

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

Chapter 6. Security in Ad-hoc and Sensor Networks Ms. Preeti Gupta	28-33
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.	
Chapter 7. Data Mining and Machine Learning methods for Cyber Security Ms. Preeti Gupta	34-38
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.	
Chapter 8. Intrusion Detection System and Intrusion Prevention System Ms. Preeti Gupta	39-42
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.	

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.

Security for Sensor and Ad-hoc Networks

Ms. Preeti Gupta

ABSTRACT

Ad-hoc and sensor networks are finding increasing applications in everything from environmental monitoring to military operations. These networks, characterized by their dynamic topologies and resource-constrained devices, face unique security challenges that must be addressed to ensure reliable and secure communication.

This paper explores the current state of security in ad-hoc and sensor networks, identifying key threats such as node capture, eavesdropping, denial of service (DoS) attacks, and routing attacks. The inherent vulnerabilities due to limited computational power, energy constraints, and decentralized management are analyzed in detail. We review existing security protocols and mechanisms designed to mitigate these threats, including lightweight cryptographic techniques, secure routing protocols, and intrusion detection systems. Furthermore, the potential of novel techniques like machine learning-based security solutions and blockchain technology to improve the security environment of ad hoc and sensor networks is investigated.

This study intends to guide future research directions and practical implementations by offering a thorough overview of the difficulties and developments in this sector, ultimately aiding in the development of more resilient and secure ad-hoc and sensor networks.

Content-

- 6.1 Introduction
- 6.2 Characteristics and Challenges
- 6.3 Security Goals
- 6.4 Security Threats in Ad Hoc Networks
- 6.5 Security Mechanisms
- 6.6 Conclusion

6.1 Introduction

The advent of sensor and ad-hoc networks has revolutionized the field of wireless communication, offering unique capabilities in areas such as environmental monitoring, healthcare, military applications, and disaster management. However, the decentralized and open nature of these networks presents significant security challenges. This chapter explores the key security issues and solutions in sensor and ad-hoc networks, providing a comprehensive understanding of the mechanisms required to ensure the integrity, confidentiality, and availability of these networks.

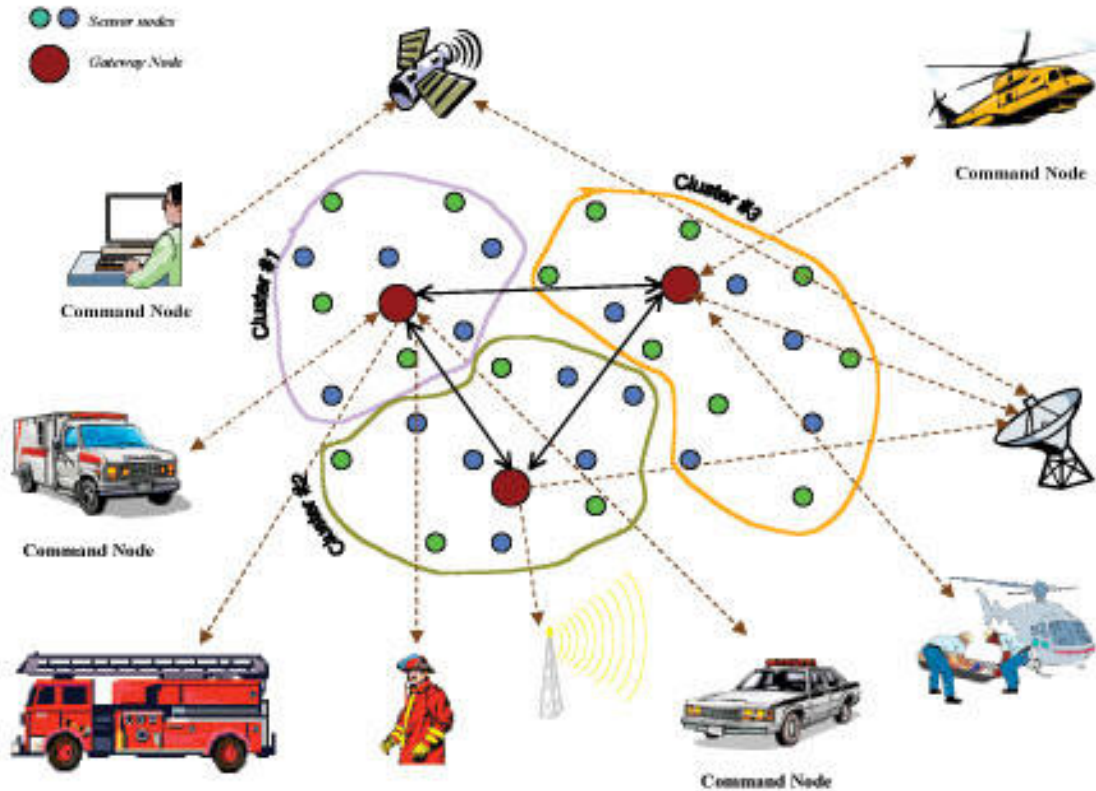


Fig 6.1 Ad-hoc Sensor Networks

6.2 Characteristics and Challenges

Sensor and ad-hoc networks are composed of nodes that communicate wirelessly without relying on a fixed infrastructure. This inherent flexibility and scalability come with several security challenges:

- (i) **Resource Constraints:** Nodes in these networks typically have limited processing power, memory, and battery life, making it difficult to implement resource-intensive security protocols.
- (ii) **Dynamic Topologies:** Frequent changes in network topology due to node mobility and varying communication ranges necessitate robust and adaptive security mechanisms.
- (iii) **Decentralization:** The lack of a central authority to manage security poses challenges in key management and trust establishment.
- (iv) **Physical Vulnerability:** Nodes are often deployed in unattended or hostile environments, making them susceptible to physical attacks and tampering.

6.3 Security Goals

The primary security goals in sensor and ad-hoc networks include:

- (i) **Confidentiality:** Ensuring that sensitive information is only accessible to authorized entities.
- (ii) **Integrity:** Protecting data from being altered or tampered with during transmission.

- (iii) Authentication: Verifying the identity of nodes to prevent unauthorized access.
- (iv) Availability: Ensuring that network services are accessible and functional even in the presence of attacks.
- (v) Non-repudiation: Guaranteeing that the sender of a message cannot deny having sent it.

6.4 Security Threats in Ad Hoc Networks

Ad hoc networks, characterized by their decentralized nature and lack of fixed infrastructure, face a variety of security threats. Below is a comprehensive overview of these threats, categorized by their nature and impact on the network.

(i) Passive Attacks

Eavesdropping

- Threat: Unauthorized nodes intercepting and listening to the network communication.
- Impact: Confidentiality breach, leading to sensitive information disclosure.
- Mitigation: Encryption of data packets to ensure that intercepted data cannot be easily understood.

Traffic Analysis

- Threat: Observing the patterns of communication to infer valuable information about the network.
- Impact: Identification of critical nodes and traffic flows, potentially leading to targeted attacks.
- Mitigation: Use of techniques such as packet padding and traffic mixing to obscure traffic patterns.

(ii) Active Attacks

Denial of Service (DoS)

- Threat: Overloading the network or specific nodes with excessive traffic or requests.
- Impact: Network disruption, making it unusable for legitimate users.
- Mitigation: Implementing rate limiting, and intrusion detection systems (IDS), and using robust authentication mechanisms.

Man-in-the-Middle (MitM)

- Threat: Attacker intercepts and possibly alters the communication between two nodes.
- Impact: Data manipulation, unauthorized access, and breach of confidentiality and integrity.
- Mitigation: Strong mutual authentication and end-to-end encryption.

Wormhole Attack

- Threat: Attacker records packets at one location and tunnels them to another location in the network.

- Impact: Disruption of normal routing, leading to network partition or routing loops.
- Mitigation: Using geographic packet leashes or time-based packet leashes to detect and prevent tunneling.

Blackhole Attack

- Threat: Malicious node falsely advertises a good path to the destination and drops all received packets.
- Impact: Loss of data packets, resulting in communication failure.
- Mitigation: Use of trust-based routing protocols and secure route discovery methods.

Sybil Attack

- Threat: A single node presents multiple identities to other nodes.
- Impact: Undermining redundancy mechanisms, manipulating vote-based decisions, and causing routing disruptions.
- Mitigation: Using identity verification mechanisms and resource testing (e.g., computational puzzles).

Replay Attack

- Threat: Attacker captures legitimate messages and replays them later.
- Impact: Disruption of network operations and potential unauthorized access.
- Mitigation: Implementing timestamping and nonce-based authentication methods.

(iii) Node Compromise and Insider Attacks

Node Capture

- Threat: Physical capture and tampering with a node to extract sensitive information.
- Impact: Exposure of cryptographic keys, network topology, and other sensitive data.
- Mitigation: Use of tamper-resistant hardware and periodic key updates.

Byzantine Attack

- Threat: Compromised nodes behave maliciously and cooperatively disrupt network operations.
- Impact: Routing inconsistencies, packet drops, and network partitioning.
- Mitigation: Use of fault-tolerant routing protocols that can detect and isolate malicious nodes.

(iv) Routing Attacks

Routing Table Overflow

- Threat: Attacker attempts to create routes to non-existent nodes.
- Impact: Exhaustion of resources, leading to denial of service.
- Mitigation: Limit the number of routes a node can create and authenticate routing messages.

Rushing Attack

- Threat: Attacker quickly forwards route request packets to gain priority in route discovery.
- Impact: Legitimate routes are ignored, leading to suboptimal or malicious routes being used.
- Mitigation: Use secure neighbor discovery and delay-based defenses to detect and mitigate rushing behavior.

(v) Resource Depletion Attacks

Battery Exhaustion

- Threat: Repeatedly sending messages to deplete the battery of a node.
- Impact: Nodes run out of power, leading to network fragmentation.
- Mitigation: Implement energy-aware protocols and monitoring mechanisms to detect abnormal power consumption.

Sleep Deprivation

- Threat: Preventing nodes from entering low-power sleep modes by keeping them constantly engaged.
- Impact: Rapid battery depletion and reduced network lifetime.
- Mitigation: Use of sleep scheduling protocols and activity monitoring to identify and mitigate such behavior.

(vi) Collusion Attacks

Collaborative Attacks

- Threat: Multiple compromised nodes collaborate to disrupt the network.
- Impact: Enhanced attack efficacy, making detection and mitigation more challenging.
- Mitigation: Use of trust and reputation systems, and cross-layer security mechanisms to detect colluding nodes.

6.5 Security Mechanisms

To counter these threats, various security mechanisms can be employed:

- (i) **Cryptographic Techniques:** Employing encryption and decryption to protect data confidentiality and integrity. Symmetric-key algorithms (e.g., AES) and asymmetric-key algorithms (e.g., RSA) are commonly used.
- (ii) **Key Management:** Establishing and distributing cryptographic keys securely. Techniques include pre-distribution schemes, dynamic key generation, and public key infrastructure (PKI).
- (iii) **Intrusion Detection Systems (IDS):** Monitoring network traffic to detect and respond to malicious activities. Anomaly-based and signature-based IDS are popular approaches.

- (iv) **Secure Routing Protocols:** Designing routing protocols that incorporate security features to prevent attacks such as wormholes and blackholes. Examples include Secure Efficient Ad hoc Distance vector (SEAD) and Ad hoc On-Demand Distance Vector (AODV) with security extensions.
- (v) **Trust Management:** Establishing trust relationships between nodes to ensure cooperation and secure communication. Reputation-based and recommendation-based systems are commonly used.

6.6 Conclusion

Ensuring the security of sensor and ad-hoc networks is critical for their successful deployment in various applications. By understanding the unique challenges and employing appropriate security mechanisms, it is possible to protect these networks from diverse threats and attacks. Ongoing research and technological advancements will continue to enhance the security and reliability of sensor and ad-hoc networks, enabling their wider adoption and more robust performance in the future.