

## Detecting Cyber Threats With a Graph-Based NIDPS

Brendan Ooi Tze Wen, Najihah Syahriza, Nicholas Chan Wei Xian, Nicki Gan Wei, Tan Zheng Shen, Yap Zhe Hin, Siva Raja Sindiramutty, Teah Yi Fan Nicole

Source Title: Cybersecurity Measures for Logistics Industry Framework (/book/cybersecurity-measures-logistics-industry-framework/308981)

Copyright: © 2024


Pages: 39

DOI: 10.4018/978-1-6684-7625-3.ch002

**OnDemand:**  
(Individual Chapters)

**\$18.75**

List Price: ~~\$37.50~~

 Available

[Current Special Offers](#)



### Abstract

This chapter explores the topic of a novel network-based intrusion detection system (NIDPS) that utilises the concept of graph theory to detect and prevent incoming threats. With technology progressing at a rapid rate, the number of cyber threats will also increase accordingly. Thus, the demand for better network security through NIDPS is needed to protect data contained in networks. The primary objective of this chapter is to explore the concept of a novel graph based NIDPS through four different aspects: data collection, analysis engine, preventive action, and reporting. Besides analysing existing NIDS technologies in the market, various research papers and journals were explored. The authors' solution covers the basic structure of an intrusion detection system, from collecting and processing data to generating alerts and reports. Data collection explores various methods like packet-based, flow-based, and log-based collections in terms of scale and viability.

### Chapter Preview

Top

### Introduction

According to Kumar, Gupta, and Arora (2021) and Sulaiman et. al. (2021), an intrusion detection system abbreviated as IDS, is software that can detect unauthorised traffic or entry into a host or network by detecting unusual behaviours or by examining multiple data streams within the host or network processes. The demand for sophisticated IDSs is necessary in the 21st century due to rapid advancements in the field of Internet of Things (IoT) with more devices than ever being connected to the Internet. Such advancements have also encouraged the wide-spread use of cloud technologies, which may be storing confidential or sensitive user data (Sulaiman et al., 2021). The move to cloud technologies have caused these services to be prone to cyber-attacks from malicious users resulting in data breaches, Distributed Denial of Services (DDoS), compromised communication between senders and receivers among other issues (Kumar, Gupta and Arora, 2021; Ponnusamy, Humayun, et al., 2022). Before the discovery and deployment of the IDS, other steps have been taken to overcome the vulnerabilities such as the implementation of more secure internet protocols. HyperText Transfer Protocol Secure (HTTPS) and Secure Socket Layer (SSL) were among the protocols introduced as well as Firewalls and various cryptography techniques to further secure these spaces. Figure 1.0 provides an overview of the types, detection mechanisms and techniques used in various types of IDS.

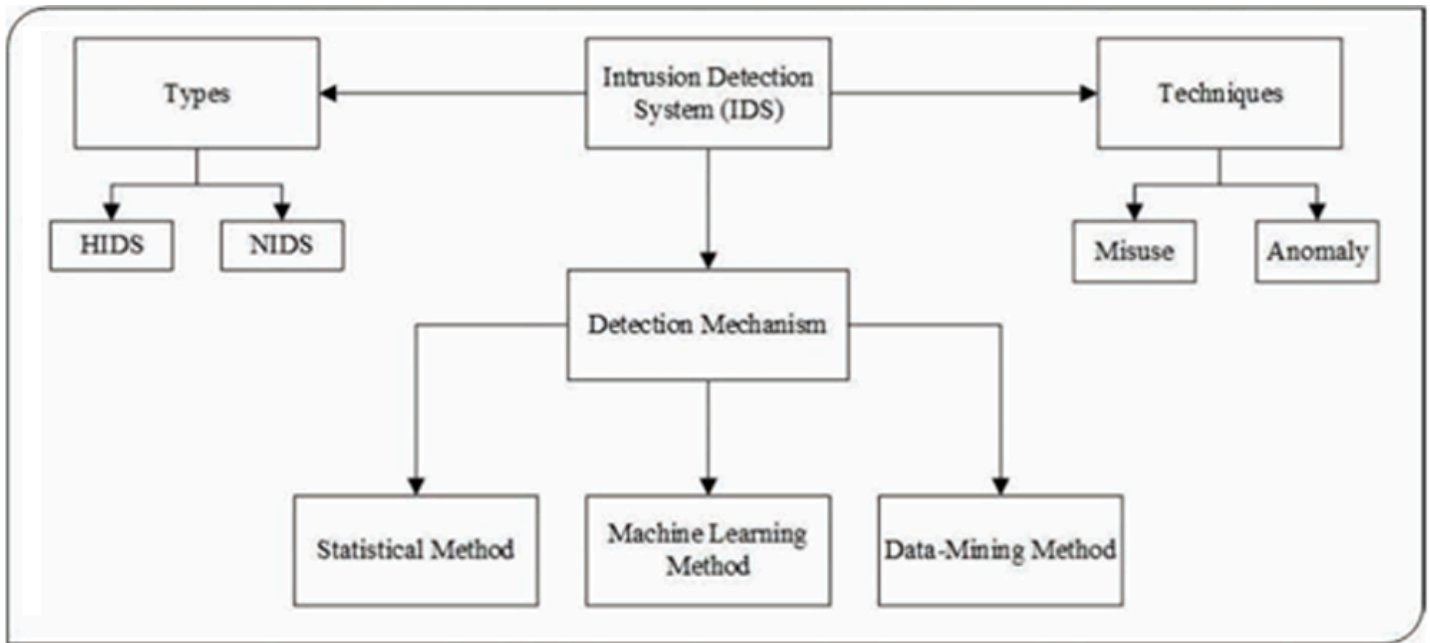
Figure 1. Overview of IDS

([https://igiprodst.blob.core.windows.net/443/source-content/9781668476253\\_308981/978-1-6684-7625-3.ch002.f01.png?sv=2015-12-11&sr=c&sig=aAhrus0EZTHry7hxusqJ3XEqRDIKfBBzgu6MBp3%2F0i0%3D&se=2024-03-16T15%3A41%3A58Z&sp=r](https://igiprodst.blob.core.windows.net/443/source-content/9781668476253_308981/978-1-6684-7625-3.ch002.f01.png?sv=2015-12-11&sr=c&sig=aAhrus0EZTHry7hxusqJ3XEqRDIKfBBzgu6MBp3%2F0i0%3D&se=2024-03-16T15%3A41%3A58Z&sp=r))

Source: Aljanabi, Ismail, and Ali (2021)

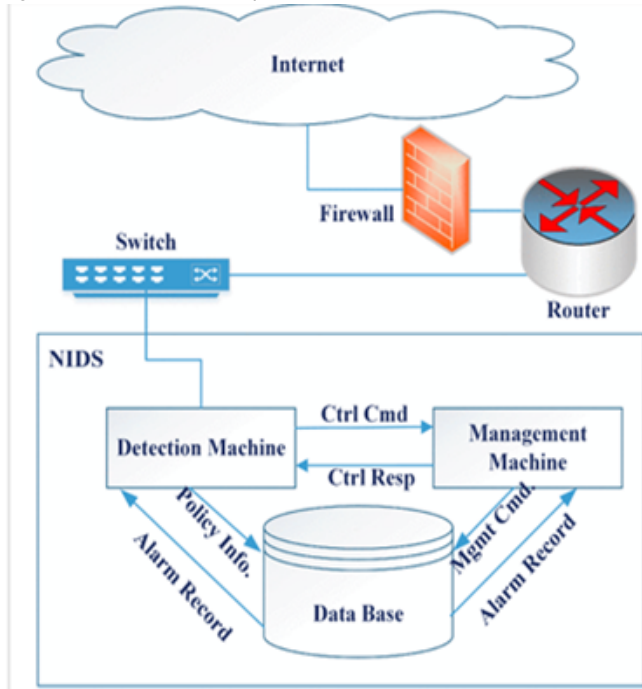
### Definition and Importance of IDS and NIDS

Among the common detection mechanisms that are employed on Intrusion Detection Systems are rule-based detection and statistical-based detection (Adnan et. al, 2021). Rule-based detection also known as knowledge-based detection is where an administrator or a super-user would define set parameters also known as rules for normal use. When a user who may be a regular user or intruder performs an action or activity that is not within the



defined parameters, an alert will be sounded, and countermeasures will take place. Such systems could also be trained using datasets that contain information on normal activities or actions, an intrusion into the system will then be detected when an action outside of the training model is performed (Aljanabi, Ismail, and Ali, 2021; Ponnusamy, Aun, et al., 2022). Another detection mechanism that is commonly employed is statistical-based detection. Statistical-based detection is where an IDS would compare the traffic of a system with a general model of defined or known normal usage patterns. The IDS would know an attack is taking place when the difference between the reported model and general model is sufficiently large (Adnan et. al., 2021; Annadurai et al., 2022). Another example of how statistical models work would be through the application of multiple mathematical models or techniques and specialist structures to create the profile of a normal user through the analysis of the collected data. An attack profile will be put together for actions that do not match the profile of a normal user. The primary goal of a Network Based IDS or Network Intrusion Detection System (NIDS) is to identify and log information as well as report the abnormality to the network admin (Kumar, Gupta and Arora, 2021; Seong et al., 2021). Figure 2.0 shows the components of a NIDS:

Figure 2. NIDS with its components



([https://igiprodst.blob.core.windows.net:443/source-content/9781668476253\\_308981/978-1-6684-7625-3.ch002.f02.png?sv=2015-12-](https://igiprodst.blob.core.windows.net:443/source-content/9781668476253_308981/978-1-6684-7625-3.ch002.f02.png?sv=2015-12-)

11&sr=c&sig=aAhrus0EZTHry7hxusqJ3XEqRDlKfBBzgu6MBp3%2F0i0%3D&se=2024-03-16T15%3A41%3A58Z&sp=r)  
 Source: Kumar, Gupta, and Arora (2021)

Among the logical components in a NIDS would be a detection machine, management machine and database. The detection machine is responsible for running the detection software which detects abnormalities within the data stream. The management machine is responsible for managing the detection algorithms and strategies. The database component in a NIDS is used for general data logging, to keep track of abnormalities as well as normal data. To maximise the efficiency of the NIDS, it is usually installed at switches and routers within a network to screen data packets and user traffic.

# Complete Chapter List

Search this Book:

[Reset](#)

## Table of Contents

[View Full PDF \(/pdf.aspx?tid=339242&ptid=308981&ctid=15&t=Table of Contents&isxn=9781668476253\)](#)

## Detailed Table of Contents

[View Full PDF \(/pdf.aspx?tid=339243&ptid=308981&ctid=15&t=Detailed Table of Contents&isxn=9781668476253\)](#)

## Preface

Noor Zaman Jhanjhi, Imdad Ali Shah

[View Full PDF \(/pdf.aspx?tid=339244&ptid=308981&ctid=15&t=Preface&isxn=9781668476253\)](#)

## Chapter 1

Risk Management and Cybersecurity in Transportation and Warehousing (/chapter/risk-management-and-cybersecurity-in-transportation-and-warehousing/339245) (pages 1-35)

Azeem Khan, Noor Zaman Jhanjhi, Haji Abdul Hafidz B. Haji Omar, Dayang Hajah Tiawa B. Awang Haji Hamid

[Preview Chapter \(/viewtitlesample.aspx?id=339245&ptid=308981&t=Risk Management and Cybersecurity in Transportation and Warehousing&isxn=9781668476253\)](#) **\$37.50** [Add to Cart](#)

## Chapter 2

Detecting Cyber Threats With a Graph-Based NIDPS (/chapter/detecting-cyber-threats-with-a-graph-based-nidps/339246) (pages 36-74)

Brendan Ooi Tze Wen, Najihah Syahriza, Nicholas Chan Wei Xian, Nicki Gan Wei, Tan Zheng Shen, Yap Zhe Hin, Siva Raja Sindiramutty, Teah Yi Fan Nicole

[Preview Chapter \(/viewtitlesample.aspx?id=339246&ptid=308981&t=Detecting Cyber Threats With a Graph-Based NIDPS&isxn=9781668476253\)](#) **\$37.50** [Add to Cart](#)

## Chapter 3

A Distributed Model for IoT Anomaly Detection Using Federated Learning (/chapter/a-distributed-model-for-iot-anomaly-detection-using-federated-learning/339247) (pages 75-91)

Sidra Tahir, Anam Zaheer

[Preview Chapter \(/viewtitlesample.aspx?id=339247&ptid=308981&t=A Distributed Model for IoT Anomaly Detection Using Federated Learning&isxn=9781668476253\)](#) **\$37.50** [Add to Cart](#)

## Chapter 4

Network Intrusion Detection to Mitigate Jamming and Spoofing Attacks Using Federated Leading: A Comprehensive Survey (/chapter/network-intrusion-detection-to-mitigate-jamming-and-spoofing-attacks-using-federated-leading/339248) (pages 92-115)

Tayyab Rehman, Noshina Tariq, Muhammad Ashraf, Mamoona Humayun

[Preview Chapter \(/viewtitlesample.aspx?id=339248&ptid=308981&t=Network Intrusion Detection to Mitigate Jamming and Spoofing Attacks Using Federated Leading: A Comprehensive Survey&isxn=9781668476253\)](#) **\$37.50** [Add to Cart](#)

**Chapter 5**

IoT Security, Future Challenges, and Open Issues (/chapter/iot-security-future-challenges-and-open-issues/339249) (pages 116-140)

Noshina Tariq, Tehreem Saboor, Muhammad Ashraf, Rawish Butt, Masooma Anwar, Mamoona Humayun

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339249&ptid=308981&t=IoT Security, Future Challenges, and Open Issues&isxn=9781668476253) [Add to Cart](#)

**Chapter 6**

Enhancing Identification of IoT Anomalies in Smart Homes Using Secure Blockchain Technology (/chapter/enhancing-identification-of-iot-anomalies-in-smart-homes-using-secure-blockchain-technology/339250) (pages 141-155)

Sidra Tahir

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339250&ptid=308981&t=Enhancing Identification of IoT Anomalies in Smart Homes Using Secure Blockchain Technology&isxn=9781668476253) [Add to Cart](#)

**Chapter 7**

Securing the Digital Supply Chain Cyber Threats and Vulnerabilities (/chapter/securing-the-digital-supply-chain-cyber-threats-and-vulnerabilities/339251) (pages 156-223)

Siva Raja Sindiramutty, Noor Zaman Jhanjhi, Chong Eng Tan, Navid Ali Khan, Bhavin Shah, Loveleen Gaur

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339251&ptid=308981&t=Securing the Digital Supply Chain Cyber Threats and Vulnerabilities&isxn=9781668476253) [Add to Cart](#)

**Chapter 8**

Internet of Things (IoT) Impact on Inventory Management: A Review (/chapter/internet-of-things-iot-impact-on-inventory-management/339252) (pages 224-247)

Azeem Khan, Noor Zaman Jhanjhi, Dayang Hajah Tiawa Binte Awang Haji Hamid, Haji Abdul Hafidz B. Haji Omar

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339252&ptid=308981&t=Internet of Things (IoT) Impact on Inventory Management: A Review&isxn=9781668476253) [Add to Cart](#)

**Chapter 9**

Applications of Blockchain Technology in Supply Chain Management (/chapter/applications-of-blockchain-technology-in-supply-chain-management/339253) (pages 248-304)

Siva Raja Sindiramutty, Noor Zaman Jhanjhi, Chong Eng Tan, Navid Ali Khan, Abdalla Hassan Gharib, Khor Jia Yun

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339253&ptid=308981&t=Applications of Blockchain Technology in Supply Chain Management&isxn=9781668476253) [Add to Cart](#)

**Chapter 10**

The Internet of Things (IoT) Applications in Inventory Management Through Supply Chain (/chapter/the-internet-of-things-iot-applications-in-inventory-management-through-supply-chain/339254) (pages 305-321)

Yesim Deniz Ozkan-Ozen

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339254&ptid=308981&t=The Internet of Things (IoT) Applications in Inventory Management Through Supply Chain&isxn=9781668476253) [Add to Cart](#)

Chapter 11

QR Multilevel Codes to Reduce Cybersecurity Risks in the Logistics of Freight Transport in Ports (/chapter/qr-multilevel-codes-to-reduce-cybersecurity-risks-in-the-logistics-of-freight-transport-in-ports/339255) (pages 322-349)

Gerardo Reyes Ruiz

Preview Chapter **\$37.50**

(/viewtitlesample.aspx?id=339255&ptid=308981&t=QR Multilevel Codes to Reduce Cybersecurity Risks in the Logistics of Freight Transport in Ports&isxn=9781668476253) Add to Cart

About the Contributors

View Full PDF (/pdf.aspx?tid=339257&ptid=308981&ctid=17&t=About the Contributors&isxn=9781668476253)

Index

View Full PDF (/pdf.aspx?tid=339258&ptid=308981&ctid=17&t=Index&isxn=9781668476253)

Learn More

About IGI Global (/about/) | Partnerships (/about/partnerships/) | COPE Membership (/about/memberships/cope/) | Contact Us (/contact/) | Job Opportunities (/about/staff/job-opportunities/) | FAQ (/faq/) | Management Team (/about/staff/)

Resources For

Librarians (/librarians/) | Authors/Editors (/publish/) | Distributors (/distributors/) | Instructors (/course-adoption/) | Translators (/about/rights-permissions/translation-rights/)

Media Center

Webinars (/symposium/) | Blogs (/newsroom/) | Catalogs (/catalogs/) | Newsletters (/newsletters/)

Policies

Privacy Policy (/about/rights-permissions/privacy-policy/) | Cookie & Tracking Notice (/cookies-agreement/) | Fair Use Policy (/about/rights-permissions/content-reuse/) | Accessibility (/accessibility/) | Ethics and Malpractice (/about/rights-permissions/ethics-malpractice/) | Rights & Permissions (/about/rights-permissions/)

(http://www.facebook.com/pages/IGI-Global/138206739534176?ref=sgm)

(http://twitter.com/igiglobal)

(https://www.linkedin.com/company/igi-global) (http://www.igi-global.org) (http://www.igi-global.org) (http://www.igi-global.org) (http://www.igi-global.org)

(https://publicationethics.org/category/publisher/igi-global)

