JISSec
Journal of Information
System 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.

Editor-in-Chief
Gurpreet Dhillon
University of North Texas, USA

Managing Editor
Filipe de Sá-Soares
University of Minho, Portugal

Publishing Manager
Mark Crathorne
ISEG, Universidade de Lisboa, Portugal

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 19, Issue 3

www.jissec.org

EDITORIAL

All the three papers of this Issue concern mechanisms designed to protect against information systems' vulnerabilities, ranging from ciphering for secured image data communication, through to the design of an IoT threat detection artifact and research on the relation between reducing the vulnerabilities of PoS system and the consequent increase in customer's intention to use.

The first paper, entitled 'Review of AES Methods and Suggested Abstract Ciphering for Secured Image Data Communication in IOT and AI Applications', is by Haneen Dweik, Mohammed Abutaha, Adnane Cabani and Karim Hammoudi, from Palestine and France. It presents a review of ciphering methods for secure image communications in the contexts of Internet of Things (IoT) and artificial intelligence and then establishes a systematic understanding of lightweight image encryption in IoT applications and an abstract ciphering approach towards limiting the image-related de-anonymization attacks which can occur over publicly shared trained image sets.

In the second paper, 'Envisioning Organizational IoT: Embracing Design Science to Address the IoT Vulnerabilities', the authors, Michael Lapke, Jackson Walker and Malayo Magee, from the USA, utilize the design-science methods approach (Hevner, 2004) to guide the development, assessment and communication of the design of an IoT threat detection artifact to better understand how this hazard can be managed in organizations and report on the development and evaluation of this artifact.

The third paper is entitled 'How does Vulnerability Awareness impact Consumer Behavioral Intention: Evidence from PoS Systems', and is by Muhmmad Al-Abdullah, Yazan Alnsour and Mohamad Alsharo, from Jordan and the USA. Their research focuses on understanding the effects of customers' awareness of PoS system vulnerabilities on the intentions to use the PoS system by extending the Technology Acceptance Model (TAM) by Perceived Risk (PR) and technology Vulnerability Awareness (VA) constructs. The results show that customers' awareness of existing vulnerabilities reduces their intention to use the PoS system, due to the increase in their perception of risks. In addition, the authors demonstrate that customers' evaluation of PoS technologies usage is affected by both the technology's perceived usefulness (PU) and the technology's perceived ease of use (PEOU).

I hope that you enjoy reading this last Issue of 2023.

Gurpreet Dhillon, Editor-in-Chief