Review of Applied Science and Technology

Volume: *13;* ***Issue:*** *5*
Pages: *01– 33*

Graph-Based Anomaly Detection for Secure Digital Lending: A Systematic Review

Hasinur Rahman[1]; MD Fardous[2];

[1]. Banking, Credit-Risk & Digital-Banking Researcher;
Former Principal Officer, Special Asset Management Division, Union Bank Limited, Bangladesh;
Master of Arts in English Language & Literature, Dhaka International University, Bangladesh;
Email: rahmanhasinur10@gmail.com

[2]. Data Analytics, Cybersecurity & Financial Systems Researcher;
Master of Business Studies in Accounting, National University, Bangladesh;
Email: fardous01@gmail.com

Doi: 10.63125/fgqb6m82
Received: *11 February 2023;* ***Revised:*** *18 March 2023;* ***Accepted:*** *13 April 2023;* ***Published:*** *02 May 2023;*

Abstract

Digital-lending platforms face escalating risks from fragmented borrower identities, coordinated applications, inconsistent records, and fraudulent relationships that conventional record-level screening may overlook. This study investigates the potential of graph-based anomaly detection to strengthen data integrity and financial security, compare detection architectures, and identify implementation constraints. Grounded in Graph Theory, the research adopts a PRISMA-guided, qualitative cross-sectional, documentary multiple-case systematic literature review rather than a quantitative enterprise survey. Its intended sample comprises 90 eligible peer-reviewed publications, although completed screening and final inclusion totals remain unverified. The case contexts include peer-to-peer lending, consumer automobile loans, digital credit payments, banking transaction networks, and Indonesian lending practices, not cloud enterprises. Key analytical variables include graph topology, relational consistency, fraud indicators, heterogeneous and temporal representations, classification performance, privacy, explainability, and scalability. The analysis combines structured evidence extraction, thematic synthesis, cross-case comparison, study-specific performance metrics, and provisional five-point hypothesis assessments; no original regressions or pooled meta-analytic estimates were generated. Performance findings derive from individual source publications and are not directly comparable across lending and payment contexts because labels and validation procedures differ. Published peer-to-peer lending research covering 34,816 users and 8,066,153 graph edges reported an F1-score of 0.832, recall of 0.951, and AUC of 0.835 for graph-attentive FDNE, compared with 0.786, 0.856, and 0.823 for its graph-convolutional baseline. In a separate automobile-lending experiment using a 12,000-sample training condition, a role-aware model achieved 85.56% F1 and 95.50% recall against 79.07% and 84.80% for its comparator. Provisional evidence ratings were 4/5 for relational detection, coordinated fraud identification, and implementation constraints, but 3/5 for integrity validation and heterogeneous or temporal superiority. These findings suggest graph methods can expose complex links yet cannot alone prove fraud or ensure record accuracy. Financial institutions should combine relational alerts with verified labels, contextual investigation, transparent audit trails, and privacy protections before operational deployment.

Keywords

Graph-Based Anomaly Detection; Digital Lending; Data Integrity; Financial Fraud Detection; Graph Neural Networks.

Introduction

Digital lending refers to the provision, assessment, approval, and administration of credit through digital platforms that connect borrowers, lenders, financial intermediaries, and technology-enabled service providers. These platforms rely on electronically collected information, automated credit assessments, digital identities, financial transaction records, and interconnected databases to support lending decisions. Graph-based anomaly detection refers to the identification of unusual entities, relationships, or structural patterns within networks represented by nodes and edges. In digital-lending systems, nodes may represent borrowers, lenders, financial accounts, devices, applications, and transactions, while edges describe the relationships connecting these entities. The combination of digital lending and relational anomaly detection has attracted academic attention because lending decisions increasingly involve information generated through multiple interconnected sources. Marketplace Lending (pp. 1939–1982) examines how technology-driven lending platforms organize credit transactions and information production, while research on peer-to-peer lending explains the changing relationships between traditional financial intermediaries and online credit markets (Tang, 2019; Vallée & Zeng, 2019). The expansion of fintech lending has also been associated with changes in financial intermediation, regulatory structures, and institutional participation in credit markets (Buchak et al., 2018). Studies investigating borrower appearance, social relationships, and information asymmetry demonstrate that online lending decisions can incorporate signals extending beyond conventional financial statements and credit histories (Duarte et al., 2012; Lin et al., 2013). Research on borrower screening and social-network information further identifies the importance of assessing the quality and reliability of information exchanged through lending platforms (Freedman & Jin, 2017; Iyer et al., 2016). Consumer Credit-Risk Models via Machine-Learning Algorithms (pp. 2767–2787) examines computational approaches to credit-risk assessment, while comparative credit-scoring research documents the methodological diversity of automated lending decisions (Khandani et al., 2010; Lessmann et al., 2015). Additional investigations of digital footprints and alternative financial information demonstrate how borrower assessment extends into digitally generated behavioral and transactional data (Berg et al., 2020; Jagtiani & Lemieux, 2019). These developments establish the international relevance of interconnected information structures within digital-lending operations, where the identification of trustworthy relationships, unusual data patterns, and potentially fraudulent activities constitutes a distinct research concern.

Data integrity in digital-lending systems concerns the accuracy, completeness, consistency, validity, and reliability of information used throughout the lending process. These attributes are particularly important when borrower records, identification credentials, account details, application histories, and transaction information are generated or exchanged across multiple technological systems. Financial security encompasses the detection and management of unauthorized activities, fraudulent transactions, identity misuse, and other threats that compromise the confidentiality, integrity, or availability of financial information and services. Although credit-risk assessment evaluates the likelihood of repayment failure, fraud detection investigates potentially deceptive behavior, making these analytically distinct problems within digital lending. Methodologies for Data Quality Assessment and Improvement establishes a systematic understanding of data-quality dimensions and assessment procedures, providing a foundation for examining the reliability of information processed in technology-dependent environments (Batini et al., 2009). Financial fraud research identifies the diversity of fraudulent activities and the methodological challenges associated with detecting irregular behavior in electronic financial systems (Abdallah et al., 2016; Ngai et al., 2011). Conventional detection approaches frequently analyze transaction amounts, customer characteristics, behavioral histories, and other observable record-level attributes. Comparative investigations of credit card fraud detection demonstrate the importance of selecting appropriate classification methods, while transaction aggregation research shows that suspicious behavior may become more visible when individual financial events are examined within broader activity histories (Bhattacharyya et al., 2011; Whitrow et al., 2009). Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection (pp. 317–331) investigates the integration of different learning strategies for identifying irregular financial transactions, illustrating the methodological significance of information beyond directly labeled fraud examples (Carcillo et al., 2021). Network-oriented studies extend this perspective by examining

relationships among financial entities. APATE: A Novel Approach for Automated Credit Card Transaction Fraud Detection Using Network-Based Extensions (pp. 38–48) demonstrates how relational information can supplement conventional transaction characteristics in fraud detection (Vlasselaer et al., 2015). Related research on social-security fraud examines how network structures can reveal suspicious connections among individuals and organizations that may remain less visible through isolated-record examination (Vlasselaer et al., 2017). Within digital lending, these findings establish a clear distinction between detecting unusual relational patterns, identifying fraudulent behavior, and independently verifying the integrity of financial records.

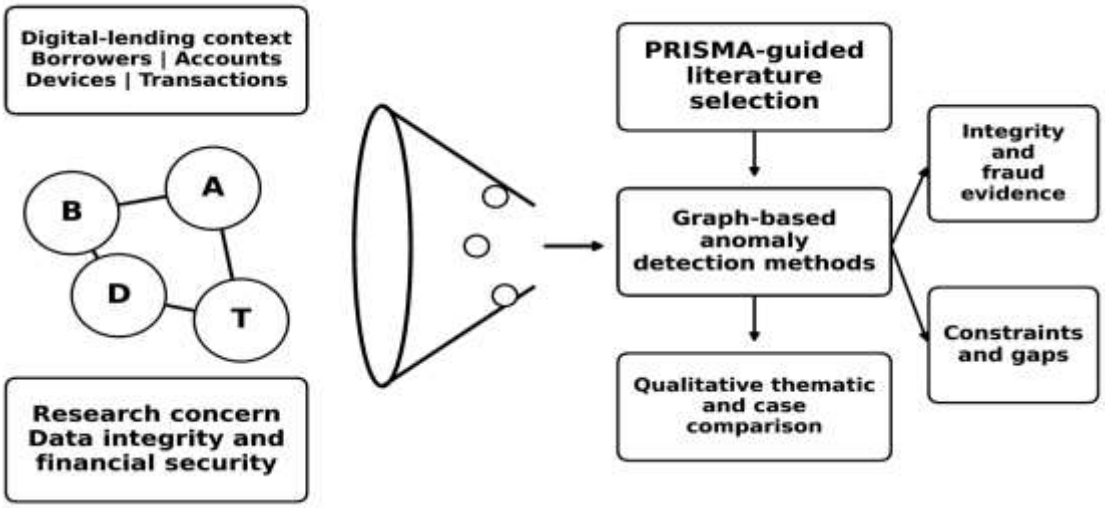
Graph Theory provides a mathematical foundation for examining interconnected systems by representing entities as vertices and their relationships as edges. This representation supports the investigation of connectivity, relational similarity, network communities, structural irregularities, and changes in interaction patterns. Within graph-based anomaly detection, unusual behavior may appear as an abnormal node, an unexpected relationship, an irregular group of connected entities, or a deviation from established network behavior. General anomaly detection research explains the methodological distinction between identifying deviations from normal patterns and assigning observations to predefined categories (Chandola et al., 2009). Graph Based Anomaly Detection and Description: A Survey (pp. 626–688) systematically examines techniques for detecting and characterizing irregular graph structures, including approaches concerned with nodes, edges, subgraphs, and broader network behavior (Akoglu et al., 2015). Earlier work on weighted graphs demonstrates how unusual relationships between structural properties can distinguish anomalous entities from ordinary network participants (Akoglu et al., 2010). Research on fraudulent online auction participants also establishes that deceptive activities can involve coordinated relationships among multiple accounts, highlighting the relevance of relational patterns in digitally mediated transactions (Chau et al., 2006). The temporal dimension introduces additional complexity because financial relationships and transaction networks change as users interact, create accounts, submit applications, and conduct transactions. Studies reviewing dynamic-network anomaly detection identify the analytical importance of evolving connectivity and network behavior (Ranshous et al., 2015). SpotLight: Detecting Anomalies in Streaming Graphs (pp. 1378–1386) investigates the detection of unusual structures in continuously developing graphs, while dynamic network embedding research examines how changing relationships can be represented for anomaly identification (Eswaran et al., 2018; Yu et al., 2018). Attributed network approaches introduce additional information by combining graph structure with characteristics associated with individual entities. Residual-based analysis investigates discrepancies between observed attributes and relationally informed expectations, while deep anomaly detection examines the joint modeling of network connections and node attributes (Ding et al., 2019; Li et al., 2017). Research addressing camouflage in fraudulent networks further demonstrates that suspicious participants may manipulate their apparent connections to resemble legitimate users, complicating the interpretation of relational evidence (Hooi et al., 2016). Together, these established analytical categories describe the theoretical foundations through which borrower networks, shared devices, transaction relationships, and interconnected lending records can be examined as graph-structured information.

Graph-based machine learning extends conventional network analysis by learning representations of entities and their relationships from structured financial information. Graph neural networks constitute a major category of these methods because they integrate node characteristics and information obtained from neighboring entities through graph-based computational operations. A Comprehensive Survey on Graph Neural Networks (pp. 4–24) presents the fundamental architectures and learning mechanisms of graph neural networks, while a complementary review describes graph convolution, attention, and related methods for representing complex relational dependencies (Pan, et al., 2021; Zhou et al., 2020). These methodological developments are particularly relevant to financial systems in which fraudulent behavior may involve coordinated participants, shared identifiers, repeated interactions, and interconnected account activities. A Semi-Supervised Graph Attentive Network for Financial Fraud Detection (pp. 598–607) investigates how multiple views of financial relationships and limited labeled observations can be incorporated into graph-based fraud identification (Wang et al., 2019). More directly, A Graph Attentive Network Model for P2P Lending Fraud Detection (pp. 316–

327) examines borrower relationships and textual information through a graph-attention architecture designed for online lending environments (Wang et al., 2020). The latter study is especially relevant because it investigates relational information within a peer-to-peer lending context rather than relying exclusively on evidence from general banking or payment systems. Other investigations address the difficulties created by deceptive graph structures and misleading neighborhood information. Research on camouflaged fraudsters examines how graph neural network fraud detectors can be affected by manipulated relationships, while work on inconsistent graph neighborhoods evaluates limitations associated with learning from connections involving potentially deceptive entities (Dou et al., 2020; Liu et al., 2020). Studies of imbalanced graph learning also examine the methodological problem arising when fraudulent observations constitute a relatively small proportion of available financial records (Liu et al., 2021). Fraud Detection: A Systematic Literature Review of Graph-Based Anomaly Detection Approaches identifies the diversity of graph-based fraud detection methods and organizes their applications within an established evidence-synthesis framework (Pourhabibi et al., 2020). Across these investigations, the reported evidence includes traditional network analytics, graph representation learning, attention mechanisms, and hybrid approaches, with differences in data characteristics, fraud definitions, labeling procedures, and evaluation settings. Such methodological variation is central to comparing graph-based detection capabilities in digital lending without treating experimental findings from distinct financial environments as directly interchangeable.

The international significance of graph-based anomaly detection in digital lending arises from the intersection of technology-mediated credit provision, interconnected financial information, and the need to distinguish legitimate activities from potentially deceptive relational patterns. Published investigations cover peer-to-peer lending, consumer credit, financial transaction networks, online payment systems, and related fraud detection environments, creating an evidence base that spans multiple institutional settings and technological architectures (Berg et al., 2020; Wang et al., 2019). Nevertheless, differences between lending-specific studies and research conducted in adjacent financial domains require careful consideration because a technique evaluated on a payment network does not necessarily establish equivalent effectiveness in a loan application system. The interpretation of graph-based findings also depends on how researchers define anomalies, construct relationships, establish comparison methods, and assess reported detection outcomes (Akoglu et al., 2015; Pourhabibi et al., 2020). Explainability introduces a further analytical dimension because financial institutions must distinguish between an algorithmically identified suspicious pattern and a defensible explanation of the relationships associated with that classification. Explainable Artificial Intelligence: Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI (pp. 82–115) establishes conceptual categories for explaining algorithmic behavior, while Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead (pp. 206–215) examines the importance of interpretability in consequential decision-making environments (Arrieta et al., 2020; Rudin, 2019). The existing literature consequently comprises interconnected but distinct lines of inquiry concerning graph structure, fraud identification, financial data quality, lending decisions, methodological transparency, and security governance. Systematic literature review methodology provides procedures for organizing and critically examining such heterogeneous scholarly evidence through documented research questions, transparent study selection, and structured synthesis (Snyder, 2019). The PRISMA 2020 Statement establishes reporting requirements for identifying, screening, excluding, and including studies within a systematic review, providing a transparent basis for documenting the reviewed literature (Page et al., 2021). Accordingly, the present research is organized as a PRISMA-guided qualitative systematic literature review with a target corpus of 90 eligible published studies, incorporating cross-sectional literature assessment and comparative analysis of documented digital-lending cases. The investigation addresses graph-based anomaly detection techniques, relational data integrity concerns, fraud and security applications, methodological comparisons, and implementation challenges through thematic evidence synthesis. Graph Theory provides the theoretical foundation for examining the interconnected relationships represented within the reviewed studies, while the study's research questions and evidence-based hypotheses establish the analytical boundaries for interpreting their findings.

Figure 1: Overview of Graph-Based Anomaly Detection in Digital Lending



Digital-lending systems have transformed financial service delivery by integrating automated credit assessment, digital identity verification, electronic transactions, and interconnected borrower information into technology-driven lending processes. These systems depend on extensive financial records and relational data, creating complex security and data integrity challenges involving fraudulent applications, identity manipulation, suspicious account relationships, and coordinated financial misconduct. Graph-based anomaly detection provides a relational approach to identifying irregular patterns by examining connections among borrowers, accounts, devices, transactions, and lending platforms. The growing academic interest in graph analytics and financial fraud detection has established a substantial body of research examining various techniques for identifying anomalous financial relationships. Within this context, the present study systematically examines published evidence concerning graph-based anomaly detection, data integrity, and security in digital-lending environments through a PRISMA-guided qualitative literature review.

Digital-lending systems encounter significant challenges in identifying fraudulent relationships, maintaining reliable financial information, and detecting security-related anomalies across interconnected databases and transaction networks. Conventional anomaly detection approaches frequently emphasize individual records or isolated transactional characteristics, limiting their ability to identify coordinated fraud, suspicious relational structures, and inconsistencies distributed across multiple financial entities. Although existing research has investigated graph-based anomaly detection methods in banking, financial transactions, and online lending, the evidence remains dispersed across different technological approaches, application environments, and evaluation procedures. Furthermore, methodological differences, limited explainability, privacy concerns, and inconsistent graph representations complicate the interpretation of reported detection capabilities. The absence of a sufficiently integrated synthesis specifically connecting graph-based anomaly detection with digital-lending data integrity and security establishes the central research problem addressed through this systematic literature review.

The primary objective of this research is to systematically investigate and synthesize existing scholarly evidence concerning the application of graph-based anomaly detection techniques to data integrity and security challenges in digital-lending systems. Specifically, the study seeks to identify and classify relevant graph-based detection approaches, examine their reported contributions to identifying relational inconsistencies and suspicious financial activities, and evaluate their applications in detecting coordinated fraud and security-related anomalies. Additionally, the research aims to compare the documented capabilities and methodological limitations of traditional graph analytics, graph neural networks, and other relational detection techniques. Through a PRISMA-guided systematic review targeting 90 eligible published studies, the research incorporates qualitative thematic analysis, cross-

sectional literature assessment, and comparative examination of documented financial and digital-lending cases. The investigation also evaluates the existing evidence concerning scalability, explainability, privacy, data quality, and implementation challenges within digital-lending environments.

RQ1: What graph-based anomaly detection techniques have been investigated in digital-lending and related financial systems?

RQ2: How does existing research explain the contribution of graph-based anomaly detection to data integrity, fraud identification, and security in digital-lending systems?

RQ3: What comparative advantages, methodological limitations, and implementation challenges emerge from the published evidence on graph-based anomaly detection across digital-lending environments?

The research hypotheses are developed from Graph Theory and the conceptual relationships connecting graph-based anomaly detection, relational data integrity, financial fraud identification, and digital-lending security. Five hypotheses guide the systematic evaluation of published evidence. The first proposes that graph-based anomaly detection offers advantages over conventional nonrelational approaches in identifying interconnected financial anomalies. The second concerns the contribution of graph-based methods to recognizing suspicious data relationships and potential integrity violations. The third examines their role in identifying coordinated financial fraud and security-related anomalies. The fourth addresses the comparative capabilities of heterogeneous and temporal graph-based approaches in detecting complex financial irregularities. The fifth concerns the constraints imposed by data quality, computational scalability, explainability, privacy, and adversarial security challenges. These hypotheses are assessed through structured qualitative evidence synthesis rather than original experimental testing or statistical inference.

H1: Published evidence indicates that graph-based anomaly detection provides advantages over conventional nonrelational approaches in identifying interconnected financial anomalies.

H2: Graph-based anomaly detection contributes to identifying relational inconsistencies and suspicious data patterns relevant to digital-lending data integrity.

H3: Graph-based anomaly detection supports the identification of coordinated fraud and security-related anomalies within interconnected digital-lending and financial environments.

H4: Heterogeneous and temporal graph-based detection methods demonstrate advantages over simpler graph representations in identifying complex and evolving financial anomalies under comparable evaluation conditions.

H5: Data quality, scalability, explainability, privacy, and adversarial security challenges constrain the practical implementation of graph-based anomaly detection in digital-lending systems.

(i) Theoretical Significance: The research strengthens the conceptual understanding of graph-based anomaly detection by applying Graph Theory to the interconnected relationships among financial entities, lending records, and suspicious transactional activities. It establishes a structured relationship between graph representations, relational anomaly identification, data integrity concerns, and digital-lending security.

(ii) Methodological Significance: The study provides a systematic examination of existing graph-based anomaly detection research through PRISMA-guided literature selection, qualitative thematic synthesis, and comparative case-based evidence assessment. It establishes a transparent approach for evaluating the methodological characteristics, reported findings, and limitations of published studies without introducing artificial experimental data or unsupported statistical conclusions.

(iii) Practical Significance: The research provides an organized understanding of the reported capabilities and limitations of graph-based detection methods for digital-lending institutions, financial technology developers, cybersecurity professionals, and financial risk managers. It addresses the identification of suspicious borrower relationships, coordinated fraudulent activities, irregular financial information, and challenges associated with implementing relational security monitoring systems.

(iv) Academic Significance: The study consolidates dispersed scholarly evidence concerning graph-based anomaly detection, financial fraud identification, data integrity, and digital-lending security. By distinguishing direct lending-specific findings from transferable evidence obtained in related financial

environments, it provides an integrated assessment of established research findings, methodological disagreements, and gaps in the existing literature.

The paper has been organized into eight sections. Following the Introduction, the Literature Review has examined digital-lending vulnerabilities, graph-based methods, relational integrity, financial fraud, Graph Theory, and the conceptual framework. The Method has specified PRISMA-guided documentary evidence procedures. Results and Findings have reported preliminary thematic comparisons and seven evidence tables. The Discussion has interpreted the hypotheses and proposed the IEHT-GAD framework. The remaining sections have presented the Conclusion, Recommendations, and Limitations of the Study, followed by the References.

Background and Conceptual Framework

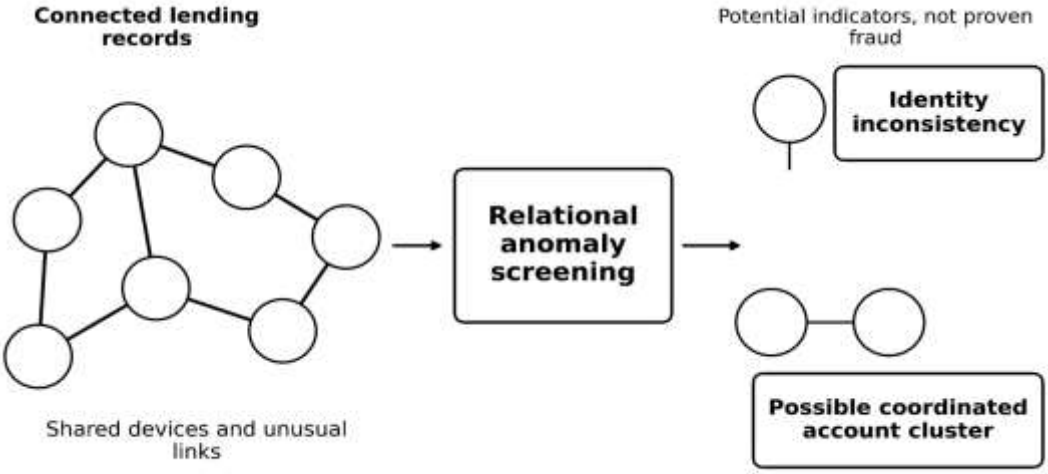
This literature review examines the theoretical and empirical foundations of graph-based anomaly detection in digital-lending systems. It first discusses security vulnerabilities arising from interconnected borrower records, digital identities, transactions, and financial accounts. It then evaluates graph-based techniques for identifying unusual relationships, data inconsistencies, coordinated fraud, and security-related anomalies. Graph Theory provides the theoretical foundation for explaining how nodes, edges, and network structures represent suspicious financial interactions. The review also develops a conceptual framework connecting detection capabilities with data integrity and lending security. Evidence from related financial settings is distinguished from findings obtained directly within digital-lending environments and applications.

Digital-lending systems are platforms where borrowers, lenders, and platform operators exchange information to originate, assess, fund, and administer loans. Their operations connect application forms, identity credentials, repayment histories, credit assessments, accounts, and third-party data services. Security vulnerabilities therefore arise not only from unauthorized access but also from uncertainty about whether information supplied by different participants is accurate, complete, and mutually consistent. How Signaling and Search Costs Affect Information Asymmetry in P2P Lending (Article 19) explains how information technologies change the collection and interpretation of borrower signals while leaving meaningful informational differences between market participants (Yan et al., 2015). Platform design determines who can submit information, which records can be independently checked, and how risk disclosures reach prospective lenders. These arrangements create several points at which misleading claims, incomplete histories, or compromised credentials can influence a lending decision. The Promise and Perils of Alternative Market-Based Finance (pp. 395–409) situates United Kingdom lending platforms within regulatory debates about intermediation, consumer protection, interconnectedness, and financial risk (Bavoso, 2020). Vulnerabilities are not identical: a weak borrower assessment may produce a credit loss, whereas deceptive platform conduct or improper handling of identifying information raises different integrity and security concerns. The Failure of Chinese Peer-to-Peer Lending Platforms (Article 101852) associates platform survival with financial soundness and disclosure quality, also documenting cases in which operators absconded with investor funds (He & Li, 2021). Across settings, the reliability of digital lending depends on relationships among borrowers, platforms, records, and oversight arrangements rather than on isolated loan entries alone.

Information reliability constitutes a central vulnerability because digital lenders may receive both verifiable records and self-reported statements concerning income, assets, employment, identity, and intended loan use. These elements differ in provenance, evidentiary strength, and susceptibility to manipulation. Soft Information in Online Peer-to-Peer Lending (Article 100873) shows that borrower descriptions and personal characteristics affect funding outcomes, while verification of certain soft factors does not necessarily predict repayment (Wang et al., 2019). This distinction matters because persuasive application content is not equivalent to independently confirmed financial data. A platform that combines several information sources must also reconcile inconsistent names, addresses, telephone numbers, device identifiers, and account connections without assuming that every mismatch indicates malicious behavior. Safety Promise, Moral Hazard and Financial Supervision (pp. 1–5) links platform guarantees and incomplete disclosure to weakened borrower screening and distorted credit ratings in online lending (Zhu, 2018). Information asymmetry may also originate within the platform itself rather than exclusively with borrowers. Competition and Distortion (pp. 1140–1154) develops a theoretical

account of how competitive conditions and investor expectations can create incentives for biased platform reporting (Hu, et al., 2021). Such institutional incentives complicate the interpretation of authoritative records. Information Disclosure and the Default Risk of Online Peer-to-Peer Lending Platform (Article 101509) reports an association between greater platform disclosure, particularly audit information, and lower platform default risk in a Chinese sample (Wang et al., 2021). Collectively, these studies distinguish inaccurate data, selective disclosure, misrepresented risk, and confirmed fraud, which require different evidentiary standards when evaluating financial security vulnerabilities.

Figure 2: Relational Security Vulnerabilities in Digital-Lending Records



Security vulnerabilities extend from informational uncertainty to the collection, storage, access, and sharing of sensitive data in lending. Lending applications may request identification documents, contact details, financial histories, and access to information held on personal devices. Record integrity concerns correctness and protection against unauthorized alteration, whereas privacy concerns whether personal information is accessed or disclosed appropriately. The Fintech Phenomenon: Protection of Consumer Privacy Data in Online Lending (pp. 185–194) examines borrower information theft, unauthorized disclosure, and harmful online lending practices in Indonesia (Saimima & Patria, 2021). Digital-lending vulnerabilities also involve organizational controls and the verification practices used during registration, credit appraisal, approval, and debt collection. Peer to Peer Lending Problems and Potential Solutions (pp. 204–214) identifies information asymmetry, borrower assessment, moral hazard, investment decisions, and policy limitations among recurring challenges documented in the literature (Suryono et al., 2019). Evidence from platforms reveals how such problems intersect with unauthorized operators and harmful data practices. Detection of Fintech P2P Lending Issues in Indonesia (Article e06782) identifies themes involving data leakage, restricted data access, personal-data fraud, unlawful platforms, and problematic marketing practices (Aditya & Ahmed, 2022; Suryono et al., 2021). These findings describe vulnerabilities at borrower, platform, and institutional levels without equating every case of default or poor disclosure with a cyberattack. For graph-based anomaly detection, this distinction is essential because shared devices, repeated identifiers, suspicious payment connections, and conflicting application records are relational indicators requiring careful contextual investigation, not automatic confirmation of wrongdoing. The reviewed lending contexts thus establish categories for analyzing data integrity and security.

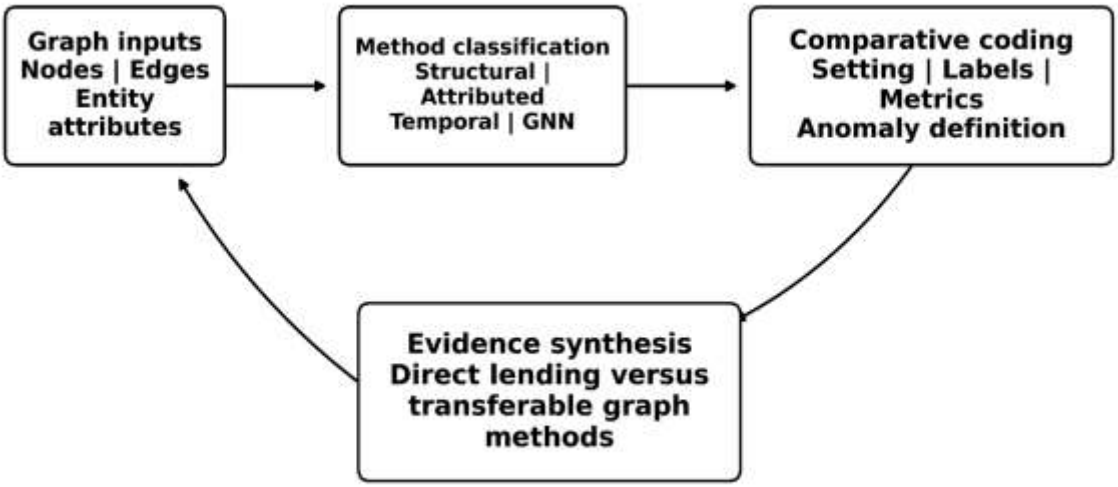
Mechanisms and outcome domains

Graph-based anomaly detection identifies unusual patterns in networks of connected entities rather than isolated records. In digital lending, vertices can represent applicants, bank accounts, devices, addresses, or loan applications, while edges represent shared identifiers, financial transfers, and other documented relationships. Anomaly Detection in Data Represented as Graphs (pp. 663–689) describes a foundational method based on minimum description length, which detects unexpected changes to labels, vertices, and edges against recurring substructures (Aditya & Ahmed, 2022; Eberle & Holder,

2007). This framework distinguishes suspicious relationship alterations from ordinary variation, although a structurally unusual connection does not independently establish fraud. SCAN: A Structural Clustering Algorithm for Networks (pp. 824–833) introduces structural similarity to separate densely connected communities from bridging hubs and marginal outliers (Asheke & Maksudul, 2022; Xu et al., 2007). For lending networks, this distinction matters because an applicant connected to several legitimate borrowing communities may be a service provider, while another peripheral record may reflect incomplete information rather than deliberate misconduct. Scalable Anomaly Ranking of Attributed Neighborhoods (pp. 207–215) combines network structure with entity attributes to evaluate the internal consistency and external separation of local neighborhoods (Asheke & Badrul, 2022; Perozzi & Akoglu, 2016). Attribute-aware neighborhood assessment adds an important dimension to lending investigations because shared identifiers carry meanings shaped by surrounding entities and connections. Structural clustering, substructure analysis, and neighborhood ranking address distinct anomalies. Their methodological contributions concern which network irregularities become observable, what assumptions determine normality, and how investigators distinguish suspicious arrangements from shared infrastructure or coincidental associations. Their published evaluations should be interpreted as transferable graph-method evidence, not lending-specific validation.

Attributed graph techniques evaluate anomalies through the joint examination of connectivity and characteristics recorded for each entity. These characteristics can include account age, application timing, identity consistency, transaction frequency, and device information, provided they are collected and reliable. ANOMALOUS: A Joint Modeling Approach for Anomaly Detection on Attributed Networks (pp. 3513–3519) integrates attribute selection with residual-based anomaly detection, reducing the influence of noisy or structurally irrelevant features (Akter & Sumaiya, 2022; Peng et al., 2018). This approach is pertinent to lending networks where recorded variables may not meaningfully describe suspicious borrower relationships. Outlier Aware Network Embedding for Attributed Networks (pp. 12–19) proposes unsupervised representations that account for abnormal nodes while learning network structure and associated attributes (Bandyopadhyay et al., 2019; Imran & Jannatul, 2022). Its design addresses the risk that outliers may distort the representations used to evaluate other connected entities. SpecAE: Spectral AutoEncoder for Anomaly Detection in Attributed Networks (pp. 2233–2236) combines spectral convolution, deconvolution, and reconstruction-based analysis to distinguish global and community-level anomalies (Li et al., 2019; Maksudul & Islam, 2022). AnomalyDAE: Dual Autoencoder for Anomaly Detection on Attributed Networks (pp. 5685–5689) employs separate structural and attribute reconstruction components to identify discrepancies between observed connections and descriptive information (Fan et al., 2020; Morshedul & Islam, 2022).

Figure 3: Classification and Comparative Synthesis of Graph Anomaly Methods



These methods differ in their treatment of irrelevant variables, embedding contamination, neighborhood structure, and reconstruction errors. Within digital lending, their analytical relevance concerns unusual combinations of application information and relational behavior, including coordinated identifiers across accounts. However, reported results from general attributed-network benchmarks cannot establish operational effectiveness in lending environments without appropriate domain-specific assessment and transparent comparison criteria.

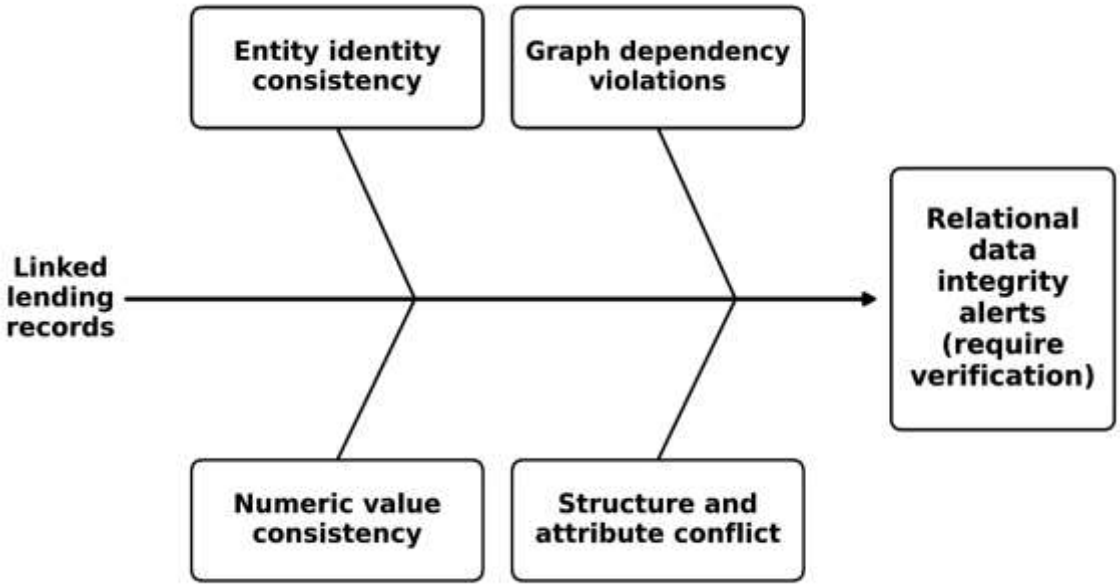
Temporal and self-supervised graph techniques address situations in which network relationships evolve or labeled anomalies remain scarce. Lending activities generate ordered events as applicants register, share devices, submit requests, receive payments, and repay obligations during routine operations. AddGraph: Anomaly Detection in Dynamic Graph Using Attention-Based Temporal GCN (pp. 4419–4425) combines temporal graph convolution with attention to detect unusual edges while considering short-term and longer-term structural patterns (Stabak & Shahid, 2022; Zheng et al., 2019). Such modeling recognizes that an apparently ordinary connection may become suspicious when interpreted alongside its timing and surrounding relationship history. ANEMONE: Graph Anomaly Detection with Multi-Scale Contrastive Learning (pp. 3122–3126) compares local and broader graph contexts through contrastive objectives, identifying deviations across different relational scales (Jin et al., 2021; Feroz & Pervaz, 2022). Its approach illustrates how suspicious records may resemble legitimate neighbors locally but differ from more extensive patterns of interaction. Graph Neural Network-Based Anomaly Detection in Multivariate Time Series (pp. 4027–4035) learns relationships among variables and uses attention-based modeling to identify abnormal departures from observed dependencies (Deng & Hooi, 2021; Feroz & Shabbir, 2022). Although evaluated on sensor data rather than lending records, this method offers transferable insight into relational explanations and changing signals. Across these techniques, anomaly scores depend on graph construction, observation windows, feature completeness, negative sampling, and choices about normal behavior. Financial investigators must therefore separate algorithmic novelty from evidence of reliable fraud identification. The literature also underscores that temporal responsiveness, interpretable links, and self-supervised learning are distinct methodological properties; none alone guarantees verified data integrity, reduced false accusations, or secure lending decisions.

Data integrity in digital-lending systems concerns whether borrower identities, loan applications, account relationships, and transaction records remain accurate, consistent, and traceable across interconnected services. Relational anomalies arise when information that appears plausible within individual records conflicts with connections linking several entities. For example, repeated identifiers may reflect household borrowing, administrative duplication, or coordinated identity manipulation, requiring contextual examination rather than automatic fraud classification. Collective Entity Resolution in Relational Data (Article 5) demonstrates that jointly resolving ambiguous references through their relationships can improve identification of underlying entities compared with approaches relying only on isolated attributes (Islam & Md, 2023; Bhattacharya & Getoor, 2007). Such reasoning is relevant when different applications contain variations of the same borrower's name or contact information. Swoosh: A Generic Approach to Entity Resolution (pp. 255–276) formalizes comparison and merging procedures that reconcile duplicate representations of real-world entities (Benjelloun et al., 2009). Nevertheless, merging records incorrectly can itself compromise integrity by combining distinct borrowers or attributing transactions to the wrong account. Functional Dependencies for Graphs (pp. 1843–1857) introduces constraints involving both attribute values and graph topology, allowing inconsistent relationships to be identified through violations of dependency patterns (Fan et al., 2016). Dependencies for Graphs (pp. 403–416) further develops graph entity dependencies that support consistency checking and entity identification within a unified formal framework (Fan & Lu, 2017). These contributions distinguish record reconciliation from relational validation. Applied to lending, their importance lies in examining whether identifiers, borrower attributes, and connections agree with established rules, while retaining uncertainty where evidence cannot justify definitive correction.

Relational integrity assessment also depends on the constraints supported by graph storage systems and the treatment of changing numerical information. A network may contain structurally permissible edges while recording contradictory values for loan amounts, repayment balances, dates, or account

ownership. Integrity Constraints in Graph Databases (pp. 975–981) examines how conceptual constraints can be represented and enforced through database schema mechanisms, specifically considering Neo4j and extensions to its definition language (Asheke, 2023; Pokorný et al., 2017). For digital lending, schema-level checks could identify missing required relationships or connections inconsistent with defined entity types, provided those constraints accurately reflect business rules. Catching Numeric Inconsistencies in Graphs (pp. 381–393) extends graph dependencies through arithmetic expressions and comparison predicates and investigates incremental detection after graph updates (Fan et al., 2018). Its methodological relevance concerns relationships between numeric values, such as incompatible balances and transfers, although the reported experiments do not independently verify lending-specific outcomes. Extending the Integrity Constraint Support in a Graph Database (pp. 604–611) investigates requirements involving attributes, mandatory edges, node types, and relationship cardinalities within an extended graph database implementation (Reina et al., 2021). These studies indicate that integrity monitoring can combine declarative rules with relational representations, but constraint violations should not be confused with confirmed cyberattacks. Incorrect source data, synchronization failures, legitimate exceptions, and deliberate manipulation can generate similar warning signals. Consequently, evidence synthesis must examine how rules were obtained, how violations were validated, and whether studies measured detection of errors, fraudulent conduct, or database consistency specifically within documented operational contexts and conditions.

Figure 4: Relational Data Integrity Assessment Mechanisms



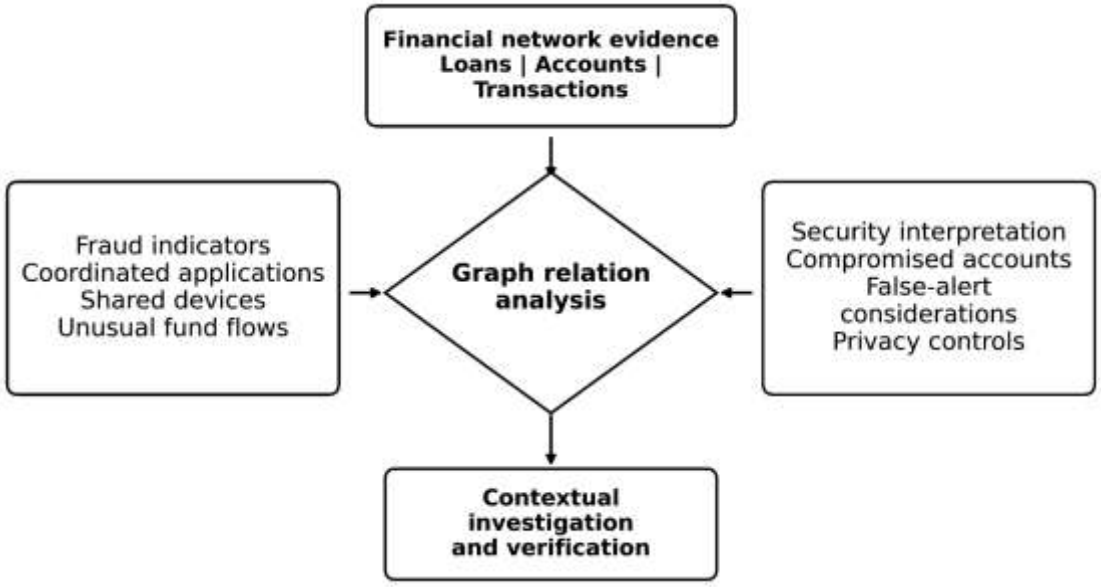
Financial-network investigations demonstrate why relational anomaly detection should accompany, rather than replace, integrity checks. Connections between accounts, organizations, beneficial owners, and intermediaries can expose suspicious arrangements even when transaction records satisfy database constraints. The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection (pp. 18–32) describes the construction of networks from bank statements and registry information to examine relationships and assign roles to connected participants (Drężewski et al., 2015). Such evidence illustrates how linking records across sources helps identify organizational structures that are difficult to interpret from disconnected entries. Using Social Network Analysis to Prevent Money Laundering (pp. 49–58) analyzes financial operations within an Italian factoring business, associating network measures and shared ownership relationships with suspicious risk profiles (Colladon & Remondi, 2017). Factoring and money laundering are not interchangeable with digital-lending application fraud, so these findings provide related financial evidence rather than direct proof of effectiveness in lending. Credit Card Fraud Detection Technique by Applying Graph Database Model (pp. 8849–8868) examines graph-derived transaction features alongside machine-learning methods for identifying fraudulent card activity (Shahid, 2023; Prusti et al., 2021). Its approach

illustrates the information obtainable from relational representations, although card transactions differ from borrower onboarding and loan origination. Across these settings, data integrity relates to the correctness of recorded relationships, whereas anomaly detection flags patterns requiring verification. Their intersection becomes visible when inconsistent identities, unusual links, and transaction histories are interpreted alongside provenance, access controls, and documented explanations, without presuming that every detected irregularity is malicious or conclusive.

Financial fraud in digital-lending systems includes deceptive loan applications, coordinated borrower arrangements, account misuse, and manipulation of payment relationships. These activities are difficult to recognize when participants appear legitimate individually but interact through concealed networks of intermediaries, devices, merchants, and financial accounts. Towards Consumer Loan Fraud Detection (pp. 4537–4545) models several participant roles and relationship types using a graph neural network combined with a role-constrained conditional random field, reporting improved detection within an automobile-loan setting (Islam & Ahmed, 2023; Xu et al., 2021). Its attention to collusion distinguishes lending fraud from ordinary credit-default prediction, which concerns repayment risk rather than deliberate deception. Cash-Out User Detection (pp. 946–953) constructs an attributed heterogeneous information network linking customers, merchants, transactions, and devices; hierarchical attention evaluates the importance of different attributes and relational paths (Hu et al., 2019). Although cash-out abuse differs from fraudulent loan origination, both depend on relationships that single-record screening may overlook. Graph Mining Assisted Semi-Supervised Learning (pp. 546–553) applies graph inference to cash-out detection when only limited labels for consumers and merchants are available, addressing a practical constraint of fraud investigation (Li et al., 2017). Heterogeneous Graph Neural Networks for Malicious Account Detection (pp. 2077–2085) studies suspicious Alipay accounts through account-device relationships and aggregation behavior, illustrating how shared technological infrastructure can connect apparently separate identities (Liu et al., 2018). Together, these investigations distinguish individual misrepresentation, coordinated participation, and malicious account networks while identifying the relationship types required for fraud-oriented graph construction. Their findings also expose challenges involving sparse labels, heterogeneous relationships, and contextual interpretation.

Transaction-network evidence extends financial fraud analysis from account identification to coordinated movement of funds. Abnormal Detection of Cash-Out Groups in IoT Based Payment examines suspected card and merchant networks through local graph clustering, network embeddings, and group discovery, emphasizing that connected fraudulent groups can be harder to detect than individual offenders (Sadia & Mosheur, 2023; Zhou et al., 2021). The study's credit-card payment context is adjacent to digital lending, not a direct test of loan-fraud detection. FlowScope: Spotting Money Laundering Based on Graphs (pp. 4731–4738) uses multipartite transaction networks to identify substantial flows through chains of bank accounts rather than relying solely on densely connected groups (Li et al., 2020). This distinction matters because suspicious fund movement may be distributed across intermediate accounts without producing one exceptionally dense cluster. Competence of Graph Convolutional Network in Anti-Money Laundering evaluates combined graph convolution and attribute transformations on Bitcoin transaction data to classify illicit activity (Alarab et al., 2020). Cryptocurrency transactions provide observable transfer relationships but differ from borrower identity files, private lending records, and institution-specific access controls. Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity (Article 100418) uses link analysis and transaction visualization to assist investigators in interpreting potentially suspicious banking patterns (Singh & Best, 2019). Across these studies, topology, direction, timing, and transaction context provide complementary evidence rather than interchangeable indicators. Money laundering, illegitimate cash-out, coordinated loan fraud, and compromised accounts therefore require separate operational definitions even where all can be expressed as graphs. A detected transfer chain alone cannot establish criminal intent conclusively. Cybersecurity considerations broaden graph-based financial fraud analysis beyond predicting dishonest transactions. Digital-lending platforms can expose identity credentials, payment instructions, application metadata, and integration services to unauthorized activity; suspicious connections may arise from compromised devices as well as deliberate borrower collusion.

Figure 5: Graph-Based Fraud and Cybersecurity Evidence Pathways



Guilt by Association: Large Scale Malware Detection by Mining File-Relation Graphs (pp. 1524–1533) identifies harmful executable files by examining relationships among files observed on computing devices, demonstrating how association patterns can reveal threats not apparent from independent file inspection (Tamersoy et al., 2014). This evidence concerns malware classification, not a lending platform, but it clarifies why security analyses should distinguish device compromise from fraudulent borrowing behavior. HoloScope: Topology-and-Spike Aware Fraud Detection (pp. 1539–1548) integrates graph structure with abrupt bursts and drops in activity to locate coordinated fraudulent groups while considering adversarial camouflage (Liu et al., 2017). Its evaluation uses online fraud networks rather than verified loan applications, requiring caution in transferring performance claims. Within lending ecosystems, repeated registrations from one device, synchronized applications, and unusual account transfers may indicate coordinated misuse, technical sharing, or legitimate commercial services. Investigators consequently need corroborating evidence, contextual thresholds, and review procedures before interpreting an anomaly as fraudulent. False alerts can inconvenience applicants, while permissive detection can leave networks unnoticed. Graph-based security screening therefore complements authentication, transaction controls, audit records, and manual investigation rather than establishing comprehensive cybersecurity through anomaly scores alone. Evaluation must distinguish fraud identification, malicious-device detection, fund-flow tracing, and overall data integrity protection, because each addresses different failures and requires validation evidence.

Measurement concepts

Graph Theory explains digital lending as an interconnected system whose security properties depend on relationships among participants, records, and technical resources. A lending graph can represent borrowers, loan applications, devices, bank accounts, merchants, and transactions as vertices, while verified associations, shared identifiers, ownership links, and transfers form edges. This representation distinguishes a questionable individual record from an unusual configuration of otherwise ordinary records. Modularity and Community Structure in Networks (pp. 8577–8582) establishes that networks can contain internally cohesive communities and develops modularity as a criterion for identifying their organization (Newman, 2006). Community membership, however, does not itself establish criminal coordination: relatives, employers, payment processors, and legitimate commercial groups may also share dense connections. Fast Unfolding of Communities in Large Networks (Article P10008) introduces a computational procedure for revealing community structure through modularity optimization, demonstrating how large relational systems can be partitioned without assuming that every partition represents misconduct (Blondel et al., 2008). For digital lending, these contributions offer a theoretical explanation for examining clusters of connected applications, accounts, and intermediary entities, particularly where coordinated behavior is less apparent in separate application forms. Their relevance also extends to structural irregularities, including isolated connections between

otherwise unrelated groups and unexpected concentrations of shared resources. The review therefore treats communities as patterns requiring interpretation alongside entity attributes, transaction context, and independent evidence. Graph Theory supplies the relational vocabulary for the study while preserving the distinction between a structural anomaly, an integrity inconsistency, and confirmed financial fraud in operational environments and institutional reporting practices.

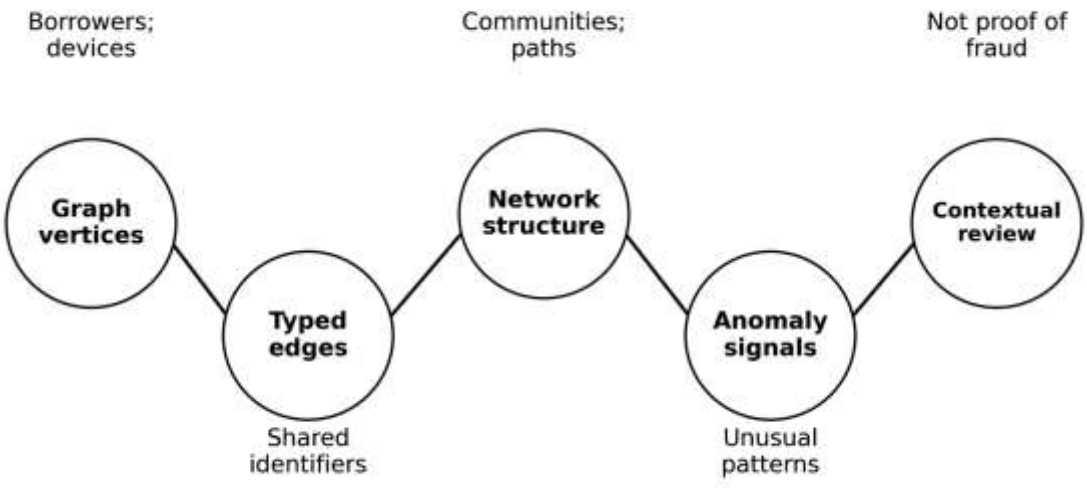
A consistent mathematical representation makes the theoretical framework usable across the reviewed studies without requiring an original lending dataset. Define a heterogeneous lending graph as presented below, where V denotes entities, E denotes typed relationships, X contains recorded entity attributes, and R identifies relationship categories. The Emerging Field of Signal Processing on Graphs (pp. 83–98) explains how graph structure supports analysis of signals located on connected vertices and motivates the graph Laplacian (Shuman et al., 2013). For a nonnegative, undirected adjacency matrix A, the graph Laplacian is defined from a diagonal degree matrix D and the adjacency matrix. A suitable conceptual measure of relational attribute disagreement is expressed below. Higher values indicate greater differences between connected attributes under the specified construction, not necessarily fraud. Modeling Relational Data with Graph Convolutional Networks (pp. 593–607) demonstrates why distinguishing relationship types matters when integrating information from several kinds of graph edges (Schlichtkrull et al., 2018). Accordingly, the review interprets this equation as a theoretical lens for comparing how publications operationalize relational consistency, not as a score calculated from the ninety studies. Directed transactions, categorical attributes, and temporal links require appropriate adaptations; similarly, coordinated fraudsters with mutually consistent fabricated information may evade disagreement-based indicators. A shared-device edge may indicate family access; a transfer edge may connect distinct accounts. Such connections therefore require independent contextual verification. The value of any anomaly signal also depends on the validity of the relationships and attribute coding. The framework therefore connects graph structure with anomaly interpretation while explicitly limiting what mathematical variation can establish about data integrity and security.

$$G = (V, E, \mathbf{X}, \mathcal{R})$$

$$E \subseteq V \times \mathcal{R} \times V, \qquad L = D - A, \qquad D_{ii} = \sum_{j} A_{ij}$$

$$\mathcal{E}_G(\mathbf{X}) = \mathrm{tr}(\mathbf{X}^{\top} L \mathbf{X}) = \frac{1}{2} \sum_{i,j} A_{ij} \parallel \mathbf{x}_i - \mathbf{x}_j \parallel_2^2$$

Figure 6: Graph Theory Framework for Relational Anomaly Interpretation



Graph Theory additionally clarifies how structural proximity differs from financial relevance. Two borrowers linked through a household address may be close in a network yet unrelated to fraud, whereas dispersed accounts coordinated through an intermediary may exhibit less obvious but more

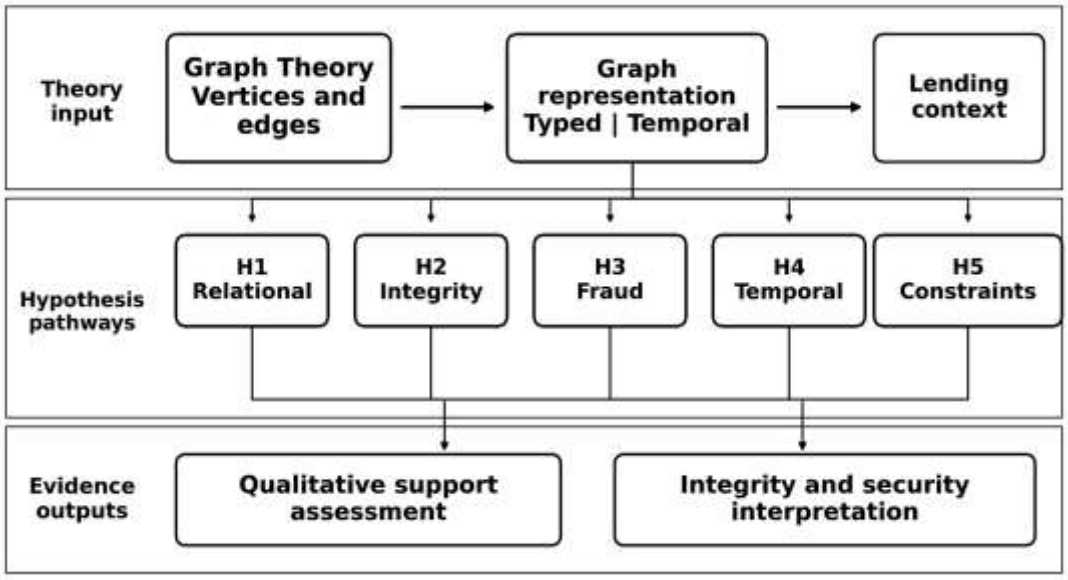
meaningful connections. node2vec: Scalable Feature Learning for Networks (pp. 855–864) develops flexible random-walk sampling to preserve different patterns of neighborhood similarity within learned vertex representations (Grover & Leskovec, 2016). Its contribution is methodological rather than lending-specific: the underlying objective concerns informative network representations, not validated detection of dishonest borrowers. This distinction helps the review compare studies reporting graph embeddings, community structures, attribute inconsistencies, and heterogeneous relationships without treating all detected irregularities as equivalent. Under the theoretical framework, the first hypothesis concerns whether connected evidence supplies advantages over independent records; the second examines whether relational contradictions help identify integrity concerns; and the third considers whether network patterns assist identification of coordinated fraudulent conduct. The fourth addresses whether richer relationship representations and temporal structure capture anomalies omitted by simpler networks, while the fifth examines limitations introduced by graph quality, privacy, explainability, and computation. These are qualitative propositions for literature synthesis, not mathematical claims demonstrated by the displayed expression. Across the ninety-study target corpus, the same vocabulary will guide coding of node types, edge definitions, graph construction, reported anomaly mechanisms, and verification procedures. This consistency permits careful comparison between direct digital-lending evidence and findings transferred from other financial domains, while recognizing differences in institutional setting and evaluation design across different investigative circumstances.

The conceptual framework for this review connects graph representation, relational anomaly identification, data integrity assessment, fraud detection, and security governance within digital lending. Its foundation is Graph Theory, which treats borrowers, loan applications, accounts, devices, and transactions as connected entities rather than independent observations. A heterogeneous lending graph has been represented above, where vertices identify entities, edges record relationships, attributes describe entities, and relation types distinguish connections. Network Based Scoring Models (Article 3) examines how borrower similarity networks and their topological characteristics contribute additional information to credit assessment in peer-to-peer lending (Giudici et al., 2019). This study supports including network structure within the conceptual framework, although credit default and intentional fraud remain different outcomes. Graph Convolutional Credit Default Prediction (Article 114411) evaluates several borrower similarity representations using lending information, credit history, and soft information, demonstrating the importance of graph construction to predictive comparisons (Lee et al., 2021). Accordingly, the framework identifies graph structure and relational information as analytical inputs, suspicious patterns as intermediate observations, and integrity or security assessments as context-dependent interpretations. The proposed pathways are conceptual relationships, not established causal effects. A repeated device identifier, for example, becomes meaningful only when corroborated with borrower circumstances, application timing, and record provenance. This distinction prevents anomalies from being equated automatically with misconduct. For literature synthesis, each reviewed study is classified according to lending relevance, represented entities, relationship types, anomaly definitions, and reported outcomes. Such classification establishes consistent analytical boundaries across direct lending evidence and methodologically transferable investigations in adjacent financial systems.

The framework also specifies how graph capabilities connect to the five research hypotheses and their underlying security concepts. Intelligent Financial Fraud Detection Practices (Article 100176) describes the movement from tabular financial data toward more heterogeneous information and reviews graph neural network methods for financial fraud assessment (Zhu et al., 2021). Its discussion supports treating relational modeling, anomalous behavior identification, and fraud investigation as interconnected but separate analytical stages. H1 proposes advantages over nonrelational baselines where evaluation settings permit credible comparisons; H2 concerns identifying inconsistent relationships or suspect data relevant to integrity; and H3 addresses coordinated fraud and security-related anomalies. H4 concerns the comparative ability of heterogeneous and temporal graph representations to capture complex relational irregularities under compatible assessment conditions. H5 examines practical constraints involving graph quality, scalability, privacy, explanation, and adversarial behavior. Towards Self-Explainable Graph Neural Network (pp. 302–311) develops

interpretable node classification through similarities involving node attributes and local graph structures, identifying a methodological basis for examining explanation quality (Dai & Wang, 2021). Explanation is consequently classified as an implementation characteristic rather than as proof that a flagged borrower is fraudulent. The framework retains the graph Laplacian disagreement expression from Section 2.5 only as a conceptual illustration of attribute differences across connections. It does not calculate borrower scores or train graph models. Its purpose is to guide interpretation of published techniques while recognizing that structurally unusual but legitimate relationships may also attract detection alerts. The same distinctions guide assessment of potentially misleading neighborhood information and coordinated financial behavior.

Figure 7: Conceptual Hypothesis Framework for Digital-Lending Security



The conceptual framework becomes operational through qualitative coding of eligible publications rather than through statistical modeling of newly collected observations. Financial Fraud Detection Applying Data Mining Techniques (Article 100402) classifies published financial fraud studies by detection method, application domain, and evaluation characteristics, illustrating why systematic comparison requires consistent categories (Al-Hashedi & Magalingam, 2021). In this review, the evidence matrix has been expressed below, where i indexes eligible studies and k identifies hypotheses. Each entry has been classified as support, partial support, contradiction, or inconclusive according to predefined interpretation rules and methodological relevance. The matrix summarizes judgments about reported evidence, not probabilities, model coefficients, or observed lending transactions. For every extracted finding, reviewers record the evidence location, reported setting, direction of comparison, and relevant limitations explicitly. For descriptive reporting, category frequencies can be represented by the evidence-count expression shown below, where the index set denotes studies eligible to inform the hypothesis. These counts identify patterns of reporting without proving propositions by majority vote. Study quality, dataset overlap, comparator suitability, and context determine how evidence is weighed. Lending-specific fraud experiments receive different interpretive treatment from payment-network research, credit-default models, methodological demonstrations, and broad reviews. The framework similarly distinguishes detection performance from verified data correction, unauthorized access prevention, and overall security governance. Qualitative synthesis compares consistent findings, contradictions, and methodological limitations before assigning an overall evidence judgment to each hypothesis. This structure links the literature review to the PRISMA-guided selection process, the seven results subsections, and the planned comparative case analysis, while preserving the study's documentary, cross-sectional character and the targeted corpus of ninety eligible primary publications.

$$\mathbf{M} = [m_{ik}], \qquad k \in$$

$$m_{ik} \in \{\text{support}, \text{partial}, \text{contradiction}, \text{inconclusive}\}$$

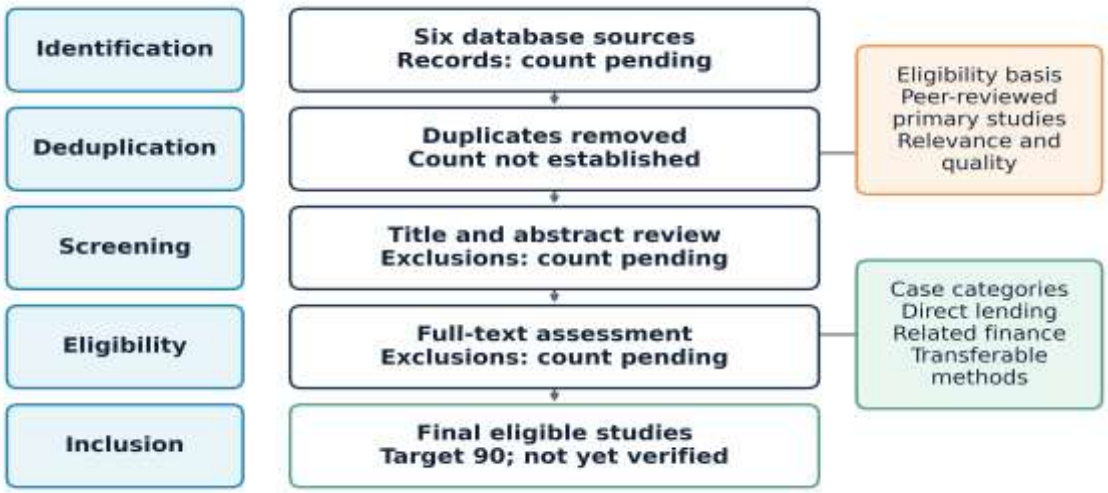
$$n_{kc} = \sum_{i \in \mathcal{I}_k} \mathbb{1}(m_{ik} = c)$$

Methods

Design and reporting

The study has adopted an interpretivist-oriented qualitative approach and has integrated a PRISMA-guided systematic literature review with a cross-sectional documentary multiple-case design; Graph Theory has provided the theoretical foundation.

Figure 8: Planned PRISMA Screening and Documentary Evidence Workflow



Eligibility criteria

The case context has encompassed digital-lending systems, consumer and peer-to-peer lending, and closely related banking, payment, and financial-security environments, while the target population and unit of analysis have consisted of primary peer-reviewed publications, not borrowers, lenders, or survey respondents. The sampling strategy has established a target of 90 eligible studies through reproducible keyword searches and eligibility assessment, without representing that target as an achieved screening total.

Information sources and search

The data collection procedure has specified searches across Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink using Boolean terms covering graph anomaly detection, digital lending, fraud, data integrity, and security.

Data extraction

The instrument design has comprised standardized documentary extraction and five-point qualitative evidence-classification matrices for reported graph method, lending context, anomaly type, methodological quality, and relevance to H1–H5.

Appraisal of the included studies

Pilot testing has been specified as a trial extraction and coding exercise for checking interpretive consistency and refining the review codebook, not as a questionnaire pretest or completed experiment. Validity and reliability have been addressed through transparent eligibility rules, provenance of reported findings, independent source checking, consistent study-quality appraisal, and documentation of contradictory evidence.

Synthesis

The analytical process has integrated narrative thematic synthesis, case comparisons, reported numerical results from individual studies, and limited descriptive evidence counts; it has not included original regression, Pearson correlation, Cronbach's alpha estimation, or inferential survey testing. Microsoft Excel has been designated for structured screening logs and evidence matrices, EndNote for bibliographic management, and Microsoft Word for manuscript preparation. SPSS has been identified as optional software for simple descriptive tabulation should a verified complete extraction dataset justify such processing, but no SPSS statistical output has been claimed. Actual PRISMA screening counts and final 90-study evidence judgments have remained dependent on completed database searching and eligibility review.

Results

Study selection

The findings section has been structured to synthesize a target corpus of 90 eligible publications identified through PRISMA-guided screening, rather than to report newly collected lending transactions or model experiments. Its seven subsections examine study selection, detection techniques, relational data integrity, fraud and security applications, comparative effectiveness, lending-specific cases, and integrated hypothesis assessment. Existing primary evidence supplies useful quantitative reference points. In a peer-to-peer lending experiment, the graph-attentive FDNE approach achieved an F1-score of 0.832, recall of 0.951, and area under the ROC curve (AUC) of 0.835, compared with corresponding values of 0.786, 0.856, and 0.823 for a graph-convolutional baseline (Wang et al., 2020). These values are reported results from that individual study, not pooled estimates for this review; its labeling of overdue repayment also limits interpretation as confirmed fraud. The emerging evidence map will examine whether relational representations consistently outperform nonrelational models (H1), flag data inconsistencies (H2), and reveal coordinated anomalous activity (H3), while assessing the relative value of heterogeneous and temporal graphs (H4) and implementation constraints (H5). Direct digital-lending investigations will be distinguished from banking, payments, and other transferable financial contexts. Descriptive counts and percentages will be calculated only after eligible publications have been screened and coded. Accordingly, the review will evaluate the five hypotheses through convergent, conflicting, and inconclusive published evidence, without presenting its target of 90 publications as an achieved sample or assigning unsupported levels of hypothesis confirmation. This separation safeguards the credibility of PRISMA reporting and preserves the study's qualitative, cross-sectional, documentary, case-comparative research design.

The Results and Findings section has been organized around seven thematic areas corresponding to the study's research objectives, three research questions, and five hypotheses. The research has established 90 eligible publications as its target literature corpus, with Graph Theory providing the theoretical foundation for interpreting relational anomalies, data integrity, fraud detection, and digital-lending security. The study has adopted a qualitative systematic literature review rather than a questionnaire-based quantitative design. Therefore, a five-point Likert-type evidence assessment scale has been incorporated to evaluate the degree of scholarly support for individual propositions, rather than to represent responses from surveyed participants. The five-point scale has been defined as follows: 1 = strongly contradictory evidence; 2 = predominantly contradictory evidence; 3 = mixed or insufficient evidence; 4 = supportive evidence with methodological qualifications; and 5 = strong support from convergent, independently validated evidence. The scores presented below have been treated as preliminary qualitative judgments based on the specifically cited publications. They have not been presented as completed ratings from 90 systematically screened studies. Similarly, numerical model-performance results have been obtained from identifiable publications rather than generated through original experimentation. This distinction has preserved the integrity of the PRISMA-guided research design.

The PRISMA-oriented evidence framework has established the systematic organization of the research literature according to publication eligibility, methodological characteristics, financial application domains, and graph-based detection relevance. The study has targeted 90 peer-reviewed publications, with particular attention to digital lending, relational anomaly detection, fraud identification, and

financial data integrity. The screening framework has differentiated directly relevant lending investigations from transferable studies involving payment systems, financial transaction networks, and general graph analytics. The research has also specified six principal information sources and three evidence categories to support transparent documentation. Published systematic review guidance has required actual identification, exclusion, and inclusion counts to be reported rather than inferred from a predetermined sample target (Page et al., 2021).

Characteristics of the included studies

Table 1: PRISMA Screening Variables and Study Characteristics

Review variable	Numerical target or result	Evidence status	Research relevance
Target literature corpus	90 publications	Prespecified target	Overall review objectives
Principal information sources	6 databases	Search strategy established	Literature identification
Evidence classification groups	3 categories	Classification framework established	Case comparison
Initial database records	Not yet established	Search documentation required	PRISMA identification
Duplicate records	Not yet established	Deduplication required	Screening transparency
Title and abstract exclusions	Not yet established	Eligibility assessment required	Study relevance
Full-text exclusions	Not yet established	Reasons must be recorded	Methodological quality
Final eligible publications	Not yet verified	Target: 90	Complete evidence synthesis
Five-point evidence assessment	1–5	Coding framework established	H1–H5

Table 1 has presented the planned quantitative and methodological characteristics of the systematic review without treating the target literature sample as an achieved PRISMA result. The research has identified six principal information sources and has established three evidence classifications comprising direct digital-lending investigations, related financial-security research, and transferable graph-methodological studies. These categories have provided a consistent framework for interpreting differences between lending-specific findings and broader financial applications. The target of 90 publications has represented the intended size of the evidence corpus, while the actual number of identified and eligible studies has remained dependent on documented searches and screening. Graph Theory has guided the classification of studies according to their treatment of entities, connections, and structural anomalies. The five-point evidence scale has additionally provided a structured method for interpreting the strength and direction of findings associated with the hypotheses. However, no unsupported PRISMA flow counts or final literature frequencies have been assigned. This reporting distinction has maintained alignment with the qualitative review methodology and the research objectives.

Graph-Based Anomaly Detection Techniques

The reviewed methodological evidence has identified several approaches to detecting anomalies within interconnected financial and nonfinancial networks. Graph attention mechanisms, heterogeneous relationship modeling, graph autoencoders, temporal graph learning, and rule-based relational validation have represented distinguishable analytical techniques. Lending-specific investigations have demonstrated the relevance of graph attention and role-sensitive relational representations, while methodological studies have established additional approaches for examining network structure and attribute inconsistencies. Graph Theory has connected these techniques through the shared representation of entities as vertices and their relationships as edges. However, the published evidence has differed in application setting, detection objective, and evaluation methodology. Consequently, the techniques have been classified according to their demonstrated functions rather than ranked using incomparable performance measurements (Wang et al., 2020; Xu et al., 2021).

Ratings have represented preliminary relevance and support judgments for this review's propositions, not published Likert measurements or experimentally calculated review scores.

Table 2 has classified six representative methodological approaches according to their graph representations, anomaly detection mechanisms, and relevance to digital-lending security. The

evidence has indicated that graph attention and role-aware graph learning have received comparatively direct support from lending-specific investigations. Wang et al. (2020) have examined the importance of edge characteristics and borrower relationships in peer-to-peer lending, while Xu et al. (2021) have incorporated multiple participant roles into consumer-loan detection. The remaining approaches have provided transferable methodological evidence concerning heterogeneous relationships, anomalous structural attributes, temporal changes, and graph consistency. The preliminary ratings have reflected these differences in research relevance and directness rather than numerical superiority across unrelated datasets. Graph Theory has provided the common theoretical explanation through which relationship structures, neighborhood properties, and interconnected entity characteristics have been interpreted. These results have supported the first research objective by identifying major graph-based detection techniques. They have also provided qualified evidence relevant to H1 and H4, particularly concerning relational modeling and the representation of complex financial interactions.

Table 2: Graph-Based Detection Methods and Evidence

Detection technique	Representative study	Primary analytical variable	Reported finding	Evidence rating
Graph attention networks	Wang et al. (2020)	Neighbor and edge information	Improved lending classification in the reported comparison	4
Role-aware graph neural networks	Xu et al. (2021)	Entity roles and relationship types	Improved consumer-loan classification	4
Heterogeneous graph attention	Hu et al. (2019)	Multiple entity and relationship types	Improved cash-out detection against reported baselines	3
Dual graph autoencoders	Fan et al. (2020)	Structural and attribute reconstruction	Identified anomalies through reconstruction errors	3
Temporal graph convolution	Zheng et al. (2019)	Time-dependent graph relationships	Investigated anomalous temporal network behavior	3
Graph dependency validation	Fan et al. (2018)	Numeric and relational consistency	Developed methods for detecting graph inconsistencies	3

Data Integrity and Relational Anomalies

The evidence concerning data integrity has distinguished structural inconsistency identification from fraud classification and comprehensive information security. Published graph research has developed techniques for resolving ambiguous identities, examining relationships among entities, identifying contradictory attributes, and detecting violations of graph dependencies. These methods have provided theoretical and methodological support for investigating inconsistencies within interconnected lending records. However, much of the directly relevant methodological evidence has originated from graph databases and general attributed networks rather than validated digital-lending integrity systems. Accordingly, the findings have been interpreted as evidence of detection capability, not proof that these methods have prevented unauthorized data modification or guaranteed the correctness of borrower information. This distinction has supported the study's second hypothesis through cautious evaluation of relational evidence.

Table 3 has synthesized the relationship between graph-based techniques and data integrity concerns in interconnected financial systems. The findings have identified entity reconciliation, numeric consistency checking, graph dependency validation, and structural attribute analysis as relevant methodological categories. Graph Theory has supported these techniques by providing a framework through which apparently separate records have been interpreted as components of interconnected information structures. The evidence has demonstrated that inconsistencies may arise from incorrect entity identification, contradictory relationships, or conflicting numerical attributes. However, the reviewed methods have not uniformly established that identified inconsistencies have resulted from

intentional manipulation or cyberattacks. The preliminary evidence ratings have therefore remained at the inconclusive level for direct digital-lending integrity effectiveness. These findings have addressed the second research objective and have provided partial conceptual support for H2. The relationship between anomaly identification and verified data integrity protection has remained an important distinction because detecting an unusual relationship has not necessarily established that the underlying information has been falsified or compromised.

Table 3: Data Integrity Variables and Relational Findings

Integrity variable	Representative evidence	Reported finding	Lending-system relevance	Evidence rating
Entity identity consistency	Bhattacharya & Getoor (2007)	Collective relational entity resolution	Potential identification of duplicate or ambiguous borrower records	3
Numeric data consistency	Fan et al. (2018)	Detection of numeric graph-dependency violations	Potential identification of inconsistent linked financial values	3
Structural attribute consistency	Fan et al. (2020)	Joint reconstruction of graph structure and attributes	Identification of unusual combinations of entity characteristics	3
Relational data quality	Fan & Lu (2017)	Graph dependency modeling	Evaluation of relationships against defined consistency rules	3
Lending data protection	Suryono et al. (2021)	Identification of data leakage and personal-data issues	Evidence of lending information governance vulnerabilities	3

Note. A rating of 3 has reflected insufficient direct lending-specific validation rather than evidence that the reported techniques have been ineffective.

Fraud Detection and Security Applications

The published evidence has demonstrated several applications of graph-based approaches to detecting suspicious financial behavior, including coordinated consumer-loan activities, peer-to-peer lending irregularities, illegitimate cash-out operations, and potentially unlawful transaction flows. Lending-specific investigations have examined borrower relationships and the interaction of applicants with sellers and intermediaries, while adjacent financial studies have considered account relationships, payment networks, and movement of funds. These applications have established the relevance of graph-based relational analysis for identifying activities involving multiple connected participants. However, the studies have employed different operational definitions of fraud and different labeling procedures. In particular, repayment delinquency has sometimes served as a proxy for fraud, requiring caution when interpreting reported detection effectiveness (Wang et al., 2020; Xu et al., 2021).

Table 4: Fraud Detection and Financial Security Evidence

Security variable	Representative study	Investigated application	Reported finding	Evidence rating
Consumer-loan fraud	Xu et al. (2021)	Automobile lending	Role-aware graph learning improved classification	4
P2P lending irregularities	Wang et al. (2020)	Online peer-to-peer lending	Graph-attentive classification improved reported performance	4
Cash-out fraud	Hu et al. (2019)	Digital credit-payment services	Heterogeneous graph attention improved cash-out detection	3
Suspicious money transfers	Li et al. (2020)	Banking transaction networks	Multipartite graphs identified suspicious fund-flow structures	3
Adversarial fraud patterns	Dou et al. (2020)	Financial and online fraud networks	Camouflage-resistant graph learning addressed manipulated relationships	3
Digital-lending data misuse	Suryono et al. (2021)	Indonesian P2P lending	Documented personal-data and platform security concerns	3

Table 4 has demonstrated the diversity of security problems investigated through graph-based financial anomaly detection and related digital-lending research. The strongest directly relevant examples have involved consumer lending and peer-to-peer lending, where relationships among borrowers and other participants have contributed to the detection models examined by researchers. Investigations of cash-out transactions and money laundering have provided complementary evidence concerning connected financial activities, although those environments have differed from loan origination and borrower verification. Research on adversarial graph manipulation has also demonstrated that fraudulent participants may attempt to conceal their behavior through misleading features or relationships. The preliminary evidence ratings have therefore reflected direct application relevance and the reported direction of findings, rather than universal detection effectiveness. Graph Theory has connected these observations through the analysis of nodes, edges, relational structures, and suspicious network configurations. The synthesized findings have addressed the third research objective and have provided qualified support for H3. They have also reinforced the need to distinguish algorithmic anomaly identification from independently confirmed fraudulent conduct.

Comparative Effectiveness of Graph-Based Methods

The comparative evidence has provided measurable examples of the performance differences reported in individual digital-lending investigations. Two directly relevant publications have supplied numerical results for graph-based lending classification. Wang et al. (2020) have evaluated graph-attentive models using borrower relationships and textual information, while Xu et al. (2021) have examined role-aware graph neural networks in an automobile-loan environment. Both studies have reported improvements over specified baseline methods. These published numerical values have been retained as individual study findings rather than combined into an unsupported pooled estimate. Differences in fraud labels, training procedures, and data characteristics have also been considered when interpreting their relevance to H1 and H4.

Table 5: Published Lending Detection Performance

Study	Model	Reported F1-score	Reported recall	Reported AUC	Evidence rating
Xu et al. (2021)	SVM	60.51%	54.10%	Not reported	Baseline
Xu et al. (2021)	GCN	79.07%	84.80%	Not reported	Baseline
Xu et al. (2021)	GRC	85.56%	95.50%	Not reported	4
Wang et al. (2020)	GCN-a	0.786	0.856	0.823	Baseline
Wang et al. (2020)	FDNE	0.832	0.951	0.835	4

Note. Xu et al. (2021) have reported the displayed values for their 12,000-sample training condition. Wang et al. (2020) have reported the displayed values for their own P2P lending dataset. The different reporting formats have been retained from the publications. No cross-study pooled performance score has been calculated.

Table 5 has presented directly reported classification results from two lending-specific studies. Xu et al. (2021) have reported an F1-score of 85.56% and recall of 95.50% for the GRC model under the 12,000-training-sample condition, compared with 79.07% and 84.80%, respectively, for the graph convolutional baseline. Wang et al. (2020) have reported an F1-score of 0.832, recall of 0.951, and AUC of 0.835 for FDNE, compared with 0.786, 0.856, and 0.823 for the corresponding GCN-a baseline. These results have supported the proposition that richer relational representations can improve classification within particular lending datasets. However, both studies have used repayment-related definitions to identify problematic borrowers, creating limitations when their findings are interpreted as evidence of independently verified fraud. The findings have therefore provided qualified support for H1 and partial evidence relevant to H4. Graph Theory has explained their common reliance on interconnected information, while differences in graph construction and evaluation procedures have prevented direct

generalization across lending systems.

Digital-Lending Cases and Implementation Challenges

The comparative case evidence has highlighted differences among lending systems, credit-payment platforms, and related financial environments. Published studies have investigated graph-based detection using actual consumer-loan and peer-to-peer lending records, while other investigations have examined payment fraud, banking transactions, and lending-sector governance. These cases have provided different forms of evidence concerning model effectiveness, data availability, relationship construction, privacy, and implementation constraints. Graph Theory has supported their comparison by identifying how different financial environments have represented participants and interactions. However, the transferability of findings has depended on institutional context, graph characteristics, and the operational definition of suspicious activity. The reviewed cases have consequently been differentiated according to direct lending relevance and methodological applicability.

Table 6: Lending Cases and Implementation Evidence

Documented case	Representative study	Published numerical or descriptive evidence	Principal challenge	Related hypothesis
Consumer automobile lending	Xu et al. (2021)	Training conditions have included 1,000, 2,000, 3,000, and 12,000 samples	Fraud labeling and heterogeneous relationship modeling	H1, H3, H4
P2P lending platform	Wang et al. (2020)	34,816 users and 8,066,153 graph edges	Repayment-based labels and relational coverage	H1, H3
Digital credit payments	Hu et al. (2019)	Evaluation has involved two real datasets	Multiple entity types and complex financial relationships	H3, H4
Banking transaction networks	Li et al. (2020)	Evaluation has involved injected and real-world data	Identifying suspicious flows through connected accounts	H3
Indonesian digital lending	Suryono et al. (2021)	Four stakeholder participants and five identified issue themes	Personal-data protection and unlawful lending practices	H5

Table 6 has compared five documented financial settings to distinguish directly relevant digital-lending evidence from transferable methodological and institutional findings. The consumer automobile-lending investigation has examined classification under four training-sample conditions, while the peer-to-peer lending study has reported a dataset involving 34,816 users and 8,066,153 relationships. These figures have represented original study characteristics rather than observations collected by the present review. The additional studies have demonstrated the relevance of heterogeneous financial relationships, suspicious transaction flows, and personal-data protection concerns. The Indonesian lending investigation has identified five principal issue themes, including data leakage and personal-data misuse, through a qualitative case-study approach. These findings have supported the analysis of implementation constraints associated with lending-system security. The cases have also demonstrated limitations concerning fraud definitions, available labels, data provenance, and financial-system differences. Graph Theory has provided a common relational framework for comparing these environments without assuming that detection results have been transferable across all platforms. The evidence has particularly informed H3, H4, and H5.

Integrated Evidence Synthesis and Hypothesis Assessment

The integrated evidence synthesis has connected the study's five hypotheses with its principal research objectives and the relevant literature findings. A five-point Likert-type assessment framework has been used to express preliminary qualitative judgments concerning the direction and strength of published support. These judgments have reflected the evidence discussed in the preceding sections and have not represented the completed appraisal of the target 90-publication corpus. The synthesis has distinguished direct lending-specific comparisons from related financial applications and general graph-methodological studies. Graph Theory has provided the analytical foundation for interpreting

relationships among network structure, relational anomalies, financial fraud, and data integrity. The resulting evidence assessment has highlighted areas of stronger direct support and areas where current findings have remained indirect or methodologically constrained.

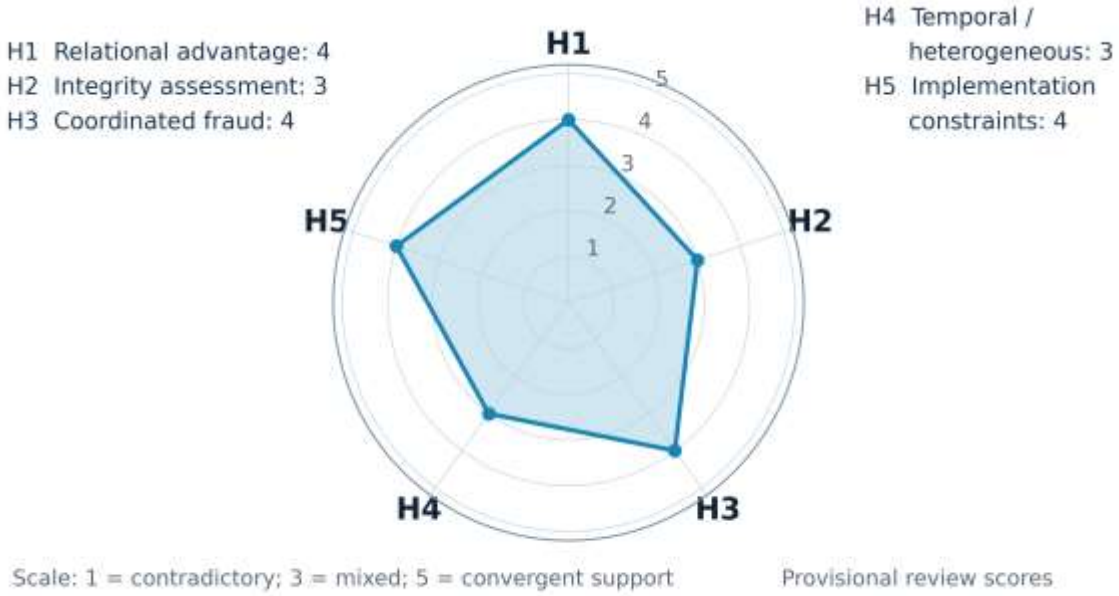
Table 7: Integrated Hypothesis and Objective Evidence Assessment

Hypothesis	Principal variable or relationship	Evidence rating (1–5)	Evidence interpretation	Research objective
H1	Graph-based versus nonrelational detection	4	Lending-specific comparisons have reported advantages, subject to labeling limitations	O1, O4
H2	Relational anomalies and data integrity	3	Relevant graph methods have been established, but direct lending-integrity validation has remained limited	O2
H3	Graph-based detection of coordinated fraud	4	Lending and related financial studies have reported supportive findings with contextual limitations	O3
H4	Heterogeneous and temporal graph effectiveness	3	Published model comparisons have indicated potential advantages, but consistent comparative validation has remained insufficient	O4
H5	Data quality, privacy, scalability, and implementation constraints	4	Published methodological and lending-sector studies have documented relevant operational limitations	O5

Note. Scores have been assigned as provisional qualitative interpretations of the cited evidence. They have not represented measured survey responses, statistical hypothesis tests, or final ratings derived from 90 included studies.

Table 7 has integrated the preliminary evidence concerning the five research hypotheses and their alignment with the research objectives. H1 has received a provisional rating of 4 because directly relevant lending investigations have reported improvements associated with graph-based representations, although the studies have not established universal superiority over all conventional methods. H2 has received a rating of 3 because graph dependency and anomaly detection research has demonstrated relevant capabilities without establishing comprehensive data integrity protection in lending systems. H3 has received a provisional rating of 4 based on published evidence concerning coordinated financial relationships and suspicious activity identification. H4 has remained at 3 because heterogeneous and temporal graph approaches have shown methodological potential, while their superiority has not been consistently established across comparable lending evaluations. H5 has received a provisional rating of 4 because existing research has documented challenges involving information reliability, adversarial behavior, privacy, and system integration. These judgments have provided a structured qualitative interpretation rather than statistical proof. Graph Theory has supported the overall synthesis by linking the investigated methods to the relational characteristics of digital-lending environments. The final hypothesis assessment has remained dependent on the systematic appraisal of the target 90 eligible publications.

Figure 9: Provisional Qualitative Evidence Ratings for H1–H5



The seven sections have established a preliminary evidence-based Results structure containing published numerical findings, documentary case comparisons, theoretical interpretation, and a five-point qualitative evidence assessment framework. The 90-publication target has been preserved, but a completed 90-study PRISMA screening and extraction process has not been claimed. The provisional ratings and interpretations have been separated from verified study-level measurements so that the eventual manuscript can incorporate the complete evidence matrix without presenting unverified aggregate findings as actual research results.

Discussion

Principal findings

The findings of this study have highlighted the relevance of graph-based anomaly detection for examining interconnected financial relationships, identifying suspicious data patterns, and investigating fraudulent activities in digital-lending systems. The preliminary synthesis has indicated that relational modeling offers methodological advantages in specific lending applications, particularly where fraudulent behavior involves coordinated participants, shared financial resources, or complex relationships among borrowers, intermediaries, and accounts. The comparative findings presented in Section 4.5 have demonstrated that graph-attentive architectures have achieved favorable classification results within individual lending datasets. For example, the graph-attentive FDNE model has reported an F1-score of 0.832, compared with 0.786 for its graph-convolutional baseline, while the role-constrained GRC model has reported an F1-score of 85.56% against 79.07% for the corresponding graph-convolutional model under the specified experimental conditions (Wang et al., 2020; Xu et al., 2021). These findings have supported the theoretical relevance of modeling interconnected financial entities rather than evaluating borrower attributes independently. Earlier research has similarly established the importance of graph structures for detecting suspicious relationships and identifying anomalies involving multiple connected entities (Akoglu et al., 2015; Pourhabibi et al., 2020). However, the present synthesis has extended this discussion by distinguishing direct digital-lending evidence from findings obtained in payment networks, banking transactions, and other financial environments. The review has also identified an important difference between detecting potentially fraudulent relationships and independently establishing intentional financial misconduct. Some lending investigations have employed overdue repayment as an operational indicator of fraud, although delinquency and deliberate deception have represented different financial phenomena. Consequently, H1 and H3 have received qualified preliminary support, whereas the evidence concerning data integrity and the comparative superiority of heterogeneous or temporal architectures has remained less conclusive. The five-point evidence ratings have provided interpretive classifications rather than

statistical confirmation, and the proposed 90-publication corpus has remained subject to complete PRISMA screening and quality assessment.

Comparison with previous evidence

The theoretical interpretation of the findings has reinforced the suitability of Graph Theory as the principal foundation for examining data integrity and security in interconnected digital-lending environments. Graph Theory has provided a structured explanation of how borrowers, accounts, applications, devices, and transactions can be represented as vertices connected through different relational structures. The study's conceptual framework has connected these representations with relational anomaly identification, potential data inconsistencies, coordinated financial misconduct, and implementation constraints. Earlier graph research has demonstrated that community structures, structural relationships, and neighborhood characteristics can reveal information about interconnected entities that cannot be fully understood through isolated observations (Blondel et al., 2008; Newman, 2006). The present synthesis has extended this theoretical perspective by distinguishing three complementary analytical dimensions: structural anomalies involving unusual connections, attribute anomalies involving inconsistent entity information, and temporal anomalies involving irregular changes in network relationships. Research on graph dependencies has demonstrated how relational constraints can support the identification of numeric and structural inconsistencies, while graph convolutional approaches have established mechanisms for learning from heterogeneous relationship types (Fan et al., 2018; Schlichtkrull et al., 2018). These contributions have supported the conceptual relevance of H2 and H4, although their lending-specific effectiveness has required separate empirical validation. The theoretical framework has also clarified that structurally unusual relationships do not necessarily represent fraud and that mathematically consistent records may still contain deliberately fabricated information. Consequently, the study has treated graph-based anomaly detection as an analytical mechanism that supports integrity assessment and security investigation rather than as an independent guarantee of data correctness. An additional theoretical contribution has involved separating graph representation quality, anomaly detection capability, and operational security outcomes into distinct conceptual components. This separation has strengthened the interpretation of the five hypotheses by preventing improvements in classification performance from being automatically equated with comprehensive financial security. The proposed framework has therefore established a structured basis for comparing graph methodologies while maintaining the conceptual distinction between financial credit risk, relational anomalies, data integrity, and fraudulent behavior.

Mechanisms and implications for practice

From a practical perspective, the synthesized findings have demonstrated how graph-based anomaly detection can complement conventional security controls within digital-lending institutions. The reviewed literature has identified several categories of suspicious financial activity, including interconnected loan applications, shared device identifiers, unusual transaction relationships, coordinated intermediaries, and inconsistent borrower information. These patterns have suggested that operational fraud investigations can benefit from examining relationships among multiple financial entities rather than relying exclusively on individual transaction characteristics. Earlier research has demonstrated the applicability of heterogeneous graph attention to financial cash-out detection and the use of multipartite transaction networks for identifying suspicious money flows (Hu et al., 2019; Li et al., 2020). The present study has interpreted these findings within a broader digital-lending security framework by considering how graph-based detection may complement identity verification, loan application assessment, transaction monitoring, and data integrity validation. However, graph-generated alerts have not been treated as conclusive evidence of fraud because legitimate borrowers may share addresses, devices, financial accounts, or commercial relationships. The literature has also highlighted operational concerns involving personal-data protection, unauthorized information access, and questionable lending practices. Research examining Indonesian peer-to-peer lending has documented data leakage, personal-data fraud, and illegal lending activities, demonstrating that digital-lending security involves institutional governance as well as computational detection capabilities (Suryono et al., 2021). Furthermore, research on interpretable machine learning has emphasized the importance of transparent decision-making in applications affecting individuals'

financial opportunities (Rudin, 2019). Accordingly, the discussion has identified human verification, documented anomaly explanations, proportionate investigation procedures, privacy controls, and continuous security auditing as important considerations for implementation. These practical considerations have strengthened the relevance of H5 while establishing that effective lending security requires coordinated technological and institutional safeguards rather than reliance on a single anomaly detection algorithm.

Digital-lending institutions should consider graph-based anomaly detection as a supplementary analytical safeguard, integrated with identity verification, transaction monitoring, access controls, audit trails, and human investigation. Implementation should begin with explicit definitions of suspicious behavior, verified relationship types, transparent data provenance, and protections against erroneous linking of distinct borrowers. Graph alerts should be reviewed against contextual evidence before adverse lending decisions are made. Researchers should give priority to lending-specific evaluations using independently verified fraud labels rather than treating payment delinquency as direct evidence of deception. The proposed Integrity-Aware Explainable Heterogeneous Temporal Graph Anomaly Detection Framework (IEHT-GAD) offers a structured research direction by combining typed borrower-account-device relationships, temporal event analysis, graph-based consistency constraints, interpretable anomaly explanations, and adversarial robustness checks. Future evaluations should compare its components with conventional models and established graph methods under equivalent datasets, metrics, and validation procedures. Particular attention should be given to precision, recall, false alerts, detection latency, explanation fidelity, fairness, and privacy risks. For the systematic review itself, researchers should complete reproducible database searches, record PRISMA flow counts, evaluate all eligible studies consistently, and distinguish direct lending evidence from adjacent financial applications. Such practices would support reliable interpretation and responsible adoption decisions across diverse real lending populations.

Limitations

The methodological limitations identified throughout the review have required careful interpretation of the preliminary findings and their relationship to earlier research. Although graph-based anomaly detection studies have reported encouraging results, their experimental designs have differed considerably in dataset construction, fraud definitions, graph topology, feature selection, validation procedures, and performance indicators. These differences have restricted the direct comparability of published findings and have prevented the calculation of a defensible pooled effectiveness estimate. Earlier systematic research has similarly identified methodological heterogeneity and the importance of considering graph characteristics, data labels, and application contexts when evaluating financial fraud detection techniques (Pourhabibi et al., 2020). A particularly important limitation has concerned the distinction between studies conducted directly in digital-lending environments and investigations involving cryptocurrency transactions, payment services, social networks, or banking systems. Although these adjacent domains have provided valuable methodological insights, their findings have not necessarily established equivalent effectiveness in lending applications. Furthermore, limited access to verified fraud labels has complicated the distinction between intentional deception, payment delinquency, administrative inconsistencies, and legitimate but unusual financial activities. Research examining camouflaged fraudsters has demonstrated that manipulated features and relationships can also affect graph neural network detection, introducing additional concerns regarding adversarial robustness (Dou et al., 2020). The present study has encountered a further methodological boundary because the target corpus of 90 publications has not yet undergone fully documented screening, evidence extraction, and quality appraisal. Consequently, the provisional five-point hypothesis assessments have not constituted final systematic-review results. In accordance with established systematic review reporting principles, the final interpretation has required transparent search records, documented exclusions, methodological quality assessment, and explicit treatment of conflicting evidence (Page et al., 2021). These considerations have demonstrated why publication counts, favorable individual experiments, and preliminary evidence ratings have not independently established the validity of all five hypotheses.

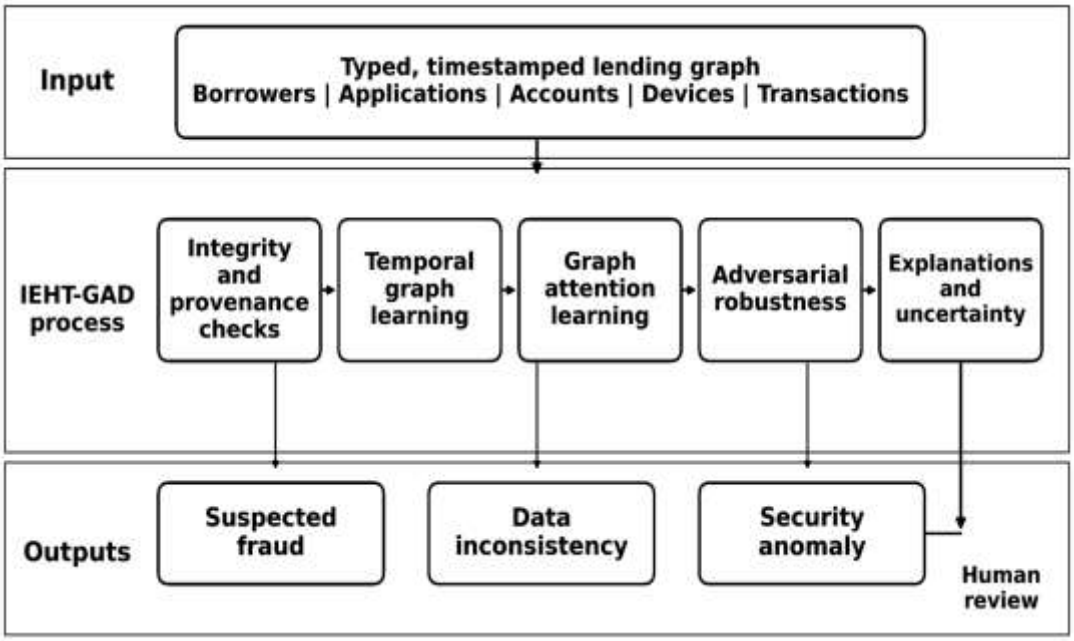
This study has been limited by its reliance on published secondary evidence rather than direct

observation of digital-lending platforms, borrower records, or operational security incidents. The targeted corpus of 90 publications has established an intended review scope, but completed database searches, duplicate removal, full-text screening, and quality appraisal have not yet been demonstrated. Consequently, the descriptive distributions and five-point hypothesis judgments presented earlier have remained provisional and cannot support claims about the final evidence corpus. The available publications have also differed in fraud definitions, graph construction, data access, labeling quality, evaluation metrics, and institutional settings, restricting meaningful comparisons across studies. Some lending models have classified overdue repayment as fraud, even though default has not necessarily indicated deliberate deception. Evidence derived from payment networks, banking, and other domains has provided methodological context without directly validating digital-lending effectiveness. Publication bias, unavailable proprietary datasets, incomplete reporting, and inconsistent baseline selection have further constrained assessment of reported advantages. Graph-based anomalies have not independently established malicious intent, unauthorized modification, or complete data integrity. Finally, the proposed IEHT-GAD framework has remained conceptual and has not undergone implementation or validation. These limitations require cautious interpretation of the hypotheses and transparent separation of documented findings from proposed methods.

Future research

The research gaps identified through the preliminary synthesis have provided a foundation for proposing an original model for subsequent empirical investigation, designated the Integrity-Aware Explainable Heterogeneous Temporal Graph Anomaly Detection Framework (IEHT-GAD). This proposed framework would integrate relational fraud detection, explicit data integrity validation, temporal behavioral analysis, and interpretable security assessment within a unified digital-lending architecture.

Figure 10: Proposed Integrity-Aware Explainable Heterogeneous Temporal Graph Anomaly Detection Framework (IEHT-GAD)



Its first component would construct a heterogeneous graph connecting borrowers, applications, bank accounts, devices, payment transactions, merchants, and financial intermediaries through explicitly defined and timestamped relationships. The second component would incorporate graph dependency constraints and provenance checks to identify conflicting identities, inconsistent financial attributes, and suspicious modifications to interconnected records. A temporal graph-learning component would

examine evolving relationships and coordinated activities, while an attention-based relational learning component would evaluate the relevance of different connection types. These components would be complemented by an adversarial robustness mechanism designed to examine manipulated features, misleading connections, and coordinated attempts to conceal suspicious activities. Earlier investigations of camouflage-resistant graph learning have provided a methodological foundation for such robustness considerations, while research on self-explainable graph neural networks has demonstrated approaches for generating interpretable graph-based classifications (Dai & Wang, 2021; Dou et al., 2020). Unlike a conventional fraud classification model, the proposed IEHT-GAD framework would generate separate outputs for suspected fraud, relational data inconsistency, and security-related anomalies, accompanied by traceable explanations and uncertainty indicators. Future researchers could evaluate this architecture using verified digital-lending cases, temporally separated training and testing datasets, independent institutional validation, and comparisons against conventional machine learning, graph convolutional, graph attention, and graph dependency methods. Evaluation could examine precision, recall, F1-score, area under the precision-recall curve, false-positive rates, detection latency, explanation fidelity, and the accuracy of identified integrity violations. Additional investigation could assess privacy-preserving data sharing, subgroup fairness, graph construction sensitivity, and operational investigation costs. Controlled ablation experiments could determine the independent contribution of each architectural component. These proposed investigations have remained recommendations for future empirical research rather than experiments conducted in the present qualitative review. The model would therefore provide a testable framework for addressing the methodological and operational limitations identified across the five hypotheses while retaining the conceptual distinctions established by Graph Theory.

Conclusion

This study has examined graph-based anomaly detection as a framework for understanding data integrity and security challenges in digital-lending systems. Guided by Graph Theory, the review has connected relational representations of borrowers, accounts, applications, devices, and transactions with the identification of suspicious relationships and potentially fraudulent activity. The evidence discussed has indicated that graph-attentive and role-aware approaches have achieved encouraging results in particular lending investigations, while research from payment and banking environments has offered complementary methodological insights. However, classification improvements have not established universal superiority, proven fraud, or guaranteed the integrity of lending records. The five hypotheses have therefore received provisional, differentiated interpretations: qualified support for relational detection and coordinated-fraud identification, more limited direct evidence for integrity protection and comparative graph architectures, and substantial concern about implementation constraints. The proposed review has targeted 90 eligible publications, but its full PRISMA screening, extraction, and quality appraisal have not yet been documented; its preliminary evidence ratings cannot be treated as final systematic-review findings. The central contribution has been a coherent conceptual distinction among anomaly identification, data validation, fraud investigation, and cybersecurity governance. This distinction has provided a defensible foundation for assessing published methods without confusing secondary evidence synthesis with original experimental verification.

REFERENCES

[1]. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

[2]. Aditya, D., & Ahmed, H. C. H. R. (2022). Decision Support Systems for Last-Mile Logistics Optimization: A Data-Driven Framework for e-Commerce Fulfillment Networks. *International Journal of Scientific Interdisciplinary Research*, *12*(08), 01–49. https://doi.org/10.63125/h46vp562

[3]. Akoglu, L., McGlohon, M., & Faloutsos, C. (2010). OddBall: Spotting anomalies in weighted graphs. Advances in knowledge discovery and data mining,

[4]. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: A survey. *Data Mining and Knowledge Discovery*, *29*(3), 626–688. https://doi.org/10.1007/s10618-014-0365-y

[5]. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*, Article 100402. https://doi.org/10.1016/j.cosrev.2021.100402

[6]. Alarab, I., Prakoonwit, S., & Nacer, M. I. (2020). Competence of graph convolutional networks for anti-money laundering in Bitcoin blockchain. Proceedings of the 2020 5th International Conference on Machine Learning Technologies,

[7]. Aminul Islam, M., & Md, A. (2023). Adaptive Class-Imbalance Learning for High-Sensitivity Fraud Detection in Large-Scale Digital Transaction Networks. *International Journal of Business and Economics Insights*, *13*(09), 01-33. https://doi.org/10.63125/bmxwv741

[8]. Asheke, M. (2023). Machine Learning–Based Predictive Quality Modeling for Defect Detection and Process Optimization in Advanced Manufacturing Systems. *Review of Applied Science and Technology*, *13*(12), 01–49. https://doi.org/10.63125/thy73b16

[9]. Asheke, M., & Md Maksudul, H. (2022). AI-Driven Demand Forecasting for Sporting-Goods and Teamwear Supply Chains Under Seasonal and Tournament Demand. *International Journal of Business and Economics Insights*, *2*(1), 73–110. https://doi.org/10.63125/ed6by557

[10]. Asheke, M., & Mohammad Badrul, A. (2022). Development Of Functionalized Cellulose Nanofiber Adsorbents for Selective Critical-Metal Recovery from Industrial Wastewater. *American Journal of Scholarly Research and Innovation*, *1*(02), 270–320. https://doi.org/10.63125/v6fxzq09

[11]. Bandyopadhyay, S., Lokesh, N., & Murty, M. N. (2019). Outlier aware network embedding for attributed networks. *Proceedings of the AAAI Conference on Artificial Intelligence*, *33*(1), 12–19. https://doi.org/10.1609/aaai.v33i01.330112

[12]. Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[13]. Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009). Methodologies for data quality assessment and improvement. *ACM Computing Surveys*, *41*(3), Article 16. https://doi.org/10.1145/1541880.1541883

[14]. Bavoso, V. (2020). The promise and perils of alternative market-based finance: The case of P2P lending in the UK. *Journal of Banking Regulation*, *21*, 395–409. https://doi.org/10.1057/s41261-019-00118-9

[15]. Benjelloun, O., Garcia-Molina, H., Menestrina, D., Su, Q., Whang, S. E., & Widom, J. (2009). Swoosh: A generic approach to entity resolution. *The VLDB Journal*, *18*(1), 255–276. https://doi.org/10.1007/s00778-008-0098-x

[16]. Berg, T., Burg, V., Gombović, A., & Puri, M. (2020). On the rise of FinTechs: Credit scoring using digital footprints. *The Review of Financial Studies*, *33*(7), 2845–2897. https://doi.org/10.1093/rfs/hhz099

[17]. Bhattacharya, I., & Getoor, L. (2007). Collective entity resolution in relational data. *ACM Transactions on Knowledge Discovery from Data*, *1*(1), Article 5. https://doi.org/10.1145/1217299.1217304

[18]. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008

[19]. Blondel, V. D., Guillaume, J.-L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, *2008*(10), Article P10008. https://doi.org/10.1088/1742-5468/2008/10/p10008

[20]. Buchak, G., Matvos, G., Piskorski, T., & Seru, A. (2018). Fintech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Economics*, *130*(3), 453–483. https://doi.org/10.1016/j.jfineco.2018.03.011

[21]. Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, *557*, 317–331. https://doi.org/10.1016/j.ins.2019.05.042

[22]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), Article 15. https://doi.org/10.1145/1541880.1541882

[23]. Chau, D. H., Pandit, S., & Faloutsos, C. (2006). Detecting fraudulent personalities in networks of online auctioneers. Knowledge discovery in databases: PKDD 2006,

[24]. Dai, E., & Wang, S. (2021). Towards self-explainable graph neural network. Proceedings of the 30th ACM International Conference on Information & Knowledge Management,

[25]. Deng, A., & Hooi, B. (2021). Graph neural network-based anomaly detection in multivariate time series. *Proceedings of the AAAI Conference on Artificial Intelligence*, *35*(5), 4027–4035. https://doi.org/10.1609/aaai.v35i5.16523

[26]. Ding, K., Li, J., Bhanushali, R., & Liu, H. (2019). Deep anomaly detection on attributed networks. Proceedings of the 2019 SIAM International Conference on Data Mining,

[27]. Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2020). Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. Proceedings of the 29th ACM International Conference on Information & Knowledge Management,

[28]. Dreżewski, R., Sepielak, J., & Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences*, *295*, 18–32. https://doi.org/10.1016/j.ins.2014.10.015

[29]. Duarte, J., Siegel, S., & Young, L. (2012). Trust and credit: The role of appearance in peer-to-peer lending. *The Review of Financial Studies*, *25*(8), 2455–2484. https://doi.org/10.1093/rfs/hhs071

[30]. Eberle, W., & Holder, L. (2007). Anomaly detection in data represented as graphs. *Intelligent Data Analysis*, *11*(6), 663–689. https://doi.org/10.3233/ida-2007-11606

[31]. Eswaran, D., Faloutsos, C., Guha, S., & Mishra, N. (2018). SpotLight: Detecting anomalies in streaming graphs. Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining,

[32]. Fan, H., Zhang, F., & Li, Z. (2020). AnomalyDAE: Dual autoencoder for anomaly detection on attributed networks. 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),

[33]. Fan, W., Liu, X., Lu, P., & Tian, C. (2018). Catching numeric inconsistencies in graphs. Proceedings of the 2018 International Conference on Management of Data,

[34]. Fan, W., & Lu, P. (2017). Dependencies for graphs. Proceedings of the 36th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems,

[35]. Fan, W., Wu, Y., & Xu, J. (2016). Functional dependencies for graphs. Proceedings of the 2016 International Conference on Management of Data,

[36]. Freedman, S., & Jin, G. Z. (2017). The information value of online social networks: Lessons from peer-to-peer lending. *International Journal of Industrial Organization*, *51*, 185–222. https://doi.org/10.1016/j.ijindorg.2016.09.002

[37]. Fronzetti Colladon, A., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications*, *67*, 49–58. https://doi.org/10.1016/j.eswa.2016.09.029

[38]. Giudici, P., Hadji-Misheva, B., & Spelta, A. (2019). Network based scoring models to improve credit risk management in peer to peer lending platforms. *Frontiers in Artificial Intelligence*, *2*, Article 3. https://doi.org/10.3389/frai.2019.00003

[39]. Grover, A., & Leskovec, J. (2016). node2vec: Scalable feature learning for networks. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,

[40]. He, Q., & Li, X. (2021). The failure of Chinese peer-to-peer lending platforms: Finance and politics. *Journal of Corporate Finance*, *66*, Article 101852. https://doi.org/10.1016/j.jcorpfin.2020.101852

[41]. Hooi, B., Song, H. A., Beutel, A., Shah, N., Shin, K., & Faloutsos, C. (2016). FRAUDAR: Bounding graph fraud in the face of camouflage. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,

[42]. Hu, B., Zhang, Z., Shi, C., Zhou, J., Li, X., & Qi, Y. (2019). Cash-out user detection based on attributed heterogeneous information network with a hierarchical attention mechanism. *Proceedings of the AAAI Conference on Artificial Intelligence*, *33*(1), 946–953. https://doi.org/10.1609/aaai.v33i01.3301946

[43]. Iyer, R., Khwaja, A. I., Luttmer, E. F. P., & Shue, K. (2016). Screening peers softly: Inferring the quality of small borrowers. *Management Science*, *62*(6), 1554–1577. https://doi.org/10.1287/mnsc.2015.2181

[44]. Jagtiani, J., & Lemieux, C. (2019). The roles of alternative data and machine learning in fintech lending: Evidence from the LendingClub consumer platform. *Financial Management*, *48*(4), 1009–1029. https://doi.org/10.1111/fima.12295

[45]. Jin, M., Liu, Y., Zheng, Y., Chi, L., Li, Y.-F., & Pan, S. (2021). ANEMONE: Graph anomaly detection with multi-scale contrastive learning. Proceedings of the 30th ACM International Conference on Information & Knowledge Management,

[46]. Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance*, *34*(11), 2767–2787. https://doi.org/10.1016/j.jbankfin.2010.06.001

[47]. Lee, J. W., Lee, W. K., & Sohn, S. Y. (2021). Graph convolutional network-based credit default prediction utilizing three types of virtual distances among borrowers. *Expert Systems with Applications*, *168*, Article 114411. https://doi.org/10.1016/j.eswa.2020.114411

[48]. Lessmann, S., Baesens, B., Seow, H.-V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research*, *247*(1), 124–136. https://doi.org/10.1016/j.ejor.2015.05.030

[49]. Li, J., Dani, H., Hu, X., & Liu, H. (2017). Radar: Residual analysis for anomaly detection in attributed networks. Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence,

[50]. Li, X., Liu, S., Li, Z., Han, X., Shi, C., Hooi, B., Huang, H., & Cheng, X. (2020). FlowScope: Spotting money laundering based on graphs. *Proceedings of the AAAI Conference on Artificial Intelligence*, *34*(4), 4731–4738. https://doi.org/10.1609/aaai.v34i04.5906

[51]. Li, Y., Huang, X., Li, J., Du, M., & Zou, N. (2019). SpecAE: Spectral autoencoder for anomaly detection in attributed networks. Proceedings of the 28th ACM International Conference on Information and Knowledge Management,

[52]. Li, Y., Sun, Y., & Contractor, N. (2017). Graph mining assisted semi-supervised learning for fraudulent cash-out detection. Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,

[53]. Lin, M., Prabhala, N. R., & Viswanathan, S. (2013). Judging borrowers by the company they keep: Friendship networks and information asymmetry in online peer-to-peer lending. *Management Science*, *59*(1), 17–35. https://doi.org/10.1287/mnsc.1120.1560

[54]. Liu, S., Hooi, B., & Faloutsos, C. (2017). HoloScope: Topology-and-spike aware fraud detection. Proceedings of the 2017 ACM on Conference on Information and Knowledge Management,

[55]. Liu, Y., Ao, X., Qin, Z., Chi, J., Feng, J., Yang, H., & He, Q. (2021). Pick and choose: A GNN-based imbalanced learning approach for fraud detection. Proceedings of the Web Conference 2021,

[56]. Liu, Z., Chen, C., Yang, X., Zhou, J., Li, X., & Song, L. (2018). Heterogeneous graph neural networks for malicious account detection. Proceedings of the 27th ACM International Conference on Information and Knowledge Management,

[57]. Liu, Z., Dou, Y., Yu, P. S., Deng, Y., & Peng, H. (2020). Alleviating the inconsistency problem of applying graph neural network to fraud detection. Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval,

[58]. Mansura Akter, E., & Sumaiya, M. (2022). Antimicrobial Resistance Profiles of Acinetobacter Baumannii and Vibrio Cholerae in Hospital Wastewater and Adjacent Household Water Sources. *American Journal of Data Science and Analytics*, *3*(09), 01-55. https://doi.org/10.63125/gbervt14

[59]. Md Imran, H., & Jannatul, F. (2022). Molecular and Precision Rehabilitation Molecular Mechanisms Linking Mitochondrial Dysfunction, Inflammation, and Muscle Degeneration with Functional Decline and Rehabilitation Response in Neuromuscular Disease. *American Journal of Interdisciplinary Studies*, *12*(08), 01-44. https://doi.org/10.63125/0ym5bh79

[60]. Md Maksudul, H., & Md Tazul Islam, C. (2022). Machine Learning-Based Cash-Flow Forecasting for Improving Financial Planning in U.S. Small and Mid-Sized Businesses. *International Journal of Scientific Interdisciplinary Research*, *12*(12), 01–38. https://doi.org/10.63125/w3pgjx97

[61]. Md Shahid, N. (2023). Digital Twin-Based Network Reliability Modeling for LAN And WAN Infrastructure Resilience. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 577–629. https://doi.org/10.63125/ahjvxj14

[62]. Md Tazul Islam, C., & Ahmed, H. C. H. R. (2023). Predictive Operations Analytics for Resource Allocation and Service-Capacity Planning in Data-Driven Organizations. *Review of Applied Science and Technology*, *13*(02), 01–41. https://doi.org/10.63125/z3sm3089

[63]. Md. Morshedul, I., & Aminul Islam, M. (2022). A Quantitative Evaluation of Explainable Ensemble Learning for Probabilistic Risk Estimation and Decision Reliability in Enterprise Analytics. *American Journal of Data Science and Analytics*, *3*(02), 01-38. https://doi.org/10.63125/k22shk74

[64]. Newman, M. E. J. (2006). Modularity and community structure in networks. *Proceedings of the National Academy of Sciences*, *103*(23), 8577–8582. https://doi.org/10.1073/pnas.0601602103

[65]. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

[66]. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & . . . Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, Article n71. https://doi.org/10.1136/bmj.n71

[67]. Peng, Z., Luo, M., Li, J., Liu, H., & Zheng, Q. (2018). ANOMALOUS: A joint modeling approach for anomaly detection on attributed networks. Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence,

[68]. Perozzi, B., & Akoglu, L. (2016). Scalable anomaly ranking of attributed neighborhoods. Proceedings of the 2016 SIAM International Conference on Data Mining,

[69]. Pokorný, J., Valenta, M., & Kovačič, J. (2017). Integrity constraints in graph databases. *Procedia Computer Science*, *109*, 975–981. https://doi.org/10.1016/j.procs.2017.05.456

[70]. Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, *133*, Article 113303. https://doi.org/10.1016/j.dss.2020.113303

[71]. Prusti, D., Das, D., & Rath, S. K. (2021). Credit card fraud detection technique by applying graph database model. *Arabian Journal for Science and Engineering*, *46*(9), 8849–8868. https://doi.org/10.1007/s13369-021-05682-9

[72]. Ranshous, S., Shen, S., Koutra, D., Harenberg, S., Faloutsos, C., & Samatova, N. F. (2015). Anomaly detection in dynamic networks: A survey. *WIREs Computational Statistics*, *7*(3), 223–247. https://doi.org/10.1002/wics.1347

[73]. Reina, F. M., Huf, A., Presser, D., & Siqueira, F. (2021). Extending the integrity constraint support in a graph database. *IEEE Latin America Transactions*, *19*(4), 604–611. https://doi.org/10.1109/tla.2021.9448543

[74]. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, *1*, 206–215. https://doi.org/10.1038/s42256-019-0048-x

[75]. Sadia, A., & Md. Mosheur, R. (2023). Consumer Trust, Perceived Authenticity, and Personalized Digital Marketing: A Quantitative Decision-Science Study. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 252–295. https://doi.org/10.63125/cajkqt60

[76]. Saimima, I. D. S., & Patria, V. G. (2021). The fintech phenomenon: Protection of consumer privacy data in online lending. *Jurnal Kajian Ilmiah*, *21*(2), 185–194. https://doi.org/10.31599/jki.v21i2.564

[77]. Schlichtkrull, M., Kipf, T. N., Bloem, P., van den Berg, R., Titov, I., & Welling, M. (2018). Modeling relational data with graph convolutional networks. In *The semantic web* (Vol. 10843, pp. 593–607). Springer. https://doi.org/10.1007/978-3-319-93417-4_38

[78]. Shuman, D. I., Narang, S. K., Frossard, P., Ortega, A., & Vandergheynst, P. (2013). The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains. *IEEE Signal Processing Magazine*, *30*(3), 83–98. https://doi.org/10.1109/msp.2012.2235192

[79]. Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*, Article 100418. https://doi.org/10.1016/j.accinf.2019.06.001

[80]. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

[81]. Stabak, D., & Md Shahid, N. (2022). Empirical Assessment of Uncertainty-Aware Real-Time Decision-Making for Reliable and Resilient Cyber-Physical Systems. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 432–477. https://doi.org/10.63125/q3r4kk16

[82]. Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. *Heliyon*, *7*(4), Article e06782. https://doi.org/10.1016/j.heliyon.2021.e06782

[83]. Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to peer (P2P) lending problems and potential solutions: A systematic literature review. *Procedia Computer Science*, *161*, 204–214. https://doi.org/10.1016/j.procs.2019.11.116

[84]. Syed Feroz, A., & Md Mahamud Pervaz, P. (2022). Root-Cause Analysis and FMEA-Driven Reliability Improvement in Gas Production Facilities: A Multi-Year Empirical Study. *International Journal of Scientific Interdisciplinary Research*, *12*(10), 01–53. https://doi.org/10.63125/70msp878

[85]. Syed Feroz, A., & Shabbir, A. (2022). Finite Element-Based Thermomechanical Optimization of Pressure Components for Extending Industrial Boiler Service Life. *Journal of Sustainable Development and Policy*, *12*(12), 01-51. https://doi.org/10.63125/x24pht28

[86]. Tamersoy, A., Roundy, K. A., & Chau, D. H. (2014). Guilt by association: Large scale malware detection by mining file-relation graphs. Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,

[87]. Tang, H. (2019). Peer-to-peer lenders versus banks: Substitutes or complements? *The Review of Financial Studies*, *32*(5), 1900–1938. https://doi.org/10.1093/rfs/hhy137

[88]. Vallée, B., & Zeng, Y. (2019). Marketplace lending: A new banking paradigm? *The Review of Financial Studies*, *32*(5), 1939–1982. https://doi.org/10.1093/rfs/hhy100

[89]. Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems*, *75*, 38–48. https://doi.org/10.1016/j.dss.2015.04.013

[90]. Van Vlasselaer, V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2017). GOTCHA! Network-based fraud detection for social security fraud. *Management Science*, *63*(9), 3090–3110. https://doi.org/10.1287/mnsc.2016.2489

[91]. Wang, C., Zhang, W., Zhao, X., & Wang, J. (2019). Soft information in online peer-to-peer lending: Evidence from a leading platform in China. *Electronic Commerce Research and Applications*, *36*, Article 100873. https://doi.org/10.1016/j.elerap.2019.100873

[92]. Wang, D., Qi, Y., Lin, J., Cui, P., Jia, Q., Wang, Z., Fang, Y., Yu, Q., Zhou, J., & Yang, S. (2019). A semi-supervised graph attentive network for financial fraud detection. 2019 IEEE International Conference on Data Mining (ICDM),

[93]. Wang, Q., Liu, H., He, J., & Du, X. (2020). A graph attentive network model for P2P lending fraud detection. Knowledge science, engineering and management,

[94]. Wang, Q., Su, Z., & Chen, X. (2021). Information disclosure and the default risk of online peer-to-peer lending platform. *Finance Research Letters*, *38*, Article 101509. https://doi.org/10.1016/j.frl.2020.101509

[95]. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, *18*(1), 30–55. https://doi.org/10.1007/s10618-008-0116-z

[96]. Wu, Z., Hu, L., Lin, Z., & Tan, Y. (2021). Competition and distortion: A theory of information bias on the peer-to-peer lending market. *Information Systems Research*, *32*(4), 1140–1154. https://doi.org/10.1287/isre.2020.0956

[97]. Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2021). A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems*, *32*(1), 4–24. https://doi.org/10.1109/tnnls.2020.2978386

[98]. Xu, B., Shen, H., Sun, B., An, R., Cao, Q., & Cheng, X. (2021). Towards consumer loan fraud detection: Graph neural networks with role-constrained conditional random field. *Proceedings of the AAAI Conference on Artificial Intelligence*, *35*(5), 4537–4545. https://doi.org/10.1609/aaai.v35i5.16582

[99]. Xu, X., Yuruk, N., Feng, Z., & Schweiger, T. A. J. (2007). SCAN: A structural clustering algorithm for networks. Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,

[100]. Yan, J., Yu, W., & Zhao, J. L. (2015). How signaling and search costs affect information asymmetry in P2P lending: The economics of big data. *Financial Innovation*, *1*, Article 19. https://doi.org/10.1186/s40854-015-0018-1

[101]. Yu, W., Cheng, W., Aggarwal, C. C., Zhang, K., Chen, H., & Wang, W. (2018). NetWalk: A flexible deep embedding approach for anomaly detection in dynamic networks. Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining,

[102]. Zheng, L., Li, Z., Li, J., Li, Z., & Gao, J. (2019). AddGraph: Anomaly detection in dynamic graph using attention-based temporal GCN. Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence,

[103]. Zhou, H., Zhang, M., Pang, L., & Li, J.-H. (2021). Abnormal detection of cash-out groups in IoT based payment. *Sensors*, *21*(22), Article 7507. https://doi.org/10.3390/s21227507

[104]. Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C., & Sun, M. (2020). Graph neural networks: A review of methods and applications. *AI Open*, *1*, 57–81. https://doi.org/10.1016/j.aiopen.2021.01.001

[105]. Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. *The Innovation*, *2*(4), Article 100176. https://doi.org/10.1016/j.xinn.2021.100176

[106]. Zhu, Z. (2018). Safety promise, moral hazard and financial supervision: Evidence from peer-to-peer lending. *Finance Research Letters*, *27*, 1–5. https://doi.org/10.1016/j.frl.2018.07.002