Editorial

We present the second issue of this fifteenth volume of the **Journal of Information Security Research**, which includes the papers below.

In the first paper, “**Synchronization processors in the distributed multiprocessor real-time locking protocols,”** the authors establish the minimum and maximum priority inversion blocking limits unavailable in the existing protocols. The current research proved that, in the case of distributed semaphore protocols, two task allocation scenarios exist that give rise to distinct lower bounds. The established bounds are shown to be asymptotically tight with the construction of two new distributed real-time locking protocols.

In the following paper, “**Impact of Neural Networks on Improving Cloud Computing Security with AI-powered Smart Intrusion Detection,”** the authors presented a highly effective method for identifying harmful network activity by leveraging the power of artificial neural networks—the proposed artificial neural network design distinguished between harmless and harmful network traffic. The experimental findings demonstrated that our proposed technique surpasses current leading methods in the field.

In the last paper, “**A model to increase password security in online personal profiles and accounts,”** the authors provided a model to increase the security of personal and online accounts. This work delves into the idea of a two-dimensional game where participants confront specific challenges designed to replace outdated, weak passwords with new, more robust ones while navigating to avoid losing access to multiple platforms.

We hope that these papers make a good impact on security research.

Editors