IJIMAI journal

International Journal of Interactive Multimedia and Artificial Intelligence

SCIENCE CITATION INDEX EXPANDED
2023 JCR
IF 3.4
Q2
CLARIVATE ANALYTICS

# Special Section

*AI Cybersecurity Challenges*

***Eds.***: Juan Ramón Bermejo Higuera
Javier Bermejo Higuera

## Aims and Scope

The increasing integration of Artificial Intelligence (AI) and machine learning (ML) technologies in cybersecurity is reshaping the landscape of digital defense mechanisms. As attackers increasingly leverage AI, it is essential to understand how these technologies can be harnessed for security, while also identifying and mitigating the challenges they pose. This special issue aims to explore the intersection of AI and cybersecurity, focusing on both the opportunities AI provides to enhance security and the challenges it introduces. Contributions are invited that address a range of issues in AI-driven cybersecurity, from innovative applications to the novel risks and threats they create.

The special section seeks to bring together cutting-edge research that addresses the integration of AI in cybersecurity, with an emphasis on both enhancing security postures and mitigating new risks introduced by AI itself. The aim is to advance the scientific understanding of AI's role in modern cybersecurity and to provide insights into the future directions of AI and security in an increasingly digital and interconnected world.

## Topics of Interest

Papers are welcomed on the following topics but not confined to:

1. AI-Driven Threat Detection and Prevention:
   - Machine learning models for anomaly detection, intrusion detection, and threat intelligence.
   - AI in network traffic analysis and cybersecurity defense systems.
   - Automation of threat hunting using AI/ML algorithms.
2. AI-Based Security Solutions:
   - Development of AI tools for malware detection, phishing, and fraud prevention.
   - Use of AI in identity and access management (IAM).
   - AI for securing critical infrastructures and IoT networks.
   - Use of AI to detect and correct security vulnerabilities in source code.
3. Challenges in Adversarial Machine Learning:
   - AI model vulnerabilities to adversarial attacks.
   - Defenses against adversarial machine learning in security systems.
   - Generative models for cybersecurity: threats and safeguards.
4. Ethical and Privacy Concerns in AI Security:
   - Implications of AI in terms of privacy and data protection.
   - Ethical issues in deploying AI for surveillance and monitoring.
   - Responsible AI: Accountability and transparency in cybersecurity decisions.
5. AI-Powered Cyber Attacks:
   - Use of AI and deep learning by cybercriminals.
   - AI-based attack vectors, including automated social engineering and data breaches.
   - Countermeasures for AI-enabled threats and mitigation strategies.
6. AI for Incident Response and Cyber Forensics:
   - Automation in incident detection, analysis, and response.
   - AI-powered digital forensics tools.
   - The role of AI in investigating and mitigating cybercrimes.
   - Use of AI for detection of unknown malware.

Author guidelines and online paper submission form available at www.ijimai.org

unir
LA UNIVERSIDAD
EN INTERNET

IJIMAI journal

International Journal of Interactive Multimedia and Artificial Intelligence

SCIENCE CITATION INDEX EXPANDED
2023 JCR
IF 3.4
Q2
CLARIVATE ANALYTICS

# Special Section

## *AI Cybersecurity Challenges*

***Eds.***: Juan Ramón Bermejo Higuera
Javier Bermejo Higuera

7. AI and Cybersecurity in Emerging Technologies:
   - AI applications in 5G networks, blockchain, and cloud security.
   - The role of AI in securing autonomous systems and smart cities.
   - Cybersecurity challenges in AI-enabled IoT ecosystems.
8. AI and Cybersecurity Policy:
   - Policy frameworks for AI in cybersecurity.
   - Legal and regulatory aspects of AI-driven cybersecurity solutions.
   - Collaboration between AI developers and cybersecurity experts.
9. Generative AI for security audits:
   - Performing pentesting audits through the use of generative AI.
   - Audits of cryptographic protocol implementations aided by generative AI.
   - Using generative AI to audit application source code.
10. Blockchain cybersecurity challenges:
    - Blockchain Security Protocols.
    - Cryptography and Blockchain.
    - Blockchain-Based Attacks and Threats.
    - Blockchain and Identity Management.
    - Regulatory, Legal, and Compliance Challenges.
    - Incident Detection and Response in Blockchain Networks.
    - Blockchain Security Audits and Penetration Testing.
    - Emerging cybersecurity challenges with the integration of AI, IoT, and blockchain.

## Important Dates

**30 September 2025**
Paper Submission Deadline

**10 November 2025**
Notification of the first round review

**22 December 2025**
Revision due

**31 January 2026**
Final Decision

## Guest Editors

**Juan Ramón Bermejo Higuera**
Universidad Internacional de La Rioja (UNIR)
Logroño, Spain
juanramon.bermejo@unir.net

**Javier Bermejo Higuera**
Universidad Internacional de La Rioja (UNIR)
Logroño, Spain
javier.bermejo@unir.net

Author guidelines and online paper submission form available at www.ijimai.org

unir
LA UNIVERSIDAD
EN INTERNET