Utilizing Generative AI for Cyber Defense Strategies

Noor Zaman Jhanjhi (/affiliate/noor-zaman-jhanjhi/415447/)

Release Date: September, 2024

Pages: 546
DOI: 10.4018/979-8-3693-8944-7
ISBN13: 9798369389447
ISBN13 Softcover: 9798369389454
EISBN13: 9798369389461

Hardcover: $382.50
List Price: ~~$425.00~~
(/bookaltbizing-generative-cyber-defense-strategies/353340?f=hardcover&i=1)
Benefits & Incentives

E-Book: $382.50
List Price: ~~$425.00~~
(/bookaltbizing-generative-cyber-defense-strategies/353340?f=e-book&i=1)
Benefits & Incentives

Hardcover + E-Book: $459.00
List Price: ~~$510.00~~
(/bookaltbizing-generative-cyber-defense-strategies/353340?f=hardcover-e-book&i=1)
Benefits & Incentives

Softcover: $288.00
List Price: ~~$320.00~~
(/bookaltbizing-generative-cyber-defense-strategies/353340?f=softcover&i=1)
Benefits & Incentives

OnDemand:
(Individual Chapters) $33.75
List Price: ~~$37.50~~
(/bookaltbizing-generative-cyber-defense-strategies/353340#table-of-contents)
Benefits & Incentives

Description & Coverage

Description:

As cyber threats become increasingly sophisticated, the need for innovative defense strategies becomes urgent. Generative artificial intelligence (AI) offers a revolutionary approach to enhance cybersecurity. By utilizing advanced algorithms, data analysis, and machine learning, generative AI can simulate complex attack scenarios, identify vulnerabilities, and develop proactive defense mechanisms while adapting to modern-day cyber-attacks. AI strengthens current organizational security while offering quick, effective responses to emerging threats. Decisive strategies are needed to integrate generative AI into businesses defense strategies and protect organizations from attacks, secure digital data, and ensure safe business processes.

Utilizing Generative AI for Cyber Defense Strategies explores the utilization of generative AI tools in organizational cyber security and defense. Strategies for effective threat detection and mitigation are presented, with an emphasis on deep learning, artificial intelligence, and Internet of Things (IoT) technology. This book covers topics such as cyber security, threat intelligence, and behavior analysis, and is a useful resource for computer engineers, security professionals, business owners, government officials, data analysts, academicians, scientists, and researchers.

Coverage:

The many academic areas covered in this publication include, but are not limited to:

- Anomaly Detection
- Authentication Technologies
- Behavior Analysis
- Cyber Security
- Data Analytics
- Deep Learning
- Defense Strategies

- Federated Learning
- Generative AI
- Information Sharing
- Internet of Things (IoT)
- Malware
- Risk Assessment and Mitigation
- Threat Intelligence
- Variational Autoencoders (VAEs)

Table of Contents

Search this Book: Full text search terms

Reset

Chapter 6

Generative AI for Threat Intelligence and Information Sharing (/chapter/generative-ai-for-threat-intelligence-and-information-sharing/356582) (pages 191-234)

Siva Raja Sindiramutty, Krishna Raj V. Prabagaran, N. Z. Jhanjhi, Raja Kumar Murugesan, Sarfraz Nawaz Brohi, Goh Wei Wei

Collaboration in providing threat intelligence and disseminating information enables cyber security professionals to embrace digital security most...

Preview Chapter (/viewtitlesample.aspx?id=356582&ptid=353340&t=Generative AI for Threat Intelligence and Information Sharing&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 7

Generative AI for Threat Hunting and Behaviour Analysis (/chapter/generative-ai-for-threat-hunting-and-behaviour-analysis/356583) (pages 235-286)

Siva Raja Sindiramutty, N. Z. Jhanjhi, Rehan Akbar, Manzoor Hussain, Sayan Kumar Ray, Fathi Amsaad

Cyber threats are becoming more advanced, and so is cybersecurity, which is getting more intellectual and better at hiding its presence. The requirement to...

Preview Chapter (/viewtitlesample.aspx?id=356583&ptid=353340&t=Generative AI for Threat Hunting and Behaviour Analysis&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 8

A Methodical Approach to Exploiting Vulnerabilities and Countermeasures Using AI (/chapter/a-methodical-approach-to-exploiting-vulnerabilities-and-countermeasures-using-ai/356584) (pages 287-308)

Basheer Riskhan, Md Amin Ullah Sheikh, Md Shakil Hossain, Khalid Hussain, Manzoor Hussain

The present research explores a methodical approach to vulnerability exploits and countermeasure implementation. Threat modeling for proactive risk...

Preview Chapter (/viewtitlesample.aspx?id=356584&ptid=353340&t=A Methodical Approach to Exploiting Vulnerabilities and Countermeasures Using AI&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 9

Variational Autoencoders (VAEs) for Anomaly Detection (/chapter/variational-autoencoders-vaes-for-anomaly-detection/356585) (pages 309-326)

Sidra Tahir

In the present era of the internet, there is a growing abundance of tools and techniques that can be employed to target and breach private networks. Anomaly...

Preview Chapter (/viewtitlesample.aspx?id=356585&ptid=353340&t=Variational Autoencoders (VAEs) for Anomaly Detection&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 10

A Novel Approach for Intrusion Detection System Using Deep Learning Architecture (/chapter/a-novel-approach-for-intrusion-detection-system-using-deep-learning-architecture/356586) (pages 327-344)

C. U. Om Kumar, Nitika Sinha, M. Suguna, G. Sudhakaran, Nirbhay Kumar Chaubey

In recent years, network security has become increasingly complex due to rapid advancements in information and communication technologies. This complexity...

Preview Chapter (/viewtitlesample.aspx?id=356586&ptid=353340&t=A Novel Approach for Intrusion Detection System Using Deep Learning Architecture&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 11

A New Approach for Detecting Malware Using a Convolutional Autoencoder With Kernel Density Estimation (/chapter/a-new-approach-for-detecting-malware-using-a-convolutional-autoencoder-with-kernel-density-estimation/356587) (pages 345-362)

C. U. Om Kumar, K. H. Nihal Mubeen, R. Krithiga, G. Sudhakaran, Nirbhay Kumar Chaubey

The increasing use of the internet and digital devices has led to an exponential growth in cyber-attacks, with malware being one of the most prevalent forms...

Preview Chapter (/viewtitlesample.aspx?id=356587&ptid=353340&t=A New Approach for Detecting Malware Using a Convolutional Autoencoder With Kernel Density Estimation&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 12

Scouting the Juncture of Internet of Things (IoT), Deep Learning, and Cybercrime: Powering Legal Perspectives on Advanced Data Analytics (/chapter/scouting-the-juncture-of-internet-of-things-iot-deep-learning-and-cybercrime/356588) (pages 363-398)

Bhupinder Singh, Christian Kaunert

The internet of things (IoT) and deep learning technologies has revolutionized the cyber-crimes investigation which providing law enforcement with...

Preview Chapter (/viewtitlesample.aspx?id=356588&ptid=353340&t=Scouting the Juncture of Internet of Things (IoT), Deep Learning, and Cybercrime: Powering Legal Perspectives on Advanced Data Analytics&isxn=9798369389447)

Download This Chapter

$37.50

Add to Cart

Chapter 13

Muscles of Deep Learning (DL) and Internet of Things (IoT) in Cyber Crimes Investigation: Legal Dimensions in Space-Age Data

Preview Chapter (/viewtitlesample.aspx?

Download This Chapter

Analytics (/chapter/muscles-of-deep-learning-dl-and-internet-of-things-iot-in-cyber-crimes-investigation/356589) (pages 399-420)

Bhupinder Singh, Christian Kaunert, Rishabha Malviya

Deep learning (DL) and internet of things (IoT) technologies have completely changed the investigation of cybercrimes via bringing with them innovative...

Chapter 14

Safeguarding the Future: Advancements in Cybersecurity via Generative AI (/chapter/safeguarding-the-future/356590) (pages 421-432)

Jimmy Singla

The utilization of generative artificial intelligence (AI) techniques offers a viable approach to improving defense measures and protecting digital assets in...

About the Contributors

Index

Editor/Author Biographies

Noor Zaman Jhanjhi (N.Z Jhanjhi) is currently working as a Professor in Computer Science (Cybersecurity and AI), Program Director for the Postgraduate Research Degree Programmes in computer science, Director of the Center for Smart Society (CSS5) at the School of Computer Science at Taylor's University, Malaysia. He has been nominated as the world's top 2% research scientist globally; he is among the top five computer science researchers in Malaysia and was nominated as an Outstanding Faculty Member by the MDEC Malaysia for the year 2022. He has highly indexed publications in WoS/ISI/SCI/Scopus, and his collective research Impact factor is more than 900 plus points. His Google Scholar H index is 60, and I-10 Index is close to 275, and his Scopus H index is 39, with more than 600 publications on his credit. He has several international patents on his account, including Australian, German, and Japanese patents. He edited/authored over 50 research books published by world-class publishers, including Springer, IGI Global USA, Taylors and Frances, Willeys, Intech Open, etc. He has excellent experience supervising and co-supervising postgraduate students, and more than 37 Postgraduate scholars graduated under his supervision. Prof. Jhanjhi serves as Associate Editor and Editorial Assistant Board for several reputable journals, such as PeerJ Computer Science, CMC Computers, Materials & Continua, Computer Systems Science and Engineering CSSE, Frontier in Communication and Networks, etc. He received the Outstanding Associate Editor award for IEEE ACCESS. Active reviewer for a series of top-tier journals has been awarded globally as a top 1% reviewer by Publons (Web of Science). He is an external Ph.D./Master thesis examiner/evaluator for several universities globally and has evaluated 60 plus theses. He has completed more than 40 internationally funded research grants successfully. He has been a keynote/invited speaker for over 60 international conferences and has chaired international conference sessions. He has vast experience in academic qualifications, including ABET, NCAAA, and NCEAC, for 10 years. His research areas include Cybersecurity, IoT security, Wireless security, Data Science, Software Engineering, and UAVs. .

Archiving

All of IGI Global's content is archived via the CLOCKSS and LOCKSS initiative. Additionally, all IGI Global published content is available in IGI Global's InfoSci® platform.