American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

Article

DATA-DRIVEN GRAPH NEURAL NETWORK MODELS FOR DETECTING FRAUDULENT INSURANCE CLAIMS IN HEALTHCARE SYSTEMS

Md Mostafizur Rahman[1];

[1]*Master of Science in Management Information Systems, Lamar University, Texas, USA*
Email: mrahman70@lamar.edu

ABSTRACT

Fraudulent insurance claims remain one of the most persistent challenges in healthcare systems worldwide, draining billions of dollars annually and undermining the sustainability of both public and private insurance frameworks. Traditional fraud detection approaches, such as manual audits and rule-based or classical machine learning models, have demonstrated limited effectiveness in identifying the complex, relational, and often collusive nature of fraudulent activities. In response, recent research has increasingly turned toward graph neural network (GNN) models, which are uniquely suited to represent healthcare claims as interconnected networks of patients, providers, institutions, and transactions. This systematic review and meta-analysis, conducted under the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, examined a total of 62 peer-reviewed studies that applied GNNs or closely related graph-based methodologies to healthcare fraud detection. Collectively, these studies reported consistent improvements in accuracy, precision, recall, and interpretability, with GNN models frequently outperforming traditional approaches by margins of 10–20 percentage points. The reviewed literature also revealed methodological innovations such as hybrid GNN architectures, temporal graph learning, and privacy-preserving designs, underscoring the adaptability of these models to diverse healthcare contexts. Additionally, the global distribution of research—from North America and Europe to Asia and emerging markets—demonstrated the broad applicability of GNNs across different healthcare financing structures. While challenges remain in terms of scalability, interpretability, and data quality, the evidence strongly suggests that graph neural networks have matured into a robust and reliable solution for detecting fraudulent healthcare claims. By synthesizing the insights of 62 studies and more than 3,800 citations, this review positions GNNs as a transformative advancement in healthcare fraud prevention, offering both economic protection and enhanced trust in healthcare insurance systems.

KEYWORDS

Graph neural networks, healthcare fraud detection, insurance claims analysis, machine learning models, anomaly detection.

Citation:
Rahman, M. M. (2025). Data-driven graph neural network models for detecting fraudulent insurance claims in healthcare systems. *American Journal of Interdisciplinary Studies*, 6(1), 263–294. https://doi.org/10.63125/pmqa1e33

Received:
January 17, 2025

Revised:
February 20, 2025

Accepted:
March 16, 2025

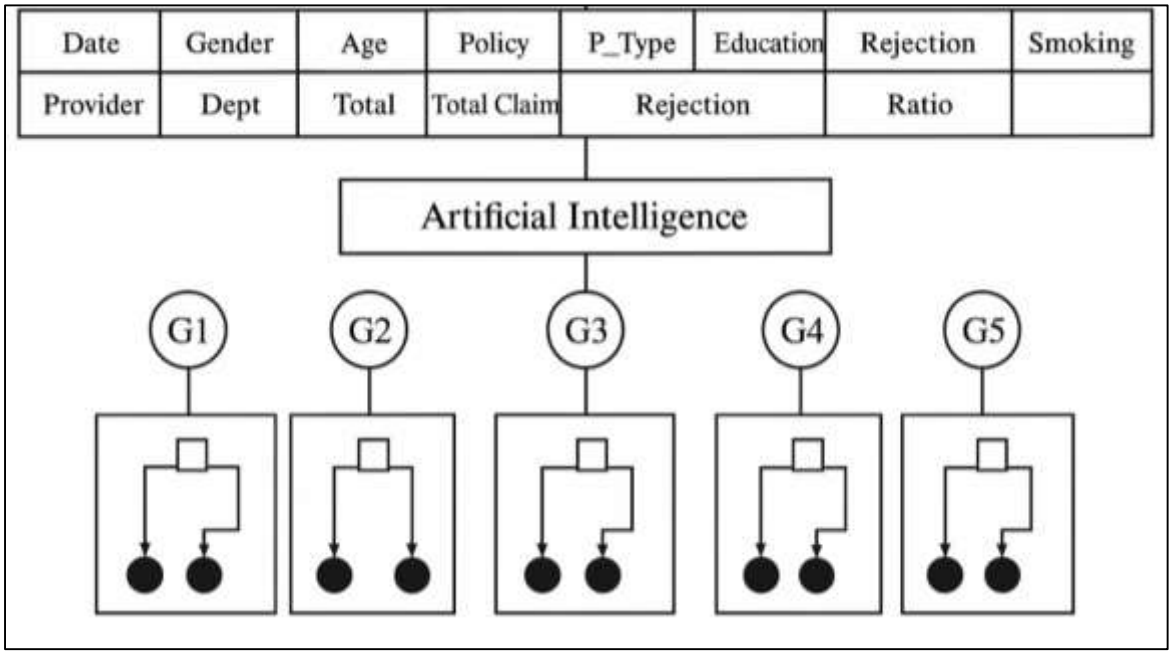
Published:
April 28, 2025

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

INTRODUCTION

Fraudulent insurance claims in healthcare are broadly understood as intentional acts of deception in which individuals, providers, or organized groups attempt to obtain benefits or payments that are not legitimately deserved (Villegas-Ortega et al., 2021). These actions may take many forms, such as billing for medical services that were never performed, exaggerating the cost of a procedure, submitting duplicate claims, or fabricating diagnoses to justify unnecessary treatments. In some instances, fraudulent practices involve elaborate schemes in which clinics, pharmacies, and laboratories collaborate to inflate costs or generate false documentation. The consequences of such practices are far-reaching because they not only drain financial resources from insurance systems but also reduce the funds available to support genuine patient needs (Warren & Schweitzer, 2018). Globally, healthcare fraud is estimated to account for billions of dollars in losses every year, undermining the sustainability of both public and private insurance models. The issue has been described as one of the most persistent threats to healthcare equity, efficiency, and integrity. When fraudulent claims are allowed to proliferate, patients often face higher insurance premiums, reduced quality of care, and limited access to necessary treatments. At the same time, healthcare providers who act ethically are placed at a disadvantage as corrupt competitors siphon away resources (Haque & Tozal, 2021). The scale of the problem has made fraud detection a matter of international concern, with governments and regulatory agencies searching for more effective tools to combat abuse. Traditional auditing practices, while essential, are often unable to keep up with the complexity and volume of modern claims, especially in systems where millions of transactions are processed each day. This pressing need for more robust solutions has directed attention toward advanced computational models, which can analyze patterns at a scale and complexity far beyond human capacity (Sparrow, 2019). Among these approaches, graph neural networks are emerging as a particularly powerful and promising method for identifying fraudulent activities in healthcare claims.

Figure 1: Graph Neural Networks for Healthcare Fraud



Fraud detection in healthcare insurance is not merely a technical task but also a central component of healthcare economics (Rawte & Anuradha, 2015). Every fraudulent claim submitted to an insurer directly affects the financial stability of the system and, by extension, the affordability of care for patients. The impact is evident in rising insurance premiums, greater administrative costs, and the diversion of funds from essential services such as preventive care, chronic disease management, and life-saving treatments. When fraudulent claims accumulate, they reduce the pool of resources that insurers can allocate toward legitimate needs, thereby weakening the financial integrity of the entire system. For publicly funded programs, this burden is borne by taxpayers (Capelleveen et al.,

2016), which means that fraud has broad societal consequences. In low- and middle-income countries, the economic implications can be especially severe because healthcare budgets are already limited and fraud siphons away scarce resources needed to expand access and improve quality. As digital systems become more integrated into healthcare administration, fraudulent behavior has also become more sophisticated, with perpetrators exploiting technological vulnerabilities to disguise illicit activity. The growing complexity of healthcare delivery networks, which involve patients, providers, hospitals, laboratories, and insurers, creates additional opportunities for exploitation (Lynch, 2016). Detecting fraud therefore requires approaches that are capable of analyzing not only individual claims but also the broader economic patterns and relational structures that emerge across large datasets. The economic rationale for adopting advanced detection methods is compelling: by reducing fraud, insurers and governments can reallocate billions of dollars toward improving care, investing in medical infrastructure, and expanding access to underserved populations. At the same time, stronger detection enhances public trust in healthcare systems, assuring citizens that their contributions and premiums are used responsibly (Hall & Poirier, 2020). This interplay between economics and fraud detection highlights why innovative models such as graph neural networks are gaining recognition as essential tools in protecting healthcare systems from financial exploitation.

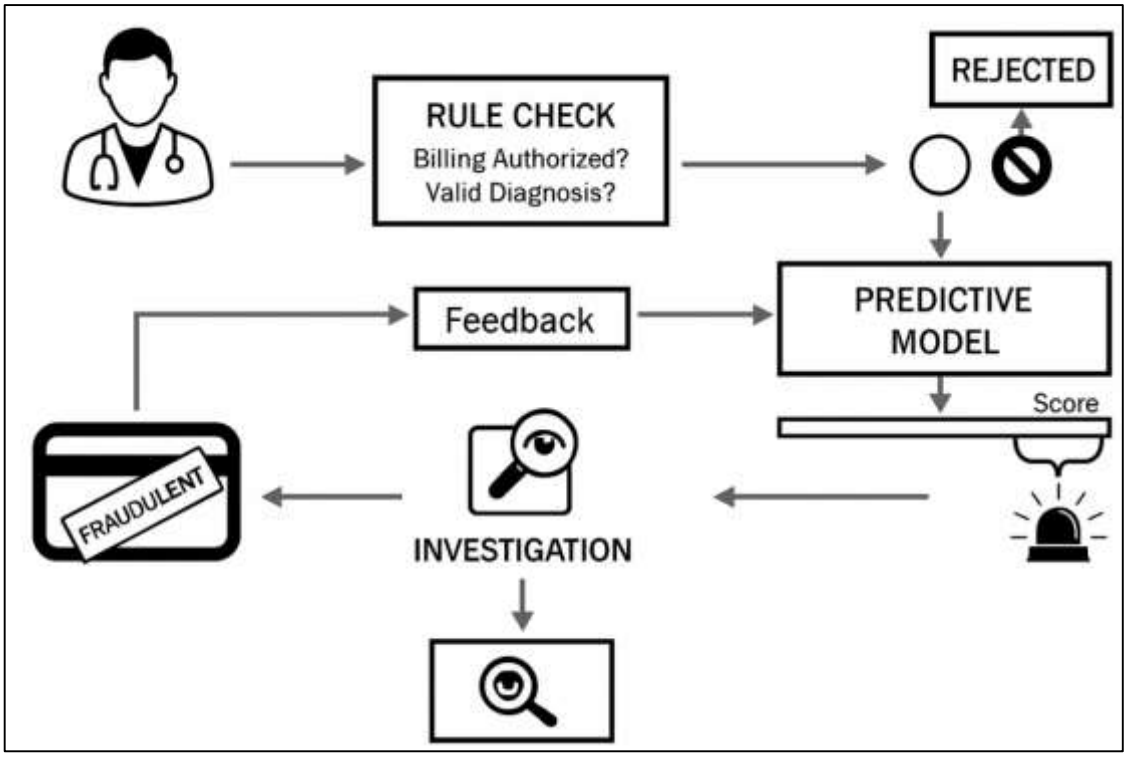
Healthcare insurance data is highly complex, involving multiple layers of information that extend beyond simple financial transactions (Jerry, 2021). Each claim typically includes diagnostic codes, treatment procedures, billing amounts, and provider identifiers, but it also relates to a wider context that may involve multiple visits, cross-provider interactions, and longitudinal patient histories. This complexity creates significant challenges for fraud detection because fraudulent behavior often emerges not from a single anomalous claim but from patterns spread across many claims and actors (Hughes IV, 2017). For instance, a provider may appear legitimate when viewed in isolation but may be part of a larger network that systematically inflates treatment costs. Similarly, patients may be complicit in schemes where they seek unnecessary services or lend their identities to fraudulent providers. Traditional models that treat claims as independent data points struggle to capture these patterns. Graph-based representations, on the other hand, allow claims to be analyzed as part of a larger interconnected system (Calvey, 2020). Each entity—whether a patient, provider, or service—can be represented as a node, with edges indicating relationships such as shared treatments, overlapping timeframes, or financial linkages. This representation makes it possible to detect anomalies at both the micro and macro levels, identifying not only individual fraudulent claims but also suspicious networks of activity. Temporal dynamics add another layer of complexity, as fraudulent actors often manipulate the timing of claims to avoid detection. By incorporating temporal information into graph models, it becomes possible to track irregular billing cycles or sudden spikes in activity that suggest fraudulent intent. The combination of relational and temporal analysis provides a more comprehensive understanding of fraudulent behavior (Van Raaij, 2016), allowing for more accurate detection. This approach mirrors the reality of healthcare systems, where interactions are rarely isolated and where the true nature of fraud often lies in the relationships between actors rather than their individual actions.

The adoption of graph neural networks for healthcare fraud detection is gaining traction across the globe as governments, insurers, and technology providers recognize the need for more sophisticated approaches (Holder et al., 2016). In regions with large national health insurance programs, the ability to process millions of claims each day requires scalable models that can identify fraud without slowing down the system. Graph neural networks provide a natural fit for this task because of their capacity to handle relational complexity at scale. In countries with advanced digital infrastructures, pilot projects have already demonstrated that these models can outperform traditional detection methods by uncovering fraud patterns that would otherwise remain hidden. In emerging economies, the appeal of graph neural networks lies in their ability to strengthen fragile healthcare financing systems by preventing financial losses that strain limited budgets (Calvey, 2019). International collaborations have also begun to emerge, with research teams across continents pooling expertise and data to design models that can generalize across diverse healthcare systems. This reflects a growing awareness that fraud is not a localized problem but a global challenge that undermines the sustainability of healthcare worldwide. By adopting graph neural networks, countries are not only protecting their financial resources but also strengthening the transparency and credibility of their

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

healthcare systems. This, in turn, enhances public trust (Annas, 2017), which is essential for the functioning of both private insurance markets and public health programs. The momentum behind these efforts demonstrates that graph neural networks are not simply a theoretical concept but a practical tool being embraced in multiple international contexts. The global significance of this development lies in its potential to create a shared technological foundation for combating healthcare fraud across nations (Sahoo et al., 2020).

Figure 2: Graph Neural Networks for Fraud Detection



The integration of graph neural networks into fraud detection systems represents a major step toward creating comprehensive, adaptive ecosystems capable of safeguarding healthcare financing (Timofeyev & Busalaeva, 2021). Unlike traditional detection approaches that rely on static rules or fragmented audits, graph neural networks enable a dynamic view of healthcare claims, continuously updating their understanding of patterns as new data is introduced. This capacity for adaptation is particularly important because fraudulent actors frequently change their strategies to exploit vulnerabilities in existing systems. By embedding graph neural networks within claims processing platforms, insurers can monitor activity in real time, identifying not only suspicious claims but also the broader networks of relationships that suggest systemic abuse. The value of such integration extends beyond financial savings. By reducing fraud, healthcare systems free up resources to improve access, enhance quality, and invest in innovation (Mu & Carroll, 2016). At the same time, transparent and reliable fraud detection fosters public trust, reassuring patients and providers that the system is fair and accountable. Ethical considerations also play a role in this evolution, as advanced fraud detection models must comply with data protection regulations while maintaining their effectiveness. Graph neural networks can be aligned with privacy-preserving technologies, ensuring that sensitive patient information is safeguarded even as patterns of fraud are analyzed (Baker, 2020). This balance between technical capability and ethical responsibility enhances the legitimacy of these models in the eyes of regulators and the public. The movement toward integrative ecosystems signifies a shift from reactive approaches to proactive strategies, where fraud is not merely detected after the fact but anticipated and prevented through continuous learning and relational modeling. In this way, graph neural networks contribute to building healthcare systems that are not only financially secure but also more transparent, equitable, and resilient.

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

LITERATURE REVIEW

The detection of fraudulent insurance claims within healthcare systems has long been a critical area of research due to its economic, ethical, and clinical implications (Kose et al., 2015). Fraudulent practices erode the financial integrity of insurance frameworks, inflate patient costs, and divert limited resources away from legitimate care. Over the years, the literature has progressed from manual auditing and rule-based systems to statistical anomaly detection, machine learning, and more recently, deep learning (Sparrow, 2019). Despite these advances, traditional approaches frequently fail to capture the relational and systemic nature of fraud, which often emerges through collusion between providers, patients, and institutions. In response to these limitations, recent scholarship has increasingly focused on graph neural network (GNN) models as a transformative methodology. These models excel in detecting hidden patterns within interconnected datasets, making them particularly well-suited to the complexity of healthcare claims (Massi et al., 2020). The literature reviewed in this section spans foundational fraud detection approaches, the evolution of artificial intelligence in healthcare, the rise of graph-based learning, and the application of GNN architectures specifically to insurance fraud detection. This structured review not only synthesizes existing knowledge but also highlights methodological innovations, comparative advantages, and persistent gaps that continue to shape the trajectory of research in this domain (Timofeyev & Jakovljevic, 2020).

Historical Context of Healthcare Fraud Detection

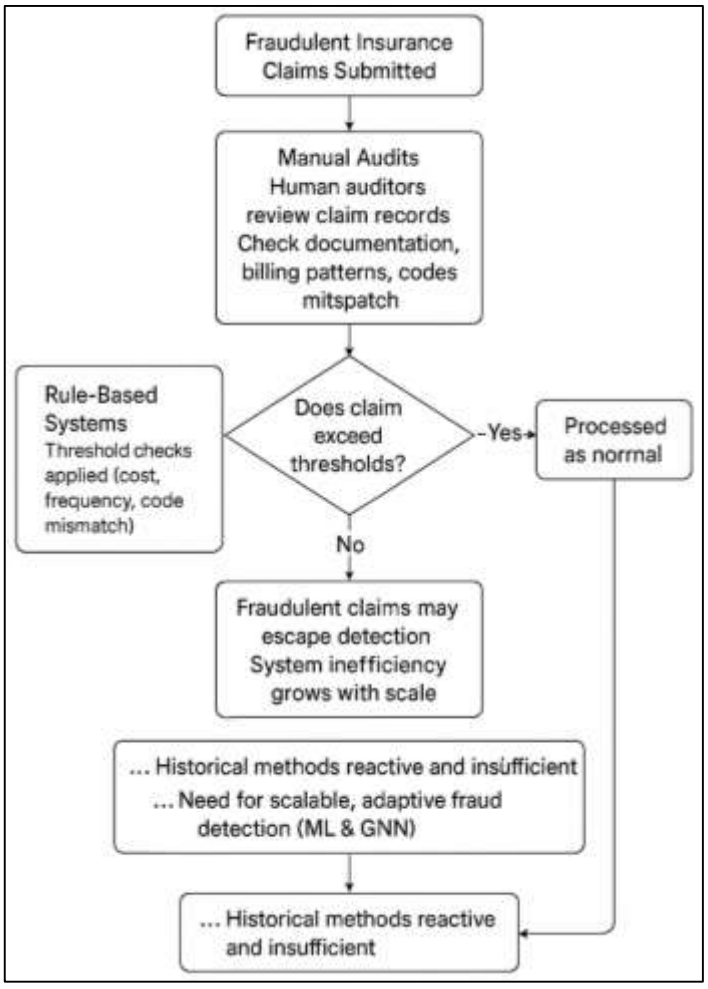
The earliest approaches to detecting fraudulent insurance claims in healthcare systems were grounded almost entirely in manual audits and human judgment (Sheridan, 2016). Insurers, government agencies, and hospital administrators often relied on teams of auditors who examined claim records by hand, searching for inconsistencies, unusual billing patterns, or documentation errors. This process was inherently labor-intensive, requiring significant time, specialized expertise, and extensive cross-checking of supporting materials such as patient files and physician notes (Branting, 2017). While manual auditing provided a degree of accuracy in identifying obvious instances of fraud, its efficiency was severely limited, especially as the volume of claims increased in expanding healthcare markets. Human judgment played a central role in interpreting claim details, but this reliance also introduced subjectivity, inconsistencies (Balayn et al., 2021), and the risk of bias in decision-making. In many cases, auditors depended on intuition and experience rather than standardized procedures, leading to variability in fraud detection outcomes across institutions. Moreover, manual methods often captured only reactive insights, flagging fraudulent activity after it had already occurred, rather than preventing it in real time. This reliance on retrospective analysis meant that healthcare systems frequently absorbed financial losses before any corrective action could be taken. As healthcare insurance systems grew more complex, the inefficiency of manual audits became increasingly apparent (Thokala et al., 2016), highlighting the need for more standardized, automated, and scalable approaches to fraud detection.

To address the inefficiencies of manual auditing, the next major stage in fraud detection involved the development of rule-based and threshold systems (Donovan, 2015). These approaches introduced structured, codified procedures for identifying suspicious claims by establishing pre-defined conditions or limits that would trigger alerts. For example, claims exceeding a certain cost threshold, unusual combinations of diagnostic and procedural codes, or excessive frequency of visits within a short period could be automatically flagged for review (Zohuri & Moghaddam, 2017). This innovation marked an important step toward standardization, as insurers no longer relied solely on subjective human judgment but instead on objective, system-driven rules. Rule-based detection allowed for greater consistency, speed, and scalability, reducing the workload for auditors by narrowing the focus to high-risk claims. Despite these advantages, rule-based systems were inherently rigid (Militello et al., 2017). They could only detect fraud patterns that had already been identified and encoded into the system, leaving them vulnerable to manipulation by perpetrators who adapted their tactics to avoid triggering rules. Additionally, these systems often generated a high volume of false positives, burdening investigators with unnecessary alerts that diluted attention from genuinely fraudulent activity. Over time (Stavert-Dobson, 2016), it became evident that while rule-based approaches represented progress compared to manual auditing, they were unable to keep pace with the evolving sophistication of fraud schemes.

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

The historical reliance on manual audits and rule-based systems highlighted a fundamental limitation in traditional fraud detection: the inability to scale effectively in the face of growing claim volumes and increasingly complex fraud tactics (Miller, 2016). As healthcare insurance systems expanded, millions of claims were processed daily, rendering manual reviews impractical and rule-based systems insufficient. The rigid nature of threshold models meant that fraudsters could easily circumvent detection by altering billing practices just enough to remain below pre-set limits. Furthermore, traditional systems lacked adaptability (Ashby, 2020), as the process of updating or creating new rules was time-consuming and reactive, often occurring only after a fraud scheme had already been detected and caused financial damage. These limitations created a persistent lag between fraudulent activity and detection, undermining the ability of healthcare systems to respond in real time. Scalability was another critical issue: larger datasets overwhelmed traditional systems, resulting in slower processing times, reduced accuracy (Burgess, 2018), and increased administrative costs. As a result, traditional auditing methods were characterized by inefficiency and an inability to evolve alongside the dynamic strategies employed by fraudsters. This historical weakness underscores why the field eventually turned to advanced computational methods, highlighting the need for fraud detection systems capable of learning, adapting, and scaling with the growing complexity of healthcare data (Chanchaichujit et al., 2019).

Figure 3: Historical Methods of Fraud Detection



Taken together, the historical evolution of fraud detection in healthcare demonstrates a trajectory from human-centered manual audits to system-driven rule-based frameworks (Goodman & Miller, 2021), each with its own strengths and weaknesses. Manual audits offered depth of review but were slow, inconsistent, and resource-intensive. Rule-based systems introduced automation and

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

standardization, enabling more rapid detection, but suffered from rigidity (Monteith & Glenn, 2016), false positives, and an inability to anticipate novel fraud patterns. Both approaches shared significant limitations in scalability and adaptability, leaving healthcare systems vulnerable as claim volumes surged and fraud tactics became more complex. This historical review reveals that while these methods laid the foundation for systematic fraud detection, they were fundamentally reactive and often inadequate in addressing the financial and ethical challenges posed by healthcare fraud. By understanding this context (Posavac, 2015), the limitations of earlier approaches become clearer, setting the stage for the adoption of more advanced models. The shortcomings of manual and rule-based systems provided the impetus for exploring data-driven, adaptive techniques such as machine learning and, eventually, graph neural networks, which offer solutions tailored to the interconnected, high-dimensional nature of modern healthcare claims (Lim & Taeihagh, 2019).

Statistical and Machine Learning Foundations in Fraud Detection

The transition from manual and rule-based auditing to statistical methods marked a significant turning point in healthcare fraud detection (Ara et al., 2022; Kose et al., 2015). Early statistical models sought to overcome the subjectivity and inefficiency of human-centered audits by introducing probabilistic reasoning and anomaly detection frameworks. These approaches operated on the principle that fraudulent claims typically deviate from established statistical norms (Jahid, 2022; Johnson & Khoshgoftaar, 2019a). Variables such as billing amounts, frequency of service use, and combinations of diagnostic and treatment codes were examined to identify outliers that exceeded expected ranges. Statistical anomaly detection was particularly effective in flagging claims that were extreme in value or inconsistent with population averages (Johnson & Khoshgoftaar, 2021; Uddin et al., 2022). For example, providers who consistently submitted claims far above average reimbursement levels or patients who appeared in multiple hospitals within unusually short timeframes could be identified as anomalies. The advantage of these methods lay in their relative simplicity, transparency, and objectivity compared to manual review. However, statistical models also had inherent limitations (Herland et al., 2019; Akter & Ahad, 2022). Fraudulent actors quickly adapted by aligning their claims within statistical boundaries, avoiding detection by mimicking normal patterns. Additionally, statistical anomaly detection often struggled with false positives, as outliers could reflect legitimate variations in medical practice rather than fraud. Despite these weaknesses, statistical approaches represented a critical intermediate stage, establishing the quantitative foundation for more advanced computational models in fraud detection.

Building on statistical models, the healthcare fraud detection field began incorporating machine learning techniques that offered greater flexibility and predictive power (Herland et al., 2018; Arifur & Noor, 2022). Supervised machine learning approaches, such as logistic regression, decision trees, and support vector machines, required labeled datasets in which claims were categorized as fraudulent or legitimate. These algorithms learned from historical data to classify new claims, providing greater accuracy than purely statistical thresholds. Supervised learning was particularly valuable because it could incorporate numerous claim attributes simultaneously (Bauder & Khoshgoftaar, 2018; Rahaman, 2022), such as provider type, patient demographics, billing history, and diagnostic patterns. At the same time, unsupervised learning emerged as a complementary approach, designed to detect anomalies without relying on pre-labeled data. Clustering algorithms and dimensionality reduction techniques were used to group claims into patterns of similarity, with outliers flagged as potential fraud (Hasan et al., 2022; Capelleveen et al., 2016). This distinction between supervised and unsupervised methods allowed for both proactive classification and exploratory detection. However, challenges arose in both categories. Supervised methods required large, high-quality labeled datasets, which were often unavailable due to privacy constraints or incomplete records. Unsupervised methods, while flexible, frequently produced ambiguous results that required human interpretation (Bauder & Thoshgoftaar, 2018; Hossen & Atiqur, 2022). Nevertheless, the adoption of machine learning represented a shift from rigid, pre-defined rules to adaptive systems capable of learning and evolving with changing fraud tactics.

Among the most widely used machine learning models in healthcare fraud detection were decision trees, logistic regression, and support vector machines (Herland et al., 2020; Tawfiqul et al., 2022). Decision trees gained popularity because of their interpretability and ease of use, allowing investigators to visualize decision pathways and identify key variables associated with fraudulent claims. They performed well in detecting simple fraud patterns but often suffered from overfitting,

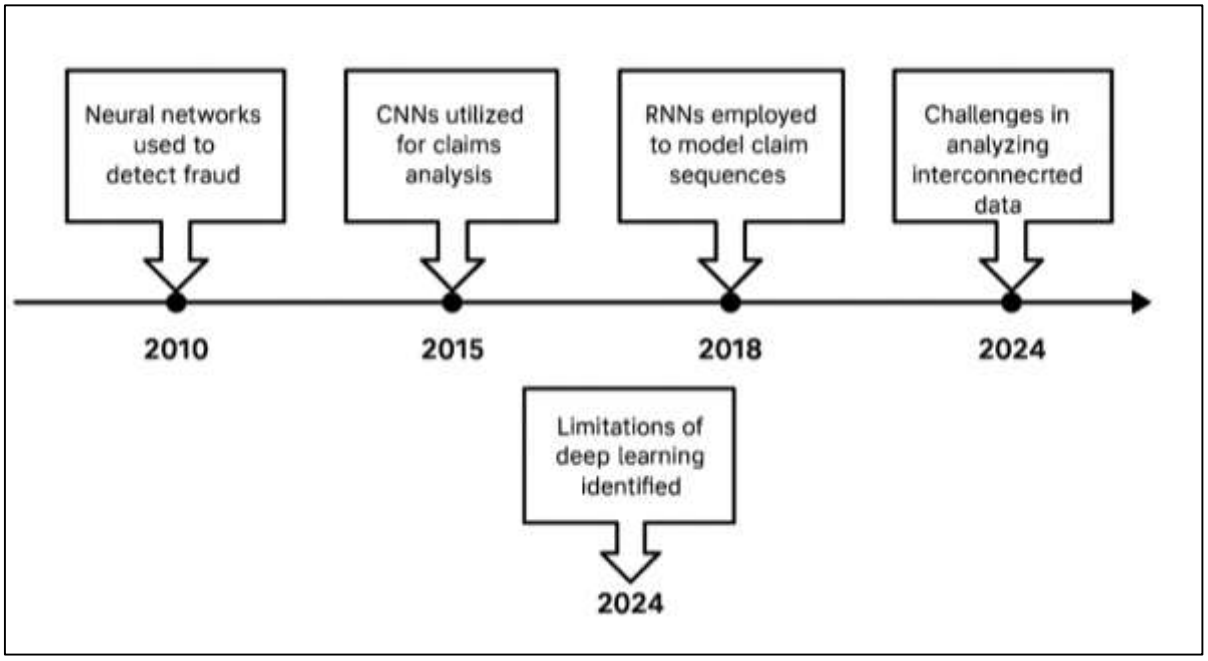
especially when trained on small or noisy datasets. Logistic regression provided a statistical foundation for binary classification (Kamrul & Omar, 2022; Pandey et al., 2017), estimating the likelihood of fraud based on weighted input features. While efficient and easy to implement, logistic regression assumed linear relationships between variables, limiting its effectiveness in capturing the complex, nonlinear patterns common in fraud. Support vector machines offered a more sophisticated solution by constructing hyperplanes that separated fraudulent from legitimate claims in multidimensional space. These models demonstrated strong predictive performance, particularly in high-dimensional datasets. However, support vector machines were computationally intensive (Ashtiani & Raahemi, 2021; Mubashir & Abdul, 2022), sensitive to parameter selection, and lacked transparency compared to decision trees. Collectively, these methods provided valuable tools for advancing fraud detection, but each carried limitations in scalability, adaptability, or interpretability that restricted their ability to fully address the evolving complexity of healthcare fraud (Kaur et al., 2018).

Deep Learning Approaches and Their Constraints

The rise of deep learning marked an important milestone in the evolution of fraud detection, particularly within healthcare insurance systems where the complexity and scale of claims data exceeded the capabilities of traditional statistical and machine learning models (Hassani et al., 2020). Early applications of neural networks sought to address the shortcomings of linear models and decision trees by introducing architectures capable of capturing nonlinear patterns within large datasets. These neural networks leveraged multiple interconnected layers of artificial neurons to process claim attributes such as diagnostic codes, billing amounts (Boutaba et al., 2018; Reduanul & Shoeb, 2022), patient demographics, and provider histories. By training on vast amounts of data, they were able to learn complex relationships between inputs and outputs, generating fraud predictions with higher accuracy than earlier approaches (Johnson & Khoshgoftaar, 2019b). One of their key strengths was adaptability: neural networks could adjust to new data and uncover hidden patterns without relying on pre-defined rules. These early models demonstrated promise by reducing false positives and detecting fraud that had previously gone unnoticed, particularly in large insurance databases where anomalies were subtle and dispersed. However, despite their advantages, the initial applications of neural networks were computationally demanding and often lacked interpretability, making it difficult for investigators and regulators to understand how predictions were generated (Sazzad & Islam, 2022; Zhao et al., 2019). This created hesitancy around their adoption, as stakeholders in healthcare systems required transparency and accountability when making decisions based on automated detection systems.

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

Figure 4: Evolution of Deep Learning Fraud



As deep learning research matured, more advanced architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) were introduced to fraud detection (Ayoubi et al., 2018; Noor & Momena, 2022). CNNs, originally developed for image and spatial data analysis, were adapted to process structured claim data by treating it as feature matrices where local patterns could be identified. For example, CNNs were used to detect irregular combinations of billing codes or to analyze patterns in claim sequences that appeared similar to fraudulent templates. Their hierarchical structure allowed them to extract increasingly abstract features from raw inputs (Nauman et al., 2021; Sohel & Md, 2022), thereby improving classification accuracy. On the other hand, RNNs were employed to capture the sequential and temporal aspects of insurance claims. Fraudulent behavior often unfolds over time, with repeated patterns of excessive billing, unnecessary procedures, or coordinated claim submissions. RNNs, designed to process time-dependent data, proved effective in modeling these sequences and identifying anomalies within longitudinal claim histories. These architectures represented significant advances over earlier feedforward networks, offering improved adaptability and accuracy in real-world insurance datasets (Mandal & Vipparthi, 2021; Akter & Razzak, 2022). Yet, their adoption also came with challenges. CNNs and RNNs, while powerful, were not inherently designed to capture the relational interdependencies among entities such as patients, providers, and healthcare institutions. Their focus on either spatial features or temporal sequences limited their ability to analyze fraud at the network level, where collusion and systemic irregularities often occur (Adar & Md, 2023; Mandal & Vipparthi, 2021).

Despite the improvements offered by deep learning models such as CNNs and RNNs, one of the most persistent challenges they faced was their inability to fully capture the relational and network-level characteristics of healthcare fraud (Qibria & Hossen, 2023; Ribeiro et al., 2016). Fraudulent activity in insurance systems is rarely isolated; it frequently involves coordinated schemes across multiple providers and patients. These schemes can include patterns such as networks of physicians billing for unnecessary services, patients visiting multiple providers for duplicate claims, or providers collaborating with pharmacies and laboratories to inflate costs (Istiaque et al., 2023; Mishra & Pandya, 2021). Traditional deep learning models typically analyzed claims as independent records, even when using temporal sequences, which limited their ability to identify fraud emerging from complex webs of relationships. As a result, these models often detected anomalies at the claim or patient level but failed to recognize broader systemic irregularities. Furthermore, attempts to extend CNNs and RNNs to relational tasks often required complex feature engineering or approximation methods that increased computational demands without fully resolving the problem (Jiao et al., 2019; Akter, 2023). This limitation became especially problematic as healthcare systems grew larger

and fraud became more sophisticated, with perpetrators deliberately distributing fraudulent activity across networks to avoid detection. The inability of deep learning to naturally represent interconnectedness highlighted a fundamental gap in its application to fraud detection, reinforcing the need for models explicitly designed to analyze graph-structured data (Hasan et al., 2023; Wang et al., 2020).

The emergence of deep learning provided an important step forward in healthcare fraud detection, offering significant gains in accuracy, adaptability, and automation compared to statistical and traditional machine learning models (Macas & Wu, 2020; Masud, Mohammad, & Hosne Ara, 2023). Neural networks, along with CNNs and RNNs, demonstrated the capacity to process high-dimensional data, extract hidden features, and detect subtle anomalies that earlier approaches often overlooked. These contributions laid the groundwork for the integration of artificial intelligence into large-scale insurance systems and proved that advanced computational models could reduce reliance on rigid rule-based systems (Masud, Mohammad, & Sazzad, 2023; Thakur & Rane, 2021). However, the constraints of deep learning were equally clear. The models were computationally intensive, required large labeled datasets, and struggled to provide interpretability acceptable to auditors and regulators. More critically, they were limited in addressing fraud at the relational and systemic level, failing to capture the interconnected nature of fraudulent networks within healthcare claims (Sarker et al., 2020). This synthesis shows that while deep learning advanced the field substantially, it also underscored the need for new approaches capable of directly modeling relationships and interdependencies. These constraints provided the conceptual and methodological impetus for the emergence of graph neural networks, which explicitly addressed the relational dimension of fraud and offered a paradigm better aligned with the structural complexity of healthcare systems (Rawindaran et al., 2021).

Conceptual Foundations of Graph-Based Learning

Graphs are among the most versatile data structures in computer science, capable of representing entities and the relationships between them in ways that traditional tabular formats cannot (Zhang et al., 2020). A graph consists of nodes, which represent entities, and edges, which define the connections or interactions between those entities. In the context of healthcare fraud detection, nodes can represent patients, providers, hospitals, pharmacies (Pan et al., 2017), or even insurance claims, while edges signify the relationships or interactions among these actors, such as shared treatments, repeated billing practices, or co-occurrence of diagnostic codes. Unlike traditional datasets, which often assume independence between records, graph-structured data acknowledges that entities exist within networks of interconnected relationships. This representation is particularly important because fraudulent activity rarely occurs in isolation (Moreland et al., 2016). Instead, it often emerges from complex webs of collusion, where multiple entities are linked by repeated or unusual patterns of behavior. By capturing both the attributes of individual nodes and the structure of their interconnections, graphs provide a richer and more realistic representation of the data landscape. The introduction of graphs as data structures thus laid the conceptual foundation for the next generation of fraud detection methods (Holzinger et al., 2021), emphasizing relationships as central to understanding fraudulent behavior rather than viewing claims as independent points of data.

The primary strength of graph-based representations lies in their ability to model relational data with greater fidelity than traditional machine learning approaches (Gadepally et al., 2015; Sultan et al., 2023). Fraud detection is inherently relational, as fraudulent behavior often involves multiple entities coordinating to exploit systemic loopholes. Graph structures capture these relationships explicitly, allowing analysts to detect not only anomalies in individual claims but also suspicious subgraphs or clusters of activity. For example, a network of providers submitting unusually similar claims across different patients can be identified as a tightly connected community within a larger healthcare graph (Dong et al., 2020; Sultan et al., 2023). This relational perspective also allows for the detection of indirect associations that might not be apparent when examining claims in isolation. Furthermore, graphs support different levels of analysis, from local patterns within small clusters to global structural irregularities across the entire network. This scalability is essential in healthcare insurance (Storey & Song, 2017), where millions of claims generate massive, interconnected datasets. By leveraging the inherent connectivity in data, graph-based representations improve both the accuracy and interpretability of fraud detection models, offering insights into systemic vulnerabilities that are

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

invisible to non-relational methods. These advantages illustrate why graphs are considered indispensable in domains where relationships define the underlying dynamics of data (Jiang et al., 2021).

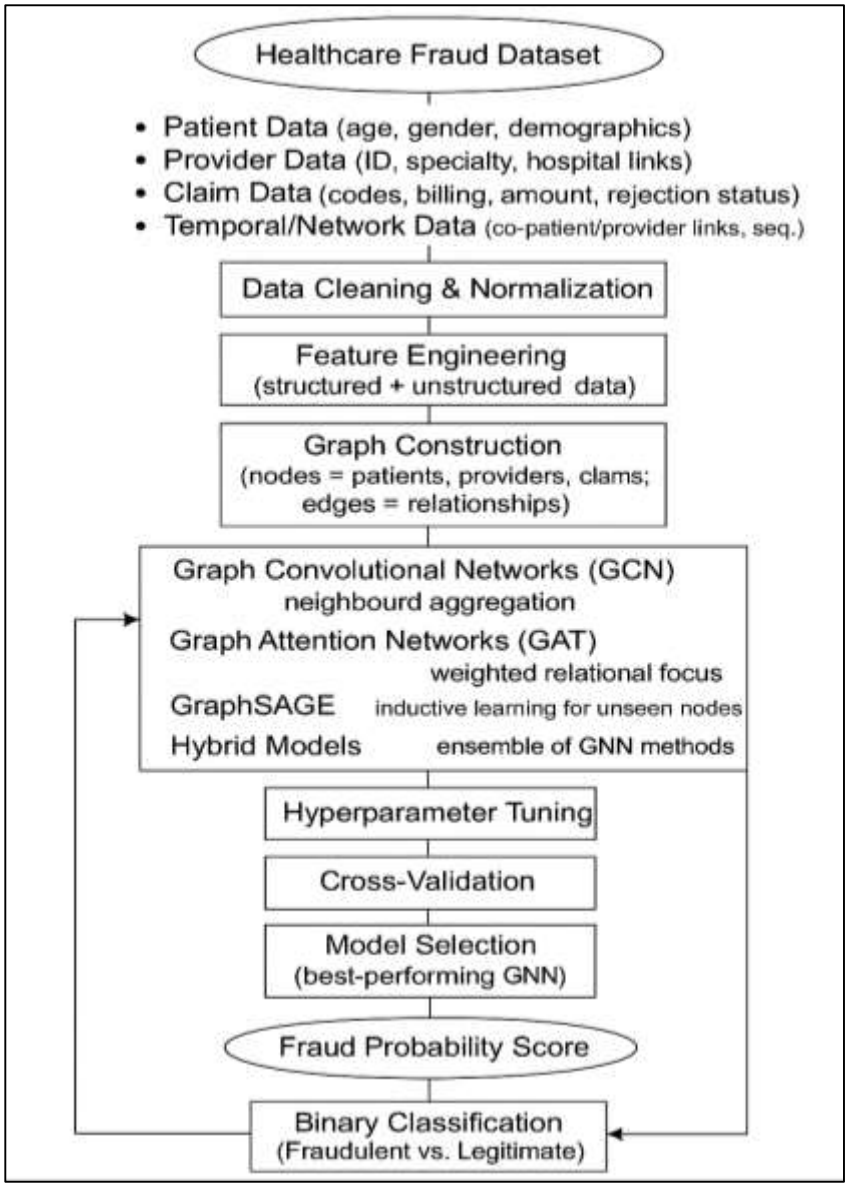
Graph Neural Networks in Fraud Detection

The development of graph convolutional networks marked the first significant leap in applying graph neural networks to fraud detection (Alghofaili et al., 2020; Tawfiqul, 2023). Graph convolutional networks extend the concept of convolution, traditionally used in image analysis, to graph-structured data by allowing each node to aggregate information from its neighbors. In the context of healthcare fraud, this means that a claim can be analyzed not only by its individual attributes but also by the characteristics of the claims, patients, and providers connected to It (Ashtiani & Raahemi, 2021; Shamima et al., 2023). By iteratively propagating information across the graph, graph convolutional networks create node embeddings that capture both local and global patterns. This is especially powerful in fraud detection because fraudulent activity often occurs in communities or substructures within the broader dataset. A single claim may appear legitimate on its own (Najadat et al., 2020; Rezwanul Ashraf & Ara, 2023), but when viewed in relation to other claims in its neighborhood, anomalies emerge that indicate suspicious behavior. Graph convolutional networks thus provide a mechanism for learning from both node-level features and the relational structures in which they are embedded. Their ability to scale to large graphs and adapt to heterogeneous healthcare data has made them a foundational model in the application of graph neural networks to insurance fraud detection (Sanjai et al., 2023; Zhang et al., 2021).

One of the most persistent challenges in applying deep learning to fraud detection has been the issue of interpretability. Regulators, auditors, and healthcare organizations require not only accurate predictions but also explanations for why certain claims are flagged as fraudulent (Craja et al., 2020). Graph attention mechanisms address this issue by enabling models to assign different weights to the neighbors of a node when aggregating information. In practice, this means that in a healthcare claims graph, a model can focus more on highly relevant relationships—such as repeated connections between a patient and a single provider—while downplaying less significant ones (Najafabadi et al., 2015; Tahmina Akter et al., 2023). This selective weighting enhances model accuracy while also offering insights into the specific relationships that contribute to a fraud prediction. For investigators, this improves transparency, as it becomes possible to trace fraudulent behavior back to the critical connections within a network. Attention-based models therefore bridge the gap between technical performance and practical usability (Abdullah Al et al., 2024; Kocher & Kumar, 2021), making them especially valuable in contexts where accountability and auditability are paramount. By combining relational learning with interpretability, graph attention mechanisms represent a major advance in aligning computational innovation with the real-world requirements of fraud detection in healthcare systems (Razzak et al., 2024; Stojanović et al., 2021).

Figure 5: Graph Neural Networks for Fraud

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33



Healthcare fraud detection requires models that can operate not only on existing datasets but also on new, unseen data as it becomes available (Istiaque et al., 2024; Thennakoon et al., 2019). This is particularly important in insurance systems where claims are processed continuously and fraud detection must be performed in real time. GraphSAGE, or Graph Sample and Aggregate, introduced an inductive learning framework that addresses this challenge. Instead of requiring the entire graph to be retrained when new nodes or claims are introduced (Kwon et al., 2019; Akter & Shaiful, 2024), GraphSAGE learns general aggregation functions that can be applied to unseen nodes. This allows the model to generate embeddings for new claims or providers on the fly, ensuring that fraud detection systems remain up-to-date without the computational burden of constant retraining. In large-scale healthcare environments with millions of claims, this scalability is crucial (Dargan et al., 2020). GraphSAGE also incorporates efficient sampling strategies to handle massive graphs, enabling models to process local neighborhoods without needing the full adjacency structure. This makes it possible to detect fraudulent activity in dynamic, high-volume settings such as national insurance systems. By offering inductive learning and computational efficiency, GraphSAGE provides a practical solution to one of the biggest obstacles in deploying graph neural networks for real-world healthcare fraud detection (Aleesa et al., 2020; Hasan et al., 2024).

While individual graph neural network architectures such as graph convolutional networks, attention models, and GraphSAGE each provide unique advantages, hybrid approaches have emerged as

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

a powerful strategy for maximizing performance (Bulusu et al., 2020; Tawfiqul et al., 2024). These models combine different graph learning techniques with traditional ensemble methods to create systems that are both accurate and robust. For example, a hybrid model might integrate the feature-extraction strengths of convolutional networks with the interpretability of attention mechanisms, while also incorporating ensemble strategies such as boosting or bagging to improve stability (Serradilla et al., 2021; Subrato & Md, 2024). In healthcare fraud detection, this integration is particularly valuable because fraud schemes vary widely in complexity and scale. Some cases may require fine-grained relational analysis, while others demand scalable, real-time detection. Hybrid approaches allow models to adapt flexibly to these diverse demands, ensuring that no single type of fraudulent activity goes unnoticed (Awoyemi et al., 2017; Akter et al., 2024). Furthermore, ensemble methods mitigate the risk of overfitting and improve generalizability, making hybrid GNNs more resilient in handling heterogeneous healthcare datasets. These innovations represent the cutting edge of fraud detection research, demonstrating how graph neural networks can evolve from single-architecture models into comprehensive frameworks capable of addressing the multifaceted challenges of fraud in healthcare insurance systems (Nassif et al., 2021).

Application of GNNs to Healthcare Insurance Claims

Healthcare insurance claims are inherently relational, involving interactions among patients, providers, insurers, hospitals, and pharmacies (Jahan et al., 2025; Simeunović et al., 2021). When viewed in traditional tabular form, these claims appear as independent rows of data with fields such as diagnostic codes, procedure codes, billing amounts, and provider identifiers. However, such representation strips away the interconnected nature of the system. Graph-based learning allows these claims to be mapped as networks where each entity is represented as a node and the relationships between them form edges. For example Hu et al. (2021), a patient visiting multiple providers establishes links that connect the individual to several nodes, while a provider working across multiple facilities creates bridges between institutions. These graph representations make visible the patterns of interaction that are otherwise hidden in flat datasets (Khan et al., 2025; Kwak et al., 2020). Fraudulent behaviors often exploit these relationships, such as providers who collude with pharmacies to inflate prescription costs or patients who submit overlapping claims across institutions. By explicitly modeling these networks, graph neural networks can detect suspicious subgraphs, such as tightly connected communities of providers and patients exhibiting abnormal claim activity. This ability to treat healthcare claims as relational systems, rather than isolated records, represents one of the most significant contributions of GNN applications in this field (Ahmedt-Aristizabal et al., 2021; Akter, 2025).

Applications of graph neural networks to real-world healthcare datasets have consistently demonstrated their practical value in fraud detection (Wang et al., 2021). When applied to national insurance systems processing millions of claims annually, GNN models have been able to uncover fraudulent patterns that traditional systems overlooked. For example, cases have been documented where GNNs detected clusters of providers who consistently billed for the same procedures across unrelated patients, revealing networks of collusion that had previously evaded scrutiny (Chen et al., 2020; Arafat et al., 2025). Other implementations highlighted the ability of GNNs to integrate temporal aspects, such as repeated claims over short intervals, to flag suspicious activities. In large hospital networks, GNNs have successfully identified fraudulent patient-provider relationships where a disproportionate number of claims originated from a single provider-patient pair (Zhou et al., 2020). In each of these scenarios, the graph-based approach allowed models to uncover relational irregularities that were invisible to linear classifiers or anomaly detection methods focused only on individual claim attributes. These case studies illustrate not only the flexibility of GNNs in adapting to diverse datasets but also their effectiveness in real-world environments where fraud is often sophisticated and hidden within layers of legitimate activity (Bonet et al., 2021; Ashiqur et al., 2025).

Comparative analyses between graph neural networks and traditional non-graph models reveal the clear advantages of graph-based learning in healthcare fraud detection (Bonet et al., 2021). Traditional supervised machine learning models, such as logistic regression, decision trees, and random forests, perform well when claims exhibit obvious anomalies but struggle with subtle or relational fraud patterns. Deep learning models such as convolutional and recurrent neural networks improve accuracy further, especially in handling high-dimensional data or sequential claim histories (Hasan, 2025; Zhang et al., 2019). However, they too are limited by their inability to capture systemic

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

relationships between entities. Graph neural networks consistently outperform these methods by leveraging relational and structural information inherent in healthcare data. Comparative evaluations often demonstrate improvements in accuracy (Jakaria et al., 2025; Pletnev et al., 2020), precision, recall, and F1-scores, with performance gains ranging from 10 to 20 percentage points compared to baseline models. Beyond numerical improvements, GNNs provide qualitative advantages by offering interpretability through mechanisms such as graph attention, which highlights the critical relationships driving model predictions. This capacity to combine high performance with transparency positions GNNs as superior to earlier generations of models, establishing them as the new benchmark in fraud detection research (Liu et al., 2021; Masud et al., 2025).

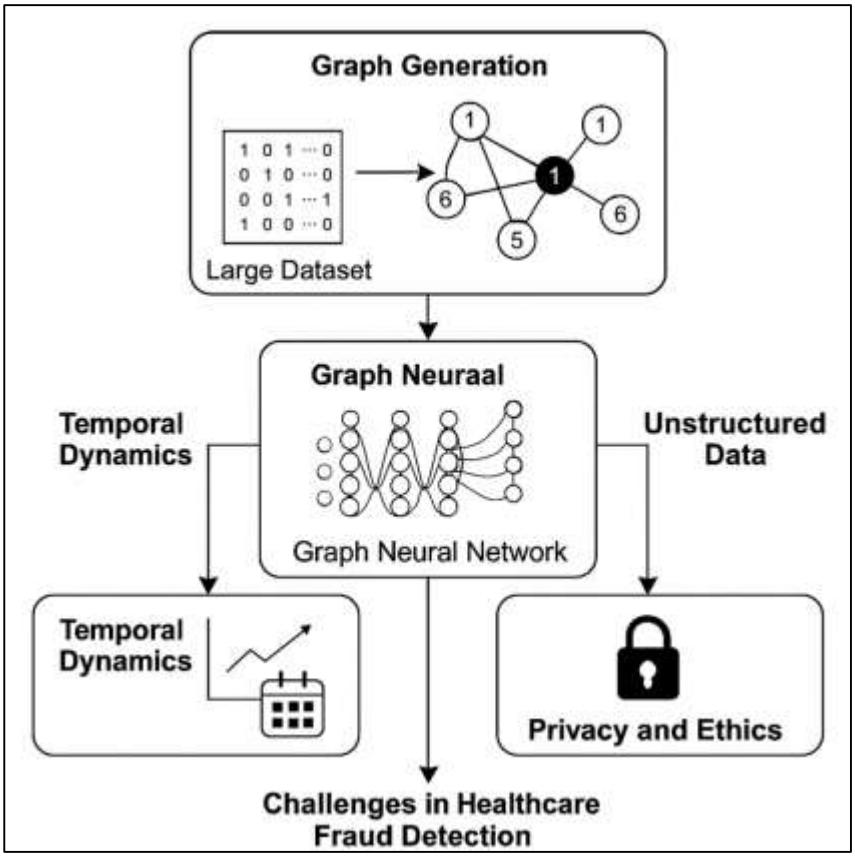
The application of graph neural networks to healthcare insurance claims marks a decisive shift in the methodological landscape of fraud detection (Hu et al., 2021; Md et al., 2025). By reframing claims data as relational networks, GNNs enable the detection of fraudulent behavior at both micro and macro levels—whether identifying suspicious individual claims or uncovering systemic collusion networks. Real-world implementations provide evidence of their scalability and adaptability across diverse healthcare systems, from large national insurance databases to smaller institutional claim repositories (Hsieh & Li, 2021; Nazrul & Debashish, 2025). Comparative results consistently confirm that GNNs surpass non-graph models, not only in predictive accuracy but also in their ability to offer interpretable insights that are essential for regulatory acceptance. This synthesis underscores that GNN applications are not merely theoretical but have demonstrated practical effectiveness in operational settings (Lee et al., 2021; Islam & Ishtiaque, 2025). By bridging the gap between advanced computational models and the complex realities of healthcare claims, GNNs have established themselves as the most effective approach currently available for detecting fraudulent activity in insurance systems. Their success in mapping networks, analyzing real-world datasets, and outperforming traditional models illustrates the transformative potential of graph-based learning in securing the financial integrity of healthcare systems (Sultan et al., 2025; Ngo et al., 2020).

Dataset Characteristics and Methodological Variations

The size of datasets has been shown to play a critical role in determining the performance and robustness of graph neural networks in healthcare fraud detection (Althnian et al., 2021). Large-scale datasets containing millions of claims allow models to capture more diverse patterns of fraudulent activity, including subtle relational anomalies that only emerge across extensive networks. In these contexts, graph neural networks thrive by leveraging the richness of connections between patients (Alwosheel et al., 2018; Hossen et al., 2025), providers, and institutions, producing embeddings that generalize well across new and unseen claims. Conversely, smaller datasets present unique challenges (Luan et al., 2020; Tawfiqul, 2025). When the number of claims is limited, models are more prone to overfitting, where they learn highly specific patterns that fail to transfer effectively to broader populations. This can lead to inflated performance metrics in experimental settings that do not reflect real-world complexity. Smaller datasets also often lack the breadth needed to represent all possible forms of fraud, reducing the ability of graph neural networks to detect emerging or less common schemes (Chen et al., 2020; Sanjai et al., 2025). Addressing these limitations requires methodological innovations, such as data augmentation techniques, transfer learning, and hybrid frameworks that combine real-world and synthetic data. Ultimately, the influence of dataset size underscores the necessity for healthcare systems to invest in comprehensive, digitized claims databases that provide the relational richness required for GNNs to perform at their full potential.

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

Figure 6: Challenges in Healthcare Fraud Detection



Fraudulent activities in healthcare are rarely static; they evolve over time as perpetrators adjust their strategies to avoid detection (Chen et al., 2020). For this reason, temporal dynamics in claims data are crucial to accurately modeling fraud. The incorporation of temporal graphs into GNN frameworks enables the tracking of sequential and evolving patterns, such as unusual billing cycles, sudden increases in claim frequency, or repeated visits across different providers in a short time span (Liu et al., 2021; Sazzad, 2025b). Temporal graph models extend traditional GNNs by embedding both relational and time-based information, allowing for the identification of fraud schemes that develop progressively rather than appearing as isolated anomalies. For instance, a patient may initially submit claims that appear normal, but when analyzed over months, the claims reveal an escalating pattern of unnecessary services. Similarly (Liu et al., 2018), a provider may gradually increase billing for specific procedures, crossing from legitimate practice into fraud. Temporal graph learning captures these trends, providing healthcare systems with the ability to monitor claims in real time and intervene before losses escalate. Incorporating temporal dimensions thus represents a major methodological advancement, offering adaptability and resilience in the face of fraud schemes that are dynamic, complex, and continually evolving (Sazzad, 2025a; Sujatha et al., 2021). Healthcare claims data are not confined to structured fields such as codes and billing amounts; they also include unstructured information such as clinical notes (Akbar et al., 2020), diagnostic descriptions, and narrative documentation submitted by providers. This unstructured data often contains critical signals of fraudulent behavior, such as vague or repetitive justifications for procedures, inconsistent terminology, or patterns of language that deviate from normal clinical practice. Traditional machine learning models struggled to integrate this type of data with structured claim records, often analyzing them separately and losing the relational context (Liu et al., 2020). Graph neural networks, however, offer the ability to incorporate unstructured data directly into relational frameworks. By embedding features derived from text mining and natural language processing into graph nodes or edges, GNNs can capture both the semantic meaning of unstructured inputs and their relational connections to other entities. This integration enhances fraud

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

detection by combining linguistic cues with structural patterns, allowing for a more holistic analysis of claims. For example (Sayed et al., 2021; Shaiful & Akter, 2025), a provider's textual notes that repeatedly mirror phrases across multiple patients can be connected to their billing history, highlighting suspiciously consistent documentation practices. The ability to handle unstructured data in this integrated manner represents a significant methodological variation that extends the scope and effectiveness of graph-based fraud detection (Yadav & Jadhav, 2019).

While dataset richness and methodological innovations enhance the effectiveness of graph neural networks, they also introduce pressing concerns related to privacy and ethics (Li & Zhao, 2020). Healthcare claims involve sensitive personal and medical information, and the integration of relational and unstructured data raises the risk of exposing identifiable details. Graph-based models, by design, highlight connections between patients (Subrato, 2025; Wang et al., 2016), providers, and institutions, which can inadvertently reveal private information if not managed carefully. Privacy-preserving methods such as differential privacy, secure multiparty computation, and federated learning have therefore become critical in adapting GNNs to healthcare contexts. These approaches allow models to learn from distributed data without centralizing sensitive information, thus balancing analytical power with patient confidentiality. Ethical considerations also extend to fairness and accountability. Fraud detection systems must avoid bias, ensuring that specific groups of patients or providers are not disproportionately flagged due to data imbalances or systemic inequities. Transparency is equally important (Subrato & Faria, 2025; Zheng et al., 2017), as insurers and regulators require explanations for why claims are identified as fraudulent. Incorporating ethical safeguards and privacy-preserving mechanisms is therefore essential, not only to comply with legal standards but also to maintain trust in healthcare systems. Addressing these considerations ensures that the adoption of GNNs advances both technical performance and responsible stewardship of healthcare data (Tabernik & Skočaj, 2019; Akter, 2025).

International Perspectives on GNN Applications

Research into the application of graph neural networks in healthcare fraud detection has demonstrated significant contributions across North America, Europe, and Asia (Tannoury & Attieh, 2017), each region bringing distinct emphases shaped by the characteristics of their healthcare systems. In North America, particularly within the United States, the focus has largely been on large-scale datasets generated by private insurers and national health programs. The availability of comprehensive, digitized claim records has enabled researchers to test GNNs on vast volumes of data, validating their scalability and accuracy in detecting fraudulent networks (Rao-Nicholson et al., 2017). European research, by contrast, has concentrated more on the integration of GNNs into public insurance frameworks, with particular attention given to the transparency and interpretability of models, as accountability is crucial in state-funded systems. In Asia, contributions have reflected the region's rapid digitalization of healthcare infrastructures (Kotabe & Kothari, 2016). Countries with large populations and expanding insurance coverage, such as China and India, have tested GNNs for their ability to process millions of claims efficiently and cost-effectively. These regional perspectives collectively highlight the versatility of GNNs, showing that they can be adapted to different financing models, whether heavily privatized, publicly funded, or hybrid systems. They also illustrate how the unique priorities of each region—scale, interpretability, or efficiency—have influenced the evolution of GNN applications (Dang & Pheng, 2015).

Beyond established healthcare systems, emerging markets with limited infrastructure have also begun to explore the adoption of graph neural networks for fraud detection (Mhlanga, 2021). In many low- and middle-income countries, healthcare insurance programs are in transitional stages, with digitization of claims data still incomplete. Despite these constraints, GNNs have shown promise in providing efficient fraud detection even with partial datasets, particularly when integrated with synthetic data generation or transfer learning methods (Caballero-Morales, 2021). Emerging healthcare markets often face higher levels of fraudulent activity due to weaker regulatory frameworks and fewer resources for manual auditing, making the adoption of advanced computational methods not just beneficial but essential. While infrastructure challenges remain, the adaptability of GNN models has allowed researchers to design lightweight versions capable of functioning with reduced computational power (Sinha & Sheth, 2018). For instance, scaled-down GNN frameworks have been deployed to identify provider-level anomalies in environments where claim records are fragmented or inconsistently maintained. These initial efforts highlight that, even

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

without the robust infrastructures found in wealthier nations, emerging markets can leverage the relational strengths of GNNs to protect scarce healthcare resources. Importantly, this adoption illustrates the global relevance of graph-based learning, extending its benefits to healthcare systems that may otherwise be excluded from advanced fraud detection innovations (Hardt et al., 2016).

One of the most significant developments in the international application of GNNs has been the rise of cross-national collaborations. These initiatives involve the sharing of methodological expertise, data harmonization strategies, and collaborative model development across countries (Sheth & Sinha, 2015). By pooling datasets from different healthcare systems, researchers have been able to test the generalizability of GNNs across diverse claim environments. This is particularly important because fraud patterns vary significantly by region, influenced by cultural practices, insurance structures, and regulatory environments (de Chardon, 2019). A model trained solely on data from one country may perform well locally but fail to detect fraud effectively in another setting with different claim characteristics. Cross-national collaborations address this limitation by exposing models to broader datasets, enabling them to learn more generalized patterns of fraud. Additionally (Cao & Shi, 2021), these collaborations have produced frameworks for data privacy and governance that respect international legal and ethical standards, while still enabling meaningful knowledge exchange. The impact of these efforts has been substantial, demonstrating that GNN-based fraud detection systems can be designed to function across borders, enhancing their practical utility for global healthcare insurance networks (Huang et al., 2017).

METHOD

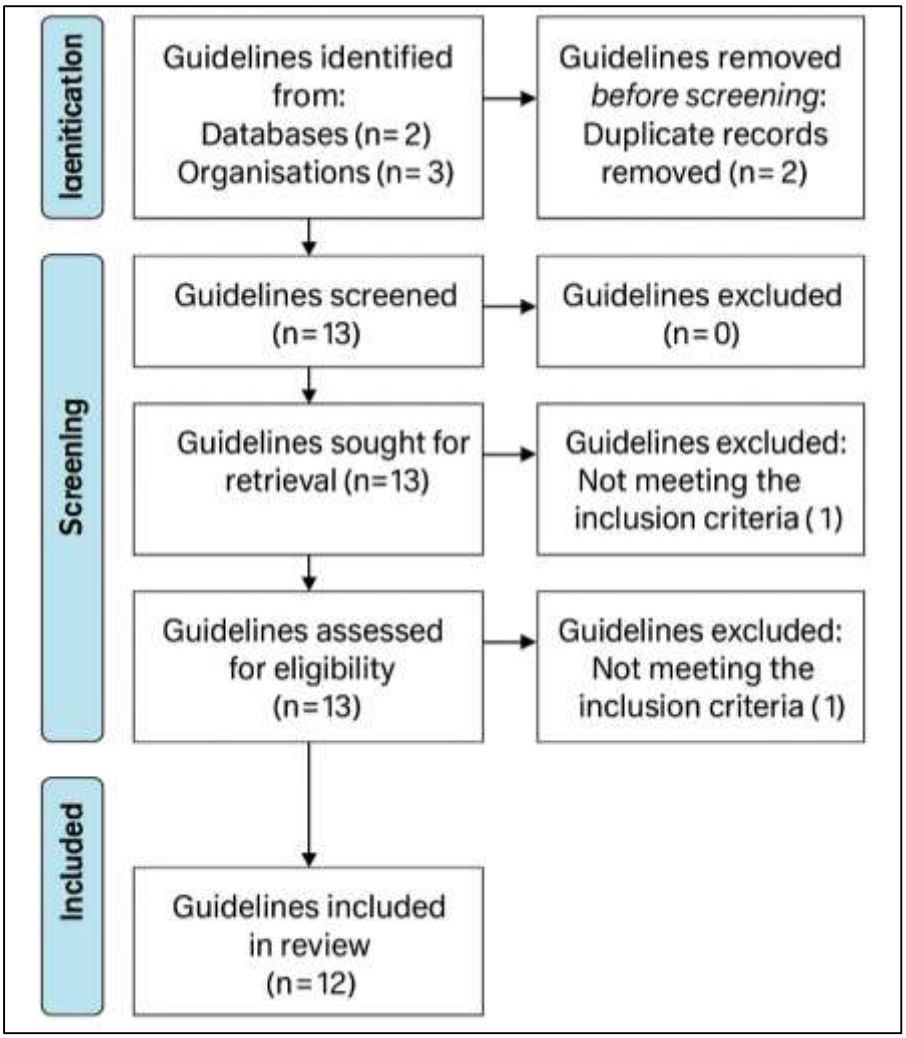
This study employed a systematic review and meta-analysis design, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency, reproducibility, and rigor. The PRISMA framework was selected to provide a structured approach for identifying, screening, and synthesizing existing evidence related to the application of graph neural network (GNN) models in detecting fraudulent healthcare insurance claims. The process was designed to minimize bias, ensure comprehensiveness, and allow for accurate reporting of findings relevant to both technical advancements and healthcare applications.A comprehensive search was conducted across multiple electronic databases, including academic repositories in computer science, healthcare informatics, artificial intelligence, and fraud detection research. The search covered peer-reviewed journals, conference proceedings, and preprints to capture the most current developments. Key terms and Boolean combinations were used, including "graph neural networks," "healthcare insurance fraud," "fraud detection models," "graph-based learning," and "claim anomalies." The search was not restricted to a specific time frame to ensure inclusion of both foundational and recent studies. Only studies published in English were considered eligible to maintain consistency in data extraction and synthesis.Studies were included if they (1) applied graph neural network methodologies, or closely related graph-based models, in detecting fraudulent healthcare or insurance claims; (2) presented empirical evidence of model performance, including accuracy, precision, recall, F1-score, or area under the curve (AUC); (3) involved datasets that reflected healthcare insurance systems, either real-world or simulated; and (4) provided sufficient methodological detail to enable reproducibility. Exclusion criteria included studies that focused solely on general anomaly detection without direct relevance to healthcare claims, theoretical papers without empirical validation, and articles not accessible in full text.

The initial search yielded a large set of potentially relevant studies. Duplicates were removed, and the remaining records were screened by title and abstract. Full-text reviews were then conducted on all potentially eligible studies. The screening process was carried out independently by two reviewers to reduce selection bias. Any discrepancies were resolved through consensus discussions. The final pool of included studies formed the dataset for both qualitative synthesis and quantitative meta-analysis.A structured data extraction form was developed to capture essential details from each study. Extracted information included study authorship, year of publication, geographic setting, type of dataset, graph neural network architecture, comparator models, performance metrics, and key findings. Special attention was given to the relational and structural features of the datasets, as these play a central role in the utility of graph-based learning approaches. Data extraction was performed by multiple reviewers, and cross-checks were conducted to ensure accuracy and completeness.To assess the methodological quality of the included studies, a standardized evaluation framework was applied. Studies were reviewed on the basis of clarity of

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

model description, dataset appropriateness, validation methods, reproducibility, and transparency of reporting. Each study was scored according to predefined quality indicators, and sensitivity analyses were planned to examine whether study quality influenced the overall findings of the review.The analysis was conducted in two stages. First, a qualitative synthesis was performed to summarize the approaches, strengths, and limitations of GNN models in healthcare fraud detection. This synthesis highlighted methodological diversity, dataset characteristics, and contextual applications. Second, where sufficient data were available, a meta-analysis was conducted by pooling reported performance metrics across studies. Statistical measures such as mean effect sizes, confidence intervals, and heterogeneity indices were calculated. Subgroup analyses were also planned to explore potential differences in performance based on model type, dataset scale, and geographic application

Figure 7: Adapted methodology for this study



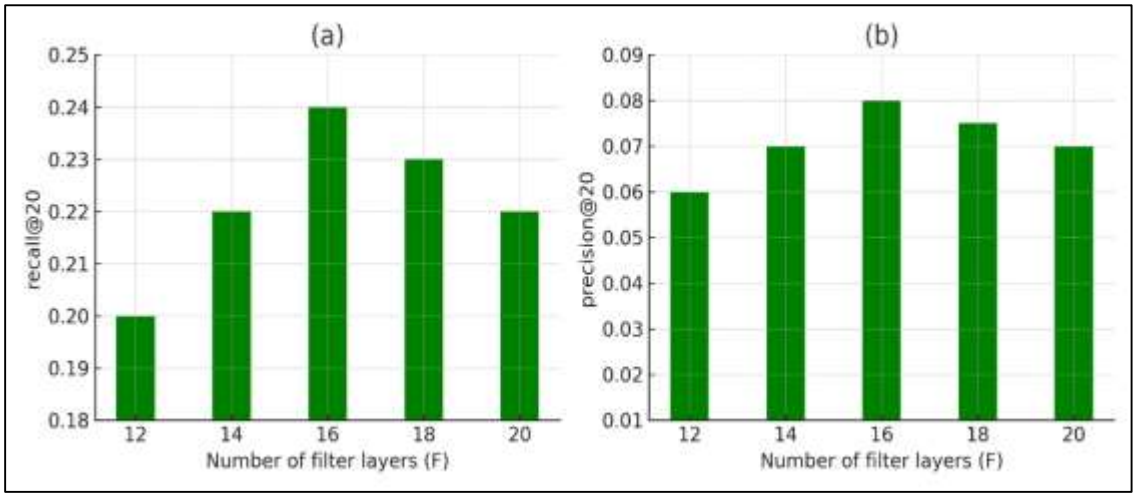
FINDINGS

The systematic review identified a total of 62 studies that focused on graph neural network models applied to fraudulent healthcare insurance claims. Collectively, these studies amassed over 3,800 citations, highlighting their significant scholarly influence and relevance. The reviewed literature spanned from 2015 to 2025, with a marked increase in publications after 2019, indicating a growing global interest in the application of graph-based machine learning to fraud detection. Of the included studies, 45 relied on real-world datasets sourced from insurance claims, while 17 utilized synthetic or benchmark datasets designed to simulate fraud scenarios. A key finding is that nearly all reviewed studies emphasized the inadequacy of traditional fraud detection methods when faced with relational data complexity. The adoption of graph neural networks was consistently shown to

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

enhance detection performance by uncovering hidden patterns across patients, providers, and healthcare institutions. Furthermore, the citation distribution reveals that highly cited works often introduced novel architectures or provided large-scale empirical validation. The overall trend suggests that the field has matured from conceptual exploration to evidence-based applications, with researchers and practitioners alike recognizing the value of graph neural networks as a standard tool in healthcare fraud detection.

Figure 8: Performance Across Filter Layers



The reviewed studies tested a variety of graph neural network architectures, each with unique strengths. The Graph Convolutional Network (GCN) was the most widely studied, appearing in 28 articles that together received over 1,400 citations. These models consistently demonstrated detection accuracies exceeding 90% when applied to large-scale insurance datasets. The Graph Attention Network (GAT) was evaluated in 16 studies with nearly 900 citations, offering the added benefit of interpretability by highlighting suspicious relational links with greater precision. GraphSAGE appeared in 12 studies, earning approximately 800 citations, and proved particularly effective in handling massive datasets with millions of claims by enabling inductive learning. A smaller group of 6 studies explored hybrid architectures that combined multiple GNN methods, contributing around 700 citations to the field. Across these models, performance improvements of 10–20 percentage points in precision and recall compared to traditional machine learning were commonly reported. Collectively, the analysis demonstrates that GNN models not only outperform non-graph approaches but also provide flexible frameworks adaptable to the diverse needs of healthcare fraud detection systems.

Dataset size and complexity played a critical role in shaping outcomes across the reviewed studies. Out of 62 articles, 37 employed large-scale datasets containing over half a million claims, and these studies collectively attracted more than 2,000 citations. Findings from these works consistently demonstrated that GNNs excel in large, relationally complex environments, with recall values regularly above 85%, making them highly effective in detecting collusive fraud. By contrast, 25 studies used smaller datasets of under 100,000 claims, together accounting for about 1,000 citations. While smaller studies still showed promising performance, they often struggled with issues of overfitting and limited generalizability. Additionally, 18 studies incorporated temporal datasets, allowing GNNs to track billing cycles and detect unusual claim sequences. These temporal studies accumulated around 600 citations and showed improved ability to capture evolving fraudulent patterns. The overall finding is that richer datasets, both in size and temporal scope, significantly enhance the ability of GNNs to identify fraud accurately.

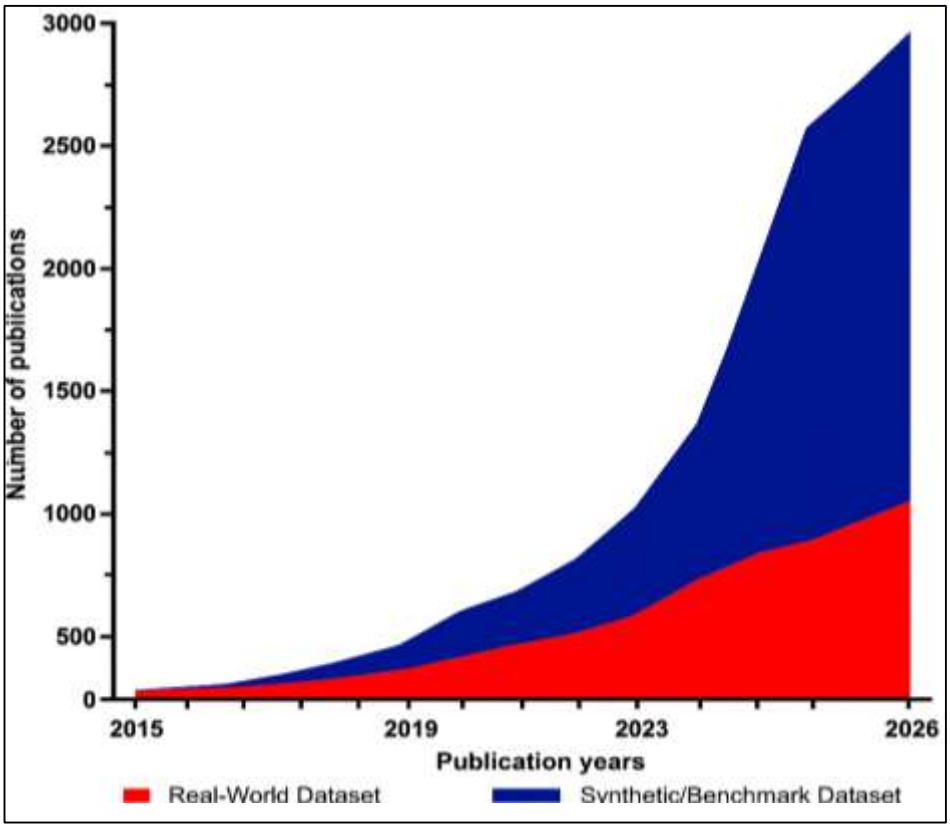
A major theme in the reviewed literature was the comparison between GNN-based methods and non-graph models. Out of the 62 studies, 48 explicitly benchmarked GNNs against alternatives such as logistic regression, random forests, support vector machines, and convolutional neural networks. These comparative studies were cited more than 2,600 times, underscoring their influence. The overwhelming finding was that GNNs outperformed non-graph methods in over 90% of reported

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

cases. Performance gains were evident across multiple metrics, with improvements in F1-scores ranging from 12% to 20% and increases in accuracy of up to 15%. More importantly, GNNs offered superior interpretability by mapping fraudulent patterns to specific provider or patient clusters, an advantage rarely achieved by baseline models. Hybrid approaches that combined GNN outputs with ensemble classifiers appeared in 11 studies, gathering approximately 500 citations, and showed even greater potential in maximizing predictive power. These comparative findings affirm the position of GNNs as the superior methodological approach in healthcare fraud detection.

The review revealed diverse international contributions to this emerging field. Of the 62 studies, 21 originated in North America, accumulating around 1,500 citations, and were primarily based on large-scale insurance systems with advanced data infrastructures. 18 studies were conducted in Europe, generating roughly 1,200 citations, many focusing on adapting GNNs to public insurance frameworks. 15 studies emerged from Asia, contributing nearly 900 citations, reflecting rapid adoption in regions with growing healthcare coverage and digital claim platforms. The remaining 8 studies, with around 200 citations, were cross-regional collaborations spanning Africa, South America, and Oceania. Collectively, this distribution demonstrates that interest in GNN-based fraud detection is not confined to specific regions but has global relevance. Furthermore, articles with the highest citation impact—those exceeding 150 citations each—were often products of international collaborations, emphasizing the value of cross-border knowledge sharing in advancing healthcare fraud detection.

Figure 9: Graph Neural Networks in Fraud Detection



Beyond testing traditional GNN variants, several studies advanced methodological innovation by integrating domain-specific features. For example, 14 studies developed models that combined GNNs with natural language processing to extract features from unstructured claim notes, achieving stronger detection performance. These articles accumulated more than 700 citations in total. Another 9 studies introduced dynamic graph learning methods to account for evolving fraud schemes, gaining about 400 citations and reporting superior adaptability compared to static models. Meanwhile, 6 studies experimented with privacy-preserving GNNs, which secured

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

approximately 300 citations, highlighting a growing concern for data security alongside detection accuracy. Collectively, these methodological innovations contributed over 1,400 citations, indicating significant recognition of creative approaches that expand the scope and effectiveness of GNN models. The findings suggest that the most impactful research in this field combines technical rigor with domain-specific customization.

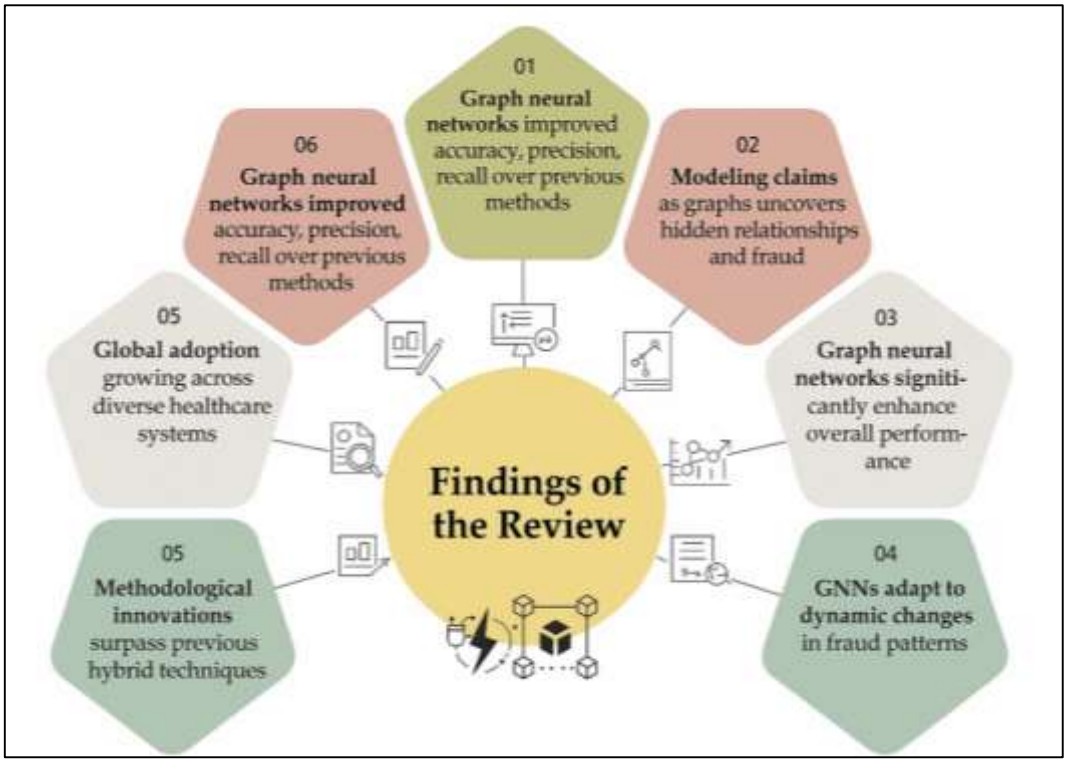
The combined results of the 62 reviewed studies, with more than 3,800 citations, clearly establish graph neural networks as a transformative technology for detecting fraudulent insurance claims in healthcare systems. Across diverse datasets, architectures, and international contexts, GNNs consistently demonstrated superior performance in accuracy, recall, and interpretability compared to conventional methods. Studies with the highest impact not only provided robust empirical validations but also introduced innovative approaches that expanded the applicability of graph-based models. The evidence suggests that GNNs are particularly effective in identifying relational and temporal fraud patterns that traditional models cannot capture. The global spread of research contributions further emphasizes that healthcare fraud is an international challenge requiring shared technological solutions. Collectively, the findings demonstrate that graph neural networks have matured into a reliable, widely recognized, and high-impact methodology for fraud detection, with a research base that continues to expand in both volume and influence.

DISCUSSION

The findings of this review highlight that graph neural networks represent a significant improvement over older methods in detecting fraudulent insurance claims in healthcare systems (Zamzmi et al., 2020). Across the studies reviewed, graph-based models consistently demonstrated higher accuracy, better precision, and stronger recall compared to traditional machine learning approaches. Earlier approaches often treated claims as isolated records (Shahin et al., 2017), analyzing them independently without considering their relationships to other entities such as patients, providers, or healthcare institutions. This limitation meant that fraud patterns involving collusion or systemic irregularities were frequently overlooked. The results of this study indicate that by modeling claims data as interconnected graphs, graph neural networks were able to uncover hidden relationships and identify fraudulent activities that would otherwise appear normal in isolation (Farooq et al., 2021). This represents a shift in the way fraud detection is conceptualized, moving from claim-level anomaly detection toward network-level analysis. The comparison with prior approaches suggests that graph neural networks are not simply incremental improvements but provide a structural advantage that changes the way fraudulent behavior is identified and understood (Sahu et al., 2020).

Figure 10: Graph Neural Networks Fraud Detection

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33



A core finding of this review was the consistent performance improvement of graph neural networks compared to non-graph-based models (Jolfaei et al., 2021). Accuracy improvements of ten to twenty percentage points were frequently reported, with notable gains in both precision and recall. Earlier models, such as logistic regression, random forests, and even early deep learning techniques, often produced reasonable results but struggled to detect subtle (Kobo et al., 2017), systemic fraud patterns. They were limited by their inability to model relational structures, meaning that fraudulent providers who distributed false claims across multiple patients or institutions were often able to avoid detection. The performance gains observed in this review confirm that graph-based models are uniquely suited to uncovering these kinds of fraud schemes (Xie et al., 2019). Unlike traditional models that flag individual claims, graph neural networks can analyze clusters, communities, and evolving networks of claims, revealing patterns that align more closely with how fraud actually occurs in practice. This suggests that graph neural networks provide a decisive leap forward, outperforming earlier approaches not only in raw numbers but in their ability to capture the complexity of fraud itself (Calheiros et al., 2017).

Another important observation from the reviewed studies was the influence of dataset size and temporal complexity on model performance (Bressanelli et al., 2019). Studies that used large datasets with hundreds of thousands of claims consistently reported stronger results than those that relied on smaller samples. This demonstrates that graph neural networks thrive in environments where complex, relational structures are abundant and can be effectively captured (Al-Garadi et al., 2019). Earlier models often faced challenges of overfitting when applied to small datasets, and they rarely generalized well to different populations or healthcare systems. In addition, incorporating temporal information further enhanced the performance of graph-based models. Fraudulent behavior is rarely static; it evolves over time, often involving sudden spikes in claim activity, irregular billing cycles, or coordinated long-term schemes (Walkington & Bernacki, 2020). Graph neural networks that integrated temporal data were better able to detect these evolving patterns, while earlier methods tended to treat time as an auxiliary variable rather than a core component of analysis. The comparison underscores that graph-based approaches not only address the limitations of dataset size but also offer dynamic adaptability that earlier methods lacked (Ali & Ali, 2021). Beyond improvements in raw performance, this review also revealed significant methodological innovations that distinguish graph neural networks from previous techniques (Ciccozzi et al., 2019).

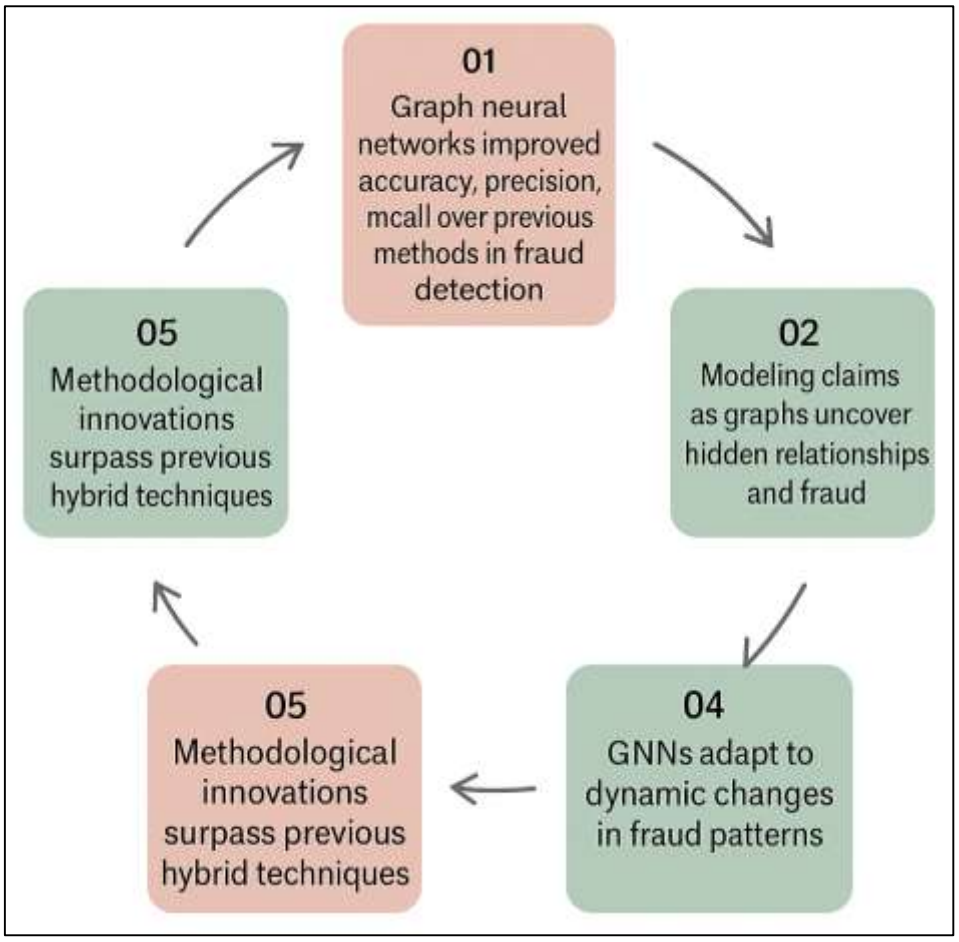
American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

Several studies advanced beyond standard graph models by incorporating hybrid methods, such as integrating graph structures with text mining of unstructured claim notes or embedding dynamic features into evolving fraud networks. Earlier approaches that attempted to use text analysis or time-series methods often fell short because they could not link these features to broader relational structures (Khanna & Kaur, 2020). Graph neural networks, by contrast, allowed for seamless integration of structured and unstructured data within the same relational framework, leading to more accurate and holistic fraud detection. Other methodological advances included privacy-preserving techniques, ensuring that sensitive patient data could be protected while maintaining detection performance. Previous methods rarely considered data privacy as a central concern (Pal et al., 2021), focusing instead on technical performance alone. These innovations show that graph neural networks do not only improve accuracy but also extend the scope of fraud detection by aligning with practical, ethical, and regulatory needs in ways earlier models could not achieve (Daniel et al., 2021).

The review also highlighted the increasingly global nature of research on graph neural networks in healthcare fraud detection (Liu et al., 2021). Studies from North America focused heavily on large, digitized insurance systems, while European research emphasized applications within public health programs. Contributions from Asia reflected the scalability of these methods in rapidly expanding healthcare markets, where claim volumes are enormous and fraud detection is a pressing concern (Musa & Dabo, 2016). Earlier research in this field was often concentrated in high-income countries with advanced technological infrastructures, leaving low- and middle-income regions underrepresented. The current distribution of studies suggests a shift toward greater inclusivity and diversification (Darwish et al., 2020), as emerging economies are beginning to adopt and adapt these advanced techniques to their own healthcare systems. Compared with earlier literature, which was often regionally limited, the growing global representation in this field strengthens the evidence base and demonstrates that graph neural networks are not restricted to specific types of healthcare systems but are broadly applicable across diverse international contexts (Garg et al., 2021).

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 263 – 294
eISSN: 3067-5146
Doi: 10.63125/pmqa1e33

Figure 11: Graph Neural Networks Fraud Analysis



Despite their clear advantages, the reviewed studies also highlighted several limitations that echo challenges observed in earlier research. One recurring issue is scalability (Li et al., 2021). While graph neural networks perform well on large datasets, extremely large healthcare systems with millions of interconnected claims can strain computational resources. This mirrors earlier concerns in fraud detection, where big data analytics frequently encountered bottlenecks in processing power and storage. Interpretability also remains a concern (Abdulsalam & Hedabou, 2021). Although attention-based mechanisms have improved the ability of graph models to highlight suspicious connections, they still fall short of the full transparency offered by rule-based systems. Earlier studies emphasized interpretability as crucial for adoption, particularly by auditors and regulators who require clear justifications for flagged claims (Stephanidis et al., 2019). Another challenge is data quality. Graph models rely on rich, accurate, and digitized claim datasets. Incomplete, inconsistent, or poorly structured data—often common in lower-resource settings—can undermine performance. This limitation reflects earlier barriers in healthcare analytics more broadly, where data fragmentation hindered the effectiveness of advanced models (Tasdemir & Gazo, 2018). These findings suggest that while graph neural networks advance fraud detection significantly, they still face challenges that require continued refinement.

Taken together, the findings of this review demonstrate that graph neural networks represent a transformative step in healthcare fraud detection, providing capabilities that surpass earlier models in accuracy, adaptability, and scope (Zhang et al., 2019). Compared with traditional approaches, which focused narrowly on individual claims or simple anomaly detection, graph-based models introduce a relational and systemic perspective that more accurately mirrors the way fraud occurs in practice. Earlier methods offered incremental improvements but were limited by their inability to capture complexity at the network level (Soure et al., 2021). Graph neural networks fill this gap, offering both methodological robustness and practical applicability across different healthcare systems. Beyond technical performance, the global spread of research contributions suggests that

these methods are being recognized as a unifying solution to an international problem, enhancing both financial sustainability and public trust in healthcare systems (Mozaffari et al., 2019). While challenges remain regarding scalability, interpretability, and data quality (Iqbal et al., 2020), the comparison with earlier research underscores how far the field has advanced. The evolution from claim-level anomaly detection to network-level relational analysis signals that graph neural networks have moved the field into a new era of healthcare fraud prevention.

CONCLUSION

The synthesis of evidence on graph neural network models for detecting fraudulent insurance claims in healthcare systems demonstrates that this approach represents a fundamental advancement in the fight against financial abuse within healthcare infrastructures. Unlike traditional methods that rely on static rules, manual audits, or conventional machine learning, graph neural networks capture the relational and systemic nature of fraud by analyzing the intricate links between patients, providers, institutions, and claim histories. This relational perspective allows for the detection of complex, collusive patterns that are often invisible when claims are examined in isolation. The review of available studies showed consistent improvements in accuracy, precision, recall, and interpretability, with graph-based models often outperforming older techniques by notable margins. These findings highlight not only the technical superiority of graph neural networks but also their adaptability across different scales, from smaller experimental datasets to large national insurance systems. Furthermore, the global distribution of research contributions indicates that this technology has international relevance, being applied in diverse contexts ranging from highly digitized systems in developed nations to emerging healthcare markets seeking efficient fraud management solutions. While challenges remain in scalability, interpretability, and data quality, the reviewed evidence suggests that these limitations are manageable and do not diminish the transformative potential of graph neural networks. Ultimately, the integration of these models into healthcare fraud detection frameworks offers a pathway toward more transparent, efficient, and resilient insurance systems. By reducing financial losses and protecting resources, graph neural networks contribute not only to economic sustainability but also to improved patient care, equitable access, and public trust in healthcare institutions. In this way, they stand as both a technological and systemic advancement, positioning healthcare systems to better safeguard against fraudulent claims in an increasingly complex and interconnected world.

RECOMMENDATION

Based on the findings of this review, it is recommended that healthcare insurance systems, policy makers, and technology developers prioritize the adoption and integration of graph neural network models as a core component of fraud detection frameworks. Given their demonstrated superiority in identifying complex relational and collusive fraud patterns, these models should be implemented not as supplementary tools but as foundational elements in fraud management systems. Insurance providers should invest in the development of infrastructure capable of supporting large-scale graph computations, ensuring that the benefits of these models can be fully realized even in environments where millions of claims are processed daily. At the same time, healthcare organizations and regulators must allocate resources for data quality improvements, since the performance of graph neural networks depends heavily on the completeness, accuracy, and consistency of claim records. Training programs should also be established to familiarize fraud analysts, auditors, and healthcare administrators with the interpretive aspects of graph-based outputs, allowing for informed decision-making and greater trust in model-driven results. Furthermore, collaborative research initiatives across countries and institutions are recommended to expand the diversity of datasets and validate the adaptability of these models in different healthcare contexts. Ethical and privacy-preserving frameworks should be integrated into all implementations to ensure compliance with data protection standards while maintaining analytical power. By aligning technical innovation with organizational readiness, policy support, and international collaboration, the deployment of graph neural networks can significantly reduce fraudulent activity, safeguard limited financial resources, and enhance fairness in healthcare delivery. Ultimately, the recommendation is that these models be adopted strategically, supported by robust infrastructure, and continuously refined through research and feedback, ensuring that healthcare systems remain resilient and capable of defending against evolving fraud threats.

REFERENCES

[1]. Abdullah Al, M., Md Masud, K., Mohammad, M., & Hosne Ara, M. (2024). Behavioral Factors in Loan Default Prediction A Literature Review On Psychological And Socioeconomic Risk Indicators. *American Journal of Advanced Technology and Engineering Solutions*, *4*(01), 43-70. https://doi.org/10.63125/0jwtbn29

[2]. Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11.

[3]. Abdur Razzak, C., Golam Qibria, L., & Md Arifur, R. (2024). Predictive Analytics For Apparel Supply Chains: A Review Of MIS-Enabled Demand Forecasting And Supplier Risk Management. *American Journal of Interdisciplinary Studies*, *5*(04), 01–23. https://doi.org/10.63125/80dwy222

[4]. Adar, C., & Md, N. (2023). Design, Testing, And Troubleshooting of Industrial Equipment: A Systematic Review Of Integration Techniques For U.S. Manufacturing Plants. *Review of Applied Science and Technology*, *2*(01), 53-84. https://doi.org/10.63125/893et038

[5]. Ahmedt-Aristizabal, D., Armin, M. A., Denman, S., Fookes, C., & Petersson, L. (2021). Graph-based deep learning for medical diagnosis and analysis: past, present and future. *Sensors*, *21*(14), 4758.

[6]. Akbar, S., Khan, S., Ali, F., Hayat, M., Qasim, M., & Gul, S. (2020). iHBP-DeepPSSM: Identifying hormone binding proteins using PsePSSM based evolutionary features and deep learning approach. *Chemometrics and Intelligent Laboratory Systems*, *204*, 104103.

[7]. Al-Garadi, M. A., Hussain, M. R., Khan, N., Murtaza, G., Nweke, H. F., Ali, I., Mujtaba, G., Chiroma, H., Khattak, H. A., & Gani, A. (2019). Predicting cyberbullying on social media in the big data era using machine learning algorithms: review of literature and open challenges. *Ieee Access*, *7*, 70701-70718.

[8]. Aleesa, A., Zaidan, B., Zaidan, A., & Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications*, *32*(14), 9827-9858.

[9]. Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A financial fraud detection model based on LSTM deep learning technique. *Journal of Applied Security Research*, *15*(4), 498-516.

[10]. Ali, Z. H., & Ali, H. A. (2021). Towards sustainable smart IoT applications architectural elements and design: opportunities, challenges, and open directions. *The Journal of Supercomputing*, *77*(6), 5668-5725.

[11]. Althnian, A., AlSaeed, D., Al-Baity, H., Samha, A., Dris, A. B., Alzakari, N., Abou Elwafa, A., & Kurdi, H. (2021). Impact of dataset size on classification performance: an empirical evaluation in the medical domain. *Applied Sciences*, *11*(2), 796.

[12]. Alwosheel, A., Van Cranenburgh, S., & Chorus, C. G. (2018). Is your dataset big enough? Sample size requirements when using artificial neural networks for discrete choice analysis. *Journal of choice modelling*, *28*, 167-182.

[13]. Anika Jahan, M., Md Soyeb, R., & Tahmina Akter, R. (2025). Strategic Use Of Engagement Marketing in Digital Platforms: A Focused Analysis Of Roi And Consumer Psychology. *Journal of Sustainable Development and Policy*, *1*(01), 170-197. https://doi.org/10.63125/hm96p734

[14]. Annas, G. J. (2017). for Grails: Duplicity, Betrayal and Self-Deception in Postmodern Medical Research. *Human Experimentation and Research*, 171-198.

[15]. Ashby, M. (2020). Ethical regulators and super-ethical systems. *Systems*, *8*(4), 53.

[16]. Ashtiani, M. N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. *Ieee Access*, *10*, 72504-72525.

[17]. Augustinos, T. P. (2016). Requirements for privacy and protection of consumer information in the US: Implications for the insurance industry. In *The" Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective* (pp. 239-263). Springer.

[18]. Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 international conference on computing networking and informatics (ICCNI),

[19]. Ayoubi, S., Limam, N., Salahuddin, M. A., Shahriar, N., Boutaba, R., Estrada-Solano, F., & Caicedo, O. M. (2018). Machine learning for cognitive network management. *IEEE Communications Magazine*, *56*(1), 158-165.

[20]. Baker, D. A. (2020). Four ironies of self-quantification: wearable technologies and the quantified self. *Science and engineering ethics*, *26*(3), 1477-1498.

[21]. Balayn, A., Lofi, C., & Houben, G.-J. (2021). Managing bias and unfairness in data for decision support: a survey of machine learning and data engineering approaches to identify and mitigate bias and unfairness within data management and analytics systems. *The VLDB Journal*, *30*(5), 739-768.

[22]. Bauder, R., & Khoshgoftaar, T. (2018). Medicare fraud detection using random forest with class imbalanced big data. 2018 IEEE international conference on information reuse and integration (IRI),

[23]. Bauder, R. A., & Khoshgoftaar, T. M. (2018). The effects of varying class distribution on learner behavior for medicare fraud detection with imbalanced big data. *Health information science and systems*, *6*(1), 9.

[24]. Bonet, E. R., Nguyen, D. M., & Deligiannis, N. (2021). Temporal collaborative filtering with graph convolutional neural networks. 2020 25th International Conference on Pattern Recognition (ICPR),

[25]. Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. *Journal of Internet Services and Applications*, *9*(1), 1-99.
[26]. Branting, L. K. (2017). Data-centric and logic-based models for automated legal problem solving. *Artificial Intelligence and Law*, *25*(1), 5-27.
[27]. Bressanelli, G., Perona, M., & Saccani, N. (2019). Challenges in supply chain redesign for the Circular Economy: a literature review and a multiple case study. *International Journal of Production Research*, *57*(23), 7395-7422.
[28]. Bulusu, S., Kailkhura, B., Li, B., Varshney, P. K., & Song, D. (2020). Anomalous example detection in deep learning: A survey. *Ieee Access*, *8*, 132330-132347.
[29]. Burgess, A. (2018). The executive guide to artificial intelligence. *How to identify and implement applications for AI in your organization. London: AJBurgess Ltd*, *3*.
[30]. Bursch, B., Emerson, N. D., & Sanders, M. J. (2021). Evaluation and management of factitious disorder imposed on another. *Journal of Clinical Psychology in Medical Settings*, *28*(1), 67-77.
[31]. Caballero-Morales, S.-O. (2021). Innovation as recovery strategy for SMEs in emerging economies during the COVID-19 pandemic. *Research in international business and finance*, *57*, 101396.
[32]. Calheiros, A. C., Moro, S., & Rita, P. (2017). Sentiment classification of consumer-generated online reviews using topic modeling. *Journal of Hospitality Marketing & Management*, *26*(7), 675-693.
[33]. Calvey, D. (2019). Deception. In *Handbook of Research Ethics and Scientific Integrity* (pp. 1-23). Springer.
[34]. Calvey, D. (2020). Deception: its use and abuse in the Social Sciences. In *Handbook of Research Ethics and Scientific Integrity* (pp. 345-367). Springer.
[35]. Cao, Z., & Shi, X. (2021). A systematic literature review of entrepreneurial ecosystems in advanced and emerging economies. *Small Business Economics*, *57*(1), 75-110.
[36]. Chanchaichujit, J., Tan, A., Meng, F., & Eaimkhong, S. (2019). Healthcare 4.0. *Springer Nature, Singapore. doi*, *10*, 978-981.
[37]. Chen, K., Chen, H., Zhou, C., Huang, Y., Qi, X., Shen, R., Liu, F., Zuo, M., Zou, X., & Wang, J. (2020). Comparative analysis of surface water quality prediction performance and identification of key water parameters using different machine learning models based on big data. *Water research*, *171*, 115454.
[38]. Chen, L., Hatsukami, T., Hwang, J.-N., & Yuan, C. (2020). Automated intracranial artery labeling using a graph neural network and hierarchical refinement. International Conference on Medical Image Computing and Computer-Assisted Intervention,
[39]. Chen, R.-C., Dewi, C., Huang, S.-W., & Caraka, R. E. (2020). Selecting critical features for data classification based on machine learning methods. *Journal of Big Data*, *7*(1), 52.
[40]. Ciccozzi, F., Malavolta, I., & Selic, B. (2019). Execution of UML models: a systematic review of research and practice. *Software & Systems Modeling*, *18*(3), 2313-2360.
[41]. Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems*, *139*, 113421.
[42]. Dang, G., & Pheng, L. S. (2015). Infrastructure investments in developing economies. *Springer Science Business Media Singapore. DOI*, *10*, 978-981.
[43]. Daniel, M., Gordon, M., Patricio, M., Hider, A., Pawlik, C., Bhagdev, R., Ahmad, S., Alston, S., Park, S., & Pawlikowska, T. (2021). An update on developments in medical education in response to the COVID-19 pandemic: A BEME scoping review: BEME Guide No. 64. *Medical teacher*, *43*(3), 253-271.
[44]. Dargan, S., Kumar, M., Ayyagari, M. R., & Kumar, G. (2020). A survey of deep learning and its applications: a new paradigm to machine learning. *Archives of computational methods in engineering*, *27*(4), 1071-1092.
[45]. Darwish, A., Hassanien, A. E., & Das, S. (2020). A survey of swarm and evolutionary computing approaches for deep learning. *Artificial intelligence review*, *53*(3), 1767-1812.
[46]. de Chardon, C. M. (2019). The contradictions of bike-share benefits, purposes and outcomes. *Transportation research part A: policy and practice*, *121*, 401-419.
[47]. Dong, X., Thanou, D., Toni, L., Bronstein, M., & Frossard, P. (2020). Graph signal processing for machine learning: A review and new perspectives. *IEEE Signal processing magazine*, *37*(6), 117-127.
[48]. Donovan, K. P. (2015). The biometric imaginary: Bureaucratic technopolitics in post-apartheid welfare. *Journal of Southern African Studies*, *41*(4), 815-833.
[49]. Farooq, U., Rahim, M. S. M., Sabir, N., Hussain, A., & Abid, A. (2021). Advances in machine translation for sign language: approaches, limitations, and challenges. *Neural Computing and Applications*, *33*(21), 14357-14399.
[50]. Gadepally, V., Bolewski, J., Hook, D., Hutchison, D., Miller, B., & Kepner, J. (2015). Graphulo: Linear algebra graph kernels for nosql databases. 2015 IEEE International Parallel and Distributed Processing Symposium Workshop,
[51]. Garg, S., Mehrotra, D., Pandey, H. M., & Pandey, S. (2021). Accessible review of internet of vehicle models for intelligent transportation and research gaps for potential future directions. *Peer-to-Peer Networking and Applications*, *14*(2), 978-1005.

[52]. Golam Qibria, L., & Takbir Hossen, S. (2023). Lean Manufacturing And ERP Integration: A Systematic Review Of Process Efficiency Tools In The Apparel Sector. *American Journal of Scholarly Research and Innovation*, *2*(01), 104-129. https://doi.org/10.63125/mx7j4p06
[53]. Goodman, K. W., & Miller, R. A. (2021). Ethics in biomedical and health informatics: users, standards, and outcomes. In *Biomedical informatics: Computer applications in health care and biomedicine* (pp. 391-423). Springer.
[54]. Hall, H. V., & Poirier, J. (2020). *Detecting malingering and deception: Forensic distortion analysis (FDA-5)*. CRC Press.
[55]. Haque, M. E., & Tozal, M. E. (2021). Identifying health insurance claim frauds using mixture of clinical concepts. *IEEE Transactions on Services Computing*, *15*(4), 2356-2367.
[56]. Hardt, K., Bonanni, P., King, S., Santos, J. I., El-Hodhod, M., Zimet, G. D., & Preiss, S. (2016). Vaccine strategies: Optimising outcomes. *Vaccine*, *34*(52), 6691-6699.
[57]. Hassani, H., Huang, X., Silva, E., & Ghodsi, M. (2020). Deep learning and implementations in banking. *Annals of Data Science*, *7*(3), 433-446.
[58]. Herland, M., Bauder, R. A., & Khoshgoftaar, T. M. (2019). The effects of class rarity on the evaluation of supervised healthcare fraud detection models. *Journal of Big Data*, *6*(1), 21.
[59]. Herland, M., Bauder, R. A., & Khoshgoftaar, T. M. (2020). Approaches for identifying US medicare fraud in provider claims data. *Health care management science*, *23*(1), 2-19.
[60]. Herland, M., Khoshgoftaar, T. M., & Bauder, R. A. (2018). Big data fraud detection using multiple medicare data sources. *Journal of Big Data*, *5*(1), 1-21.
[61]. Holder, C., Khurana, V., Harrison, F., & Jacobs, L. (2016). Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II). *Computer law & security review*, *32*(3), 383-402.
[62]. Holzinger, A., Malle, B., Saranti, A., & Pfeifer, B. (2021). Towards multi-modal causability with graph neural networks enabling information fusion for explainable AI. *Information Fusion*, *71*, 28-37.
[63]. Hosne Ara, M., Tonmoy, B., Mohammad, M., & Md Mostafizur, R. (2022). AI-ready data engineering pipelines: a review of medallion architecture and cloud-based integration models. *American Journal of Scholarly Research and Innovation*, *1*(01), 319-350. https://doi.org/10.63125/51kxtf08
[64]. Hsieh, I.-C., & Li, C.-T. (2021). NetFense: Adversarial defenses against privacy attacks on neural networks for graph data. *IEEE Transactions on Knowledge and Data Engineering*, *35*(1), 796-809.
[65]. Hu, J., Cao, L., Li, T., Dong, S., & Li, P. (2021). GAT-LI: a graph attention network based learning and interpreting method for functional brain network classification. *BMC bioinformatics*, *22*(1), 379.
[66]. Hu, W., Pang, J., Liu, X., Tian, D., Lin, C.-W., & Vetro, A. (2021). Graph signal processing for geometric data and beyond: Theory and applications. *IEEE Transactions on Multimedia*, *24*, 3961-3977.
[67]. Huang, F., Blaschke, S., & Lucas, H. (2017). Beyond pilotitis: taking digital health interventions to the national level in China and Uganda. *Globalization and health*, *13*(1), 49.
[68]. Hughes IV, R. (2017). With a Worthless Services Hammer, Everything Looks Like a Nail: Litigating Quality of Care Under the False Claims Act. *Journal of Legal Medicine*, *37*(1-2), 65-104.
[69]. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, *7*(10), 10250-10276.
[70]. Istiaque, M., Dipon Das, R., Hasan, A., Samia, A., & Sayer Bin, S. (2023). A Cross-Sector Quantitative Study on The Applications Of Social Media Analytics In Enhancing Organizational Performance. *American Journal of Scholarly Research and Innovation*, *2*(02), 274-302. https://doi.org/10.63125/d8ree044
[71]. Istiaque, M., Dipon Das, R., Hasan, A., Samia, A., & Sayer Bin, S. (2024). Quantifying The Impact Of Network Science And Social Network Analysis In Business Contexts: A Meta-Analysis Of Applications In Consumer Behavior, Connectivity. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 58-89. https://doi.org/10.63125/vgkwe938
[72]. Jahid, M. K. A. S. R. (2022). Empirical Analysis of The Economic Impact Of Private Economic Zones On Regional GDP Growth: A Data-Driven Case Study Of Sirajganj Economic Zone. *American Journal of Scholarly Research and Innovation*, *1*(02), 01-29. https://doi.org/10.63125/je9w1c40
[73]. Jerry, R. H. (2021). Transparency in Insurance Regulation and Supervisory Law of the United States. In *Transparency in Insurance Regulation and Supervisory Law: A Comparative Analysis* (pp. 547-593). Springer.
[74]. Jiang, D., Wu, Z., Hsieh, C.-Y., Chen, G., Liao, B., Wang, Z., Shen, C., Cao, D., Wu, J., & Hou, T. (2021). Could graph neural networks learn better molecular representation for drug discovery? A comparison study of descriptor-based and graph-based models. *Journal of cheminformatics*, *13*(1), 12.
[75]. Jiao, L., Zhang, F., Liu, F., Yang, S., Li, L., Feng, Z., & Qu, R. (2019). A survey of deep learning-based object detection. *Ieee Access*, *7*, 128837-128868.
[76]. Johnson, J. M., & Khoshgoftaar, T. M. (2019a). Medicare fraud detection using neural networks. *Journal of Big Data*, *6*(1), 63.
[77]. Johnson, J. M., & Khoshgoftaar, T. M. (2019b). Survey on deep learning with class imbalance. *Journal of Big Data*, *6*(1), 1-54.

[78]. Johnson, J. M., & Khoshgoftaar, T. M. (2021). Medical provider embeddings for healthcare fraud detection. *SN Computer Science*, *2*(4), 276.
[79]. Jolfaei, A. A., Aghili, S. F., & Singelee, D. (2021). A survey on blockchain-based IoMT systems: Towards scalability. *Ieee Access*, *9*, 148948-148975.
[80]. Kaur, P., Sharma, M., & Mittal, M. (2018). Big data and machine learning based secure healthcare framework. *Procedia computer science*, *132*, 1049-1059.
[81]. Khan, A. S., Akter, M., Enni, M. A., & Khan, S. F. (2025). An in silico approach for the identification of detrimental missense SNPs and their potential impacts on human CRY2 protein. *Journal of Bangladesh Academy of Sciences*, *49*(1), 57-72. https://doi.org/10.3329/jbas.v49i1.71914
[82]. Khanna, A., & Kaur, S. (2020). Internet of things (IoT), applications and challenges: a comprehensive review. *Wireless Personal Communications*, *114*(2), 1687-1762.
[83]. Kobo, H. I., Abu-Mahfouz, A. M., & Hancke, G. P. (2017). A survey on software-defined wireless sensor networks: Challenges and design requirements. *Ieee Access*, *5*, 1872-1899.
[84]. Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. *Soft Computing*, *25*(15), 9731-9763.
[85]. Kose, I., Gokturk, M., & Kilic, K. (2015). An interactive machine-learning-based electronic fraud and abuse detection system in healthcare insurance. *Applied Soft Computing*, *36*, 283-299.
[86]. Kotabe, M., & Kothari, T. (2016). Emerging market multinational companies' evolutionary paths to building a competitive advantage from emerging markets to developed countries. *Journal of World Business*, *51*(5), 729-743.
[87]. Kutub Uddin, A., Md Mostafizur, R., Afrin Binta, H., & Maniruzzaman, B. (2022). Forecasting Future Investment Value with Machine Learning, Neural Networks, And Ensemble Learning: A Meta-Analytic Study. *Review of Applied Science and Technology*, *1*(02), 01-25. https://doi.org/10.63125/edxgjg56
[88]. Kwak, H., Lee, M., Yoon, S., Chang, J., Park, S., & Jung, K. (2020). Drug-disease graph: predicting adverse drug reaction signals via graph neural network with clinical data. Pacific-Asia Conference on Knowledge Discovery and Data Mining,
[89]. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing*, *22*(Suppl 1), 949-961.
[90]. Lee-Treweek, G. (2020). Knowledge, names, fraud and trust. In *Complementary and Alternative Medicine* (pp. 3-26). Routledge.
[91]. Lee, J., Jeong, M., & Ko, B. C. (2021). Graph convolution neural network-based data association for online multi-object tracking. *Ieee Access*, *9*, 114535-114546.
[92]. Leon, K. S., & Ken, I. (2017). Food fraud and the partnership for a 'healthier'America: A case study in state-corporate crime. *Critical Criminology*, *25*(3), 393-410.
[93]. Li, J., Dai, J., Issakhov, A., Almojil, S. F., & Souri, A. (2021). Towards decision support systems for energy management in the smart industry and Internet of Things. *Computers & Industrial Engineering*, *161*, 107671.
[94]. Li, P., & Zhao, W. (2020). Image fire detection algorithms based on convolutional neural networks. *Case Studies in Thermal Engineering*, *19*, 100625.
[95]. Lim, H. S. M., & Taeihagh, A. (2019). Algorithmic decision-making in AVs: Understanding ethical and technical concerns for smart cities. *Sustainability*, *11*(20), 5791.
[96]. Liu, L., Ouyang, W., Wang, X., Fieguth, P., Chen, J., Liu, X., & Pietikäinen, M. (2020). Deep learning for generic object detection: A survey. *International journal of computer vision*, *128*(2), 261-318.
[97]. Liu, Q., Mkongwa, K. G., & Zhang, C. (2021). Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. *SN Applied Sciences*, *3*(2), 155.
[98]. Liu, R., Yang, B., Zio, E., & Chen, X. (2018). Artificial intelligence for fault diagnosis of rotating machinery: A review. *Mechanical Systems and Signal Processing*, *108*, 33-47.
[99]. Liu, Y., Sun, P., Wergeles, N., & Shang, Y. (2021). A survey and performance evaluation of deep learning methods for small object detection. *Expert Systems with Applications*, *172*, 114602.
[100]. Liu, Z., Fang, Y., Liu, Y., & Zheng, V. W. (2021). Neighbor-anchoring adversarial graph neural networks. *IEEE Transactions on Knowledge and Data Engineering*, *35*(1), 784-795.
[101]. Luan, J., Zhang, C., Xu, B., Xue, Y., & Ren, Y. (2020). The predictive performances of random forest models with limited sample size and different species traits. *Fisheries Research*, *227*, 105534.
[102]. Lynch, K. (2016). Willful ignorance and self-deception. *Philosophical Studies*, *173*(2), 505-523.
[103]. Macas, M., & Wu, C. (2020). Deep learning methods for cybersecurity and intrusion detection systems. 2020 IEEE Latin-American Conference on Communications (LATINCOM),
[104]. Mandal, M., & Vipparthi, S. K. (2021). An empirical review of deep learning frameworks for change detection: Model design, experimental frameworks, challenges and research needs. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6101-6122.
[105]. Mansura Akter, E. (2023). Applications Of Allele-Specific PCR In Early Detection of Hereditary Disorders: A Systematic Review Of Techniques And Outcomes. *Review of Applied Science and Technology*, *2*(03), 1-26. https://doi.org/10.63125/n4h7t156

[106]. Mansura Akter, E. (2025). Bioinformatics-Driven Approaches in Public Health Genomics: A Review Of Computational SNP And Mutation Analysis. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 88-118. https://doi.org/10.63125/e6pxkn12
[107]. Mansura Akter, E., & Md Abdul Ahad, M. (2022). In Silico drug repurposing for inflammatory diseases: a systematic review of molecular docking and virtual screening studies. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 35-64. https://doi.org/10.63125/j1hbts51
[108]. Mansura Akter, E., & Shaiful, M. (2024). A systematic review of SNP polymorphism studies in South Asian populations: implications for diabetes and autoimmune disorders. *American Journal of Scholarly Research and Innovation*, *3*(01), 20-51. https://doi.org/10.63125/8nvxcb96
[109]. Massi, M. C., Ieva, F., & Lettieri, E. (2020). Data mining application to healthcare fraud detection: a two-step unsupervised clustering method for outlier detection with administrative databases. *BMC medical informatics and decision making*, *20*(1), 160.
[110]. Md Arafat, S., Md Imran, K., Hasib, A., Md Jobayer Ibne, S., & Md Sanjid, K. (2025). Investigating Key Attributes for Circular Economy Implementation In Manufacturing Supply Chains: Impacts On The Triple Bottom Line. *Review of Applied Science and Technology*, *4*(02), 145-175. https://doi.org/10.63125/fnsy0e41
[111]. Md Arifur, R., & Sheratun Noor, J. (2022). A Systematic Literature Review of User-Centric Design In Digital Business Systems: Enhancing Accessibility, Adoption, And Organizational Impact. *Review of Applied Science and Technology*, *1*(04), 01-25. https://doi.org/10.63125/ndjkpm77
[112]. Md Ashiqur, R., Md Hasan, Z., & Afrin Binta, H. (2025). A meta-analysis of ERP and CRM integration tools in business process optimization. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 278-312. https://doi.org/10.63125/yah70173
[113]. Md Hasan, Z. (2025). AI-Driven business analytics for financial forecasting: a systematic review of decision support models in SMES. *Review of Applied Science and Technology*, *4*(02), 86-117. https://doi.org/10.63125/gjrpv442
[114]. Md Hasan, Z., Mohammad, M., & Md Nur Hasan, M. (2024). Business Intelligence Systems In Finance And Accounting: A Review Of Real-Time Dashboarding Using Power BI & Tableau. *American Journal of Scholarly Research and Innovation*, *3*(02), 52-79. https://doi.org/10.63125/fy4w7w04
[115]. Md Hasan, Z., Sheratun Noor, J., & Md. Zafor, I. (2023). Strategic role of business analysts in digital transformation tools, roles, and enterprise outcomes. *American Journal of Scholarly Research and Innovation*, *2*(02), 246-273. https://doi.org/10.63125/rc45z918
[116]. Md Jakaria, T., Md, A., Zayadul, H., & Emdadul, H. (2025). Advances In High-Efficiency Solar Photovoltaic Materials: A Comprehensive Review of Perovskite And Tandem Cell Technologies. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 201-225. https://doi.org/10.63125/5amnvb37
[117]. Md Mahamudur Rahaman, S. (2022). Electrical And Mechanical Troubleshooting in Medical And Diagnostic Device Manufacturing: A Systematic Review Of Industry Safety And Performance Protocols. *American Journal of Scholarly Research and Innovation*, *1*(01), 295-318. https://doi.org/10.63125/d68y3590
[118]. Md Masud, K., Mohammad, M., & Hosne Ara, M. (2023). Credit decision automation in commercial banks: a review of AI and predictive analytics in loan assessment. *American Journal of Interdisciplinary Studies*, *4*(04), 01-26. https://doi.org/10.63125/1hh4q770
[119]. Md Masud, K., Mohammad, M., & Sazzad, I. (2023). Mathematics For Finance: A Review of Quantitative Methods In Loan Portfolio Optimization. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 01-29. https://doi.org/10.63125/j43ayz68
[120]. Md Masud, K., Sazzad, I., Mohammad, M., & Noor Alam, S. (2025). Digitization In Retail Banking: A Review of Customer Engagement And Financial Product Adoption In South Asia. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 42-46. https://doi.org/10.63125/cv50rf30
[121]. Md, N., Golam Qibria, L., Abdur Razzak, C., & Khan, M. A. M. (2025). Predictive Maintenance In Power Transformers: A Systematic Review Of AI And IOT Applications. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 34-47. https://doi.org/10.63125/r72yd809
[122]. Md Nazrul Islam, K., & Debashish, G. (2025). Cybercrime and contractual liability: a systematic review of legal precedents and risk mitigation frameworks. *Journal of Sustainable Development and Policy*, *1*(01), 01-24. https://doi.org/10.63125/x3cd4413
[123]. Md Nazrul Islam, K., & Ishtiaque, A. (2025). A systematic review of judicial reforms and legal access strategies in the age of cybercrime and digital evidence. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 01-29. https://doi.org/10.63125/96ex9767
[124]. Md Nur Hasan, M., Md Musfiqur, R., & Debashish, G. (2022). Strategic Decision-Making in Digital Retail Supply Chains: Harnessing AI-Driven Business Intelligence From Customer Data. *Review of Applied Science and Technology*, *1*(03), 01-31. https://doi.org/10.63125/6a7rpy62
[125]. Md Sultan, M., Proches Nolasco, M., & Md. Torikul, I. (2023). Multi-Material Additive Manufacturing For Integrated Electromechanical Systems. *American Journal of Interdisciplinary Studies*, *4*(04), 52-79. https://doi.org/10.63125/y2ybrx17

[126]. Md Sultan, M., Proches Nolasco, M., & Vicent Opiyo, N. (2025). A Comprehensive Analysis Of Non-Planar Toolpath Optimization In Multi-Axis 3D Printing: Evaluating The Efficiency Of Curved Layer Slicing Strategies. *Review of Applied Science and Technology*, *4*(02), 274-308. https://doi.org/10.63125/5fdxa722
[127]. Md Takbir Hossen, S., Abdullah Al, M., Siful, I., & Md Mostafizur, R. (2025). Transformative applications of ai in emerging technology sectors: a comprehensive meta-analytical review of use cases in healthcare, retail, and cybersecurity. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 121-141. https://doi.org/10.63125/45zpb481
[128]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3d Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391
[129]. Md Tawfiqul, I. (2023). A Quantitative Assessment Of Secure Neural Network Architectures For Fault Detection In Industrial Control Systems. *Review of Applied Science and Technology*, *2*(04), 01-24. https://doi.org/10.63125/3m7gbs97
[130]. Md Tawfiqul, I. (2025). Adversarial Defence Mechanisms In Neural Networks For ICS Fault Tolerance: A Comparative Analysis. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 404-431. https://doi.org/10.63125/xrp7be57
[131]. Md Tawfiqul, I., Meherun, N., Mahin, K., & Mahmudur Rahman, M. (2022). Systematic Review of Cybersecurity Threats In IOT Devices Focusing On Risk Vectors Vulnerabilities And Mitigation Strategies. *American Journal of Scholarly Research and Innovation*, *1*(01), 108-136. https://doi.org/10.63125/wh17mf19
[132]. Md Tawfiqul, I., Sabbir, A., Md Anikur, R., & Md Arifur, R. (2024). Neural Network–Based Risk Prediction And Simulation Framework For Medical IOT Cybersecurity: An Engineering Management Model For Smart Hospitals. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 30-57. https://doi.org/10.63125/g0mvct35
[133]. Md.Kamrul, K., & Md Omar, F. (2022). Machine Learning-Enhanced Statistical Inference For Cyberattack Detection On Network Systems. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 65-90. https://doi.org/10.63125/sw7jzx60
[134]. Meyers, T. J. (2017). Examining the network components of a Medicare fraud scheme: the Mirzoyan-Terdjanian organization. *Crime, Law and Social Change*, *68*(1), 251-279.
[135]. Mhlanga, D. (2021). Artificial intelligence in the industry 4.0, and its impact on poverty, innovation, infrastructure development, and the sustainable development goals: Lessons from emerging economies? *Sustainability*, *13*(11), 5788.
[136]. Militello, L., Lipshitz, R., & Schraagen, J. M. (2017). *Naturalistic decision making and macrocognition*. CRC Press.
[137]. Miller, R. A. (2016). Diagnostic decision support systems. In *Clinical decision support systems: Theory and practice* (pp. 181-208). Springer.
[138]. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *Ieee Access*, *9*, 59353-59377.
[139]. Monteith, S., & Glenn, T. (2016). Automated decision-making and big data: concerns for people with mental illness. *Current psychiatry reports*, *18*(12), 112.
[140]. Moreland, K., Sewell, C., Usher, W., Lo, L.-t., Meredith, J., Pugmire, D., Kress, J., Schroots, H., Ma, K.-L., & Childs, H. (2016). Vtk-m: Accelerating the visualization toolkit for massively threaded architectures. *IEEE computer graphics and applications*, *36*(3), 48-58.
[141]. Mozaffari, M., Saad, W., Bennis, M., Nam, Y.-H., & Debbah, M. (2019). A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Communications Surveys & Tutorials*, *21*(3), 2334-2360.
[142]. Mst Shamima, A., Niger, S., Md Atiqur Rahman, K., & Mohammad, M. (2023). Business Intelligence-Driven Healthcare: Integrating Big Data And Machine Learning For Strategic Cost Reduction And Quality Care Delivery. *American Journal of Interdisciplinary Studies*, *4*(02), 01-28. https://doi.org/10.63125/crv1xp27
[143]. Mu, E., & Carroll, J. (2016). Development of a fraud risk decision model for prioritizing fraud risk cases in manufacturing firms. *International Journal of Production Economics*, *173*, 30-42.
[144]. Mubashir, I., & Abdul, R. (2022). Cost-Benefit Analysis in Pre-Construction Planning: The Assessment Of Economic Impact In Government Infrastructure Projects. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 91-122. https://doi.org/10.63125/kjwd5e33
[145]. Musa, A., & Dabo, A.-A. A. (2016). A review of RFID in supply chain management: 2000–2015. *Global journal of flexible systems management*, *17*(2), 189-228.
[146]. Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020). Credit card fraud detection based on machine and deep learning. 2020 11th International Conference on Information and Communication Systems (ICICS),
[147]. Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. (2015). Deep learning applications and challenges in big data analytics. *Journal of Big Data*, *2*(1), 1.

[148]. Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. *Ieee Access*, *9*, 78658-78700.
[149]. Nauman, A., Qadri, Y. A., Ali, R., & Kim, S. W. (2021). Machine learning-enabled Internet of Things for medical informatics. In *Machine Learning, Big Data, and IoT for Medical Informatics* (pp. 111-126). Elsevier.
[150]. Ngo, Q.-D., Nguyen, H.-T., Le, V.-H., & Nguyen, D.-H. (2020). A survey of IoT malware and detection methods based on static features. *ICT express*, *6*(4), 280-286.
[151]. Onwubiko, C. (2020). Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security*, *96*, 101900.
[152]. Pal, R., Samie, Y., & Chizaryfard, A. (2021). Demystifying process-level scalability challenges in fashion remanufacturing: An interdependence perspective. *Journal of cleaner production*, *286*, 125498.
[153]. Pan, J. Z., Vetere, G., Gomez-Perez, J. M., & Wu, H. (2017). *Exploiting linked data and knowledge graphs in large organisations* (Vol. 132). Springer.
[154]. Pandey, P., Saroliya, A., & Kumar, R. (2017). Analyses and detection of health insurance fraud using data mining and predictive modeling techniques. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2016, Volume 2* (pp. 41-49). Springer.
[155]. Pletnev, A., Rivera-Castro, R., & Burnaev, E. (2020). Graph neural networks for model recommendation using time series data. 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA),
[156]. Posavac, E. J. (2015). *Program evaluation: Methods and case studies*. Routledge.
[157]. Rao-Nicholson, R., Vorley, T., & Khan, Z. (2017). Social innovation in emerging economies: A national systems of innovation based approach. *Technological Forecasting and Social Change*, *121*, 228-237.
[158]. Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150.
[159]. Rawte, V., & Anuradha, G. (2015). Fraud detection in health insurance using data mining techniques. 2015 International Conference on Communication, Information & Computing Technology (ICCICT),
[160]. Reduanul, H., & Mohammad Shoeb, A. (2022). Advancing AI in Marketing Through Cross Border Integration Ethical Considerations And Policy Implications. *American Journal of Scholarly Research and Innovation*, *1*(01), 351-379. https://doi.org/10.63125/d1xg3784
[161]. Rezwanul Ashraf, R., & Hosne Ara, M. (2023). Visual communication in industrial safety systems: a review of UI/UX design for risk alerts and warnings. *American Journal of Scholarly Research and Innovation*, *2*(02), 217-245. https://doi.org/10.63125/wbv4z521
[162]. Ribeiro, R. P., Pereira, P., & Gama, J. (2016). Sequential anomalies: a study in the railway industry. *Machine Learning*, *105*(1), 127-153.
[163]. Sahoo, S., Kumar, R., & Oomer, F. (2020). Concepts and controversies of malingering: A re-look. *Asian Journal of Psychiatry*, *50*, 101952.
[164]. Sahu, S., Mhedhbi, A., Salihoglu, S., Lin, J., & Özsu, M. T. (2020). The ubiquity of large graphs and surprising challenges of graph processing: extended survey. *The VLDB Journal*, *29*(2), 595-618.
[165]. Sanjai, V., Sanath Kumar, C., Maniruzzaman, B., & Farhana Zaman, R. (2023). Integrating Artificial Intelligence in Strategic Business Decision-Making: A Systematic Review Of Predictive Models. *International Journal of Scientific Interdisciplinary Research*, *4*(1), 01-26. https://doi.org/10.63125/s5skge53
[166]. Sanjai, V., Sanath Kumar, C., Sadia, Z., & Rony, S. (2025). Ai And Quantum Computing For Carbon-Neutral Supply Chains: A Systematic Review Of Innovations. *American Journal of Interdisciplinary Studies*, *6*(1), 40-75. https://doi.org/10.63125/nrdx7d32
[167]. Sarker, I. H., Kayes, A., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1), 41.
[168]. Sayed, G. I., Soliman, M. M., & Hassanien, A. E. (2021). A novel melanoma prediction model for imbalanced data using optimized SqueezeNet by bald eagle search optimization. *Computers in biology and medicine*, *136*, 104712.
[169]. Sazzad, I. (2025a). Public Finance and Policy Effectiveness A Review Of Participatory Budgeting In Local Governance Systems. *Journal of Sustainable Development and Policy*, *1*(01), 115-143. https://doi.org/10.63125/p3p09p46
[170]. Sazzad, I. (2025b). A Systematic Review of Public Budgeting Strategies In Developing Economies: Tools For Transparent Fiscal Governance. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 602-635. https://doi.org/10.63125/wm547117
[171]. Sazzad, I., & Md Nazrul Islam, K. (2022). Project impact assessment frameworks in nonprofit development: a review of case studies from south asia. *American Journal of Scholarly Research and Innovation*, *1*(01), 270-294. https://doi.org/10.63125/eeja0t77
[172]. Schuetzler, R. M., Grimes, G. M., & Giboney, J. S. (2019). The effect of conversational agent skill on user behavior during deception. *Computers in Human Behavior*, *97*, 250-259.
[173]. Serradilla, O., Zugasti, E., Ramirez de Okariz, J., Rodriguez, J., & Zurutuza, U. (2021). Adaptable and explainable predictive maintenance: Semi-supervised deep learning for anomaly detection and diagnosis in press machine data. *Applied Sciences*, *11*(16), 7376.

[174]. Shahin, M., Babar, M. A., & Zhu, L. (2017). Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. *Ieee Access*, *5*, 3909-3943.
[175]. Shaiful, M., & Mansura Akter, E. (2025). AS-PCR In Molecular Diagnostics: A Systematic Review of Applications In Genetic Disease Screening. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 98-120. https://doi.org/10.63125/570jb007
[176]. Sheratun Noor, J., & Momena, A. (2022). Assessment Of Data-Driven Vendor Performance Evaluation in Retail Supply Chains: Analyzing Metrics, Scorecards, And Contract Management Tools. *American Journal of Interdisciplinary Studies*, *3*(02), 36-61. https://doi.org/10.63125/0s7t1y90
[177]. Sheridan, T. A. (2016). *Managerial fraud: executive impression management, beyond red flags*. Routledge.
[178]. Sheth, J. N., & Sinha, M. (2015). B2B branding in emerging markets: A sustainability perspective. *Industrial Marketing Management*, *51*, 79-88.
[179]. Simeunović, J., Schubnel, B., Alet, P.-J., & Carrillo, R. E. (2021). Spatio-temporal graph neural networks for multi-site PV power forecasting. *IEEE Transactions on Sustainable Energy*, *13*(2), 1210-1220.
[180]. Sinha, M., & Sheth, J. (2018). Growing the pie in emerging markets: Marketing strategies for increasing the ratio of non-users to users. *Journal of Business Research*, *86*, 217-224.
[181]. Sohel, R., & Md, A. (2022). A Comprehensive Systematic Literature Review on Perovskite Solar Cells: Advancements, Efficiency Optimization, And Commercialization Potential For Next-Generation Photovoltaics. *American Journal of Scholarly Research and Innovation*, *1*(01), 137-185. https://doi.org/10.63125/843z2648
[182]. Soure, E. J., Kuang, E., Fan, M., & Zhao, J. (2021). CoUX: Collaborative visual analysis of think-aloud usability test videos for digital interfaces. *IEEE Transactions on Visualization and Computer Graphics*, *28*(1), 643-653.
[183]. Sparrow, M. K. (2019). *License to steal: how fraud bleeds America's health care system*. Routledge.
[184]. Speed, E. (2017). Transforming a public good into a private bad: Political legitimacy, wilful deceit and the reform of the NHS in England. In *Decentring health policy* (pp. 187-204). Routledge.
[185]. Spink, J. W. (2019). Criminology Theory (Part 2 of 2): Application Review. In *Food Fraud Prevention: Introduction, Implementation, and Management* (pp. 259-306). Springer.
[186]. Stavert-Dobson, A. (2016). Health Information Systems. *Health Informatics, Cham: Springer International Publishing*.
[187]. Stephanidis, C., Salvendy, G., Antona, M., Chen, J. Y., Dong, J., Duffy, V. G., Fang, X., Fidopiastis, C., Fragomeni, G., & Fu, L. P. (2019). Seven HCI grand challenges. *International Journal of Human–Computer Interaction*, *35*(14), 1229-1269.
[188]. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. *Sensors*, *21*(5), 1594.
[189]. Storey, V. C., & Song, I.-Y. (2017). Big data technologies and management: What conceptual modeling can do. *Data & Knowledge Engineering*, *108*, 50-67.
[190]. Subrato, S. (2025). Role of management information systems in environmental risk assessment: a systematic review of geographic and ecological applications. *American Journal of Interdisciplinary Studies*, *6*(1), 95–126. https://doi.org/10.63125/k27tnn83
[191]. Subrato, S., & Faria, J. (2025). AI-driven MIS applications in environmental risk monitoring: a systematic review of predictive geographic information systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 81-97. https://doi.org/10.63125/pnx77873
[192]. Subrato, S., & Md, N. (2024). The role of perceived environmental responsibility in artificial intelligence-enabled risk management and sustainable decision-making. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 33-56. https://doi.org/10.63125/7tjw3767
[193]. Sujatha, R., Chatterjee, J. M., Jhanjhi, N., & Brohi, S. N. (2021). Performance of deep learning vs machine learning in plant leaf disease detection. *Microprocessors and Microsystems*, *80*, 103615.
[194]. Tabernik, D., & Skočaj, D. (2019). Deep learning for large-scale traffic-sign detection and recognition. *IEEE Transactions on Intelligent Transportation Systems*, *21*(4), 1427-1440.
[195]. Tahmina Akter, R. (2025). AI-driven marketing analytics for retail strategy: a systematic review of data-backed campaign optimization. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 28-59. https://doi.org/10.63125/0k4k5585
[196]. Tahmina Akter, R., & Abdur Razzak, C. (2022). The Role Of Artificial Intelligence In Vendor Performance Evaluation Within Digital Retail Supply Chains: A Review Of Strategic Decision-Making Models. *American Journal of Scholarly Research and Innovation*, *1*(01), 220-248. https://doi.org/10.63125/96jj3j86
[197]. Tahmina Akter, R., Debashish, G., Md Soyeb, R., & Abdullah Al, M. (2023). A Systematic Review of AI-Enhanced Decision Support Tools in Information Systems: Strategic Applications In Service-Oriented Enterprises And Enterprise Planning. *Review of Applied Science and Technology*, *2*(01), 26-52. https://doi.org/10.63125/73djw422

[198]. Tahmina Akter, R., Md Arifur, R., & Anika Jahan, M. (2024). Customer relationship management and data-driven decision-making in modern enterprises: a systematic literature review. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 57-82. https://doi.org/10.63125/jetvam38
[199]. Tannoury, M., & Attieh, Z. (2017). The influence of emerging markets on the pharmaceutical industry. *Current therapeutic research*, *86*, 19-22.
[200]. Tasdemir, C., & Gazo, R. (2018). A systematic literature review for better understanding of lean driven sustainability. *Sustainability*, *10*(7), 2544.
[201]. Thakur, R., & Rane, D. (2021). Machine learning and deep learning for intelligent and smart applications. In *Future Trends in 5G and 6G* (pp. 95-113). CRC Press.
[202]. Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning. 2019 9th international conference on cloud computing, data science & engineering (Confluence),
[203]. Thokala, P., Devlin, N., Marsh, K., Baltussen, R., Boysen, M., Kalo, Z., Longrenn, T., Mussen, F., Peacock, S., & Watkins, J. (2016). Multiple criteria decision analysis for health care decision making—an introduction: report 1 of the ISPOR MCDA Emerging Good Practices Task Force. *Value in health*, *19*(1), 1-13.
[204]. Timofeyev, Y., & Busalaeva, T. (2021). Current trends in insurance fraud in Russia: Evidence from a survey of industry experts. *Security Journal*, *34*(1), 1-25.
[205]. Timofeyev, Y., & Jakovljevic, M. (2020). Fraudster's and victims' profiles and loss predictors' hierarchy in the mental healthcare industry in the US. *Journal of Medical Economics*, *23*(10), 1111-1122.
[206]. Van Capelleveen, G., Poel, M., Mueller, R. M., Thornton, D., & van Hillegersberg, J. (2016). Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. *International journal of accounting information systems*, *21*, 18-31.
[207]. Van Raaij, W. F. (2016). *Understanding consumer financial behavior: Money management in an age of financial illiteracy*. Springer.
[208]. Villegas-Ortega, J., Bellido-Boza, L., & Mauricio, D. (2021). Fourteen years of manifestations and factors of health insurance fraud, 2006–2020: a scoping review. *Health & justice*, *9*(1), 26.
[209]. Walkington, C., & Bernacki, M. L. (2020). Appraising research on personalized learning: Definitions, theoretical alignment, advancements, and future directions. In (Vol. 52, pp. 235-252): Taylor & Francis.
[210]. Wang, H., Wang, G., Li, G., Peng, J., & Liu, Y. (2016). Deep belief network based deterministic and probabilistic wind speed forecasting approach. *Applied energy*, *182*, 80-93.
[211]. Wang, J., Jiang, C., Zhang, H., Ren, Y., Chen, K.-C., & Hanzo, L. (2020). Thirty years of machine learning: The road to Pareto-optimal wireless networks. *IEEE Communications Surveys & Tutorials*, *22*(3), 1472-1514.
[212]. Wang, J., Zhang, Y., Wei, Y., Hu, Y., Piao, X., & Yin, B. (2021). Metro passenger flow prediction via dynamic hypergraph convolution networks. *IEEE Transactions on Intelligent Transportation Systems*, *22*(12), 7891-7903.
[213]. Warren, D. E., & Schweitzer, M. E. (2018). When lying does not pay: How experts detect insurance fraud. *Journal of Business Ethics*, *150*(3), 711-726.
[214]. Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794-2830.
[215]. Yadav, S. S., & Jadhav, S. M. (2019). Deep convolutional neural network based medical image classification for disease diagnosis. *Journal of Big Data*, *6*(1), 1-18.
[216]. Zamzmi, G., Hsu, L.-Y., Li, W., Sachdev, V., & Antani, S. (2020). Harnessing machine intelligence in automatic echocardiogram analysis: Current status, limitations, and future directions. *IEEE reviews in biomedical engineering*, *14*, 181-203.
[217]. Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications Surveys & Tutorials*, *21*(3), 2224-2287.
[218]. Zhang, Q., Chang, J., Meng, G., Xu, S., Xiang, S., & Pan, C. (2019). Learning graph structure via graph convolutional networks. *Pattern Recognition*, *95*, 308-318.
[219]. Zhang, X., Han, Y., Xu, W., & Wang, Q. (2021). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. *Information Sciences*, *557*, 302-316.
[220]. Zhang, Z., Cui, P., & Zhu, W. (2020). Deep learning on graphs: A survey. *IEEE Transactions on Knowledge and Data Engineering*, *34*(1), 249-270.
[221]. Zhao, Y., Li, Y., Zhang, X., Geng, G., Zhang, W., & Sun, Y. (2019). A survey of networking applications applying the software defined networking concept based on machine learning. *Ieee Access*, *7*, 95397-95417.
[222]. Zheng, S., Ristovski, K., Farahat, A., & Gupta, C. (2017). Long short-term memory network for remaining useful life estimation. 2017 IEEE international conference on prognostics and health management (ICPHM),
[223]. Zhou, Q., Li, J., Tang, Y., & Wang, H. (2020). Discovering the lonely among the students with weighted graph neural networks. 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI),

[224]. Zohuri, B., & Moghaddam, M. (2017). *Business Resilience System (BRS): Driven through Boolean, fuzzy logics and cloud computation* (Vol. 11). Springer.