International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory

Chris Gilbert[1], Mercy Abiola Gilbert[2]
[1]Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman *University*
[2]Department of Guidance and Counseling/College of Education/William V.S. Tubman University/
Corresponding Author Email Address: cabilimi@tubmanu.edu.lr

Abstract*—Intrusion Detection Systems (IDSs) play a pivotal role in maintaining cybersecurity within increasingly complex and dynamic network environments. This study introduces a novel algorithmic framework that integrates graph-theoretic modeling with advanced machine learning techniques to enhance the performance and adaptability of IDSs. Central to the proposed approach is the development of a centroid-based graph measure that enables automatic labeling of training data, accommodating the time-variant nature of network traffic. By representing network communication as weighted graphs, where nodes denote network endpoints and edges capture interaction links; the method facilitates the detection of anomalous behavior through both supervised and unsupervised learning strategies. The framework utilizes clustering, graph coloring, and preferential graph models to identify changing intrusion patterns and enhance detection detail. Experimental evaluations, including tests on the Knowledge Discovery and Data Mining (KDD) Cup 99 dataset, demonstrate that the proposed models significantly enhance detection accuracy, computational efficiency, and scalability. Furthermore, this work addresses key limitations of traditional IDSs by proposing consequence-oriented, graph-enhanced classification algorithms capable of adapting to real-world network dynamics. The findings underscore the promise of integrating graph theory with data-driven learning to support more resilient and intelligent security architectures*.

***Keywords*—** *Intrusion Detection Systems, Graph Theory, Anomaly Detection, Centroid Effect, Network Security, Clustering Algorithms, Machine Learning, Graph-Based Modeling, Dynamic Networks, Cybersecurity Analytics*.

I. INTRODUCTION

Recent advances in machine learning and data mining particularly clustering techniques have positioned these methods as pivotal tools in modern research (Sandosh, Bala & Kodipyaka, 2024). Their proven success across various applications has spurred significant interest in leveraging them to enhance intrusion detection systems (IDSs) (Khanan et al., 2024). Adaptive IDSs, capable of evolving in response to dynamic network environments, have become a focal point of investigation. For instance, Brughmans et al. proposed an adaptive model that integrates evolutionary computing with global behavior modeling to continuously update IDS functionalities. Their approach utilizes neural networks optimized via evolutionary algorithms to refine a full-sensor flooding detection model, thus supporting the evolving needs of distributed systems. Despite these innovations, challenges remain, especially in harnessing the full anomaly detection capabilities of neural networks within real-time systems.

Maintaining the confidentiality, integrity, and availability of data is crucial for any organization. Effective security management relies on continuous monitoring, rapid threat detection, and timely responses (Almehdhar et al., 2024; Opoku-Mensah, Abilimi, & Amoako, 2013). Although automated IDSs are widely deployed, many systems suffer from outdated rule sets, which diminish their threat detection efficacy. As cyber threats grow more complex, traditional defenses are frequently circumvented by advanced malware (Diana, Dini and Paolini, 2025). This reality underscores the urgent need for more adaptive and responsive approaches to intrusion detection.

1.1 Background

Our research is motivated by the need to improve the performance of IDSs by integrating innovative classification techniques with robust graph-based analysis. The proposed approach combines the strengths of our novel algorithm with those of established classification methods to mitigate the evolving tactics of cyber adversaries (Walling & Lodh, 2025). Central to our method is the concept of the "centroid effect," a graph-based measure derived from training data that facilitates automatic labeling. By executing a clustering algorithm on the centroids generated during training, our method accommodates the variability in normal behavior over different time frames, addressing a key limitation of traditional anomaly detection systems (Houichi, Jaidi & Bouhoula, 2024).

The approach is designed to tackle three interrelated challenges in anomaly-based detection:

1. Automatic Labeling: Utilizing the centroid effect to map training data into a weighted graph with defined classes (normal, suspect, and infected), thereby enabling automatic and accurate labeling (Kwame, Martey & Chris, 2017).
2. Effective Classification: Adapting clustering algorithms to handle the inherent time-variant nature of network behavior, which complicates conventional classification methods.
3. Practical Deployment: Enhancing the applicability of IDS models in corporate environments by incorporating graph theory to represent network traffic—where nodes represent network addresses and edges indicate communication links—thus facilitating more intuitive analysis of intrusion patterns.

The above (Figure 1) illustrates a structured approach to anomaly-based intrusion detection that addresses three

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

interconnected challenges. It begins with automatic labeling, where the centroid effect is used to transform training data into a weighted graph, enabling the system to distinguish between normal, suspect, and infected behaviors without manual labeling

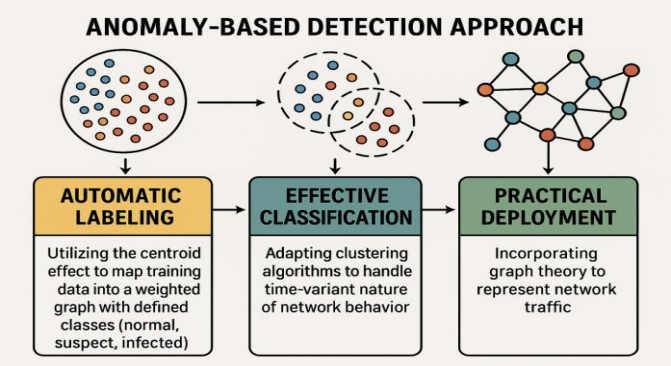

Figure 1: Structured overview of an anomaly-based detection approach

1.2 Research Objectives

The primary objective of this study is to enhance intrusion detection systems through the integration of advanced machine learning and graph-theoretic techniques.
Specific objectives include to:

i. Develop a novel centroid-based graph measure to automatically label training data for IDSs.
ii. Refine clustering algorithms to improve the detection and classification of anomalous network behavior, accounting for non-planar and time-variant data distributions.
iii. Transform network traffic data into a graph structure that facilitates the identification of intrusion patterns based on inter-host communication.
iv. Combine unsupervised community detection with supervised clustering techniques to better capture and classify diverse attack patterns.
v. Validate the proposed methods on realistic datasets, assessing their performance in terms of efficiency, reliability, and scalability within dynamic network environments.

Emerging communication technologies have dramatically increased the volume and complexity of network traffic, thereby expanding the attack surface for cybercriminals. In this context, IDSs must not only process large-scale, heterogeneous data in real time but also deliver high reliability with minimal false alarms. By leveraging the synergy between machine learning and graph theory, our research aims to develop a robust framework that significantly improves the detection, classification, and overall performance of intrusion detection systems.

1.3 Research Questions

i. How can a novel centroid-based graph measure be developed to automatically label training data for IDSs, and what is its impact on improving anomaly detection accuracy?
ii. In what ways can clustering algorithms be refined to enhance the classification of anomalous network behavior, particularly in non-planar and time-variant data distributions?
iii. How can network traffic data be effectively transformed into graph structures that reveal intrusion patterns based on inter-host communication?
iv. How can unsupervised community detection methods be integrated with supervised clustering techniques to capture and classify diverse attack patterns, and how do these methods perform in real-world dynamic network environments?

1.4 Scope and Significance

The design and deployment of algorithmic models for monitoring computing environments often face significant trade-offs in terms of time and space complexity, especially with graph-based approaches. Such complexities can render many existing proposals impractical. One of the primary contributions of this paper is the development of an efficient model tailored specifically for the intrusion detection problem. While the graph-theoretic literature has traditionally placed little emphasis on efficiency, our work addresses this gap by presenting a model that partitions incoming and outgoing event categories with high precision. This partitioning is crucial for programmatically detecting a wide array of event types ideally, as many as possible. Our basic assumption is that certain anomalies or system faults, introduced by intrusions, require the aggregation of multiple events to be reliably identified.

This paper pursues a twofold objective. First, it seeks to simplify and refine algorithms for well-established problems by leveraging the increased computational power available in modern systems. Second, it aims to develop consequence-oriented algorithms capable of detecting novel and diverse types of anomalies in dynamic computing environments. In doing so, the research focuses on two critical aspects of intrusion detection: the granularity of the detection process and the integration of machine learning algorithms to enhance detection capabilities. IDSs operate at various levels from packet-level monitoring by routers and switches to higher-level analyses at the application or operating system level, and our approach is designed to be adaptable across this spectrum. By integrating ensemble machine learning techniques, our model aims to improve the accuracy and responsiveness of IDSs in identifying intrusions.

1.5 Research Methodology

Our research methodology combines advanced machine learning techniques with graph-theoretic approaches to develop and evaluate an efficient intrusion detection system (IDS). The overall approach is structured into several key phases, as described below:

i. Data Collection and Preprocessing: The initial phase involved the systematic collection of detailed data packets from diverse network environments. This process was designed to capture both process-level details and the intricate dependencies among system

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

calls. Recognizing that network traffic originates from heterogeneous sources with varied semantics, we applied robust preprocessing techniques (Kumar, 2025). These techniques included normalization, smoothing, and partitioning to ensure that the data was suitable for subsequent analysis. Special emphasis was placed on addressing the challenges of missing data and class imbalance, which are critical in constructing reliable training datasets for IDS applications.

ii. Feature Extraction and Automatic Labeling: To facilitate accurate classification, we developed a novel graph-based measure, termed the "centroid effect." This measure was employed to automatically label training data by mapping it into a weighted graph structure. In this graph, nodes represent network addresses, and edges capture communication links between hosts. By applying clustering algorithms to the centroids derived from this graph, we were able to classify network traffic into distinct categories (example: normal, suspect, infected) (Putra et al., 2024). This automatic labeling mechanism is particularly effective in handling the time-variant nature of network behavior and in supporting multi-layered service dependencies.

iii. Graph-Theoretic Modeling and Algorithm Design: Building on the preprocessing and feature extraction stages, we formulated several graph-based models to represent network traffic. Our approach leverages the inherent properties of complex networks, such as small-world and scale-free characteristics, to develop preferential graphs that encode known intrusion signatures. We introduced novel graph coloring techniques alongside traditional methods to enhance the representation of intrusion-related patterns. These models were designed to operate across multiple levels of the protocol stack, thereby ensuring broad applicability and scalability (Alizadeh & Khansari, 2023). We also integrated dynamic graph updates and semantic weighting mechanisms to reflect the evolving nature of network traffic and threat landscapes.

iv. Integration with Machine Learning: In parallel with graph-based modeling, we incorporated supervised and unsupervised machine learning techniques to improve the detection and classification of anomalies. The features extracted from the graph models were used to train classifiers, such as linear support vector machines, which then generated predictions based on new network traffic data (Alharbi & Alsubhi, 2021). By comparing these predictions against known traffic patterns and anomalies, we were able to refine our models and improve detection accuracy. This integration enables the system to adapt over time and to detect both known and previously unseen attack patterns.

v. Experimental Evaluation: The final phase of our methodology involved extensive experimental evaluation using benchmark datasets, including the KDD Cup 99 dataset. We assessed the performance of our proposed IDS framework based on several criteria (Waqas, 2024):

a. Detection Accuracy: Evaluating the system's ability to correctly identify intrusions while minimizing false positives.
b. Computational Efficiency: Measuring the reduction in computational overhead achieved through our graph-theoretic algorithms compared to traditional methods.
c. Scalability: Testing the model's performance in handling large-scale network traffic and diverse protocol types, including Ethernet and DNS.
d. Robustness: Validating the system's ability to maintain high performance across different network conditions and attack scenarios.

Through iterative testing and refinement, our experimental results confirmed that the integration of graph theory with machine learning substantially enhances the performance and scalability of intrusion detection systems.

This comprehensive, multi-phase methodology not only addresses the inherent challenges in traditional IDS design but also paves the way for future advancements in real-time, adaptive intrusion detection systems.

This diagram visually breaks down a comprehensive research methodology for building an intrusion detection system (IDS), using a combination of graph theory and machine learning. It's organized into four main phases, each with its own set of tasks and techniques.

II. Fundamentals of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are essential technologies for safeguarding computing resources. They play a critical role in the security infrastructure of organizations by monitoring, capturing, and analyzing network traffic and system activity to detect potentially malicious behavior (Opoku-Mensah, Abilimi & Boateng, 2013). IDSs operate by identifying abnormal patterns in traffic content, communication activities, and traffic volume, which may indicate cyberattacks or intrusion events (Arisdakessian et al., 2022; Opoku-Mensah, Gilbert & Gilbert, 2024a; Abilimi & Amoako, 2013). Typically, IDSs utilize profiles of known threats, predefined policies, sensor data, or anomaly detection methods to flag suspicious activities.

There are two primary types of IDSs:

- Network-based Intrusion Detection Systems (NIDS): These systems focus on monitoring traffic across network links to identify potential intrusions.
- Host-based Intrusion Detection Systems (HIDS): These systems are installed on individual hosts to monitor and analyze internal activities (Lagraa et al., 2024).

This diagram (Figure 3) breaks down how Intrusion Detection Systems (IDS) work. At the top level, IDS are tools used to detect potential threats or malicious activity in a computer system. They come in two main forms; Network-based (NIDS), which keeps an eye on data moving through the network, and Host-based (HIDS), which monitors what's happening inside individual computers or devices. NIDS focuses on tracking traffic and spotting any odd behavior in

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

the network, while HIDS looks at what users and programs are doing on a specific machine and makes sure security policies are being followed. Both types feed into a central threat detection system that analyzes this information to spot security issues.

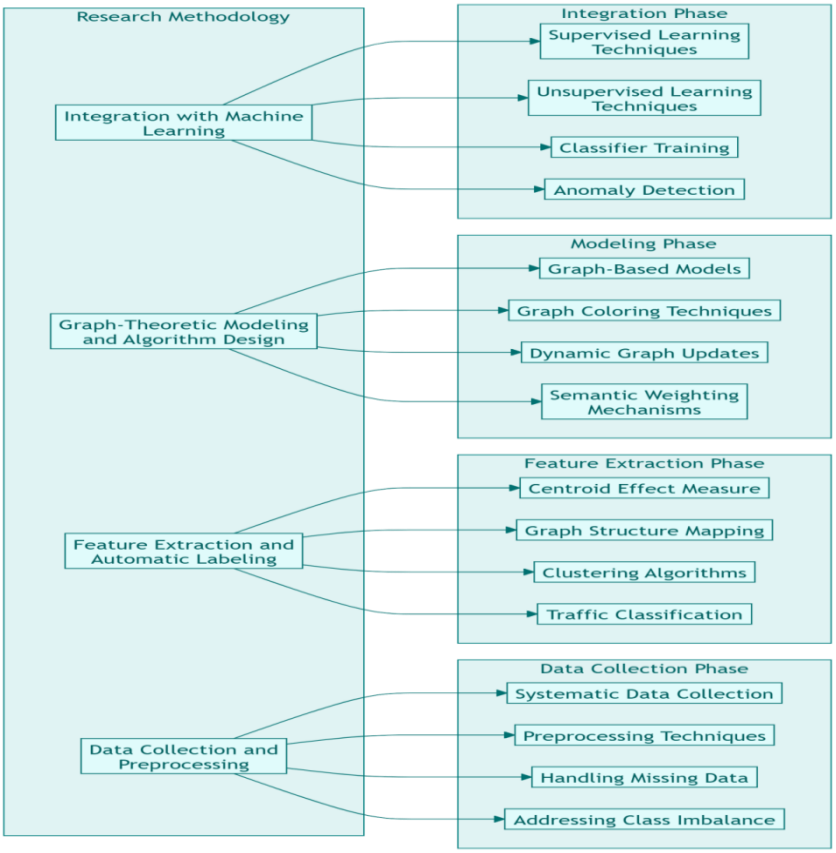

Figure 2: A comprehensive Research methodology

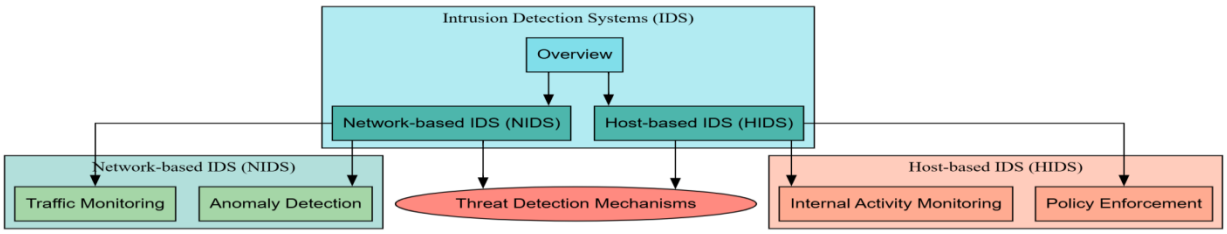

Figure 3: Fundamentals components of Intrusion Detection Systems (IDS)

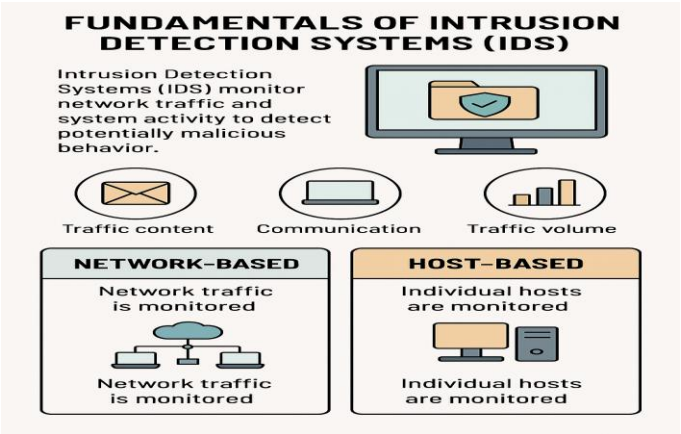

Figure 4: Basic components of Intrusion Detection Systems (IDS)

This diagram (Figure 4) is showing the basic introduction to what Intrusion Detection Systems (IDS) are all about. At the core, IDS tools are designed to keep an eye on network traffic and system activity to catch anything that looks suspicious or potentially harmful kind of like a security guard for your digital environment. It highlights three main things these systems monitor: the content of traffic (like what's being sent), the communication between devices, and the volume of traffic (how much is being sent). All of this helps spot unusual or dangerous behavior.

2.1. Overview of IDS

HIDS and NIDS differ primarily in the type and source of data they monitor. Signature-based IDSs rely on predefined patterns or signatures of known attacks, while anomaly-based

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

systems detect deviations from established normal behavior (Trisolino, 2023; Yeboah, Opoku-Mensah & Abilimi, 2013a). The effectiveness of an anomaly-based approach hinges on determining the appropriate level of detection, which remains a challenging aspect of IDS design (Heidari & Jabraeil Jamali, 2023; Yeboah, Odabi & Abilimi Odabi, 2016). IDSs are instrumental in alerting administrators to potential security breaches by identifying anomalies that either match predefined profiles, deviate entirely from known patterns, or indicate that the existing profiles have become outdated.

2.2. Types of IDS

IDSs can be broadly categorized into two types: misuse detection and anomaly detection.

- Misuse Detection Systems: These systems identify intrusions by searching for traces that match known attack patterns, often defined as sequences of system calls or heuristic rules (Otoum & Nayak, 2021).
- Anomaly Detection Systems: These systems establish a baseline of normal behavior during a training period and subsequently detect deviations from this norm to flag potential intrusions (Hajj et al., 2021; Gilbert & Gilbert, 2025d).

Misuse detection typically involves the use of signature-based or rule-based methods, whereas anomaly detection relies on learning algorithms that continuously adapt to the evolving characteristics of network traffic (Martins et al., 2022). Both approaches play critical roles in modern IDS implementations and are often combined to enhance overall system effectiveness.

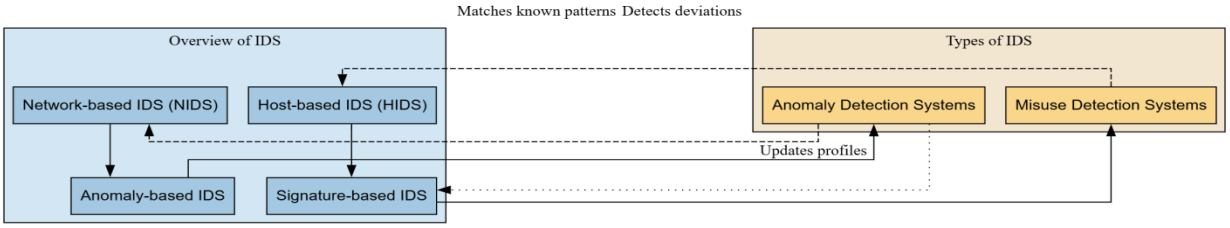

Figure 5: The structured view of Intrusion Detection Systems (IDS)

This diagram explains how intrusion detection systems (IDS) function by linking where they're deployed and how they detect threats. IDS can be set up either on individual devices (Host-based or HIDS) or across a network (Network-based or NIDS). Regardless of where they're used, they typically follow one of two detection methods: signature-based, which identifies known threats using stored attack patterns, and anomaly-based, which flags unusual activity that doesn't match normal behavior.

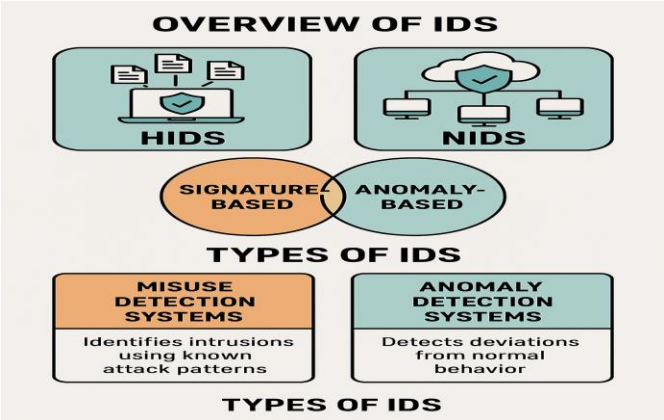

Figure 6: The breakdown of Intrusion Detection Systems (IDS).

Figure 6, offers a simplified yet informative breakdown of Intrusion Detection Systems (IDS). It begins by distinguishing between two primary deployment methods: Host-based IDS (HIDS), which monitors activity on individual devices, and Network-based IDS (NIDS), which oversees data traffic across an entire network. At the core of how IDS operates are two detection strategies: Signature-based detection, which identifies threats by matching known attack patterns, and Anomaly-based detection, which spots suspicious activity by flagging deviations from expected behavior. These two strategies form the foundation for the two main types of IDS.

III. Graph Theory Basics

As illustrated in Figure below, a graph consists of a set of nodes V(G) and a set of edges E(G) forming relationships between the nodes. Edge e = {v1, v2} is used to connect two distinct nodes v1, v2. More specifically, if v1, v2 ∈ V(G) and {v1, v2} ∈ E(G), we say that nodes v1 and v2 are adjacent in graph G. The set of neighbors N(v) of a node v consists of all nodes u such that {v, u} is an edge. The degree of node v in graph G, denoted by deg(v) for undirected graphs or deg(x) for directed graphs, is the number of edges at v. A graph G is connected if a path exists between every pair of distinct nodes.

Graphs capture intrinsic properties of many complex systems and play an important role in formulating practical problems in areas as diverse as computational biology, program analysis, and other domains as shown in Das & Soylu (2023). Typically, a graph consists of nodes representing important entities and edges being the relations that determine how the entities interact. The topology and structures of graphs offer substantial insight into roles of the individual nodes (entities) as well as how to exploit these patterns to investigate relationships among system components (Torres et al., 2021). We consider graphs in both a practical and

theoretical sense and demonstrate their versatile use for constructing robust and efficient intrusion detection algorithms.

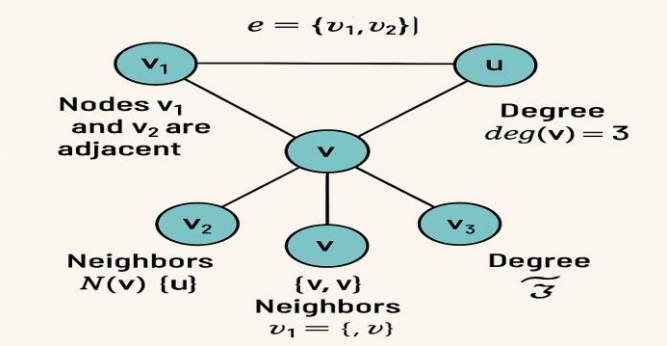

Figure 7: Basic graph theory concepts

This Figure 7 is a simple graph showing how nodes and edges work — kind of the ABCs of graph theory. We see a bunch of circles labeled with letters like v_1, v_2, v_3, v, and u. These circles represent nodes, and the lines between them are the edges — the connections. At the top, there's a label e = {v_1, v_2} — that just means there's an edge linking v_1 and v_2, so those two nodes are adjacent (connected directly). That's the first concept — adjacency. Now, look at the node in the center labeled v. It's got lines connecting it to u, v_2, and v_3. So if we count those, it has 3 edges, which gives it a degree of 3. That's what the deg(v) = 3 label is telling us. Basically, the degree is just how many connections a node has.

3.1. Introduction to Graphs

Graph theory has matured significantly and now plays a critical role in a wide array of scientific and engineering disciplines (Dörfler, Simpson-Porco & Bullo, 2018). One of its primary advantages is the ability to transform complex algebraic problems into more intuitive graphical representations. This simplification makes it easier to analyze and understand the properties and behaviors of rarely occurring or subtle phenomena. In this work, we leverage graph theory to enhance intrusion detection in computer security (Kolbeck et al., 2022; Yeboah, Opoku-Mensah & Abilimi, 2013b). As intrusion detection becomes increasingly vital for protecting network infrastructures, the capacity to identify and mitigate unauthorized activities in real time is paramount.

Although various methodologies have been employed to tackle intrusion detection, relatively few have adopted graph-theoretic models as their foundation (Gross, Yellen & Anderson, 2018). Our approach explores the application of graph theory to design more efficient algorithms for intrusion detection systems. Specifically, we extend previous research by introducing novel graph coloring techniques alongside established methods, to develop preferential graphs that encode known intrusion signatures. We also provide performance evaluations to demonstrate the effectiveness of our approach in detecting and classifying intrusion activities.

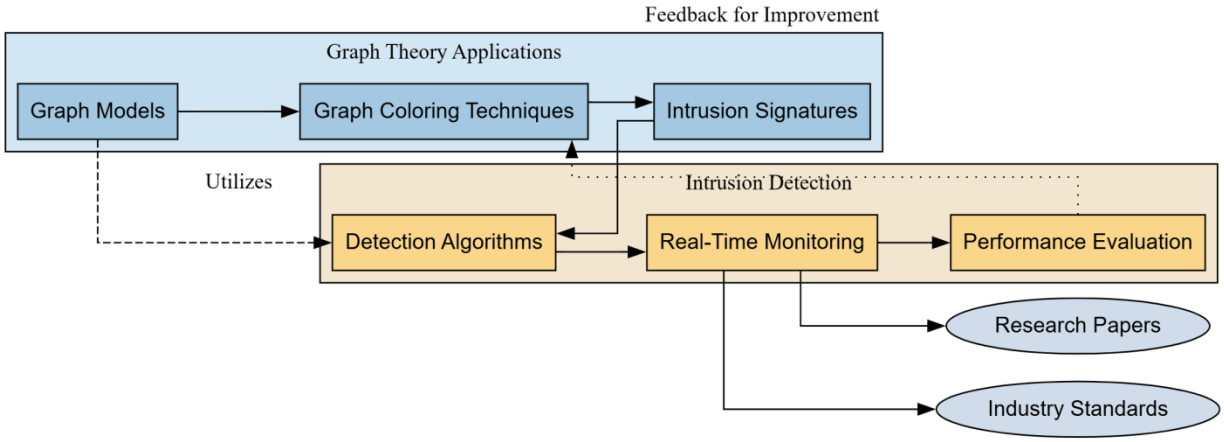

Figure 8: How graph theory is applied to improve intrusion detection systems.

This diagram shows how graph theory is applied to improve intrusion detection systems. At the top, we start with Graph Models, which lead into Graph Coloring Techniques and then help identify Intrusion Signatures. These signatures are then used by the intrusion detection process. In the lower section, the intrusion detection workflow kicks in starting with Detection Algorithms, moving into Real-Time Monitoring, and ending with Performance Evaluation. The results from performance evaluation feed into Research Papers and Industry Standards, which in turn help improve the graph-based methods above. So it's basically a loop: graph theory helps build better intrusion detection systems, and insights from those systems feed back into improving the theory and tools.

3.2. Key Concepts and Terminology

In our study, a directed graph is applied to the computation of NSDBC because a message contains a single sequence of time-related message states. In addition, the transfer path over a communication network may be affected by one-way delay (Kolbeck et al., 2022). Such a problem is known as a routing problem in networks. The combination of sequential states with routing is also implemented for intrusion detection

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

systems (IDS), in which the network traffic contains both gold and unknown activities (Chartrand et al., 2024; Abilimi et al., 2015).

A graph G = (V, E) is composed of a set of nodes V and a set of connections E between pairs of nodes, which can be further characterized by mainly two types: the vertex and the edge. A specific vertex of a graph G is denoted by a unique node v, whereas a specific edge is denoted by the connection between two arrays nodes (Dörfler, Simpson-Porco & Bullo, 2018).

TABLE 1: The key concepts and terminology

Concept / Term	Description
Directed Graph	A graph whose edges have a direction; used to model the time-sequenced states of messages in NSDBC.
NSDBC	The computational framework applying directed graphs to single sequences of time-related message states.
One-way Delay	A latency affecting message transfer paths in a network, giving rise to routing challenges.
Routing Problem	The network issue of determining or optimizing paths when delays or one-way constraints exist.
Sequential Message States	An ordered series of time-stamped states that a message passes through.
Intrusion Detection System (IDS)	A system that combines sequential state modeling with routing analysis to detect known and unknown traffic.
Graph G = (V, E)	The formal definition of a graph: V is the set of vertices (nodes) and E is the set of edges (connections).
Vertex (v)	An individual node in the graph, denoted by a unique label.
Edge (e)	A connection between two vertices, denoted $\{v_1, v_2\}$, which may be directed or undirected.
Path-based Anomaly Detection	An IDS method that examines paths in the graph to spot deviations from expected behavior.
Distributed IDS	A scalable, network-wide intrusion detection approach built on graph-theoretic principles.

In this section of the paper, we briefly introduce the concepts and terminology used in graph theory. Thereafter, we move onto a path-based anomaly detection method, in which we propose a kind of distributed intrusion detection approach based on graph theory.

IV. Graph-Based Models for Intrusion Detection

Complex networks provide robust tools for addressing real-world networking challenges. Their large-scale, often random topologies, characterized by small-world and scale-free properties; enable the development of sophisticated algorithms for tasks such as routing, congestion control, and resource sharing in IP networks (Liao et al., 2024). In the context of intrusion detection, these network features offer two major advantages. First, the sheer volume of traffic and the high connectivity among nodes yield a rich dataset for analysis. Second, the inherent structure of these networks facilitates the identification of logical relationships among various types of connections such as attack paths, backdoor channels, or rootkit communications which cybercriminals often exploit or try to conceal (Ortega et al., 2018).

Graph-based models are widely used in IDS research. Most approaches represent network traffic as a graph, with subgraphs corresponding to either normal or attack traffic (Silva et al., 2018). In these representations, vertices typically denote hosts or IP addresses, while edges represent the communication links between them. One common method involves constructing separate communication graphs for regular user interactions and for suspected attack scenarios, and then comparing these graphs to differentiate between benign and malicious activities (Alrumaih & Alenazi, 2023).

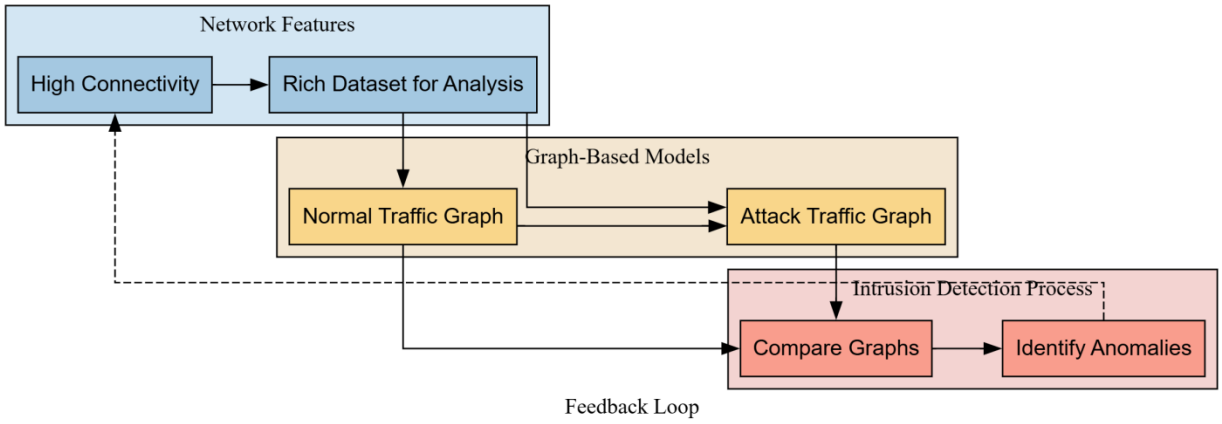

Figure 9: Network characteristics to detecting intrusions

This diagram (Figure 9), shows how we move from raw network characteristics all the way through to detecting intrusions, and then uses what we learn to keep improving. It starts with the fact that modern networks are highly connected, which produces a rich dataset ripe for analysis. From that data we build two complementary graph-based models: one representing normal traffic patterns and another capturing known attack traffic. These graphs feed into the intrusion detection process, where they're compared side by side to spot deviations and those deviations are flagged as anomalies. Finally, there's a feedback loop: the anomalies we identify don't just stop there, but are fed back into both our graph models and our understanding of network features, so the system continually refines its ability to detect new or subtle threats.

4.1. Graph Representation of Networks

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

In our models, graphs serve as a versatile data representation framework (An, Gao & Tang, 2024). Weighted edges can illustrate the strength or capacity of connections, while additional properties assigned to nodes and edges capture crucial network information, such as endpoint status and traffic statistics (Nguyen et al., 2024; Abilimi & Adu-Manu, 2013). Graphs are particularly effective in modeling complex interactions among network entities, whether for routing, topological analysis, or real-time intrusion detection (Gogoshin & Rodin, 2023). By transforming network data into graph structures, we can succinctly represent relationships between devices, nodes symbolize network endpoints, and edges denote the communication links connecting them, thus enabling more efficient analysis of network behavior.

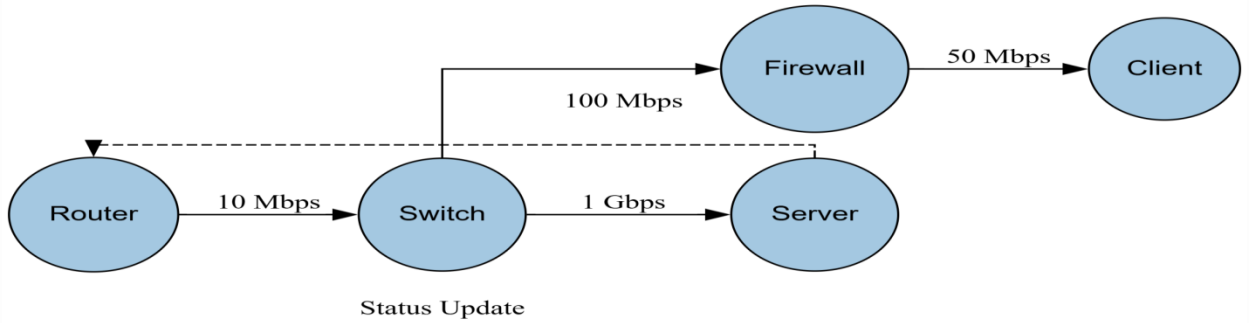

Figure 10: A simplified graph network chain

Figure 10 shows a simple network chain where the router hands off traffic at 10 Mbps to a central switch, and that switch in turn delivers data at 1 Gbps to the server. Off to the side, the switch also forwards 100 Mbps through a firewall, which then passes 50 Mbps on to the client. At the same time, the server pushes "status update" messages (dashed line) back up to the router, closing a feedback loop that lets the router adjust its behavior based on the server's state.

4.2. Graph Algorithms for Anomaly Detection

A range of algorithmic solutions for misuse and anomaly detection leverages the computational power of specialized search engines and data mining tools, especially those dedicated to string matching and pattern recognition (Ju et al., 2024). Recent advances have shown that by representing data in a graph-based format, it is possible to improve the efficiency and intelligence of anomaly detectors, particularly when dealing with large, multi-attribute databases (Luo et al., 2023). In this approach, the data is transformed into a qualitative or numerical format at the time of analysis, mitigating computational challenges and enhancing prediction accuracy.

Over the past few decades, data mining and machine learning have significantly advanced, offering powerful tools for a variety of problems, including network security. Nevertheless, the challenges associated with misuse and anomaly detection persist. This paper explores how the integration of traditional data mining techniques with graph-theoretic methods can provide improved solutions for securing computer networks (Xu et al., 2023). By reviewing state-of-the-art approaches that combine insights from computer security and graph theory, we outline how these interdisciplinary methods can enhance the classical strategies used in intrusion detection systems.

This diagram (Figure 11), explains how different technologies come together to enhance misuse and anomaly detection using graph-based algorithms. At the core is graph-based data, which serves as a unifying structure for various analysis techniques. On one side, search engines and data mining tools feed into this model by providing access to vast amounts of information and helping uncover hidden patterns in complex datasets. On the other side, string matching and pattern recognition techniques work alongside the graph structure to detect inconsistencies or unusual behavior in the data. All these components converge toward the shared goal of improving the detection of misuse and anomalies, making the entire process smarter, faster, and more adaptable to complex network environments.

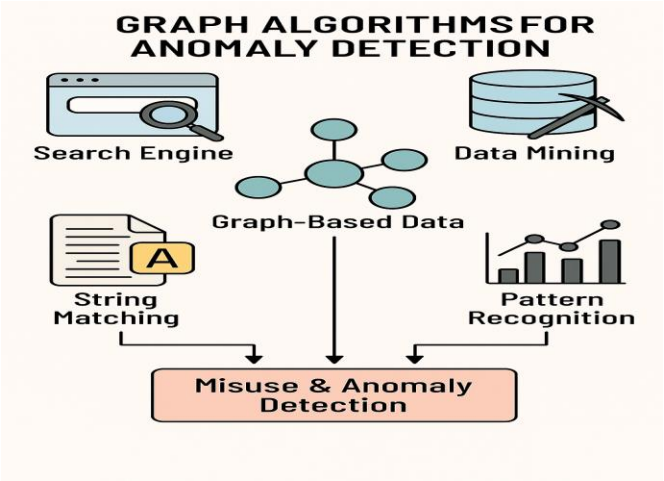

Figure 11: Anomaly detection using graph-based algorithms

Figure 12, breaks down the concept of Graph Algorithms for Anomaly Detection into four main areas: overview, techniques, challenges, and integration. The overview section introduces core ideas like data representation and how graph-based approaches can improve efficiency. Techniques used in anomaly detection include data mining, machine learning, and graph theory itself, all of which contribute to identifying misuse and irregularities in data. The challenges focus on the ongoing difficulty of detecting both misuse and anomalies,

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

especially when comparing newer methods to more traditional ones. Finally, integration emphasizes how graph-theoretic methods can be combined with existing intrusion detection systems to enhance overall network security. It paints a clear picture of how graph algorithms are being used to both strengthen and modernize cybersecurity strategies.

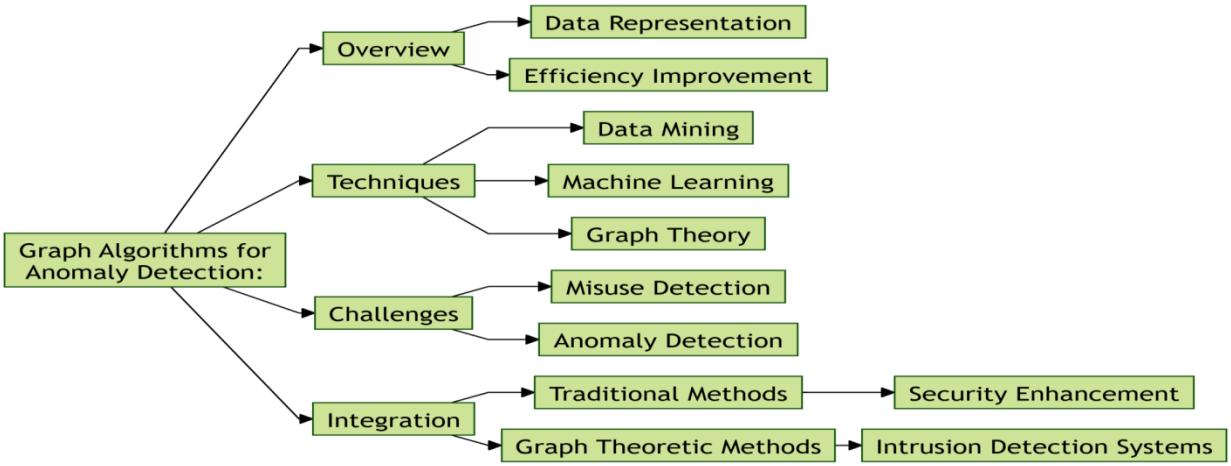

Figure 12: "Graph Algorithms for Anomaly Detection"

V. Applications of Graph Theory in IDS

Graph theory offers valuable insights for enhancing intrusion detection systems (IDS) by facilitating efficient and non-invasive monitoring of network activities (Johnson et al., 2024). In this context, the concept of "authorizations" refers to groups of network connections that can relay critical process information in real time as explained in (Abilimi et al., 2013; Chitkeshwar, 2024). Such information ranging from mandatory non-operational processes to updated policies regarding legal, ethical, or privacy concerns ensures that security teams are alerted promptly without needing to inspect the actual traffic content (Rizvi et al., 2022; Abilimi & Yeboah, 2013). In addition, higher-level authorizations can aggregate demands based on observed network behavior, such as capturing frozen traffic segments and applying relevant policy updates.

To share the detection burden effectively, the performance of IDS must improve while maintaining minimal intrusion into traffic content (Khayat et al., 2025). This involves learning the interdependencies among various network features, applying domain knowledge to achieve an optimal level of hypothesis generalization, and balancing the detection objectives across multiple shared rules (Nafees et al., 2023; Yeboah & Abilimi, 2013). Moreover, real-time evaluation of algorithm capabilities is crucial in building adaptive, unsupervised detection systems that can cater to individual network environments.

With the rapid expansion of computer networks, distributed responsibility for detecting misuse has become both a practical approach and an operational necessity (Li & Yan, 2022; Gilbert, Auodo & Gilbert, 2024). Every network user is expected to adhere to established authorizations, which not only define acceptable behavior but also help in the prompt isolation of suspicious activities (Levy Rocha et al., 2023; Gilbert, 2021). However, individual authorizations typically do not grant access to all network traffic. Instead, specialized security personnel, who have broader visibility, are tasked with gathering intelligence and containing potential misuse (YASMINA et al., 2024). Their role is critical, yet it must be balanced with strict adherence to legal and ethical standards, ensuring that any monitoring of traffic does not infringe upon user privacy or violate human rights.

TABLE 2: Applications of Graph Theory in IDS

Application	Description
Authorization Groups	Graph-based grouping of network connections to relay critical process information in real time—alerting security teams without inspecting packet contents.
Hierarchical Authorizations	Higher-level graph structures that aggregate observed behaviors (e.g., frozen traffic segments) and trigger policy updates based on those aggregated demands.
Shared Detection Framework	Use of graph models to learn interdependencies among network features, apply domain knowledge for hypothesis generalization, and balance detection objectives across multiple shared rules.
Adaptive Real-Time Evaluation	Graph-driven, unsupervised anomaly detection that continuously evaluates algorithm performance and adapts to the unique characteristics of each network environment.
Distributed Detection Responsibility	Decentralized graph-informed authorizations enforce acceptable user behavior and enable rapid isolation of anomalies, while specialized security nodes maintain broader visibility under ethical and legal constraints.

5.1. Sharing the Responsibility of Detection

As network sizes increase, the collective responsibility for identifying and mitigating misuse becomes essential (Dlamini et al., 2024). Each user is governed by specific authorizations that restrict access to traffic data, meaning that no single entity can comprehensively monitor the entire network without risking privacy violations (Sowrirajan & Manimekalai, 2024). Specialized security teams, entrusted with a more comprehensive view of network activity, share this responsibility. They implement advanced graph-theoretic models to consolidate and analyze traffic patterns across broader segments of the network. By doing so, these teams can detect anomalies and potential threats more efficiently

while respecting legal and ethical boundaries. This distributed approach not only enhances overall detection performance but also ensures that the burden of network surveillance does not fall on a single point of failure, thereby maintaining the balance between security and privacy (McMahon, Buyx & Prainsack, 2020).

5.2. Network Traffic Analysis

Intrusion detection systems (IDS) play a critical role in reducing security attacks by continuously analyzing real-time network traffic to identify abnormal activities that may harm systems (Miller & Bossomaier, 2024). One of the primary challenges in network traffic analysis is managing the computational overhead. Graph-theoretic algorithms such as those for solving the All-Pairs Shortest Path (APSP) problem offer an effective means to minimize this overhead by reducing complexity and ensuring computations are completed within acceptable time limits (McMahon, Buyx & Prainsack, 2020). This is particularly crucial for detecting large-scale DoS and DDoS attacks in real time.

In this study, we implemented three IDS security models. The first model builds upon an existing framework designed to analyze compressed log files for intrusion detection. The other two models incorporate graph theory algorithms to enable real-time attack detection (Miller & Bossomaier, 2024). Specifically, one model, referred to as the GDM model, uses an adjacency matrix to represent network connections and is secured by a TSAS-based traversal mechanism. This model employs an unrestricted investigation method that minimizes security gaps and reduces false alarms (Dlamini et al., 2024; Gilbert, 2018). By leveraging graph-theoretic approaches, particularly those that focus on identifying the shortest path, the proposed IDS models are capable of detecting DoS/DDoS attacks and tracking information changes in an online environment. Our analysis indicates that these models enhance security architecture by reducing computational load and lowering the incidence of false alarms.

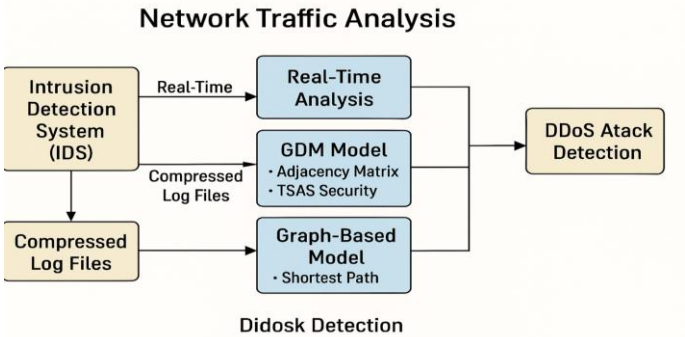

Figure 13: The different models within an Intrusion Detection System (IDS)

This diagram (Figure 13) explains how different models within an Intrusion Detection System (IDS) are used to analyze network traffic and detect DDoS attacks. Everything starts with the IDS, which handles both real-time traffic and compressed log files. Real-time traffic is fed directly into a real-time analysis model, while the compressed logs are processed using two graph-enhanced models. The first is the GDM model, which uses an adjacency matrix to map out connections and incorporates TSAS-based security for thorough traversal and coverage. The second is a more general graph-based model that applies shortest path algorithms to detect patterns and irregularities efficiently. All three models—real-time analysis, the GDM model, and the graph-based model converge toward the shared goal of detecting DDoS attacks accurately and with reduced computational strain.

5.3. Behavioral Analysis

Behavioral analysis in network traffic is a key component of modern intrusion detection systems (Alshehri et al., 2023). In this context, graph-based heuristics are employed to capture and describe the unique characteristics of network traffic over time. Traffic patterns are typically classified into categories such as random, periodic, and aperiodic patterns (Chen, Chen & Zhao, 2024). These patterns provide insights into the normal operation of a network and help in identifying deviations that may signal intrusions.

Particularly in specialized environments such as Supervisory Control and Data Acquisition(SCADA) systems, detecting and countering attacks aimed at compromising secure processors, data integrity, and tampering with critical system relations is of paramount importance (Heidari & Jabraeil Jamali, 2023). The emergence of SCADA Security Event Analysis and Response (SSEAR) frameworks reflects the industry's move toward integrating behavior analysis with real-time intrusion detection (Lam, 2021).

Behavioral analysis builds on earlier work, such as the foundational studies by (Gangadhar et al., 2025; Gilbert, Oluwatosin & Gilbert, 2024), on Behavior Consistency Checking for Anomaly Detection (BCAD). This approach to anomaly detection can be viewed from two perspectives: a statistical approach and a profile-based approach. The statistical method assumes that sufficient data is available to characterize the overall behavior of network users, while the profile-based approach focuses on modeling the behavior of individual entities over time (Shafi, Lashkari & Roudsari, (2025). Techniques employed in the profile-based approach include data cube algorithms, estimated behavioral profiles, and symbolic aggregation encoding (Amirthayogam et al., 2024). Together, these methods contribute to a more nuanced understanding of network behavior, ultimately enhancing the detection capabilities of IDSs.

This diagram illustrates how behavioral analysis is used to monitor and secure network traffic, particularly in systems like SCADA. It all begins with identifying traffic patterns, which are fed into an anomaly detection process. From there, the patterns are classified into three categories; random, periodic, and aperiodic. These classifications support the broader goal of enhancing SCADA security by helping detect irregular behaviors.

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

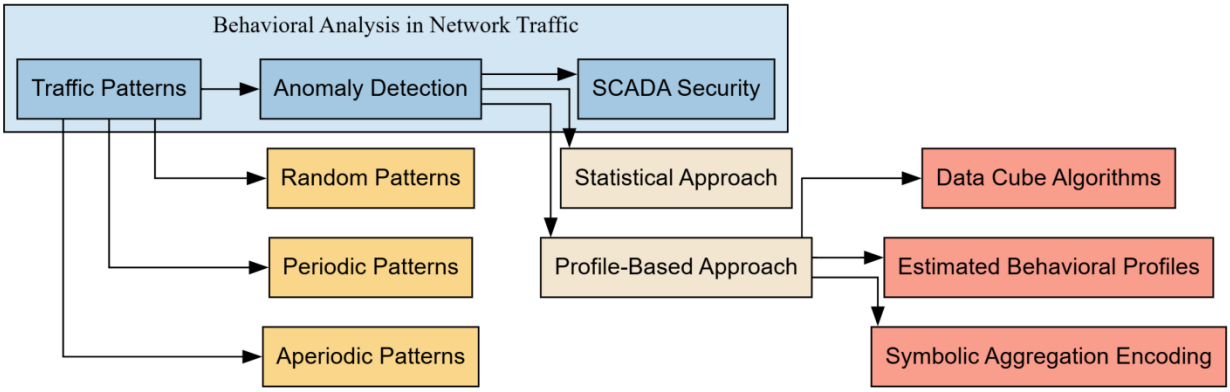

Figure 14: The behavioral analysis is used to monitor and secure network traffic

6. Challenges and Limitations

One of the most significant challenges in misuse detection is the normalization of traffic data (Guerra, Catania & Veas, 2022). Effective normalization is essential for handling data from sources with different semantics, yet many existing approaches, often based on simple mean/median scaling or standard deviation adjustments, fall short (Chan, Lim & Parthiban, 2023; Gilbert, 2012). Recent studies suggest a more sophisticated method: analyzing which fields deviate from a normal distribution and normalizing them individually (Gilbert, 2022). While this approach can be more efficient, it requires substantial prior knowledge regarding the expected distribution of various data fields, thereby exposing limitations in traditional statistical methods. Moreover, pre-processing techniques such as smoothing, partitioning, and context-sensitive rule adjustments, although promising, tend to be time-intensive, which poses additional difficulties for real-time detection. Inadequate or incorrect pre-processing not only degrades system performance but can also lead to overfitting or misclassification in detection models (Le Jeune, Goedeme & Mentens, 2021; Gilbert & Gilbert, 2025d). Although improvements in standard software for normalization are underway, the need to adjust parameters based on varying attributes remains a significant challenge.

Another critical challenge for anomaly detection is the lack of a universally accepted standard, compounded by the scarcity of labeled real-world traffic datasets. Privacy and security concerns further restrict the availability of comprehensive traffic data (Azab et al., 2024; Gilbert & Gilbert, 2024b). Consequently, unsupervised and semi-supervised methods have emerged as practical alternatives, especially for detecting unknown attacks a task that is arguably even more crucial than identifying known intrusions (Gao et al., 2019; Gilbert & Gilbert, 2024t). Research on firewall logs indicates that a notable portion of traffic (up to 11% in some studies) remains "unspecified," suggesting either model errors or genuinely anomalous behavior. The inability to promptly detect new attack vectors is a primary reason why many organizations only discover intrusions after external intervention.

6.1. Scalability Issues

Scalability remains a central concern, particularly for pattern matching in large datasets (Dong, Wang & He, 2019; Gilbert & Gilbert, 2024r). Traditional approaches, such as those employing suffix automata or Nondeterministic Finite Automata (NFA), including the factorized NFA variant, face significant challenges. These methods often rely on bitmapped NFA representations, which can be memory-intensive. To address this, our work introduces a novel graph-theoretic approach that minimizes both the number and length of edges in the automaton by pre-processing the input text to remove superfluous characters (Fernandes et al., 2019; Gilbert & Gilbert, 2024q). The resulting factorized transition-labeled NFA requires less memory and fewer transitions compared to conventional bitmap-based NFAs. Furthermore, by incorporating weighted edge criteria, this approach reduces the state space without compromising match precision (Singh, 2020; Gilbert & Gilbert, 2024p). As databases and queries continue to grow in size, ensuring that pattern-matching algorithms remain efficient is critical for next-generation intrusion detection systems.

TABLE 3: The challenges in misuse detection

Challenge / Limitation	Description
Traffic-data normalization	Simple scaling methods (mean/median, standard deviation) often fail across heterogeneous data sources; per-field normalization improves accuracy but demands extensive prior knowledge.
Pre-processing overhead	Techniques like smoothing, partitioning, and context-sensitive rule adjustments can be time-intensive, hindering the real-time performance of IDS.
Overfitting and misclassification	Inadequate or incorrect pre-processing degrades model performance, leading to overfitting or false classifications in detection algorithms.
Lack of labeled datasets & standards	There is no universally accepted benchmark for anomaly detection and labeled real-world traffic datasets are scarce, making model validation and comparison difficult.
Privacy and security constraints	Legal and ethical concerns restrict access to comprehensive traffic data, limiting the availability of high-quality training and evaluation datasets.
Unspecified traffic in logs	Studies show up to 11% of firewall log entries remain “unspecified,” reflecting either model errors or genuine anomalies and complicating detection efforts.
Delayed detection of novel attacks	Without timely recognition of new attack vectors, many intrusions are only discovered after external intervention, reducing the window for effective response.

6.2. Complexity of Attack Patterns

The vast array of attack types and their inherent complexities presents another formidable challenge for

intrusion detection (Gilbert & Gilbert, 2024o). Effective classification depends on selecting attributes that are both highly discriminative and amenable to unsupervised learning (Mahdi, Hosny & Elhenawy, 2021; Gilbert & Gilbert, 2024n). These attributes can often be categorized into discrete (enumerative) and continuous (bounded) ranges. In our work, we employ feature-value splitting to divide attributes into discrete segments where such division enhances classification accuracy (Saifudin & Widiyaningtyas, 2024; Gilbert & Gilbert, 2024m). Although our focus is on intrusion detection, these techniques have broader applicability in other security domains.

Furthermore, accurately characterizing the complexity of evasion attack patterns is an open research problem (Roy & Dutta, 2022; Gilbert & Gilbert, 2024w). Our online intrusion detection system demonstrates the difficulty of optimizing the trade-off between the number of neurons in a learning network and the overall performance of the detection scheme (Nasraoui & N'Cir, 2019; Gilbert & Gilbert, 2024v). A critical challenge is the determination of an appropriate damage function for the system, for which we have applied Dijkstra's algorithm and inequality-based methods (Nasraoui & N'Cir, 2019; Gilbert & Gilbert, 2024u; Qin et al., 2023). These techniques, along with our two-tier feature-type selection process based on statistical analysis, help our algorithm capture the internal relationships among attribute values rather than relying solely on raw data (Gilbert & Gilbert, 2024l). Experimental results on the standard Knowledge Discovery and Data Mining (KDD) Cup 99 dataset indicate that our approach substantially improves both detection accuracy and efficiency, thereby addressing some of the complex challenges inherent in intrusion detection (Alguliyev, Aliguliyev & Sukhostat, 2020; Gilbert & Gilbert, 2024k).

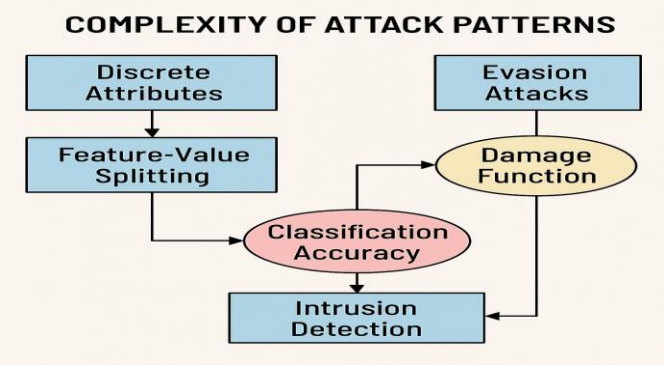

Figure 15: The complexity of attack patterns in intrusion detection

This diagram explores the complexity of attack patterns in intrusion detection by mapping out the relationship between key components. It starts with the classification of input data into discrete and continuous attributes. Discrete attributes are categorized into specific values, while continuous attributes span bounded numeric ranges. These attributes feed into the process of analyzing evasion attacks, which are designed to bypass detection systems by mimicking normal behavior. Improving classification accuracy relies on carefully selecting and splitting these features in a way that reveals meaningful distinctions. The system also evaluates how the configuration of learning models—like the number of neurons—and the choice of a damage function impact detection performance. Tools such as Dijkstra's algorithm and statistical methods help assess internal data relationships rather than just surface-level patterns. Altogether, the diagram shows how handling diverse data types and intelligently designing the detection system are essential to managing the evolving and often deceptive nature of cyberattacks.

VI. Future Directions and Research Opportunities

This paper provides a high-level overview of our detection approach and outlines several promising avenues for future research. Our methodology begins with the collection of detailed data packets that capture both process-level information and the intricate dependencies among system calls (Gilbert & Gilbert, 2024j). We then apply statistical methods to learn and identify patterns among the numerous independent service requests made by clients (Christopher, 2013). Notably, our approach is capable of handling complex services where one transaction is contingent upon another, thereby accommodating multi-layered service dependencies (Gilbert & Gilbert, 2024h; Nair & Bhagat, 2021). Detected features are subsequently used to train supervised classifiers such as linear support vector machines—to make informed predictions (Gilbert & Gilbert, 2024i). When new requests are processed, a feature vector is generated and fed into the classifier, triggering alerts for potential attacks and prompting further service reviews if necessary (Gilbert & Gilbert, 2024g; Ezugwu et al., 2022).

In addition to our statistical approach, we introduce an efficient graph-theoretic framework to address intrusion detection challenges (Gilbert & Gilbert, 2024f). By leveraging key graph theory concepts, we analyze the global interrelationships among low-level system call traces to capture higher-level behavioral patterns by Singh (2020) and Gilbert & Gilbert (2024x). The primary contribution of our algorithm is its ability to cluster graph patterns, which naturally represent and elucidate process behaviors at varying levels of abstraction. Each node and edge in these graphs corresponds to critical individual and pairwise traces, highlighting intrinsic features and statistical patterns that are easily inferred and utilized.

7.1. Enhancing Graph-Based IDS Algorithms

To overcome the limitations of existing graph-based intrusion detection systems, we propose several enhancements (Gilbert & Gilbert, 2024y). Our strategy includes the development of semantic, dynamic, and priority graphs that enrich the traditional graph models (Saifudin & Widiyaningtyas, 2024; Gilbert & Gilbert, 2024e). These enhanced features address three primary shortcomings in current methods:

1. Semantic Limitations: Traditional graph models often rely heavily on syntactic representations, which can obscure meaningful semantic information.
2. Static Analysis: Many existing systems perform only offline, static analysis, limiting their effectiveness in real-

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

time environments (Nair & Bhagat, 2021; Gilbert & Gilbert, 2024d).

3. Dynamic Weighting: Current models lack mechanisms to dynamically assign weights to elements of the intrusion graph, which is crucial for reflecting the evolving nature of network traffic and threats (Gilbert & Gilbert, 2024c; Nasraoui & N'Cir, 2019).

By integrating these enhancements into a graph-based data mining process, we aim to provide stronger support for intrusion detection systems, improving both their accuracy and responsiveness.

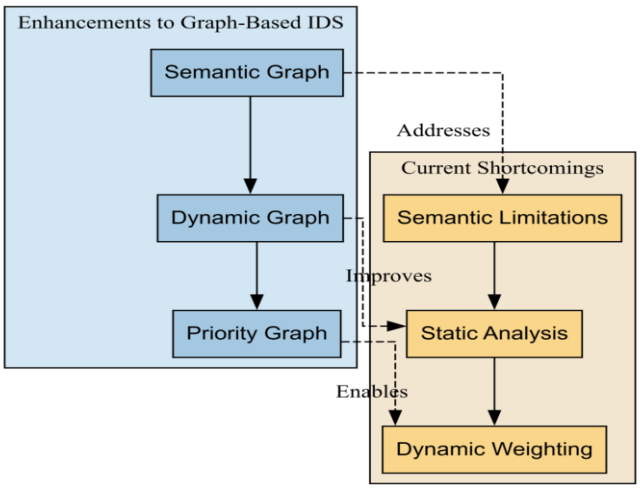

Figure 16: How graph-based intrusion detection systems (IDS) can be enhanced

This diagram breaks down how graph-based intrusion detection systems (IDS) can be enhanced to address key limitations in current models. It starts by identifying three core issues: semantic limitations, static analysis, and a lack of dynamic weighting. To tackle these, the diagram introduces three corresponding solutions. Semantic limitations are addressed with semantic graphs, which add meaningful context to data rather than relying on just structure or syntax. Static analysis, which limits real-time responsiveness, is replaced by dynamic graphs that update and adapt as network conditions evolve. Lastly, the absence of dynamic weighting is resolved by using priority graphs, which can assign importance to different network elements or events based on context. All three of these improvements feed into and enhance traditional graph models, ultimately strengthening their ability to detect intrusions more intelligently and efficiently.

7.2. Integration with Machine Learning

Graph features have proven useful in various domains, such as edge detection and object recognition in image processing. These features, when integrated into machine learning algorithms, can significantly enhance robustness and performance (Gilbert & Gilbert, 2025a). In the context of medical image recognition, for instance, several automated systems already leverage graph-based features. However, to the best of our knowledge, similar approaches have not been widely applied to conventional intrusion detection systems (Nair & Bhagat, 2021; Gilbert et al., 2025).

This section explores how graph features can be integrated with existing anomaly detection or intrusion detection frameworks (Gilbert & Gilbert, 2025c). One challenge is that graph-derived features tend to be high-dimensional and sparse, and current IDS infrastructures are not optimized to handle such data (Gilbert & Gilbert, 2024b). We propose moderating the number of graph features used and conducting systematic experiments to evaluate their effectiveness compared to traditional data mining features, such as traffic volume and host connectivity (Roy & Dutta, 2022; Gilbert & Gilbert, 2025a). Furthermore, we investigate the temporal properties of these graph features to assess their impact on detection performance.

Our preliminary results suggest that incorporating advanced graph features such as center-surround differences can significantly enhance detection rates, as evidenced by improvements in precision and recall metrics on Advanced Graph Feature (AGF) datasets (Gilbert & Gilbert, 2024a; Saifudin & Widiyaningtyas, 2024). As machine learning-based approaches continue to gain traction in the field of intrusion detection, further exploration of these graph-theoretic features promises to yield even higher detection accuracies and more robust security models.

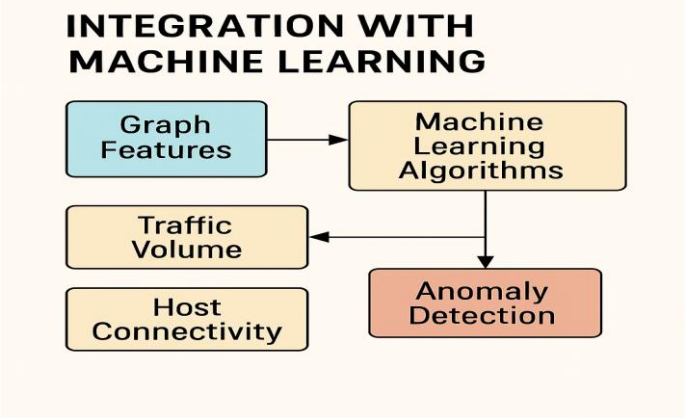

Figure 17: Integration of Graphs with Machine Learning

Figure 17, outlines how graph features are integrated into machine learning algorithms to improve anomaly detection. It begins with graph features, which serve as a foundation for the process. These features are then fed into machine learning algorithms, enhancing their ability to detect complex patterns. Alongside graph features, traditional indicators like traffic volume and host connectivity are also considered. All these inputs—graph-based and conventional—come together in the anomaly detection system, where they're analyzed to identify abnormal behaviors more accurately. The flow suggests a layered approach, showing how combining graph theory with machine learning creates a more intelligent and precise intrusion detection framework.

Chris Gilbert and Mercy Abiola Gilbert, "Algorithmic Approaches to Intrusion Detection Systems (IDS) Using Graph Theory," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 109-125, 2025.

VII. Summary of Findings, Conclusions, Recommendations, and Future Trends

This study introduces a novel algorithmic framework for intrusion detection that leverages graph-theoretic models in combination with advanced machine learning and clustering techniques. The research demonstrates that transforming network traffic into graph structures—where nodes represent network endpoints and edges capture communication links—can significantly enhance the detection and classification of anomalous behavior. Experimental evaluations, including tests on the KDD Cup 99 dataset, indicate that our approach addresses critical challenges such as missing data, class imbalance, and the variability inherent in dynamic network environments. In particular, the implementation of a centroid-based graph measure for automatic labeling, along with refined clustering algorithms, shows promising improvements in detection accuracy and computational efficiency.

The study also reveals that while our current system can effectively identify intrusions using connection data alone, it does not yet integrate fully with existing security mechanisms like firewalls or provide real-time prevention capabilities. These limitations underscore the need for further development, including expanding the framework to support a broader range of network protocols and incorporating mechanisms to actively stop attacks.

Based on our findings, we recommend several avenues for future research:

- Enhancing Graph-Based Models: Develop more sophisticated graph representations—such as semantic, dynamic, and priority graphs—to capture the evolving nature of network traffic and improve real-time detection.
- Integrating Unsupervised and Supervised Methods: Combine unsupervised community detection with supervised clustering to better classify both known and novel attack patterns.
- Scalability and Efficiency Improvements: Focus on optimizing the computational overhead associated with graph-based algorithms, particularly for large-scale networks and high-volume traffic scenarios.
- Expanding Real-World Applications: Validate and extend the framework across various protocols and operational environments, ultimately integrating it with existing security infrastructures to provide both detection and prevention capabilities.

In conclusion, the interdisciplinary approach of integrating graph theory with machine learning offers a robust pathway for advancing intrusion detection systems. Although challenges remain, particularly in scaling the solution and integrating it into broader security architectures, the promising experimental results and novel methodologies presented here lay a solid foundation for future innovations in network security.

References

1. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015
2. Abilimi, C. A., & Adu-Manu, K. S. (2013). Examining the impact of Information and Communication Technology capacity building in High School education in Ghana. International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9, September - 2013
3. Abilimi, C.A., Amoako, L., Ayembillah, J. N., Yeboah, T.(2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. International Journal of Engineering Research and Technology, 2(11), 50 - 59.
4. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November – 2013
5. Alguliyev, R. M., Aliguliyev, R. M., & Sukhostat, L. V. (2020). Efficient algorithm for big data clustering on single machine. *CAAI Transactions on Intelligence Technology*, *5*(1), 9–14.
6. Alharbi, A., & Alsubhi, K. (2021). Botnet detection approach using graph-based machine learning. *Ieee Access*, *9*, 99166–99180.
7. Alizadeh, F., & Khansari, M. (2023, November). An analysis of botnet detection using graph neural network. In *2023 13th International Conference on Computer and Knowledge Engineering (ICCKE)* (pp. 491–495). IEEE.
8. Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. *IEEE Open Journal of Vehicular Technology*.
9. Alrumaih, T. N., & Alenazi, M. J. (2023). GENIND: An industrial network topology generator. *Alexandria Engineering Journal*, *79*, 56–71.
10. Alshehri, A., Khan, N., Alowayr, A., & Alghamdi, M. Y. (2023). Cyberattack detection framework using machine learning and user behavior analytics. *Computer Systems Science & Engineering*, *44*(2).
11. Amirthayogam, G., Kumaran, N., Gopalakrishnan, S., Brito, K. A., RaviChand, S., & Choubey, S. B. (2024). Integrating behavioral analytics and intrusion detection systems to protect critical infrastructure and smart cities. *Babylonian Journal of Networking*, *2024*, 88–97.
12. An, J., Gao, M., & Tang, J. (2024). MvStHgL: Multi-View Hypergraph Learning with Spatial-Temporal Periodic Interests for Next POI Recommendation. *ACM Transactions on Information Systems*, *42*(6), 1–29.
13. Arisdakessian, S., Wahab, O. A., Mourad, A., Otrok, H., & Guizani, M. (2022). A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. *IEEE Internet of Things Journal*, *10*(5), 4059–4092.
14. Azab, A., Khasawneh, M., Alrabaee, S., Choo, K. K. R., & Sarsour, M. (2024). Network traffic classification: Techniques, datasets, and challenges. *Digital Communications and Networks*, *10*(3), 676–692.
15. Chan, R. K. C., Lim, J. M. Y., & Parthiban, R. (2023). Missing traffic data imputation for artificial intelligence in intelligent transportation systems: Review of methods, limitations, and challenges. *Ieee Access*, *11*, 34080–34093.
16. Chartrand, G., Jordon, H., Vatter, V., & Zhang, P. (2024). *Graphs & digraphs*. Chapman and Hall/crc.
17. Chen, R., Chen, X., & Zhao, J. (2024). Private and utility enhanced intrusion detection based on attack behavior analysis with local differential privacy on IoV. *Computer Networks*, *250*, 110560.
18. Chitkeshwar, A. (2024). Revolutionizing structural engineering: Applications of machine learning for enhanced performance and safety. *Archives of Computational Methods in Engineering*, *31*(8), 4617–4632.
19. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.
20. Das, R., & Soylu, M. (2023). A key review on graph data science: The power of graphs in scientific studies. *Chemometrics and Intelligent Laboratory Systems*, *240*, 104896.

21. Diana, L., Dini, P., & Paolini, D. (2025). Overview on intrusion detection systems for computers networking security. *Computers, 14*(3), 87.
22. Dlamini, T., Maseko, L., Nkosi, S., Khumalo, Z., Ndlovu, J., Smith, A., & Tshabalala, A. (2024). Evaluation of collaborative data sharing mechanisms for comprehensive cyber threat mitigation in national security crises.
23. Dong, Y., Wang, R., & He, J. (2019, October). Real-time network intrusion detection system based on deep learning. In *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)* (pp. 1–4). IEEE.
24. Dörfler, F., Simpson-Porco, J. W., & Bullo, F. (2018). Electrical networks and algebraic graph theory: Models, properties, and applications. *Proceedings of the IEEE, 106*(5), 977–1005.
25. Ezugwu, A. E., Ikotun, A. M., Oyelade, O. O., Abualigah, L., Agushaka, J. O., Eke, C. I., & Akinyelu, A. A. (2022). A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research prospects. *Engineering Applications of Artificial Intelligence, 110*, 104743.
26. Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. *Telecommunication Systems, 70*, 447–489.
27. Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X., & Zeng, X. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. *IEEE Access, 7*, 154560–154571.
28. Gangadhar, C., Mapari, R. G., Muthevi, A. K., Suneetha, A., BV, S. K., & Mouleswararao, B. (2025). Exploring the role of behavioral analytics and anomaly detection in securing mobile networks for critical infrastructure. *Information Security Journal: A Global Perspective*, 1–14.
29. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's The Road. English Journal, Volume 102, Issue Characters and Character, p. 40 - 47. https://doi.org/10.58680/ej201220821.
30. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. The Educational Forum, 83(1), 60–74. https://doi.org/10.1080/00131725.2018.1505017.
31. Gilbert, C. (2021). Walking the popular education spiral - an account and analysis of participatory action research with teacher activists. Educational Action Research, 30(5), 881–901. https://doi.org/10.1080/09650792.2021.1875856
32. Gilbert, C. (2022). Making the Invisible Visible: Professional Development to Support Teacher Activism. Kappa Delta Pi Record, 58(1), 14–19. https://doi.org/10.1080/00228958.2022.2005426
33. Gilbert, C. & Gilbert, M.A.(2024a). Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf
34. Gilbert, C. & Gilbert, M.A.(2024b). Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816
35. Gilbert, C. & Gilbert, M.A.(2024c). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441. https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.
36. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, *3*(9), 9-9.
37. Gilbert, C. & Gilbert, M.A.(2024e). Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf
38. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024,Volume 9, Issue 4, pp. 95-106.
39. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, *3*(10). https://doi.org/10.38124/ijsrmt.v3i10.54
40. Gilbert, C., & Gilbert, M. A. (2024h). Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.
41. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.
42. Gilbert, C. & Gilbert, M.A. (2024j). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.
43. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.
44. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. *International Research Journal of Advanced Engineering and Science*, *9*(4), 205–219.
45. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. *International Journal of Research Publication and Reviews*, *5*(11), 889–907. https://www.ijrpr.com
46. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, *9*(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013
47. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. *International Journal of Research Publication and Reviews*, *5*(11), 3235-3256. https://www.ijrpr.com.
48. Gilbert, C., & Gilbert, M. A. (2024p). Cryptographic Foundations And Cybersecurity Implications Of Blockchain Technology.*Global Scientific Journals*,ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com
49. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. *International Research Journal of Advanced Engineering and Science*, *9*(4), 238–251.
50. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.76
51. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.77
52. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. *International Journal of Research Publication and Reviews*, *5*(12), 507–533. https://www.ijrpr.com/
53. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, *5*(12), 1174–1191. Retrieved from www.ijrpr.com
54. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. *International*

Journal of Research Publication and Reviews, 5(12), 1149–1173. Retrieved from www.ijrpr.com
55. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. *Global Scientific Journal, 12*(12). Retrieved from www.globalscientificjournal.com
56. Gilbert, C., & Gilbert, M. A. (2024x). Investigating the challenges and solutions in cybersecurity using quantum computing and cryptography. International Research Journal of Advanced Engineering and Science, 9(4), 291–315.
57. Gilbert, C., & Gilbert, M. A. (2024y). The integration of blockchain technology into database management systems for enhanced security and transparency. International Research Journal of Advanced Engineering and Science, 9(4), 316–334.
58. Gilbert, C., & Gilbert, M. A. (2025a). *Artificial intelligence (AI) and machine learning (ML) for predictive cyber threat intelligence (CTI)*. International Journal of Research Publication and Reviews, 6(3), 584–617. http://www.ijrpr.com
59. Gilbert, C., & Gilbert, M. A. (2025b). Continuous user authentication on mobile devices. International Research Journal of Advanced Engineering and Science, 10(1), 158–173.
60. Gilbert, C., & Gilbert, M. A. (2025c). *Patterns and vulnerabilities of cryptocurrency-related cybercrimes*. *Global Scientific Journal*, 13(3), 1950-1981. https://www.globalscientificjournal.com
61. Gilbert, C., & Gilbert, M. A. (2025d). *Data encryption algorithms and risk management*. *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS), 14*(3), 479–497. https://doi.org/10.51583/IJLTEMAS.2025.140300054
62. Gilbert, C., Gilbert, M. A., Dorgbefu, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025). Enhancing detection and response using artificial intelligence in cybersecurity. *International Journal of Multidisciplinary Research and Publications (IJMRAP), 7*(10), 87-104.
63. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C. (2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.
64. Gilbert, M.A., Auodo, A. & Gilbert, C. (2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.
65. Gogoshin, G., & Rodin, A. S. (2023). Graph neural networks in cancer and oncology research: Emerging and future trends. *Cancers, 15*(24), 5858.
66. Gross, J. L., Yellen, J., & Anderson, M. (2018). *Graph theory and its applications.* Chapman and Hall/CRC.
67. Guerra, J. L., Catania, C., & Veas, E. (2022). Datasets are not enough: Challenges in labeling network traffic. *Computers & Security, 120*, 102810.
68. Hajj, S., El Sibai, R., Bou Abdo, J., Demerjian, J., Makhoul, A., & Guyeux, C. (2021). Anomaly-based intrusion detection systems: The requirements, methods, measurements, and datasets. *Transactions on Emerging Telecommunications Technologies, 32*(4), e4240.
69. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing, 26*(6), 3753–3780.
70. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing, 26*(6), 3753–3780.
71. Houichi, M., Jaidi, F., & Bouhoula, A. (2024). Cyber Security within Smart Cities: A comprehensive study and a novel intrusion detection-based approach. *Computers, Materials & Continua, 81*(1).
72. Johnson, R., Li, M. M., Noori, A., Queen, O., & Zitnik, M. (2024). Graph artificial intelligence in medicine. *Annual Review of Biomedical Data Science, 7*(2024), 345–368.
73. Ju, W., Zhao, Y., Qin, Y., Yi, S., Yuan, J., Xiao, Z., ... & Zhang, M. (2024). COOL: A conjoint perspective on spatio-temporal graph neural network for traffic forecasting. *Information Fusion, 107*, 102341.
74. Khayat, M., Barka, E., Serhani, M. A., Sallabi, F., Shuaib, K., & Khater, H. M. (2025). Empowering Security Operation Center with Artificial Intelligence and Machine Learning–A systematic literature review. *IEEE Access*.
75. Khanan, A., Mohamed, Y. A., Mohamed, A. H., & Bashir, M. (2024). From bytes to insights: A systematic literature review on unraveling IDS datasets for enhanced cybersecurity understanding. *IEEE Access*.
76. Kolbeck, L., Vilgertshofer, S., Abualdenien, J., & Borrmann, A. (2022). Graph rewriting techniques in engineering design. *Frontiers in built environment, 7*, 815153.
77. Kumar, J. (2025). GrMA-CNN: Integrating spatial-spectral layers with modified attention for botnet detection using graph convolution for securing networks. *International Journal of Intelligent Engineering & Systems, 18*(1).
78. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. Communications on Applied Electronics, 7(7), 8-13.
79. Lagraa, S., Husák, M., Seba, H., Vuppala, S., State, R., & Ouedraogo, M. (2024). A review on graph-based approaches for network security monitoring and botnet detection. *International Journal of Information Security, 23*(1), 119–140.
80. Lam, N. T. (2021). Detecting unauthorized network intrusion based on network traffic using behavior analysis techniques. *International Journal of Advanced Computer Science and Applications, 12*(4).
81. Le Jeune, L., Goedeme, T., & Mentens, N. (2021). Machine learning for misuse-based network intrusion detection: Overview, unified evaluation and feature choice comparison framework. *Ieee Access, 9*, 63995–64015.
82. Levy Rocha, S., Lopes de Mendonca, F. L., Staciarini Puttini, R., Rabelo Nunes, R., & Amvame Nze, G. D. (2023). DCIDs—Distributed container IDs. *Applied Sciences, 13*(16), 9301.
83. Li, Y., & Yan, J. (2022). Cybersecurity of smart inverters in the smart grid: A survey. *IEEE Transactions on Power Electronics, 38*(2), 2364–2383.
84. Liao, N., Wang, J., Guan, J., & Fan, H. (2024). A multi-step attack identification and correlation method based on multi-information fusion. *Computers and Electrical Engineering, 117*, 109249.
85. Luo, X., Yuan, J., Huang, Z., Jiang, H., Qin, Y., Ju, W., ... & Sun, Y. (2023, July). Hope: High-order graph ODE for modeling interacting dynamics. In *International Conference on Machine Learning* (pp. 23124–23139). PMLR.
86. Mahdi, M. A., Hosny, K. M., & Elhenawy, I. (2021). Scalable clustering algorithms for big data: A review. *IEEE Access, 9*, 80015–80027.
87. Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems, 133*, 95–113.
88. McMahon, A., Buyx, A., & Prainsack, B. (2020). Big data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. *Medical law review, 28*(1), 155–182.
89. Miller, S., & Bossomaier, T. (2024). Cybersecurity, ethics, and collective responsibility. Oxford University Press.
90. Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Computing Surveys, 55*(10), 1–36.
91. Nair, R., & Bhagat, A. (2021). An introduction to clustering algorithms in big data. In *Encyclopedia of Information Science and Technology, Fifth Edition* (pp. 559–576). IGI Global.
92. Naphade, M., Tang, Z., Chang, M. C., Anastasiu, D. C., Sharma, A., Chellappa, R., ... & Lyu, S. (2019, June). The 2019 AI City Challenge. In *CVPR workshops* (Vol. 8, p. 2).
93. Nasraoui, O., & N'Cir, C. E. B. (2019). Clustering methods for big data analytics. *Techniques, Toolboxes and Applications, 1*, 91–113.
94. Nguyen, T. T., Ren, Z., Nguyen, T. T., Jo, J., Nguyen, Q. V. H., & Yin, H. (2024). Portable graph-based rumour detection against multi-modal heterophily. *Knowledge-Based Systems, 284*, 111310.
95. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. Comput. Eng. Intell. Syst, 4, 50-57.
96. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service.

International Journal on Computer Science and Engineering (IJCSE), 760-769.
97. Ortega, A., Frossard, P., Kovačević, J., Moura, J. M., & Vandergheynst, P. (2018). Graph signal processing: Overview, challenges, and applications. *Proceedings of the IEEE, 106*(5), 808–828.
98. Otoum, Y., & Nayak, A. (2021). As-IDS: Anomaly and signature based IDS for the Internet of Things. *Journal of Network and Systems Management, 29*(3), 23.
99. Putra, M. A. R., Ahmad, T., Hostiadi, D. P., Ijtihadie, R. M., & Maniriho, P. (2024). Botnet attack analysis through graph visualization. *International Journal of Intelligent Engineering & Systems, 17*(1).
100. Qin, H., Shao, S., Wang, T., Yu, X., Jiang, Y., & Cao, Z. (2023). Review of autonomous path planning algorithms for mobile robots. *Drones, 7*(3), 211.
101. Rizvi, S., Scanlon, M., Mcgibney, J., & Sheppard, J. (2022). Application of artificial intelligence to network forensics: Survey, challenges and future directions. *Ieee Access, 10*, 110362–110384.
102. Roy, D., & Dutta, M. (2022). A systematic review and research perspective on recommender systems. *Journal of Big Data, 9*(1), 59.
103. Saifudin, I., & Widiyaningtyas, T. (2024). Systematic literature review on recommender system: Approach, problem, evaluation techniques, datasets. *IEEE Access, 12*, 19827–19847.
104. Sandosh, S., Bala, A., & Kodipyaka, N. (2024). ZKR: A novel framework in intrusion detection system through enhanced techniques. *Journal of Information Assurance & Security, 19*(2).
105. Shafi, M., Lashkari, A. H., & Roudsari, A. H. (2025). Toward generating a large scale intrusion detection dataset and intruders behavioral profiling using network and transportation layers traffic flow analyzer (NTLFlowLyzer). *Journal of Network and Systems Management, 33*(2), 44.
106. Silva, T. C., Zhao, L., Zequan, L., Zhao, Y., & Xin, C. (2018). *Machine learning in complex networks* (Vol. 1). Springer.
107. Singh, M. (2020). Scalability and sparsity issues in recommender datasets: A survey. *Knowledge and Information Systems, 62*(1), 1–43.
108. Sowrirajan, R., & Manimekalai, S. (2024). Graph-Theoretic approaches to optimizing connectivity and security in ubiquitous healthcare systems. In *Ubiquitous Computing and Technological Innovation for Universal Healthcare* (pp. 327–351). IGI Global.
109. Torres, L., Blevins, A. S., Bassett, D., & Eliassi-Rad, T. (2021). The why, how, and when of representations for complex systems. *SIAM Review, 63*(3), 435–485.
110. Trisolino, A. (2023). Analysis of security configuration for IDS/IPS (Doctoral dissertation, Politecnico di Torino).
111. Walling, S., & Lodh, S. (2025). An extensive review of machine learning and deep learning techniques on network intrusion detection for IoT. *Transactions on Emerging Telecommunications Technologies, 36*(2), e70064.
112. Waqas, A. (2024). From Graph Theory for Robust Deep Networks to Graph Learning for Multimodal Cancer Analysis (Doctoral dissertation, University of South Florida).
113. Xu, Y., Han, L., Zhu, T., Sun, L., Du, B., & Lv, W. (2023). Generic dynamic graph convolutional network for traffic flow forecasting. *Information Fusion, 100*, 101946.
114. Yasmina, A. M., Bentaleb, Y., Sharippudin, S. N., Mahadi, N., Zakaria, W. N. W., Sardjono, W., … & Vijaya, M. (2024). Latent modeling for predicting multidimensional data. *Journal of Theoretical and Applied Information Technology, 102*(1).
115. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A. (2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. Journal of Engineering, Computers & Applied Sciences (JEC&AS), 2(7).
116. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment.
117. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b). Automatic Biometric Student Attendance System: A Case Study Christian Service University College. Journal of Engineering Computers & Applied Sciences, 2(6), 117-121.
118. Yeboah T. & Abilimi C.A. (2013). Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, "2(11).