Chapter 27
Next-Generation Defence on Innovations in Data-Driven Cyber Security for Threat Detection and Mitigation

T. Sharath
https://orcid.org/0009-0009-5509-9881
Bharath Institute of Higher Education and Research, India

A. Muthukumaravel
Bharath Institute of Higher Education and Research, India

ABSTRACT

Within the current digital landscape, the issue of cybersecurity remains a prominent and urgent matter. The ever-evolving cyber threats pose significant risks to organizations across the globe. In cybersecurity, conventional methods frequently find themselves grappling to keep up with the ever-changing landscape of threats, resulting in potential weaknesses and breaches. A new approach called dynamic threat profiling using graph neural networks (GNNs) is proposed to tackle this challenge. One major issue is the lack of effectiveness in current cybersecurity methods when identifying and addressing emerging threats. GNNs provide a solution by utilizing cutting-edge machine learning methods to analyze real-time network data. They create dynamic graphs that capture the intricate connections between network entities. By extracting features and identifying anomalies within these graphs, GNNs facilitate threat detection and respond to it, thereby mitigating the consequences of cyber attacks.

INTRODUCTION

In the modern era, the issue of cybersecurity has gained significant importance for individuals and organizations (Kuragayala et al., 2023). Recent statistics indicate that the global economy risks losing over a trillion dollars annually due to cybercrime. Shockingly, cyber-attacks target businesses every 39 seconds (Gade and Reddy Reddy, 2014). These statistics highlight the pressing requirement for strong defence mechanisms to protect against cyber threats and minimize their consequences. In cybersecurity,

DOI: 10.4018/979-8-3693-9375-8.ch027

conventional methods often face difficulties adapting to the ever-evolving threat landscape (Uddin and Kazi, 2013). Insufficient defence mechanisms can leave organizations vulnerable to cyber attackers who can exploit these weaknesses (Tambaip et al., 2023). Current cybersecurity methods are inadequate in detecting and addressing emerging cyber threats, thereby leaving organizations susceptible to breaches and attacks (Rallang et al., 2023). Developing creative solutions that can respond to the ever-changing landscape of threats effectively and offer proactive defence mechanisms is crucial (Panda et al., 2011). In cybersecurity, the predominant approach is to use signature-based detection systems. However, these systems are limited when identifying new threats or zero-day attacks (Aljanabi et al., 2021). In addition, rule-based approaches can result in many false positives, which can overwhelm cybersecurity analysts and contribute to alert fatigue (Vinayakumar et al., 2019). These limitations underscore the necessity of a fundamental change in cybersecurity defence strategies towards approaches that are more adaptive and intelligent (Mankame et al., 2023).

Within the cybersecurity domain, many attacks present substantial risks to individuals, organizations, and entire networks (Singh et al., 2023). A comprehensive understanding of these attack vectors is paramount when implementing effective defence mechanisms (Ahsan et al., 2022). Common cyber attacks, also called normal attacks, take advantage of software or system vulnerabilities that have been previously identified and can be addressed with patches or security measures (Das et al., 2023). Various types of cyber attacks are prevalent, such as malware infections, phishing scams, and SQL injections (Das et al., 2015). Although they can be anticipated and reduced with proactive security measures, they still present a significant danger if not properly handled. Zero-day exploits are considered to be one of the most critical cybersecurity threats (Kasongo and Sun, 2020). These attacks focus on exploiting weaknesses in software or systems that developers or vendors are unaware of, leaving little time for implementing defences or patching before the exploit is utilized (Anand et al., 2023). Zero-day exploits can have severe repercussions like data breaches, system compromises, and unauthorized access (Kaur et al., 2023). Executing malicious scripts into web pages can result in various security risks, such as session hijacking, data theft, and unauthorized actions (Khemani et al., 2024). DDoS attacks aim to inundate a target by increasing traffic, causing it to become inaccessible to real users. These attacks can disrupt services, result in financial losses, and damage reputations (Viet and Saputra, 2020).

Denial of Service (DoS) attacks and DDoS attacks share similarities in their approach, as they both involve overwhelming a target system or network with excessive traffic. However, unlike DDoS attacks, which utilize multiple sources, DoS attacks rely on a single source to carry out the flooding (Chukhnov and Ivanov, 2021). The objective remains unchanged: to disrupt services and render resources inaccessible to authorized users (Thinesh et al., 2023). Without the target party's knowledge or approval, a third party can secretly intercept and modify their communications in a Man-in-the-Middle (MitM) attack. By exploiting this vulnerability, an unauthorized individual can secretly monitor confidential data, tamper with information, or introduce harmful elements into the system. Password attacks involve the deliberate and systematic endeavour to guess or crack passwords to gain unauthorized access to systems, accounts, or data (Li and Liu, 2021). These attacks can potentially exploit passwords, such as weak passwords, commonly used dictionary words, or easily recognizable patterns (Vinu et al., 2023). As a result, they can compromise credentials and breach security defences. Overall, different types of cyber attacks present distinct challenges and threats to cybersecurity (Adekola et al., 2024). Through a comprehensive understanding of various attack vectors and the implementation of effective defence strategies, individuals and organizations can significantly enhance their ability to safeguard against