October-2026 | Impact Factor: 3.5



Citizen-Facing Cybercrime Detection and Early Warning Systems: A Systematic Literature Review

Aakanksha Rathore, Sonal Yadav, Atul Agrawal

Department of Computer Science and Engineering, Oriental University, Indore (M.P.), India

How to Cite this Article:

Rathore, A., Yadav, S. & Agrawal, A. (2026). Citizen-Facing Cybercrime Detection and Early Warning Systems: A Systematic Literature Review. International Journal of Creative and Open Research in Engineering and Management, 02(10), 1-9. https://doi.org/10.55041/ijcope.v2i10.153

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.







https://doi.org/10.55041/ijcope.v2i10.153

ABSTRACT

Cybercrime increasingly targets individual citizens through phishing, smishing, and social-engineering scams, yet most published detection research is designed for enterprise Security Operations Centres rather than for ordinary end users. This paper presents a systematic literature review (SLR) of thirty peer-reviewed, Scopus- and IEEE-indexed studies published between 2022 and 2026, covering enterprise alert detection, citizen and smart-city scam protection, phishing and malicious-website detection, SMS smishing detection, large-language-model-based scam detection, financial fraud detection, adaptive and concept-drift-aware intrusion detection, and explainable artificial intelligence. Following the PRISMA methodology, records were identified, screened, and assessed for eligibility before thirty studies were included in the final synthesis. The review develops a thematic comparison of methods, datasets, and reported limitations, and visualises the distribution of studies by theme and publication year. The synthesis shows that while detection accuracy for individual cybercrime types is now very high, very few studies combine adaptive learning, real-time citizen-facing notification, and plain-language explanation into a single system. Seven specific research gaps are identified, and directions for future work on citizen-oriented, adaptive, and explainable cybercrime early-warning systems are proposed.

Keywords: Cybercrime detection; phishing; smishing; social engineering; adaptive learning; explainable artificial intelligence; systematic literature review; citizen cybersecurity

1. INTRODUCTION

Cybercrime has shifted from being primarily an organisational risk to being a daily threat faced by individual citizens. Phishing emails, fraudulent SMS messages, fake delivery or government notices, and voice-based social-engineering calls now cause widespread financial and emotional harm, and the people affected are often the least equipped to recognise the danger. A large body of machine-learning and deep-learning research has been published on cyber-threat detection over the last five years, producing strong results for phishing-website classification, intrusion detection, financial fraud detection, and related problems. However, this research is scattered across several independent sub-fields, and most of it is evaluated purely in terms of statistical accuracy on fixed benchmark datasets, with little attention paid to whether an ordinary citizen, rather than a trained security analyst, could use the resulting system in practice.

A systematic literature review is well suited to this situation because it allows the scattered contributions of enterprise-oriented intrusion detection, phishing and smishing detection, financial fraud detection, and explainable artificial intelligence to be brought together, compared on common ground, and examined for gaps that are not visible when each sub-field is read in isolation. The purpose of this review is threefold: first, to map the current state of the art in cybercrime detection research relevant to individual citizens; second, to compare the methods, datasets, and limitations reported across thirty recent studies; and third, to identify specific, evidence-based research gaps that can guide future work on citizen-facing, adaptive, and explainable cybercrime early-warning systems. The remainder of this paper is organised as follows. Section 2 describes the research methodology and the PRISMA-based study-selection process. Section 3 presents the thematic literature review. Section 4 reports a comparative analysis of the thirty included studies, supported



by summary visualisations. Section 5 identifies the research gaps. Section 6 discusses the overall findings, and Section 7 concludes the paper.

2. RESEARCH METHODOLOGY

This review follows a systematic, protocol-driven methodology, summarised in Figure 2, so that the selection of studies is transparent and can be repeated by other researchers.

2.1 Research Questions

The review was guided by four research questions: (RQ1) What machine-learning and deep-learning methods have been used for cybercrime detection relevant to individual citizens between 2022 and 2026? (RQ2) Which categories of citizen-facing cybercrime (phishing, smishing, financial fraud, and social engineering) have received the most and the least research attention? (RQ3) To what extent do existing systems address adaptability to new attack patterns and explainability of their decisions? (RQ4) What research gaps remain between enterprise-oriented cyber-threat detection and a genuinely citizen-facing early-warning system?

2.2 Search Strategy

Searches were carried out across major indexing platforms and publisher databases, including IEEE Xplore, MDPI, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar, using combinations of keywords such as "cybercrime detection", "phishing detection", "smishing", "social engineering detection", "credit card fraud detection", "intrusion detection concept drift", "explainable AI cybersecurity", and "large language model scam". The search was restricted to work published between 2022 and 2026 to keep the review focused on recent, methodologically current studies, and was supplemented by citation snowballing from the reference lists of initially retrieved papers.

2.3 Inclusion and Exclusion Criteria

A study was included if it (i) was published in a peer-reviewed journal or conference proceedings with a verifiable Digital Object Identifier, (ii) was indexed in Scopus or by IEEE, (iii) was published between 2022 and 2026, and (iv) addressed machine-learning or deep-learning-based detection of phishing, smishing, financial fraud, social engineering, or closely related intrusion-detection and explainability topics relevant to citizen-facing cybercrime. Studies were excluded if they lacked a verifiable DOI, fell outside the publication window, were not peer-reviewed, or were judged, after full-text reading, to be only marginally relevant to citizen-facing cybercrime detection.

2.4 Study Selection Process

Figure 1 presents the PRISMA flow diagram summarising the identification, screening, eligibility, and inclusion stages of the review. Database and citation searching identified an initial pool of records, which was reduced after duplicate removal and title/abstract screening. The remaining full-text articles were assessed against the inclusion and exclusion criteria above, and thirty studies were ultimately retained for data extraction and thematic synthesis.

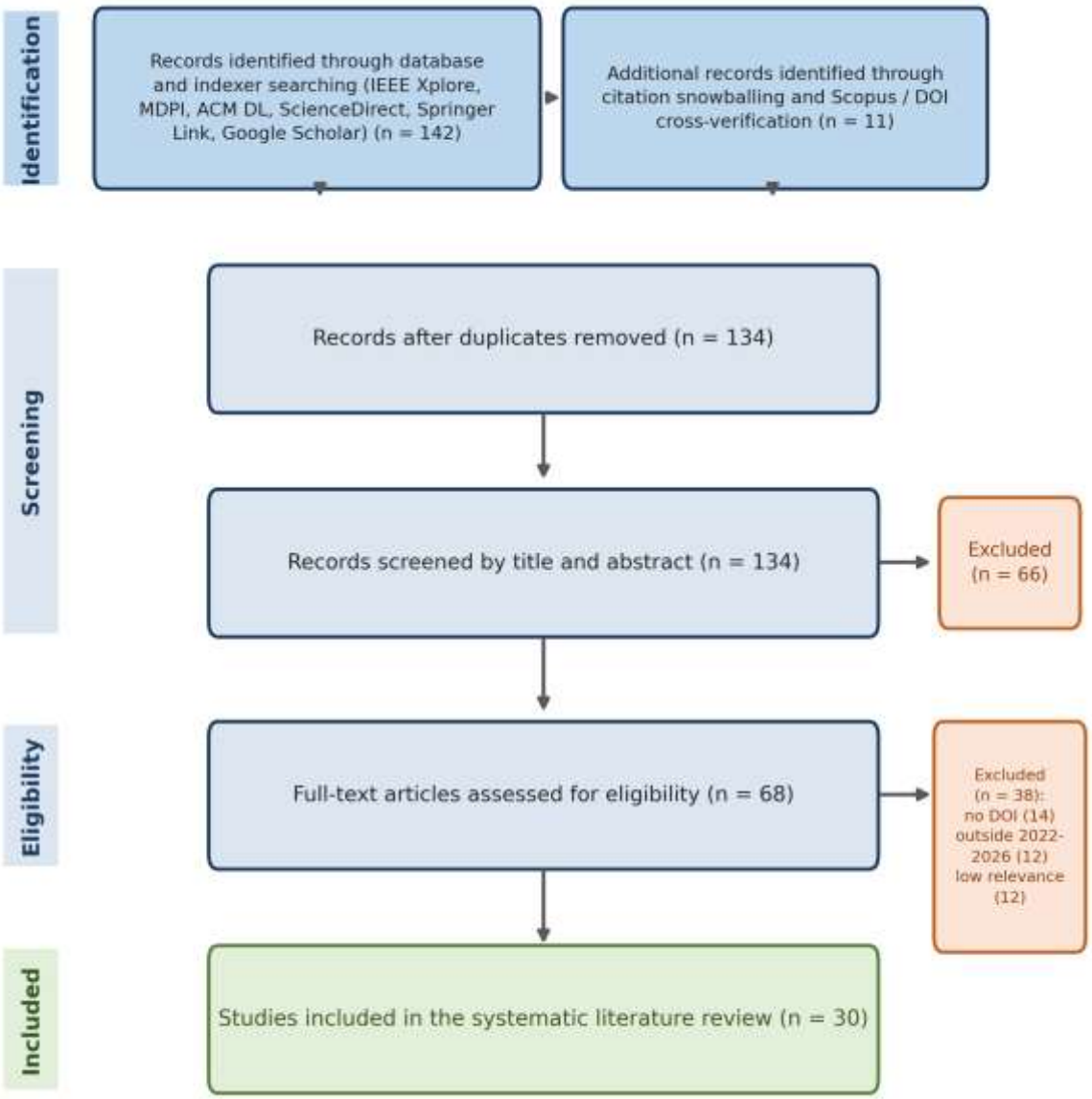


Figure 1: PRISMA Flow Diagram of the Study Selection Process



Figure 2: Research Methodology Adopted for the Systematic Literature Review



3. THEMATIC LITERATURE REVIEW

The thirty included studies were grouped into eight thematic categories, discussed below in the same order in which they are cited.

3.1 Base Enterprise Alert Detection Framework

Okafor and Lee [1] proposed an unsupervised-learning framework for cyber-threat detection, anomaly identification, and alert prioritisation for enterprise Security Operations Centres. Using density-based clustering (HDBSCAN) together with Isolation Forest anomaly detection on real honeypot-derived alert data, the framework produced a composite priority score that let analysts focus on the highest-risk alerts first. The study demonstrates that clustering and anomaly detection can transform a large, noisy alert stream into a small, ranked list of important items, but its entire design assumes a trained analyst and a technical dashboard.

3.2 Citizen and Smart-City Scam Protection

Ahmed et al. [2] proposed a honeybee-inspired, list-based filtering framework to protect smart-city citizens from phishing websites in real time. This is one of the few studies that centres the citizen rather than the enterprise, but its reliance on blacklists and simple symbol checks limits its ability to catch previously unseen scam patterns.

3.3 Phishing and Malicious-Website Detection

A mature body of work addresses phishing detection. Zieni et al. [3] and Do et al. [6] provide broad surveys showing the field's progression from blacklists to deep learning, while noting a persistent gap between high benchmark accuracy and real-world durability as attackers change tactics. Alsubaei et al. [4] and Alsaedi et al. [5] propose hybrid and multi-modal deep-learning classifiers that improve detection by combining several feature types. Alsuqayh et al. [7] combine feature engineering with SHAP-based explainability, directly supporting the case for interpretable phishing detection, while Liu et al. [8] apply a pre-trained language model with multi-level attention (PMANet) to malicious-URL detection, reflecting the field's recent shift toward language-aware deep learning.

3.4 SMS-Based Smishing Detection

Mehmood et al. [9] propose a CNN-LSTM architecture for classifying SMS messages as smishing or genuine, achieving high accuracy and low false positives. As with phishing detection, this model is trained and evaluated on a fixed dataset, with no mechanism described for adapting to new smishing wording over time.

3.5 Large-Language-Model-Based Scam and Social-Engineering Detection

Gupta et al. [10] and Roy et al. [11] document how generative artificial intelligence is simultaneously a growing threat, capable of producing highly convincing scam content, and a potential defensive tool. Wei et al. [12] survey scam detection across online social platforms, Yang et al. [13] propose Fraud-BERT for fraud-specific text classification, and Rathod et al. [14] provide a broad survey of social-engineering attacks that explicitly calls for detection tools combined with user education, a direction highly relevant to citizen-facing early-warning design.

3.6 Financial and Credit-Card Fraud Detection

This theme offers mature methodological lessons in handling severe class imbalance. Alarfaj et al. [15] and Mienye and Sun [16] show that deep-learning and ensemble methods with resampling substantially outperform traditional classifiers on imbalanced fraud data, while Mienye and Jere [17] review the field and note a lack of attention to evolving fraud patterns. Aurna et al. [18] propose a federated-learning approach (FedFusion) that preserves privacy across institutions, Alarfaji and Shahzadi [19] use graph neural networks and autoencoders to detect coordinated fraud rings, and Venčkauskas et al. [20] apply similar graph-based reasoning to money-laundering detection over blockchain transactions.

3.7 Adaptive and Concept-Drift-Aware Intrusion Detection

This theme provides the technical foundation for adaptability. Wahab [21] and Prasath et al. [22] demonstrate online and continual-learning techniques that allow intrusion-detection models to absorb new attack patterns without full retraining or catastrophic forgetting. Wu et al. [23] and Jo and Kim [24] show that transformer-based architectures



generalise well across network and vehicle-traffic domains, Oyinloye et al. [25] address class imbalance in threat detection, He et al. [26] propose an efficient two-stage detection design, and Ferrag et al. [27] demonstrate a lightweight, privacy-preserving language model suitable for resource-constrained IoT devices.

3.8 Explainable Artificial Intelligence and Ransomware Detection

Capuano et al. [28] and Rjoub et al. [29] survey explainable AI in cybersecurity and both conclude that existing explanation techniques remain designed for expert analysts rather than ordinary end users. Ispahany et al. [30] review machine-learning-based ransomware detection and identify dataset staleness and unrealistic evaluation conditions as recurring methodological weaknesses, concerns that echo across the phishing and fraud-detection literature discussed above.

4. COMPARATIVE ANALYSIS OF REVIEWED STUDIES

Table 1 summarises the method, main contribution, and principal limitation reported in each of the thirty included studies, enabling direct comparison across thematic categories.

Table 1: Comparative Summary of the Thirty Reviewed Studies

#	Author(s), Year	Method / Technique	Key Contribution	Principal Limitation
1	Okafor & Lee (2026)	HDBSCAN + Isolation Forest clustering/anomaly detection	Alert-prioritisation framework for SOC; high precision/recall on injected threats	Enterprise-only; no citizen interface or notification
2	Ahmed et al. (2023)	Rule-based blacklist/whitelist + symbol checking	Real-time phishing URL filtering for smart-city citizens	No machine learning; cannot catch unseen/zero-day scams
3	Zieni et al. (2023)	Survey	Taxonomy of phishing-website detection techniques	Highlights accuracy-vs-real-world gap; proposes no new model
4	Alsubaei et al. (2024)	Hybrid deep learning	Improved phishing detection for cybercrime forensics	Generalisability across domains not tested
5	Alsaedi et al. (2024)	Multi-modal CNN	Combines visual and URL features for malicious-website detection	Higher computational cost than single-feature models
6	Do et al. (2022)	Survey / taxonomy	Organises phishing detection into feature, similarity, and DL categories	Notes persistent zero-day phishing gap
7	Alsuqayh et al. (2024)	Hybrid features + SHAP	Explainable phishing detection with feature-level reasoning	Explanation is technical, not citizen-friendly
8	Liu et al. (2025)	Pre-trained LM + multi-level attention (PMANet)	Malicious-URL detection via deep language understanding	High compute cost; benchmark-only evaluation
9	Mehmood et al. (2024)	CNN-LSTM	SMS smishing detection with low false-positive rate	Static model; no concept-drift handling
10	Gupta et al. (2023)	Conceptual overview	Describes GenAI's dual role as cyber-threat and defence tool	No empirical detection model proposed



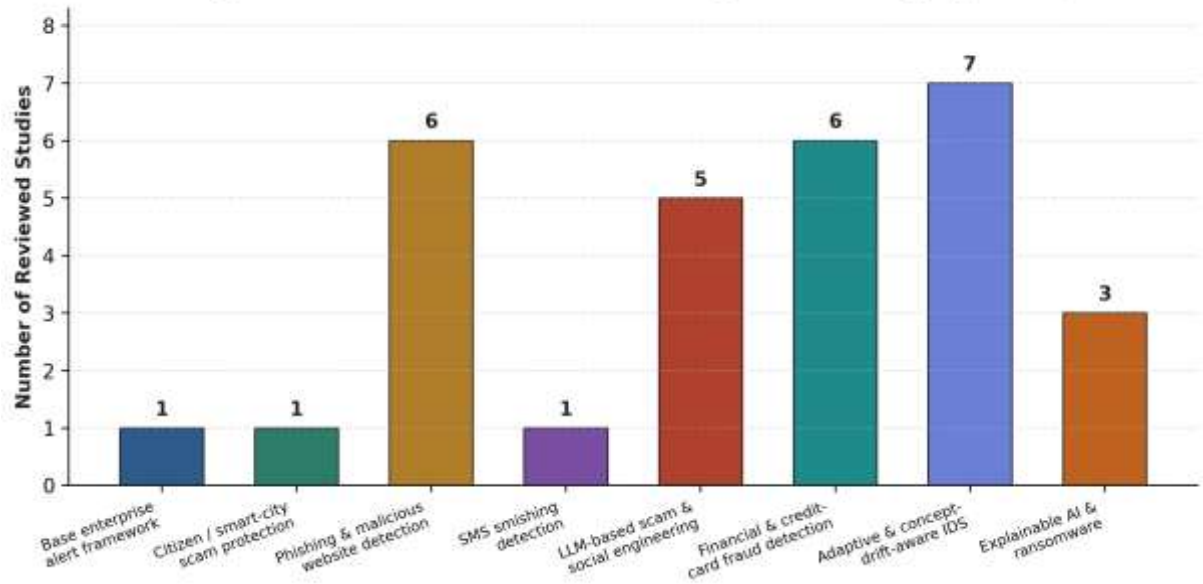
#	Author(s), Year	Method / Technique	Key Contribution	Principal Limitation
11	Roy et al. (2024)	Empirical LLM jailbreak study	Shows commercial LLMs can generate phishing scam content	Focused on attack generation, not defence
12	Wei et al. (2023)	Survey / taxonomy	Scam detection across social platforms by type and signal	Treats individual scam types in isolation
13	Yang et al. (2022)	Fraud-BERT (fine-tuned language model)	Outperforms feature-based fraud classifiers on text	Needs domain-specific fine-tuning per dataset
14	Rathod et al. (2025)	Survey	Broad coverage of social-engineering attack types	Calls for detection + education tools; none proposed
15	Alarfaj et al. (2022)	ML / DL comparison	Benchmarks classifiers on credit-card fraud with imbalance handling	Enterprise / bank-side only
16	Mienye & Sun (2023)	Ensemble DL + resampling	Improved minority-class (fraud) detection	No adaptability to evolving fraud patterns
17	Mienye & Jere (2024)	Review	Summarises DL algorithms for credit-card fraud detection	Notes lack of concept-drift testing in literature
18	Aurna et al. (2024)	Federated learning (FedFusion)	Privacy-preserving multi-bank fraud-model fusion	Added system complexity and coordination overhead
19	Alarfaji & Shahzadi (2025)	Graph neural network + autoencoder	Detects fraud rings via transaction-graph structure	Requires rich relational/graph data
20	Venčkauskas et al. (2025)	ML on blockchain transaction graphs	Money-laundering detection via wallet transaction flow	Domain-specific to cryptocurrency transactions
21	Wahab (2022)	Online deep learning + PCA drift detection	Adaptive IDS for IoT under concept drift	Tested on network data only, not text/scam data
22	Prasath et al. (2022)	Continual-learning comparison	Reduces catastrophic forgetting in intrusion detection	Still enterprise-network focused
23	Wu et al. (2022)	Transformer (RTIDS)	Robust intrusion detection via attention mechanism	High model complexity for resource-limited devices
24	Jo & Kim (2024)	Transformer (vehicle CAN bus)	Generalises transformer IDS to vehicle networks	Domain-specific to automotive CAN traffic
25	Oyinloye et al. (2025)	Improved ANN training	Corrects class-imbalance effects in threat detection	Small-scale evaluation dataset
26	He et al. (2024)	Two-stage deep learning	Efficient internal-threat detection (filter then analyse)	Insider-threat focus, not external citizen scams
27	Ferrag et al. (2024)	Lightweight BERT	Privacy-preserving on-device threat detection for IoT	Limited to IoT / IIoT device contexts

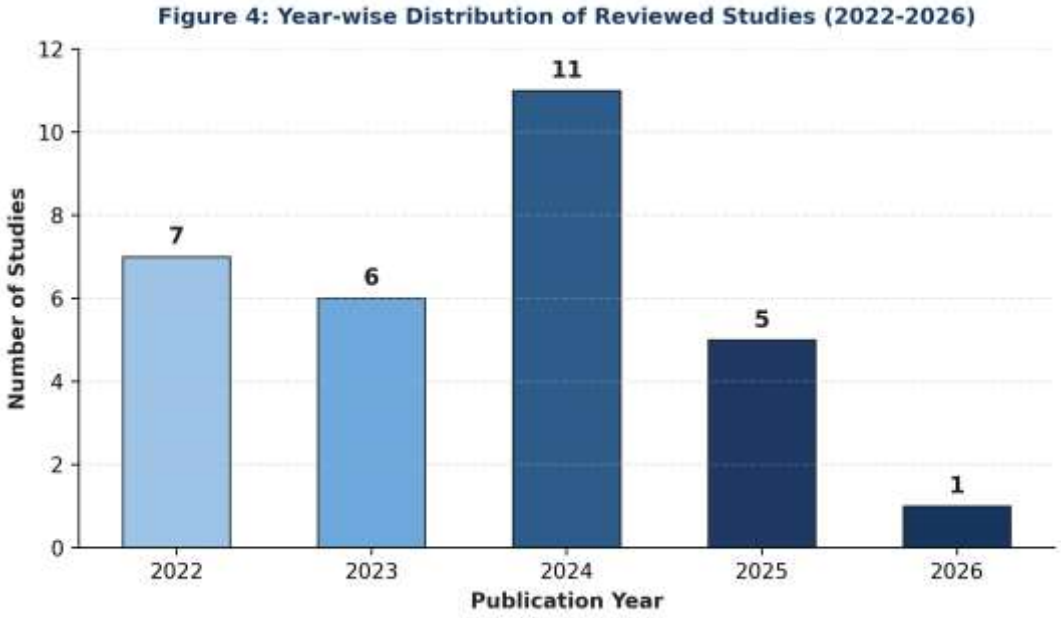


#	Author(s), Year	Method / Technique	Key Contribution	Principal Limitation
28	Capuano et al. (2022)	Survey	Maps explainable-AI techniques across cybersecurity tasks	Explanations remain expert-oriented
29	Rjoub et al. (2023)	Survey	Broader XAI-for-cybersecurity discussion; trust focus	Same expert-oriented limitation noted
30	Ispahany et al. (2024)	Review	Catalogues ransomware-detection research limitations	Dataset staleness; unrealistic evaluation highlighted

Figures 3 and 4 visualise the distribution of the included studies by thematic category and by publication year. As Figure 3 shows, adaptive and concept-drift-aware intrusion detection (seven studies) and financial and phishing-related detection (six studies each) are the most heavily represented themes, while citizen-facing scam protection and SMS smishing detection are each represented by only a single study, underlining how little direct attention the citizen-facing angle has received relative to enterprise- and finance-oriented detection. Figure 4 shows that more than half of the included studies were published in 2024 or later, confirming that the reviewed literature reflects current, methodologically up-to-date research rather than older work.

Figure 3: Distribution of Reviewed Studies by Thematic Category (N = 30)





5. RESEARCH GAPS

Based on the thematic review and comparative analysis above, seven specific research gaps are identified.

Gap 1: Enterprise-centred design. The majority of reviewed detection and alert-prioritisation frameworks, including the most comprehensive one [1], assume a trained analyst and a technical dashboard rather than an ordinary citizen.

Gap 2: Fragmented, single-purpose detectors. Phishing [3]-[8], smishing [9], and social-engineering detection [10]-[14] are studied largely in isolation, with no reviewed system unifying more than one of these citizen-facing channels.

Gap 3: Limited concept-drift handling outside enterprise networks. Adaptive and continual-learning techniques are well developed for intrusion detection [21], [22] but have not been meaningfully applied to phishing, smishing, or scam-message detection, despite scam wording changing rapidly, partly due to generative-AI-assisted attacks [10], [11].

Gap 4: Explainability designed for experts, not citizens. Where explainability has been applied [7], [28], [29], it remains oriented toward technical, feature-level reasoning rather than plain-language explanation suitable for a non-technical citizen.

Gap 5: No real-time, citizen-facing notification layer. Enterprise-oriented systems output to an analyst dashboard [1]; no reviewed citizen-oriented system [2], [9] describes a comparable real-time alerting mechanism.

Gap 6: Class imbalance well handled in finance, largely ignored for scam messages. Mature imbalance-handling techniques from the fraud-detection literature [15], [16] are rarely discussed in phishing or smishing-detection papers, despite the same underlying data characteristic.

Gap 7: Lack of locally relevant citizen-scam data. Almost all reviewed datasets are international and English-language in origin; very few studies consider region-specific scam patterns such as local courier, government-scheme, or digital-payment scams.

6. DISCUSSION

Taken together, the thirty reviewed studies show that the cybersecurity research community already possesses the individual technical components needed for a citizen-facing, adaptive, and explainable cybercrime early-warning system: strong clustering and anomaly-detection pipelines [1], mature phishing- and smishing-detection models [3]-[9], adaptive and continual-learning techniques [21], [22], and an emerging, if still expert-oriented, body of explainable-AI research [7], [28], [29]. What is missing is not a new detection algorithm but the integration of these components around the citizen as the end user, with adaptability to evolving scam patterns and plain-language explanation built in from the start, rather than treated as a separate research problem. This observation motivates a conceptual direction, consistent



with the gaps identified in Section 5, in which future citizen-facing systems reuse validated enterprise-grade detection cores while adding dedicated adaptation, notification, and explanation layers designed specifically for non-expert users.

7. CONCLUSION

This systematic literature review examined thirty recent, peer-reviewed studies on cybercrime detection relevant to individual citizens, spanning enterprise alert detection, phishing and smishing detection, large-language-model-based scam detection, financial fraud detection, adaptive intrusion detection, and explainable artificial intelligence. The review found that while detection accuracy is already high across most individual cybercrime categories, very few studies address the citizen directly, almost none combine adaptive learning with real-time notification and plain-language explanation, and explainability research remains oriented toward expert analysts. Seven specific research gaps were identified, pointing toward a clear and largely unoccupied research direction: a citizen-facing, adaptive, and explainable cybercrime early-warning system built on the strong technical foundation already established by enterprise-oriented research. Future work should focus on integrating these components and evaluating the resulting systems not only on detection accuracy but also on real-world usability for non-expert citizens.

REFERENCES

[1] E. Okafor and S. Lee, “Unsupervised Learning Framework for Cyber Threat Detection, Anomaly Identification, and Alert Prioritization,” Appl. Sci., vol. 16, no. 4, p. 1884, Feb. 2026, doi: 10.3390/app16041884.

[2] A. A. Ahmed, A. Al-Bayatti, M. Saif, W. A. Jabbar, and T. H. Rassem, “A Honeybee-Inspired Framework for a Smart City Free of Internet Scams,” Sensors, vol. 23, no. 9, p. 4284, 2023, doi: 10.3390/s23094284.

[3] R. Zieni, L. Massari, and M. C. Calzarossa, “Phishing or Not Phishing? A Survey on the Detection of Phishing Websites,” IEEE Access, vol. 11, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

[4] F. S. Alsubaei, A. A. Almazroi, and N. Ayub, “Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics,” IEEE Access, vol. 12, pp. 8373–8389, 2024, doi: 10.1109/ACCESS.2024.3351946.

[5] M. Alsaedi, F. A. Ghaleb, F. Saeed, J. Ahmad, and M. Alasli, “Multi-Modal Features Representation-Based Convolutional Neural Network Model for Malicious Website Detection,” IEEE Access, vol. 12, pp. 7271–7284, 2024, doi: 10.1109/ACCESS.2023.3348071.

[6] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, “Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions,” IEEE Access, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903.

[7] N. Alsuqayh, A. Mirza, and A. Alhogail, “A Phishing Website Detection System Based on Hybrid Feature Engineering with SHAP Explainable Artificial Intelligence Technique,” in Web Information Systems Engineering – WISE 2024 PhD Symposium, Demos and Workshops, Lecture Notes in Computer Science, 2024, pp. 3–17, doi: 10.1007/978-981-96-1483-7_1.

[8] R. Liu et al., “PMANet: Malicious URL Detection via Post-Trained Language Model Guided Multi-Level Feature Attention Network,” Inf. Fusion, vol. 105, p. 102638, 2025, doi: 10.1016/j.inffus.2024.102638.

[9] M. K. Mehmood, H. Arshad, M. Alawida, and A. Mehmood, “Enhancing Smishing Detection: A Deep Learning Approach for Improved Accuracy and Reduced False Positives,” IEEE Access, vol. 12, pp. 137176–137193, 2024, doi: 10.1109/ACCESS.2024.3463871.

[10] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, “From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy,” IEEE Access, vol. 11, pp. 80218–80245, 2023, doi: 10.1109/ACCESS.2023.3300381.

[11] S. S. Roy, P. Thota, K. V. Naragam, and S. Nilizadeh, “From Chatbots to Phishbots?: Phishing Scam Generation in Commercial Large Language Models,” in Proc. IEEE Symp. Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 36–54, doi: 10.1109/SP54263.2024.00182.

[12] M. Wei, Q. Zhang, Y. Sun, and R. Xu, “A Survey on Scam Detection in Online Social Platforms: Taxonomy, Methods, and Challenges,” ACM Comput. Surv., vol. 55, no. 7, pp. 1–36, 2023, doi: 10.1145/3576847.

[13] Y. Yang, Z. Lin, and F.-T. Li, “Fraud-BERT: A Pretrained Language Model for Fraud Detection,” IEEE Trans. Knowl. Data Eng., vol. 34, no. 9, pp. 4525–4537, 2022, doi: 10.1109/TKDE.2021.3054580.



[14] T. Rathod, N. K. Jadav, S. Tanwar, A. Alabdulatif, D. Garg, and A. Singh, "A Comprehensive Survey on Social Engineering Attacks, Countermeasures, Case Study, and Research Challenges," Inf. Process. Manag., vol. 62, no. 1, p. 103928, 2025, doi: 10.1016/j.ipm.2024.103928.
[15] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.
[16] I. D. Mienye and Y. Sun, "A Deep Learning Ensemble with Data Resampling for Credit Card Fraud Detection," IEEE Access, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.
[17] I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," IEEE Access, vol. 12, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.
[18] N. F. Aurna, M. D. Hossain, L. Khan, Y. Taenaka, and Y. Kadobayashi, "FedFusion: Adaptive Model Fusion for Addressing Feature Discrepancies in Federated Credit Card Fraud Detection," IEEE Access, vol. 12, pp. 136962–136978, 2024, doi: 10.1109/ACCESS.2024.3464333.
[19] F. K. Alarfaji and S. Shahzadi, "Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," IEEE Access, vol. 13, pp. 20633–20646, 2025, doi: 10.1109/ACCESS.2024.3466288.
[20] A. Venčkauskas, Š. Grigaliūnas, L. Pocius, R. Brūzgienė, and A. Romanovs, "Machine Learning in Money Laundering Detection Over Blockchain Technology," IEEE Access, vol. 13, pp. 7555–7573, 2025, doi: 10.1109/ACCESS.2024.3452003.
[21] O. A. Wahab, "Intrusion Detection in the IoT Under Data and Concept Drifts: Online Deep Learning Approach," IEEE Internet Things J., vol. 9, no. 20, pp. 19706–19716, Oct. 2022, doi: 10.1109/JIOT.2022.3167005.
[22] S. Prasath, K. Sethi, D. Mohanty, P. Bera, and S. R. Samantaray, "Analysis of Continual Learning Models for Intrusion Detection System," IEEE Access, vol. 10, pp. 121444–121464, 2022, doi: 10.1109/ACCESS.2022.3222715.
[23] Z. Wu, H. Zhang, P. Wang, and Z. Sun, "RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System," IEEE Access, vol. 10, pp. 64375–64387, 2022, doi: 10.1109/ACCESS.2022.3182333.
[24] H. Jo and D. H. Kim, "Intrusion Detection Using Transformer in Controller Area Network," IEEE Access, vol. 12, pp. 121932–121946, 2024, doi: 10.1109/ACCESS.2024.3452634.
[25] T. S. Oyinloye, M. O. Arowolo, and R. Prasad, "Enhancing Cyber Threat Detection with an Improved Artificial Neural Network Model," Data Sci. Manag., vol. 8, no. 1, pp. 107–115, 2025, doi: 10.1016/j.dsm.2024.05.002.
[26] D. He, X. Lv, X. Xu, S. Chan, and K.-K. R. Choo, "Double-Layer Detection of Internal Threat in Enterprise Systems Based on Deep Learning," IEEE Trans. Inf. Forensics Security, vol. 19, pp. 4741–4751, 2024, doi: 10.1109/TIFS.2024.3372771.
[27] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, and N. S. Thandi, "Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices," IEEE Access, vol. 12, pp. 23733–23750, 2024, doi: 10.1109/ACCESS.2024.3363469.
[28] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in Cybersecurity: A Survey," IEEE Access, vol. 10, pp. 93575–93600, 2022, doi: 10.1109/ACCESS.2022.3204171.
[29] G. Rjoub, J. Bentahar, O. A. Wahab, et al., "A Survey on Explainable Artificial Intelligence for Cybersecurity," IEEE Trans. Netw. Serv. Manag., early access, 2023, doi: 10.1109/TNSM.2023.3282740.
[30] J. Ispahany, M. R. Islam, M. Z. Islam, and M. A. Khan, "Ransomware Detection Using Machine Learning: A Review, Research Limitations and Future Directions," IEEE Access, vol. 12, pp. 68785–68813, 2024, doi: 10.1109/ACCESS.2024.3397921.