ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

Lateral Movement Detection in Enterprise Networks Using Temporal Graph Attention Networks (T-GATs)

Kevin William Peoples[1]

[1]University of California, San Diego

Publication Date: 2025/10/17

Abstract: In terms of cybersecurity, "Advanced Persistent Threats (APT)" attacks are the significant threat due to their adaptation, persistence, and stealth against usual detection mechanisms. With smart tactics used by APT attackers to infiltrate networks and stay undetected for longer periods of time, this study has focused on "Graph Neural Networks (GNNs)" for detecting APT attacks. GNNs are excellent in capturing complex relationships in network data, using graphical structures to identify anomalies and subtle patterns which indicate behaviors in APT. This study reports existing detailed exploration of GNNs as modern technology to improve capabilities of "Intrusion Detection Systems (IDS)". APT attacks pose significant threats because of their persistence and smart tactics, underscoring the need for innovative approaches. The study provides an in-depth survey of applications of GNN against APT attacks to protect enterprise networks, precisely analyzing different architectures of GNN and proposing a framework curated especially to evaluate the systems for APT detection. In addition, this study proposes a novel approach for APT attack detection in real-time by using time evolution and opens further opportunities for future studies. Findings of the study elucidate the significant role played by GNNs to address the rising threats posed by APTs, focusing on potential to improve cybersecurity. In addition, the study identifies future research directions and development in using graph-based and machine learning techniques for proactive and adaptive intrusion detection in complex environments.

Keywords: *Advanced Persistent Threat, Graph Neural Networks, Intrusion Detection Systems, APT Attacks, APT Detection, Machine Learning.*

How to Cite: Kevin William Peoples (2025) Lateral Movement Detection in Enterprise Networks Using Temporal Graph Attention Networks (T-GATs). *International Journal of Innovative Science and Research Technology*, 10(10), 918-929. https://doi.org/10.38124/ijisrt/25oct435

I. INTRODUCTION

These days, organizations face a lot of threats, from malicious attacks to social engineering and data breaches. These threats can affect the reputation of the company, customer trust, and profitability in a devastating way. Cybersecurity consists of preventing and anticipating threats along with reacting to them. It depends upon several technologies, practices, and procedures which are constantly updated to address the threat landscape which is constantly evolving. An enterprise network combines interlinked services and elements working with IT operations of the company. Figure 1 illustrates an example of an enterprise network with main components like servers, hosts, cloud services, cables, monitoring tools and databases (Iniewski et al, 2008).

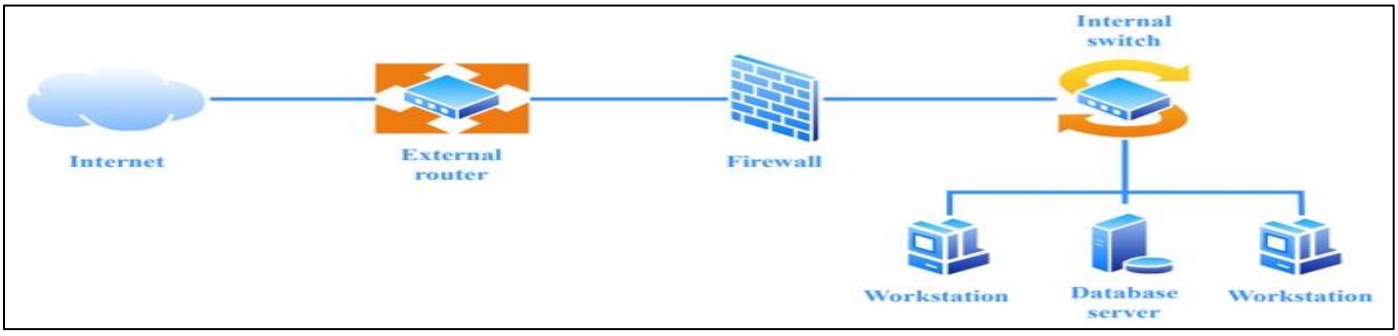

Fig 1 An Example of Enterprise Network
Source – Athmane et al (2023)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

"Advanced Persistent Threats (APT)" attacks are the class of long-term and highly sophisticated attacks, composed by highly-trained attackers or malicious entities, such as intelligence agencies and nation-states (Alshamrani et al, 2019; Yasar and Linda, 2023). APTs are well-regarded for their complex approaches, enduring nature, and well-defined and specific goals. Along with random and opportunistic actions, these attacks are defined by persistent and deliberate approach, often covering complex strategies and stages to compromise and infiltrate targeted networks or systems. The attackers responsible for APTs use modern techniques to prevent detection, attack for a longer period, and retain covert operations, making them a significant and daunting threat.

APTs majorly target government agencies, defense, energy, R&D, financial institutions, and pharma companies. These attacks can target SMEs and even MNCs. APTs are a significant threat to victims with different types of attacks like financial loss, identity theft, reputation loss, and even hitting national security by targeting critical infrastructure. APTs usually aim for long-term goals and impacts may be short-term, resulting in long-term losses and sustained disruptions. There are different definitions of APT lifecycle counted in the studies on the basis of several steps conducted by attacks. These steps are known as stages and they use different techniques. Figure 2 presents a flowchart of a typical APT lifecycle. Quintero- Bonilla and Martín del Rey (2020) conducted a survey on various classifications of APT lifecycle. While Ussath et al (2016) highlighted three stages of APT attacks, Vukalović and Delija (2015) proposed 7-stages APT attacks.

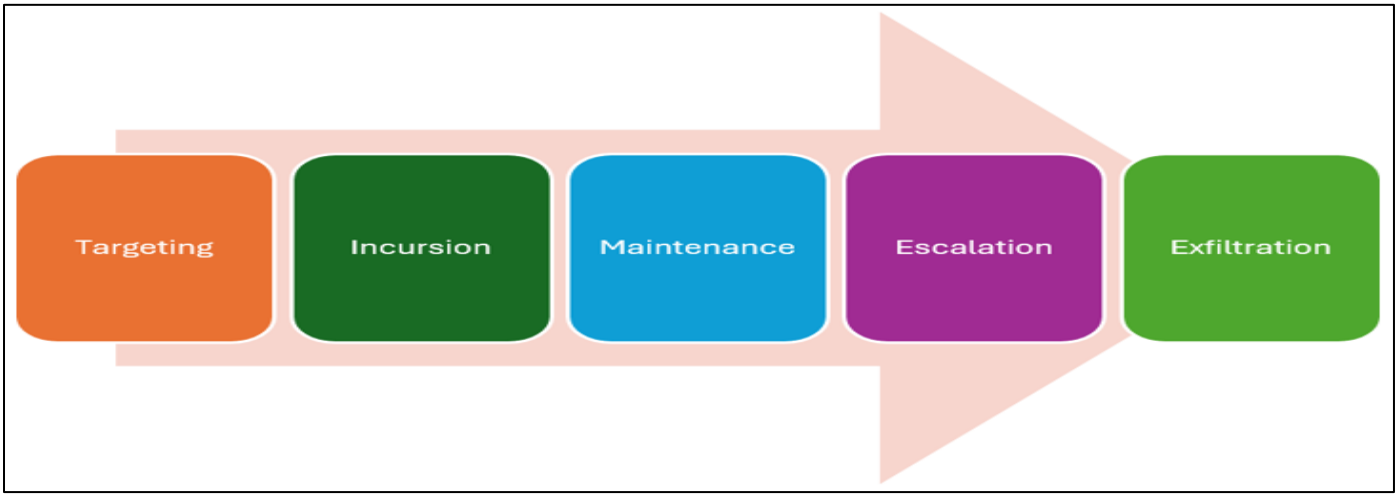

Fig 2 A Flowchart of General 5-Stage Cycle of APT Attacks
Source – Quintero-Bonilla and Martín del Rey (2020)

"Graph Neural Networks (GNNs)" are the category of "deep learning models" made for processing graph data (Liu and Zhou, 2022). GNNs are best suited to analyze and represent structured data in graphs like knowledge graphs, social networks, biological relationship, recommendation graphs, and other data. GNNs are neural networks designed to consider the graphical structure. Unlike other neural networks, operating on sequences or tabular data, GNNs work on organized data through graphs (Figure 3). GNNs have been the standard in a lot of graph-based applications based on machine learning, offering more adaptive, comprehensive, and dynamic method for representing graphical data. They are excellent in addressing several ML challenges and covering complex data, based on graphs.

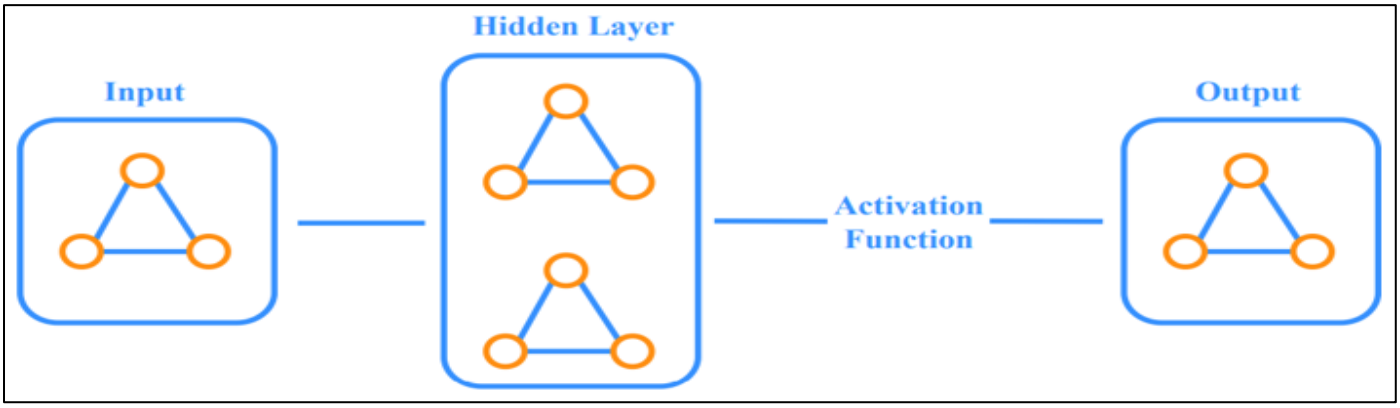

Fig 3 An Illustration of a Simple GNN Architecture
Source – Athmane et al (2023)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

APTs and cybersecurity are significant concerns in this day and age. Security is needed in networks and computer systems to maintain the integrity, confidentiality, and data availability. APTs are advanced form of threats, known for being sophisticated and persistent. Cybersecurity experts use modern techniques for response, detection and prevention. Attribution is a complex issue in APT attacks. It is also important to identify attacks and take precautionary measures. APTs are often related to state-sponsored groups, with a geopolitical aspect of such attacks. Detecting APTs early is important to reduce possible damage. Unusual patterns on accounts, anomalies in output data, and unauthorized changes in configuration are some of the red flags indicating ongoing attack.

II. LITERATURE REVIEW

With the wake of increased frequency and complexity of cyberattacks, Friji (2024) proposes innovative methods to detect network intrusion leveraging modern abilities of novel GNN protocols. For the foundation of research, they conducted a critical review of current datasets in intrusion detection and network capabilities, focusing on their efficiency to address key challenges in research. This study analyzes two of the most common datasets – "CICIDS 2017 and ToN IoT", focusing on their limitations and strengths. This approach proposes a new graph representation of flow related to flows of communication, improving existing solutions by improving robust adversarial attacks. First, they proposed the groundbreaking intrusion detection solutions based on GNN, using GNN models and graph representation to calculate the scores of maliciousness. They captured complex patterns that are often overlooked by traditional approaches. Findings of the study observed better performance of this framework over existing excellent GNN-based and machine learning solutions in terms of both robustness and accuracy.

Over the years, APT attacks have widely become a menace to cybersecurity of the country. Because of their persistent nature and complex techniques, it can be challenging for detecting anomalies and APT attacks. Now, the provenance graph is adopted majorly for analyzing APT attacks as it consists of wider semantic provenance, causation abilities and expression. Based on "network attack knowledge graphs and provenance graphs", a lot of existing anomaly detection approaches are complex by design. In addition, these approaches use features from the whole graph and overlook the rich complexities in its architecture, which affects their efficiency in detecting nodes. Peng et al (2025) introduced an innovative approach for anomaly detection for provenance graphs, using heterogenous node clustering and embedding analysis. Based on the "W3C-PROV'S PROV-DM model", a unique heterogenous graph structure is crafted. A "new meta-path strategy" is designed for getting semantic knowledge better. With "heterogenous graph learning model", node embeddings are obtained. Benign nodes are classified to get various clusters with "K-means clustering" and benign node clusters are used to differentiate between anomalous and benign nodes.

Experimental results confirmed better capacity of anomaly detection as compared to two current systems of anomaly detection – "DARPA TC dataset and Unicorn SC-2 dataset."

The "Open-source Cyber Threat Intelligence (OSCTI)" is being more influential to obtain current data of network security. A lot of studies on "Cyber Threat Intelligence" are focused on extracting threat bodies from public sources describing the events of attacks. The knowledge graph of cybersecurity aims to change threat knowledge for researchers to obtain different kinds of threat data efficiently and accurately for smart decisions. Along with security analysts, attribution technology can also detect modern threats and identify same threats from various events of attack. It is vital to trace the attackers. Ren et al (2022) used "knowledge graph technology", considering recent research on attribution of cyber threats and examined key theories and technologies in applying and building the APT knowledge graph. They designed a "CSKG4APT", a cybersecurity platform based on knowledge graph. With the "theory of ontology", this platform was designed as "APT knowledge graph model" on the basis of real scenarios of APT attacks. Then, threat knowledge model was designed for updating and finishing the knowledge graph with expert knowledge and deep learning. Finally, they proposed a practical method for APT attack attribution with countermeasures and attribution. It integrates a lot of fragmented intelligence and can adjust its defense solution. It lays the basis for dominance in network defense and attacks.

APT attacks are highly covert and threatening, making them challenging to detect with traditional measures. On the basis of trace graphs, causal analysis has been a common approach to detect APT. Previous studies have faced a lot of issues, like inability to make the most of context-based information from trace graphs, the need for previous records, and excessive overhead. Guo et al (2025) proposed an effective approach based on supervised machine learning for detecting APT attacks. With graph representation and provenance graphs, this approach achieves anomaly detection and multi-granularity detection effectively. The outlier detection techniques are adopted by the model, enabling APT detection as both batch log and entity levels. They achieved ideal detection performance while performing better than current methods for APT detection.

"Advanced Persistent Threats (APTs)" and other sophisticated attacks eventually generate undetected presence to access secret data. APTs are planned well to evade current security measures and penetrate certain organizations. These attacks need high sophistication and customization, often performed by experienced, well-funded teams of cyberattacks. Adversaries exploit vulnerabilities highlighted and high-value organizations. APTs are a huge threat to security of enterprise networks, requiring innovative approaches. Gowthami et al (2024) investigated the use of machine learning for APT detection in enterprise networks. With feeds on threat intelligence and traffic data, this approach shows excellent capabilities for APT detection

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

in comparison to traditional approaches. Experimental findings have validated effective framework, resulting in advanced enterprise network security and threat detection powered by AI. This study investigated the use of machine learning approaches to improve network security to detect APTs. The potent ML approach, "Gradient Boosting" is applied to "CICIDS2017" dataset for APT detection with excellent F1-score, precision, accuracy and recall.

Anjum et al (2022) presented highly effective ML-based system for APT detection, ANUBIS. It consists of two important components. First, ANUBIS is used well by cyber-response teams. Hence, explainable prediction is among the key features of ANUBIS. Second, system provenance graphs are used by ANUBIS to achieve high performance of detection and capture causality. The "Bayesian Neural Network" is used at the core of ANUBIS which can show its confidence in its predictions. ANUBIS is evaluated against "DARPA OpTC APT dataset and suggest that ANUBIS is capable to detect malicious activity similar to highly accurate APT attacks. In addition, ANUBIS learns patterns enabling to detect its predictions for threat analysts. ANUBIS is an effective tool for cyber defense with high predictive performance.

IDS plays a vital role in protecting networks and systems from various attacks. IDS faces huge challenges when it comes to detect APTs, which are smart cyberattacks known for their duration, advanced techniques and stealth. Recent studies have explored efficiency of GNNs in detecting APTs, leveraging their ability for analyzing complex relationships in graph data. Existing methods often depend upon models, affecting their flexibility to evolving tactics and increasing privacy issues. Mansour Bahar et al (2024) proposed "Federated Learning (FL)" architecture integrated into GNN-based IDS. In addition, it covers improved encryption model of clients to send to the server with the network. This way, "Man-in-the-Middle (MitM)" attacks can be prevented from intercepting the weights and reforming data with reverse engineering. The approach shows promising results in cutting the risks of false positives in comparison to "Provenance-based IDS (PIDS)".

Modern enterprise and government networks are targeted by sophisticated APT attacks, carried out and designed by experienced attackers. The long-term nature of APTs overwhelms the analyst with highly impractical alerts. Soliman et al (2023) proposed RANK, the novel "end-to-end AI-based architecture for APT detection". They proposed modern solutions and models for four sub-problems – "(1) alert graph construction; (2) merging and alert templating; (3) prioritizing and incident scoring; (3) alert graph partition; and (4) incident prioritization and scoring". In addition, they discussed needed techniques and optimizations to operate in real-time. They determined architecture against Mordor, 2000 DARPA and a lot of real-world datasets from networks.

Guttikonda (2024) presented a multi-layered and comprehensive detection model integrating ML techniques like "natural language processing (NLP)" and deep learning to analyze and detect APT activities across various attacks. It combines detection of phishing URLs, analyzing network traffic, achieves significant accuracy, and monitors keylogger activities across all components. With "Sequential Neural Network", the network traffic analysis has achieved 99.30% accuracy when it comes to classify various patterns of attacks. The phishing module uses combined ML and NLP based methods with 96.45% accuracy, while keylogger detection achieved 96% accuracy with tree-based models. Significant patterns are presented with feature importance across attacks and some of the major indicators are behavioral patterns and flow-based metrics. It offers adaptive mechanisms and real-time correlation which might cure significant issues of existing methods of APT detection. Despite challenges of integration costs and computational overhead, the proposed model has a lot of potential for deploying in enterprises. The results improve theoretical knowledge of designing APT systems and implementing practically, offering a foundation for future studies.

Hunting cyberthreats is a common search term in organizations for known attacks. It is a key component to deal with APT attacks. However, in provenance data, the attack behaviors may not be consistency with well-regarded attack behaviors. Wei et al (2021) proposed a GNN- based graph pattern approach, DeepHunter, which can match data of provenance over well- regarded attack behaviors. They designed a GNN architecture with "*attribute embedding networks*" which could use "Indicators of Compromise (IOCs)" and "*graph embedding networks*" to capture IOC's relationships. There are five synthetic and real scenarios in APT attacks selected to investigate DeepHunter. It can hunt all types of attacks and robustness and accuracy to perform better than modern approach, Poirot.

➢ *Research Objectives*

- To discuss most recent APT attacks and most common types of APT attacks
- To discuss the recent use of Graph Neural Networks (GNNs) for Threat Prevention
- To propose solution based on GNNs for APT detection and prevention in enterprise networks

III. RESEARCH METHODOLOGY

This study is based on systematic review of recent literature and focuses explicitly on APT detection. First, search strings are formulated with keywords based on research objectives, such as, "Advanced Persistent Threat", "APT detection", "Graph Neural Networks", and "Machine Learning". The search strings were used to search for relevant studies through their abstract and paper titles.

➢ *Here are the Exclusion Criteria to Filter out Irrelevant Data and Studies –*

- Papers published not in English language;
- Papers which are not accessible in full-text;
- Papers shorter than five pages;

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

- Data from the abstract which is irrelevant to research objectives;
- Papers which are not related to detection of APT attacks;
- Outdated papers;
- Papers employing inconsistent methodology; and
- Duplicate papers

With the above criteria, this study is based on in-depth examination of the works classified to perform added categorization and APT attack detection. Ultimately, this study offers insights on current patterns and trends as well as promising avenues for detecting APT attacks.

IV. DATA ANALYSIS

A. Most Common APTs and Recent APT Attacks

APT's landscape is constantly evolving with emerging threats over time. Listed here are some of the well-known APT attacks (Alshamrani et al, 2019; Quintero-Bonilla et al. 2020).

➢ *Titan Rain* –

It consists of a range of attacks executed in 2003 against the US for over three years. This range of attacks were aiming for organizations in the US, such as the FBI and NASA. There are multiple sources of attacks in China. It is mentioned that hackers were not capable to access any classified data. But they still managed to steal unclassified data which might harm the US.

➢ *RSA Security* –

Being the victim of APT attack, RSA Security reported that ID attack stole their generation algorithm data. Irrespective of being marked as spam by Outlook, an employee had opened an attachment, which had an Excel file, having a Flash object which exploited unwanted vulnerability at a zero-day exploit. A "Remote Access Trojan (RAT)" was installed by the malicious code and even antivirus couldn't detect the same.

➢ *Stuxnet* –

Stuxnet worm was made by both Israeli and the US intelligence agencies to target nuclear facilities in Iran by harming "Siemens SCADA systems." This attack sparked long term debate over its identification as an APT attack. Arguments in favour need expertise, technical complexity, and longer duration, suggesting determination and persistence. When it comes to APT classification, there are arguments related to challenges in attributing the attack to its unique goals and specific actors to disrupt nuclear facilities in Iran instead of constant data collection.

➢ *GhostNet* –

Identified in 2009, GhostNet is the Chinese APT which especially targets NGOs, government bodies, and media across the world. Attackers use phishing, social engineering and vulnerabilities in the system to attack target networks. The *modus operandi* is to collect sensitive data for strategic and political motives.

➢ *Recent APT Attacks*

Recent political crisis across the world has resulted in APT attacks in many states on their political enemies or direct competitors. Table 1 lists some of the recent APT attacks in industry and the states targeted (CYFIRMA, 2024; Google, 2024). It is noticed that attacks in the 4th quarter of 2023 intensified political stress, proving that nation-sponsored organizations have carried out attacks against critical sectors of other nation states. It is worth noting that discovery of APT attacks can either take several months or few days, making statistics unavailable for APT campaigns in 2024 in the Q1.

Table 1 Recent APT Attacks in Q4 of 2023

Name	Origin	Platform	Industry Sector	Target Country
CYBER-AV3NGERS	Iran	PLC	Wastewater and water management	Israel and USA
APT42	Iran	Android	Military and government organizations	Israel and USA
APT41	China	IOS and Android	Government	Other Asia Pacific countries
MUDDYWATER	Iran	Windows	Telecom	Sudan, Egypt, and Tanzania
Blacksmith	North Korea	WMWare	Manufacturing	Europe
WINTER VIVERN	Russia	RoundCube	Government	Poland, Ukraine, and France
COZYBEAR	Russia	TeamCity	Energy, Marketing	Europe and USA

Source – Athmane et al (2023)

The difference can often be confusing between a malware and "Advanced Persistent Threat (APT)" as there are different kinds of cyberthreats. First, APT attacks are conducted by highly talented people, often backed by activist groups, government bodies, or other sophisticated groups, deploying huge resources. There is no certain kind of attacker for malware and it can be deployed and created by several groups or people with various motives. Second, these types of attacks usually target large companies or government bodies in order to extract sensitive data or damaging the system. Malware can target the system in the company or even PC for different purposes in an organization or PC according to attacker's intentions (VMware, 2019). It is worth noting that APT may not be malware attacks, even though APT attacks may involve using malware. Malware is a broad term which covers malware that can exploit or harm the systems, while APT is a specific kind of cyberthreat known for its persistence, complexity, and usually politically motivated goals.

B. Using Graph Neural Networks for APT Detection

This section provides in-depth process of implementation of the method proposed. First part constructs the knowledge graph, where relationships and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

entities are collected from the descriptions in the crawled databases for network security and stored with Neo4j database by Ren et al (2023). Secondly, it proposes detection of APT attack with GNN model. The features extracted will act as inputs to the GCN model to detect APT attacks.

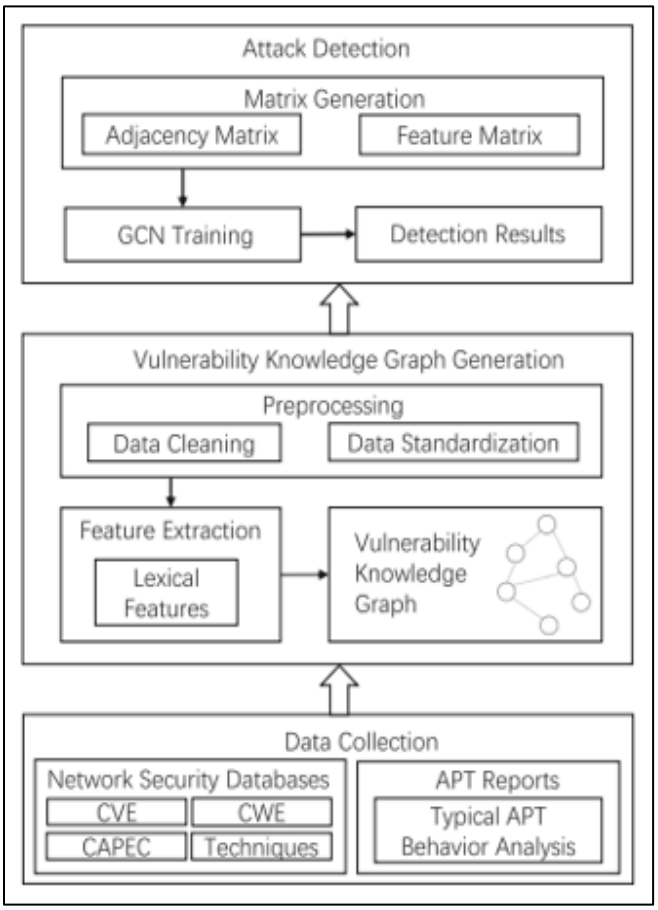

Fig 4 A Diagram of Knowledge Graph Generation
Source – Ren et al (2023)

➢ *Knowledge Graph Generation*

In this subsection, a "vulnerability knowledge graph" is generated by tracking security databases and attack reports. With CVE vulnerabilities and APT organizational behavior, relevant information is collected from such sources and organized into triplets to build relationships and entities, leading to the formulation of "vulnerability knowledge graph". It covers weaknesses, vulnerabilities, attack modes, and tactics with different types of relationships for illustrating their interconnectivity. This knowledge graph enhances proper knowledge of the relationship between attacks and vulnerabilities in the domain of software security, offering guidance and valuable resources to defend and research network security.

➢ *Gathering Security Data*

Reports of APT attacks involve ample context data. First of all, behavioral analysis is performed on typical organizations to gather the information needed, including CVE loopholes and APT organizations, techniques used, and attack modes for launching attacks. Secondly, the vulnerabilities are gathered and description and identifier of each CVE is extracted with "Common Attack Pattern Enumeration and Classification (CAPEC)" and "Common Weakness Enumeration (CWE)" from the security databases. In addition, interdependencies are established among them. Finally, data collected is stored for building knowledge graph.

➢ *Entity Modeling*

APT reports, CWE, CVE, CAPEC and other security details are used for designing vulnerability knowledge graph by Ren et al (2023). First, relationships, keywords, and entities are extracted from unstructured data and they are represented with triplets in a structured manner. They only cover relationships and entities with high confidence in this process. Figure 5 illustrates the overall knowledge graph structure having instances and ontology.

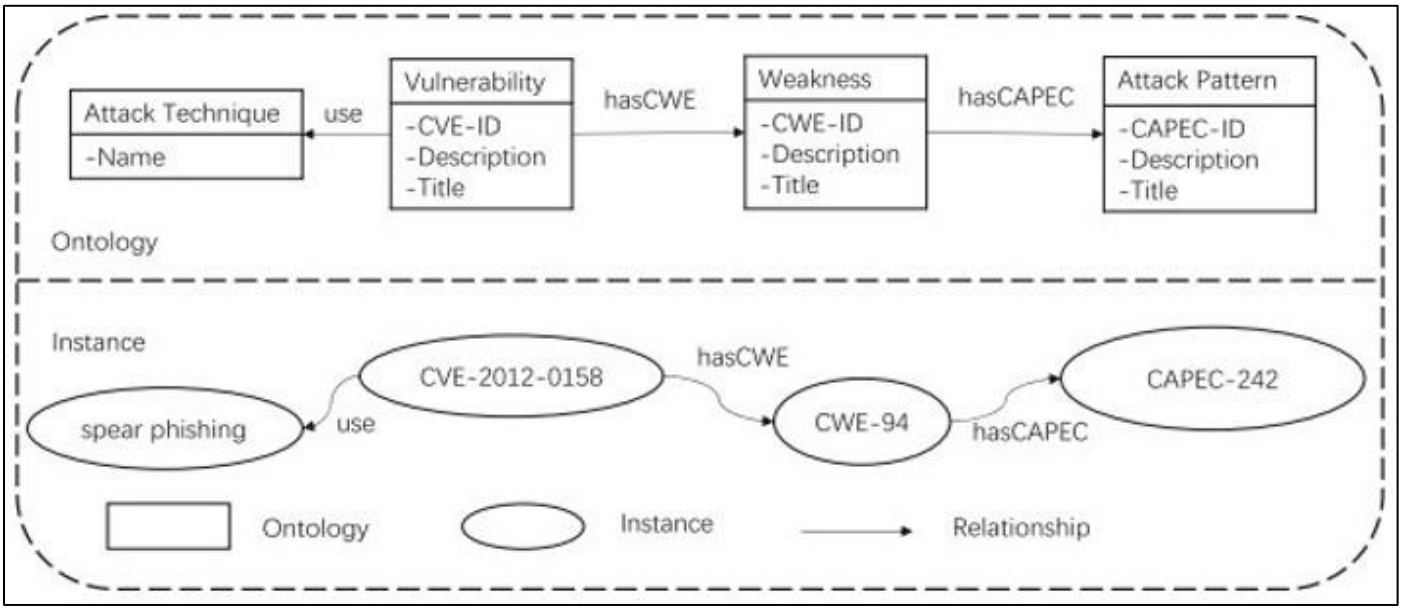

Fig 5 A Diagram of a Knowledge Graph having Attack Technique, Vulnerability, Weakness and Attack Pattern
Source - Ren et al (2023)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

The graph is divided into four parts in the ontology design – weaknesses, loopholes, attack methods and techniques with attributes. For instance, vulnerabilities consist of vulnerability description, CVE-ID, and title; weaknesses include description, CWE-ID, and title; attack methods cover description, CAPEC-ID and title; and attack techniques include approaches used in attacks like watering hole and spear-phishing attacks. With this structure, it is possible to represent the relationship between attacks and vulnerabilities, forming a complete knowledge graph. At the end, it uses the attack with spear-phishing techniques. Relationships and entities are known to be the primary goals in knowledge graph, such as "Common Weakness Enumeration (CWE) and CAPEC, along with instances like Common Vulnerabilities and Exposures (CVE)".

➢ *Extracting Relationship*

Vulnerabilities are described by APT reports used by organizations in attacks and there are cross-references among instances in CWE, CAPEC, and CVE databases. These relationships are used between APT actors, cross-references they use, and vulnerabilities as relationship among knowledge graph entities, represented through triplets. With vulnerability knowledge graph, one can have more knowledge about weaknesses, attack patterns, and vulnerabilities in software security. It is also possible to analyze and track the relationship between vulnerabilities and APT organizations with the knowledge graph. It provides ample references and resources for R&D work in security, enabling to address the ever-rising challenges in network security.

C. Proposed Solution for APT Detection with Time Evolution of Graphs

This section proposes "Graph Neural Network (GNN)" to gain understanding from the knowledge graph and classification detection is performed related to APT attacks on the basis of CVE attack and vulnerabilities. The security knowledge graph consists of different types of edges and nodes with different attributes and semantics. GNN is majorly designed to process standardized graphs and it cannot be applied directly in security graph. First, there is a need to ease the knowledge graph in homogenous one, then extraction of node features, and finally "convolutional neural networks (CNN)" are used for detecting attacks (Figure 6).

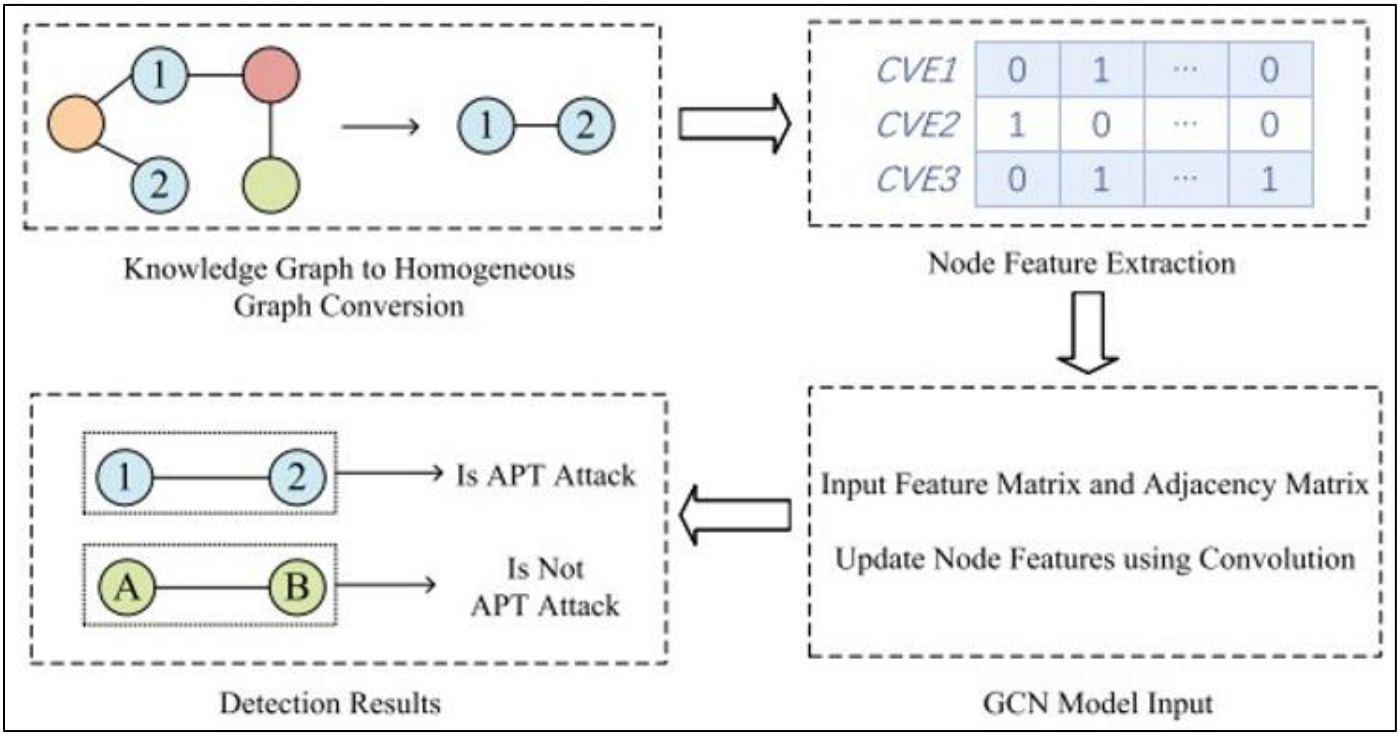

Fig 6 A Detailed Workflow of Detecting APT Attacks with GNN
Source – Ren et al (2023)

GNN is a deep learning model which is designed for effective feature learning, representing edges and nodes. Simple APT graph is used as "adjacency matrix A" and "node feature matrix X", serving as inputs to GCN model. The N*D is the feature matrix, where N refers to number of nodes, and D refers to dimension of each node. The N*N is the adjacency matrix which represents connectivity across nodes. Figure 7 illustrates the GNN model, which takes simple graph as input, performing feature extraction with CNN layers and results in final class for each node.

The feature information is sent by each red node to transform into blue nodes. Then, each node aggregates the feature details of its nearby nodes to fuse local information. After applying and aggregating "non-linear transformation (ReLU)", output turns out to represent final vector along with predicted class for node. Each CVE is treated as node with some features, covering weaknesses of CWE corresponding, type of CAPEC attack, and attack method of APT organization. Each node consists of label, which shows whether it is related to APT attack. The details of nearest

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

nodes are aggregated by GNN model with training to make consistent detection with true labels. After completing the training, findings of detection are output in test set for APT organizations.

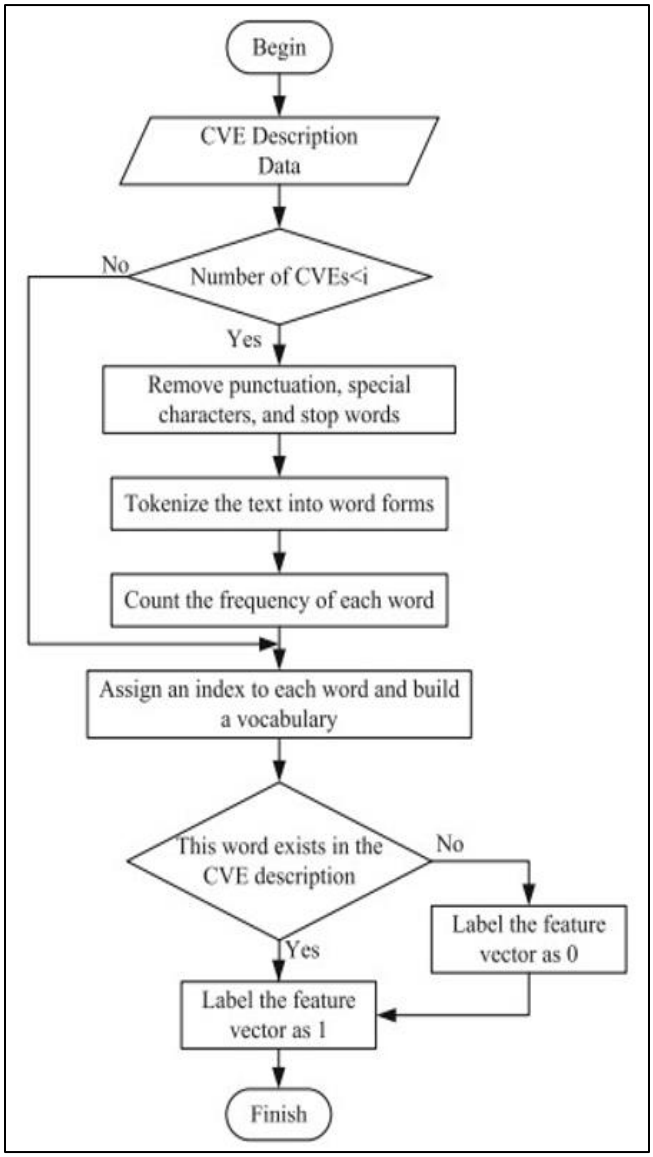

Fig 7 Flowchart of Extracting Node Feature
Source - Ren et al (2023)

➢ *Proposed Measures for Preventing and Detecting APT Attacks*

Cybersecurity systems are processes, approaches, technologies, software, and devices made for security of networks, computer systems, data, and users against threats (Sangchoolie et al, 2020). These approaches are widely used at various network layers, forming the model of security in depth (Figure 8). It represents a cybersecurity approach with layering of various security protocols to secure a network or computer system. The key here is to improve resilience over threats for making various challenges against attackers (Alsaqour et al., 2021). There are other challenges for attackers who manage to bypass one security layer.

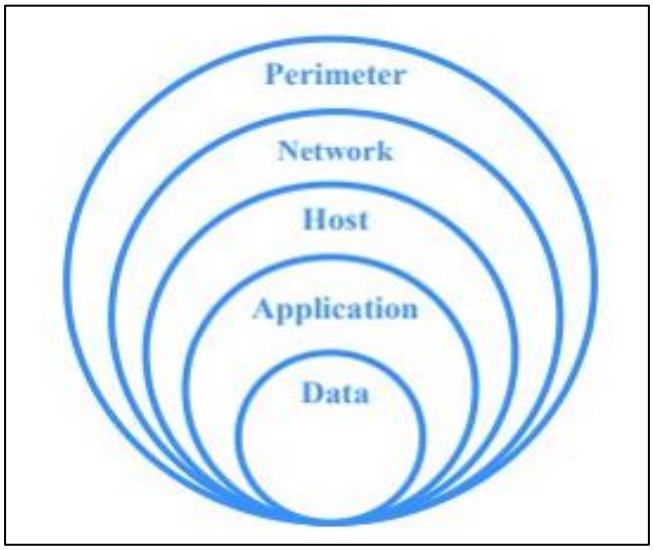

Fig 8 Layers of Security Mechanism Athmane et al (2023)

Code security and encryption are some of the approaches used in Application and Data layer, Antivirus, Firewalls, "Intrusion Detection Systems" and sensitizing Perimeter layer campaigns.

- Firewall - A firewall is a hardware or software component that can monitor and control outgoing and incoming traffic of the system or network for protecting against unwanted intrusions or threats. It plays a vital role in blocking and filtering unwanted connections, malicious codes, and cyber threats, while enabling valid traffic to go through. Overall, a firewall becomes a security challenge protecting a system or network by enabling specific rules of security for controlling data flow.
- Antimalware – This software detects, removes, and blocks malicious codes like worms, viruses, and Trojans to prevent infections. They use heuristic analysis, virus signatures, and constant updates to avoid and identify threats.
- Encryption – It protects data by turning it into unreadable format without any key. It ensures security of data even with data theft.
- IDS/IPS – "Intrusion Detection Systems (IDS)" are software or devices that can track system activities and network traffic for signatures or behaviors of threats (Jabez et al, 2015). When suspicious activity is detected by the IDS, it generates alerts to notify administrators. Usually, IDS can report and track possible intrusions without taking any action to stop attacks. On the other hand, "Intrusion Prevention System (IPS)" detects threats and can also take proactive measures to reduce or block attacks. It is possible to configure IPS to act manually or automatically responding to threats detected, making them highly proactive to protect network.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

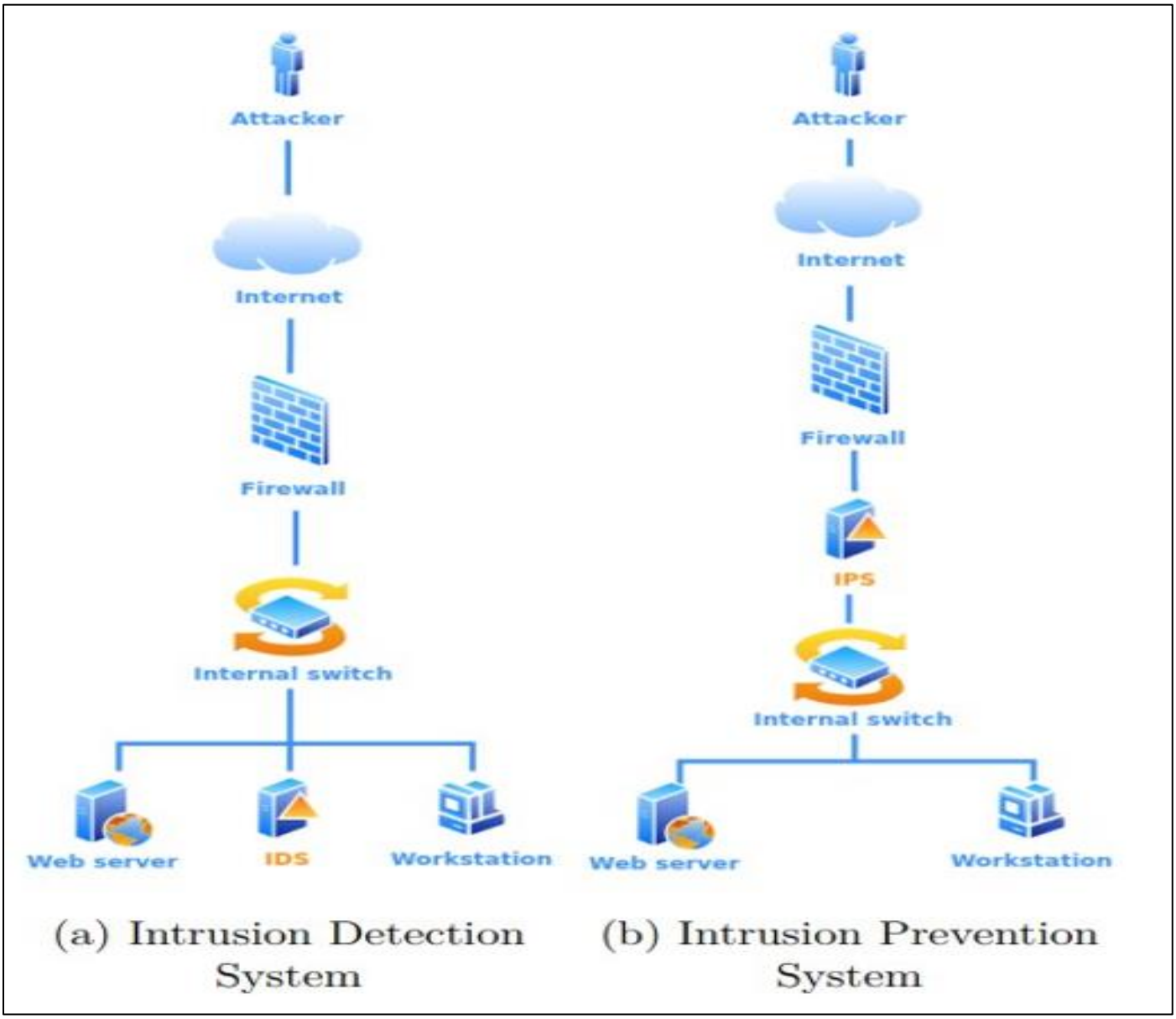

Fig 9 A Flow Diagram of IDS and IPS
Source - Athmane et al (2023)

Both IDS and IPS are cybersecurity systems that can improve security of networks. IDS acts as a vigilant spectator, system activities, and monitoring network to identify signatures or patterns related to common threats. After detecting suspicious behavior, alerts are generated by the IDS to inform admins, enabling them to respond to and investigate possible security threats. On the other hand, IDS don't stop the attacks detected. Figure 9 illustrates the difference between deploying IDS and IPS.

Meanwhile, IPS detects threats and takes ideal steps to mitigate or prevent them. IPS can manually or automatically respond to threats detected by reconfiguring rules related to firewall, malicious traffic, or adopting other actions in real-time. This way, IPS is a more dynamic aspect in cybersecurity, upsetting possible threats before they can affect network security. Though IDS plays a vital role in incidence response and monitoring, IPS acts as a proactive defense in overall security strategy in the organization. Whether an organization should use IPS or IDS depends upon their priorities and security needs. Modern approaches often use the capabilities of both IPS and IDS to ensure effective and complete defense over the threat landscape which is constantly rising. IDS are more ideal to detect anomalies and identify vulnerabilities in case of APT attacks.

V. RESULTS

Findings of the study highlighted the key progressions with GNNs in APT detection, especially in high stakes and complex environments. By treating relationships, attack patterns and vulnerabilities as interlinked edges and nodes and arranging raw data into knowledge graphs, the study provides more nuanced understanding of network behavior than previous approaches. This study proposes the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

experimental setup designed with datasets like ToN IoT and CICIDS 2017 with a complete and in-depth evaluation of effectiveness of GNN-based system relative to both graph-analytic and machine learning techniques. A GNN-based framework has been proposed for APT detection, which focuses majorly on capturing subtle patterns and complex relations in network activity data. These benchmark datasets were proposed to compare robustness, detection, and adaptability over set intrusion detection systems.

The proposed model is excellent in differentiating anomalous and benign pattern with contextual learning from graph revealing tactics, vulnerabilities, and attack vectors. Knowledge graph construction consists of attack reports, CVE details, and security databases were organized with Neo4j into triplets, which structured entities and relationships influencing propagation of vulnerability across networks. From the knowledge graph, node features were CAPEC-ID, CVE-ID, and CWE-ID, acting as input for GNNs to classify doubtful nodes. Temporal graph evolution is used to provide insights on the adaptation of APT tactics, enabling longitudinal and real-time anomaly detection ahead of static models.

A key highlight of the findings depends upon models' ability to learn from changing structure of enterprise network. Data collected from CVE reports are used in building knowledge graphs and it is enabled by attack databases and security logs to map the interrelation between methods, exploited weaknesses and vulnerabilities for APT attacks. Extracting deep node features has been supported, including types of vulnerabilities, attack patterns, and exploitation pathways to develop a robust set of features for the GNN. There is a need to integrate temporal evolution, track patterns in graph structures, lateral movements, coordinated attacks, and privilege escalation over the long term.

The GNNs have shown very high-performance metrics with experimental evaluation. As compared to shallow and static models, GNN has always achieved levels above 99% when it comes to detect different emerging and known attacks (Guttikonda, 2024). The outcomes of recall and precision have been consistently high across spatial and temporal slices, showing strong differentiation among anomalous and normal behavior, while reducing the risk of both false negatives and false positives. The framework can interpret and aggregate edge- and node-level features contributed directly to its capability to adapt to unexpected attacks.

Further comparative information was collected from the review of recent models proposed in the studies. For instance, "FedHE-graph" system was enabled with federated learning, which reduced false positives with encrypted weight sharing and training distributed model to improve privacy without affecting benefits of performance. In the same way, using Bayesian neural networks in ANUBIS framework and explainable graphs provided both actionable insights and detection accuracy for security analysis to fill the gap between loop response and automated detection. With real-time graph partitioning, alert scoring, and prioritizing automated incident, RANK architectures have shown the scalability of solutions based on GNN for large scenarios that have suggested viability for deployment.

As revealed in experiments, practical effect of APT detection based on GNN goes far beyond high accuracy. On the basis of GNNs and graph analytics, models have been used to trace smart attacks, map the risk of vulnerabilities across assets, and adopt proactive and real-time defense systems that forecast instead of reacting to adversary attacks. These models support refining context and dynamic updating with time-based graph analysis to ensure constant utility and relevance of system as threats rise up. In addition, unified implementations make way for combined protection among various bodies.

Findings of the study have also focused on various operations. Computational and integration costs have been notable, especially for smaller organizations which have lack of special infrastructure for model retraining and ingesting graphs constantly. As attackers change strategies to prevent detection, the heterogeneity of APT techniques require existing research on adaptive learning and context-based modeling to be effective. Finally, issues like transparency of the model, explainability, and human and automation loops should be refined further to integrate detection based on GNN smoothly into wider cyber defense mechanisms.

Overall, proper evaluation and deployment of GNN approaches validate their potential to improve attribution, detection, and control of smart persistent threats. Their adaptability, support, and efficiency for practical strategies set them apart as the top position for modern attack prevention with implications for policy and research in cybersecurity.

VI. CONCLUSION

This study strongly proposes GNN-derived models which are helpful in detecting APT attacks in enterprise networks, providing advanced solutions to long-term cyber threats. With representative power of deep learning and graph structures, the model captures attacks and relationships more than traditional machine learning models. GNN models constantly performed better than traditional anomaly detection models when it comes to precision, accuracy, and adaptability. Analyzing temporal graph promotes rapid response to rising APT risks and updated intelligence. Architectures like federated GNNs and ANUBIS have delivered explainable, scalable predictions which are needed for practical cybersecurity operations in large organizations and critical infrastructure.

- *Implications*

Adopting GNN approaches is known to define the next generation for APT detection for cybersecurity in organizations. Integrating antimalware, firewalls, GNN-based AI, and IDS/IPS and other defense strategies improve resilience and promote defense with minimal operational

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

risk. Prioritization systems and automated alerting improve incident response time, minimizing loss and impact of breaches. Technologies related to knowledge graph attribution improves law enforcement, strategic countermeasures, compliance, and enhance tracking of attack sources.

➢ *Future Research Directions*

The study is based on various promising avenues for future studies. Reducing false alarms and generalizability may be improved with further advancements in extracting context from unstructured behavioral indicators and threat intelligence. Distributed frameworks and light GNN architectures may be explored to expand the accessibility ahead of resource-based organizations. Improved techniques to preserve privacy and federated learning will help in sharing threat intelligence across organizations for combined, stronger cyber security. Human analysts can constantly work on interpretable models in decision-making and trust-building, especially in novel or ambiguous scenarios.

The ability to evolve rapidly as per emerging APT threats have wider implications for global law, governance, and information policy. As APTs target financial, government, and critical infrastructure, strong collaborations are needed between policymakers, stakeholders, and research for building ethical, resilient, and effective standards for cybersecurity. Overall, deploying GNN solutions marks a strong change in mitigating and detecting APTs in enterprise networks. When adopted in multilayered strategies, these models furnish organizations with both abilities to learn, proactively respond, and adapt to changing threats and with detection power. This study offers the foundation for innovation at the connection between cybersecurity, enterprise risk management, and graph learning for both researchers and practitioners.

REFERENCES

[1]. Iniewski, K., McCrosky, C., & Minoli, D. (2008). *Network infrastructure and architecture: designing high-availability networks*. John Wiley & Sons.

[2]. Yasar, K. and Linda R. (2023). *What is an advanced persistent threat (APT)?* TechTarget. Available at https://www.techtarget.com/searchsecurity/definition /advanced-persistent-threat- APT.

[3]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851-1877.

[4]. Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016, March). Advanced persistent threats: Behind the scenes. In *2016 Annual Conference on Information Science and Systems (CISS)* (pp. 181-186). IEEE.

[5]. Vukalović, J., & Delija, D. (2015, May). Advanced persistent threats-detection and defense. In *2015 38Th international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 1324-1330). IEEE.

[6]. Quintero-Bonilla, S., & Martín del Rey, A. (2020). A new proposal on the advanced persistent threat: A survey. *Applied Sciences*, *10*(11), 3874.

[7]. Liu, Z., & Zhou, J. (2022). *Introduction to graph neural networks*. Springer Nature.

[8]. Athmane, M. M. B., Soaïd, M. F. K., Hamida, M. S., Mohamed, M. M., & Karima, M. A. (2023). Building a novel Graph Neural Networks-based model for efficient detection of Advanced Persistent Threats.

[9]. Friji, H. (2024). *Graph neural network-based intrusion detection for secure edge networks*. Computer science. Institut Polytechnique de Paris, 2024. English.

[10]. Peng, Z. H., Hu, C. Z., & Shan, C. (2025). Anomaly Detection for Advanced Persistent Threats with Graph Node Embedding. *Journal of Information Science & Engineering*, *41*(3). Ren, Y., Xiao, Y., Zhou, Y., Zhang, Z., & Tian, Z. (2022). CSKG4APT: A cybersecurity knowledge graph for advanced persistent threat organization attribution. *IEEE Transactions on Knowledge and Data Engineering*, *35*(6), 5695-5709.

[11]. Ren, W., Song, X., Hong, Y., Lei, Y., Yao, J., Du, Y., & Li, W. (2023). APT attack detection based on graph convolutional neural networks. *International Journal of Computational Intelligence Systems*, *16*(1), 184.

[12]. Guo, Z., Li, X., Shen, H., Zhang, X., Wang, W., & Xie, D. (2025, January). Detecting advanced persistent threats via casual graph neural network. In *Fourth International Conference on Network Communication and Information Security (ICNCIS 2024)* (Vol. 13516, pp. 273-279). SPIE.

[13]. Gowthami, G., Sadhana, C., Silvia Priscila, S., Radhakrishnan, S., SakthiVanitha, M., & Kannan, B. (2024, October). Enhancing Enterprise Network Security with Machine Learning: An In-Depth Analysis of Advanced Persistent Threat Detection. In *International Conference on Computing and Communication Networks* (pp. 525-537). Singapore: Springer Nature Singapore.

[14]. Anjum, M. M., Iqbal, S., & Hamelin, B. (2022, April). ANUBIS: a provenance graph-based framework for advanced persistent threat detection. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing* (pp. 1684-1693).

[15]. Mansour Bahar, A. A., Ferrahi, K. S., Messai, M. L., Seba, H., & Amrouche, K. (2024, July). FedHE-graph: federated learning with hybrid encryption on graph neural networks for advanced persistent threat detection. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-10).

[16]. Soliman, H. M., Sovilj, D., Salmon, G., Rao, M., & Mayya, N. (2023). Rank: Ai-assisted end- to-end architecture for detecting persistent attacks in enterprise networks. *IEEE Transactions on Dependable and Secure Computing*, *21*(4), 3834-3850.

[17]. Guttikonda, B. (2024). *Adaptive Detection of*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct435

Advanced Persistent Threats (APT) in Multi-Layered Network Environments (Doctoral dissertation, Dublin, National College of Ireland).
Wei, R., Cai, L., Zhao, L., Yu, A., & Meng, D. (2021, September). Deephunter: A graph neural network-based approach for robust cyber threat hunting. In *International Conference on Security and Privacy in Communication Systems* (pp. 3-24). Cham: Springer International Publishing.

[18]. VMware (2019). What is Advanced Persistent Threat (APT)? Available at https://www.broadcom.com/topics/advanced-persistent-threats

[19]. Google (2024). Tool of First Resort, Israel-Hamas War in Cyber. Available at https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

[20]. Athmane, M. M. B., Soaïd, M. F. K., Hamida, M. S., Mohamed, M. M., & Karima, M. A. (2023). Building a novel Graph Neural Networks-based model for efficient detection of Advanced Persistent Threats.

[21]. Sangchoolie, B., Folkesson, P., Kleberger, P., & Vinter, J. (2020, June). Analysis of cybersecurity mechanisms with respect to dependability and security attributes. In *2020 50th*

[22]. *Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)* (pp. 94-101). IEEE.

[23]. Alsaqour, R., Majrashi, A., Alreedi, M., Alomar, K., & Abdelhaq, M. (2021). Defense in Depth: Multilayer of security. *International Journal of Communication Networks and Information Security*, *13*(2), 242-248.

[24]. Jabez, J., & Muthukumar, B. J. P. C. S. (2015). Intrusion Detection System (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science*, *48*, 338-346