

Book Description

"Secure Networks: Defending Against Blockchain, Cloud, and Cyber Threats" offers a comprehensive guide to modern network security, emphasizing the protection against evolving threats in blockchain technology, cloud computing, and cyber environments. The book delves into the intricacies of securing decentralized networks, understanding the unique vulnerabilities of cloud infrastructure, and countering sophisticated cyber attacks. Through a blend of theoretical insights and practical strategies, it equips professionals with the tools to fortify their networks, ensuring robust defense mechanisms are in place. Aimed at cybersecurity practitioners, IT professionals, and anyone interested in safeguarding digital assets, this book provides an essential roadmap to navigating and mitigating the complexities of today's threat landscape.



About the Editors:

Ms. Preeti Gupta, an esteemed academician, possesses an extensive 17 years of experience in the education sector. She has accomplished her master of technology in Computer Science. Her academic interests encompass Information Security and Artificial Intelligence. Ms. Preeti Gupta holds the position of Assistant Professor in the department of CSE at Career Point University Kota, Rajasthan. As an educator, she has contributed to institutions like Modi Institute of Technology Kota, Jodhpur Institute of Engineering and Technology Jodhpur and Career Point University, focusing on curriculum development and student mentorship.

SECURE NETWORKS: DEFENDING AGAINST BLOCKCHAIN, CLOUD, AND CYBER THREATS



 CP PUBLICATION

Also Available at
 


₹ 280.00

9 788197 458965

 CP PUBLICATION

Editor:
Ms. Preeti Gupta

Defending Against Blockchain, Cloud, and Cyber Threats

Information contained in this work has been obtained by Career Point from sources believed to be reliable. However, neither Career Point nor its authors guarantee the accuracy or completeness of any information published herein, and neither Career Point nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that Career Point and its authors are supplying information but are not attempting to render any professional services. If such services are required, the assistance of an appropriate professional should be sought.

CAREER POINT

CP Tower, Road No.-1, IPIA, Kota (Raj.)

Email : publication@cpil.in

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the Publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

This edition can be exported from India only by the publisher.

Published by Career Point Ltd.
CP Tower, Road No.-1, IPIA, Kota (Raj.)
Email : publication@cpil.in

Book No. : CPP-752

Preface

In today's interconnected world, securing networks is more critical than ever. The rapid adoption of blockchain technology, the expansive growth of cloud services, and the increasing sophistication of cyber threats necessitate a comprehensive approach to network security. This book aims to provide an in-depth understanding of these evolving challenges and the strategies to defend against them.

In the rapidly evolving landscape of modern network security, the challenges and threats faced by organizations and individuals alike have never been more complex. From the proliferation of mobile devices to the rise of blockchain technology, this comprehensive volume delves into the multifaceted issues surrounding cybersecurity in the digital age. Chapters explore the necessity of antivirus applications for smartphones, the vulnerabilities and solutions within blockchain networks, and innovative approaches to securing peer-to-peer cloud storage. Additionally, the book addresses the unique security concerns posed by ad-hoc and sensor networks, as well as the critical role of data mining and machine learning in fortifying cyber defenses. With insights into intrusion detection and prevention systems, this compilation serves as an indispensable resource for navigating the intricate terrain of contemporary cybersecurity.



Book Description

"Secure Networks: Defending Against Blockchain, Cloud, and Cyber Threats" offers a comprehensive guide to modern network security, emphasizing the protection against evolving threats in blockchain technology, cloud computing, and cyber environments. The book delves into the intricacies of securing decentralized networks, understanding the unique vulnerabilities of cloud infrastructure, and countering sophisticated cyber attacks. Through a blend of theoretical insights and practical strategies, it equips professionals with the tools to fortify their networks, ensuring robust defense mechanisms are in place. Aimed at cybersecurity practitioners, IT professionals, and anyone interested in safeguarding digital assets, this book provides an essential roadmap to navigating and mitigating the complexities of today's threat landscape.

Table of Contents

CHAPTERS TITLES	Page No.
<p>Chapter 1. Modern Network Security: Issues and Challenges Ms. Preeti Gupta</p> <p>Abstract: This chapter examines the evolving challenges in network security, highlighting key issues such as sophisticated cyber-attacks, IoT vulnerabilities, and the security implications of cloud computing. It explores advanced persistent threats, the need for robust encryption, and the role of AI in threat detection, offering strategic solutions to enhance network resilience.</p>	1-7
<p>Chapter 2. Cyber Security and Mobile Threats: The Need For Antivirus Applications for Smartphones Ms. Preeti Gupta</p> <p>Abstract: As mobile devices become increasingly integrated into our daily lives, so too do the threats they face from cyber attacks. This chapter explores the necessity of antivirus applications for smartphones, highlighting the unique vulnerabilities posed by mobile platforms and the essential role of proactive security measures in safeguarding sensitive data and ensuring user privacy.</p>	8-14
<p>Chapter 3. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network Ms. Preeti Gupta</p> <p>Abstract: "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network" would succinctly outline the key points covered in the chapter. It would touch upon the vulnerabilities and threats faced by blockchain networks, particularly within the context of the Internet of Things (IoT). Additionally, it would highlight the proposed solutions and strategies to enhance the security of these distributed systems.</p>	15-18
<p>Chapter 4. Blockchain Security in Cloud Computing Ms. Preeti Gupta</p> <p>Abstract: "Blockchain Security in Cloud Computing" explores the intersection of two transformative technologies, investigating the unique challenges and opportunities presented by their convergence. It provides a glimpse into the evolving landscape of blockchain security within the realm of cloud computing, promising advancements in resilience and trustworthiness for digital ecosystems.</p>	19-22
<p>Chapter 5. Blockchain based scheme for secure P2P cloud storage Ms. Preeti Gupta</p> <p>Abstract: Blockchain-based scheme for secure P2P cloud storage" explores the integration of blockchain technology to enhance security and reliability in peer-to-peer cloud storage systems. The abstract highlights the novel approach and its potential benefits in safeguarding data in decentralized environments.</p>	23-27

<p>Chapter 6. Security in Ad-hoc and Sensor Networks Ms. Preeti Gupta</p> <p>Abstract: Security in Ad-hoc and Sensor Networks" explores the unique challenges and solutions in safeguarding these decentralized networks, crucial for modern applications like IoT and military operations.</p>	28-33
<p>Chapter 7. Data Mining and Machine Learning methods for Cyber Security Ms. Preeti Gupta</p> <p>Abstract: This chapter includes the application of data mining and machine learning techniques in enhancing cybersecurity measures. It explores how these methods analyze large datasets to identify patterns, anomalies, and potential threats, thereby aiding in the early detection and mitigation of cyber attacks.</p>	34-38
<p>Chapter 8. Intrusion Detection System and Intrusion Prevention System Ms. Preeti Gupta</p>	39-42
<p>Abstract: This chapter explores the fundamentals and applications of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). It delves into their crucial roles in safeguarding networks against malicious activities, detailing their mechanisms, detection methodologies, and proactive defense strategies. Additionally, it highlights the evolving landscape of cyber threats and the continuous advancements in IDS/IPS technologies to adapt and counter emerging risks effectively.</p>	

Editors

Ms. Preeti Gupta, an esteemed academician, possesses an extensive 17 years of experience in the education sector. She has accomplished her master of technology in Computer Science. Her academic interests encompass Information Security and Artificial Intelligence. Ms. Preeti Gupta holds the position of Assistant Professor in the department of CSE at Career Point University Kota, Rajasthan. As an educator, she has contributed to institutions like Modi Institute of Technology Kota, Jodhpur Institute of Engineering and Technology Jodhpur and Career Point University, focusing on curriculum development and student mentorship.

Intrusion Detection System and Intrusion Prevention System

Ms. Preeti Gupta

ABSTRACT

Modern cybersecurity frameworks must include systems for detecting and preventing intrusions (IDS and IPS) in order to safeguard networks and information systems against hostile activity and unauthorized access. IDSs are mostly used to monitor and examine network traffic for indications of unusual activity. They also provide notifications to managers about any security lapses.

In contrast, IPSs build upon the functionalities of IDSs by not only detecting threats but also actively preventing them, typically through automated responses such as blocking malicious traffic or resetting connections. By reducing risks in real-time, this proactive strategy improves the security posture overall. Both systems utilize various detection methodologies, including signature-based, anomaly-based, and hybrid approaches, to identify potential intrusions.

For strong defences against a constantly changing array of cyberthreats and to guarantee the availability, integrity, and confidentiality of vital information assets, IDS and IPS must be integrated into a cohesive security plan.

Content-

8.1 Introduction

8.2 Intrusion Detection Systems (IDS)

8.3 Intrusion Prevention Systems (IPS)

8.4 Combined IDS/IPS Systems

8.5 Challenges and Future Trends

8.6 Conclusion

8.1 Introduction

As the cyber threat landscape becomes increasingly sophisticated, organizations are compelled to adopt more advanced security measures to protect their digital assets. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are critical components of a robust security framework. While IDS focuses on detecting potential security breaches, IPS extends this functionality by actively preventing detected threats. This chapter explores the principles, types, functions, and applications of IDS and IPS, as well as the challenges and future trends in these technologies.

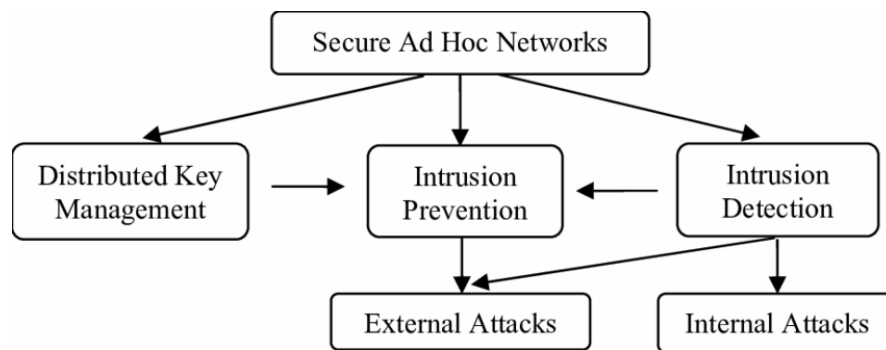


Fig 8.1 Security-Framework-for-Wireless-Ad-Hoc-Networks

8.2 Intrusion Detection Systems (IDS)

An Intrusion Detection System is designed to monitor network traffic and system activities for suspicious behavior or anomalies that may indicate a security breach.

(i) Principles of IDS

- **Monitoring:** Continuous observation of network or system activities to detect unusual patterns.
- **Analysis:** Evaluating monitored data against predefined rules or behavior baselines to identify potential threats.
- **Alerting:** Notifying administrators or security personnel about detected intrusions for further investigation.

(ii) Types of IDS

- **Network-based IDS (NIDS):** Monitors network traffic for suspicious activity.
- **Pros:** Can cover a large number of devices, detects network-level attacks.
- **Cons:** May struggle with encrypted traffic, potential for high false positives.
- **Host-based IDS (HIDS):** Monitors activities on a single host or device.
- **Pros:** Provides detailed analysis of specific systems, can detect internal threats.
- **Cons:** Limited to the host it is installed on, requires more resources per device.

(iii) Detection Methods

- **Signature-based Detection:** Compares monitored data against a database of known attack signatures.
- **Pros:** Effective at identifying known threats.
- **Cons:** Unable to detect new, unknown attacks.
- **Anomaly-based Detection:** Establishes a baseline of normal behavior and flags deviations.
- **Pros:** Can detect previously unknown threats.
- **Cons:** Higher false positive rate, requires time to establish a baseline.

(iv) Applications of IDS

- Network Security Monitoring: Detecting and responding to suspicious network activities.
- Compliance: Ensuring adherence to regulatory requirements by monitoring and reporting security incidents.
- Threat Hunting: Proactively searching for indicators of compromise (IoCs) within the network.

8.3 Intrusion Prevention Systems (IPS)

An Intrusion Prevention System builds on the capabilities of IDS by not only detecting threats but also taking action to block or mitigate them.

(i) Principles of IPS

- Prevention: Actively stopping detected threats in real-time.
- Response: Automatically responding to detected threats to minimize impact.
- Integration: Often integrated with other security tools for comprehensive threat management.

(ii) Types of IPS

- Network-based IPS (NIPS): Monitors and prevents network-level threats.
- Pros: Can protect a large number of devices, effective against network attacks.
- Cons: Similar challenges as NIDS with encrypted traffic and potential latency.
- Host-based IPS (HIPS): Monitors and prevents threats on a single host.
- Pros: Provides detailed protection for specific systems, can prevent host-level attacks.
- Cons: Limited to the host it is installed on, requires more resources per device.

(iii) Prevention Methods

- Signature-based Prevention: Blocks traffic matching known attack signatures.
- Pros: Effective at preventing known threats.
- Cons: Ineffective against new, unknown attacks.
- Anomaly-based Prevention: Blocks traffic deviating from normal behavior patterns.
- Pros: Can prevent unknown threats.
- Cons: Higher false positive rate, needs a stable baseline to function effectively.

(iv) Applications of IPS

- Real-Time Threat Mitigation: Automatically blocking malicious traffic to protect network and systems.
- DDoS Protection: Identifying and mitigating Distributed Denial of Service attacks in real-time.
- Vulnerability Exploit Prevention: Preventing exploitation of known vulnerabilities by blocking related traffic.

8.4 Combined IDS/IPS Systems

Many modern security solutions integrate both IDS and IPS functionalities to provide comprehensive detection and prevention capabilities.

(i) Benefits of Integrated Systems

- **Comprehensive Security:** Combining detection and prevention capabilities enhances overall security posture.
- **Streamlined Management:** Simplifies management and monitoring by consolidating functions into a single system.
- **Enhanced Response:** Faster and more coordinated response to detected threats.

(ii) Challenges of Integrated Systems

- **Complexity:** Integration can add complexity to system configuration and management.
- **Resource Intensive:** Requires significant resources for monitoring, analysis, and response activities.
- **False Positives:** High false positive rates can overwhelm the system and security personnel.

8.5 Challenges and Future Trends

(i) Challenges

- **Evolving Threats:** Continuous evolution of cyber threats necessitates constant updates to detection and prevention mechanisms.
- **Encrypted Traffic:** Increasing use of encryption poses challenges for both IDS and IPS in monitoring and analyzing traffic.
- **False Positives/Negatives:** Balancing the trade-off between false positives (false alarms) and false negatives (missed detections) remains a significant challenge.

(ii) Future Trends

- **Artificial Intelligence and Machine Learning:** Leveraging AI/ML to improve detection accuracy, reduce false positives, and adapt to new threats.
- **Behavioral Analysis:** Enhanced focus on understanding and modeling normal behavior patterns to detect deviations more effectively.
- **Integration with Threat Intelligence:** Incorporating threat intelligence feeds to enhance the detection and prevention capabilities of IDS/IPS systems.
- **Cloud-based IDS/IPS:** Adapting to the shift towards cloud computing by developing cloud-native IDS/IPS solutions to protect cloud environments.

8.6 Conclusion

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are vital components of modern cyber security strategies. While IDS focuses on detecting potential threats, IPS extends this capability by actively preventing them. The integration of both systems provides a comprehensive approach to safeguarding digital assets against a wide array of cyber threats. As the threat landscape continues to evolve, the adoption of advanced technologies such as AI and machine learning will be crucial in enhancing the effectiveness of IDS and IPS, ensuring robust protection for organizations and their data.