JISSec
Journal of Information Systems Security

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 20, Issue 1

www.jissec.org

EDITORIAL

This Issue commences with an Editorial Note that explores the technical, formal, and informal components of organizations and proceeds to highlight the vital importance of safeguarding information systems for organizations' resilience. The three research papers of this Issue demonstrate the switch in information security research from defending the products of hackers to the hackers themselves. The recurring theme is Blockchain – the first digital medium for securely transferring value over the Internet.

The first paper, entitled 'Online Video Games: Cyberlaundering Vulnerabilities and Controls', is by James Higgs and Stephen Flowerday, from the USA. It examines the vulnerability of online video games to cybercriminals and money launderers, especially as they operate in an environment free from legal enforcement. As regulations are struggling to keep pace with the latest money laundering strategies employed by cybercriminals, this paper explores and discusses the core vulnerabilities that enable money laundering and proposes security controls to reduce the scale of this crime.

In the second paper, 'Defeat Data Breachers' Minds: Blockchain with Bounded Rationality to Advance Information Security', the authors, Yuanxiang John Li, Benjamin K. Ngugi and Frank M. Lin, from the USA, explore how the mechanism of Blockchain combats the potential threat to information systems caused by the centralized control of the trusted third party (governments, banks, etc.). Based on its bounded rationality, Blockchain can undermine the motivations of information systems breachers to secure information assets by complementing and improving current information security defense models and thus prevent external hackers and reduce insider breaches.

The third paper is entitled 'A Secure and Safe Deep Learning-Driven Blockchain Application for Advanced Plant Stress Phenotyping', and is by Manjit Kaur and Upinder Kaur, from India. In their ground-breaking study, the authors examine the role of blockchain technology in precision agriculture, in particular its integration with ResNet deep learning technology, where the sophisticated image processing capabilities of ResNet-101 enables the use of a high-resolution image of a plant to identify stress indicators. Further, ResNet utilizes blockchain's secure, transparent framework for data management, assuring data integrity and transparency in real time, whereby data are seamlessly integrated into a blockchain, ensuring a tamper-proof, decentralized system. The authors' model promises to revolutionize agricultural practices, offering significant benefits throughout the entire supply chain by combining ResNet-101 image analysis with blockchain security.

I hope that you enjoy reading this first Issue of 2024.

Gurpreet Dhillon, Editor-in-Chief