J-BHI Special Issue on "Swarm Intelligence for Security and Privacy Services in Digital Healthcare Systems"

In digital healthcare systems, security and privacy are of vital importance. As the healthcare industry undergoes the digital transformation, more data is being stored electronically, making data security and privacy protection essential. First, security mainly involves the protection of medical data, which is highly sensitive, including patients' personal information, diagnosis results and treatment plans. To ensure the data security, a range of security measures need to be implemented, such as data encryption, access control, and secure auditing. Second, the privacy preservation is also a crucial consideration, involving the rights and interests of patients.

Yet, cost always come with benefits. Although more modern information and communication technologies are merged into digital healthcare systems, it becomes increasingly difficult to ensure the data privacy and integrity. That is, digital imaging devices in the medical platform, patients' health-related information storage on cloud servers, and the information sharing among experts using public transmission networks, all would be possibly exposed or leaked. Further, the volume and diversity of medical data also make privacy protection difficult. More precisely, healthcare systems typically generate large amounts of data, including patient records, medical images, and genetic information, making it difficult to ensure consistent privacy protection across the digital healthcare system.

Nowadays, swarm intelligence has emerged to collect, store, analyze and regulate the information of each security component in healthcare systems. It is well acknowledged that swarm intelligence is efficient when it comes to data processing and resource utilization in the decentralized and autonomous computing environments. Using the security proactive prevention technology based on swarm intelligence, potential attacks can be detected. In particular, swarm intelligence is built on a series of simple individuals with limited abilities, yet can accomplish complex security protecting tasks. Since swarm intelligence algorithm has high flexibility and is naturally distributed with strong robustness, they can be promisingly used in the data security of healthcare systems.

The aim of this special issue is to attract a combination of research articles that will highlight the use of swarm intelligence in cybersecurity, especially in security and privacy domains, to spread the awareness about the adoption and practices of swarm intelligence for cybersecurity techniques that can help the healthcare community. The topics of interest for this special issue include but not limited to:
• Swarm intelligence for providing security, integrity, and privacy solutions for digital healthcare systems
• Energy-aware solutions based on swarm intelligence for secure digital healthcare systems
• Message authentication techniques based on swarm intelligence for digital healthcare systems
• Swarm intelligence-based techniques to provide hardware security in digital healthcare systems
• Intrusion detection and prevention using swarm intelligence in digital healthcare systems
• Authentication and authorization using swarm intelligence in digital healthcare systems
• Low power swarm intelligence-based techniques for securing digital healthcare systems
• New cryptographic algorithms combined with swarm intelligence for the security and privacy of digital healthcare systems
• Providing security and privacy services for online data using swarm intelligence in digital healthcare systems
• Swarm intelligence-based communication protocols for securing communication between digital healthcare system

Guest Editors
Ming Xiao, KTH Royal Institute of Technology, mingx@kth.se
Giancarlo Fortino, University of Calabria, giancarlo.fortino@unical.it
Mian Ahmad Jan, University of Sharjah, mjan@sharjah.ac.ae
Lei Liu, Xidian University, leiliu@xidian.edu.cn

Key Dates
Deadline for Submission: 01 Jan., 2025
First Reviews Due: 01 Mar., 2025
Revised Manuscript Due: 01 May, 2025
Final Decision: 01 Jul., 2025