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 21, Issue 1

www.jissec.org

## EDITORIAL

This Issue commences with an Editorial Note which analyzes the global scale of cybercrime, and explores legislative, procedural, and collaborative efforts to mitigate its impact. The need for robust security and international cooperation is reflected in the selected papers, showing the importance of initiatives such as enhanced Captcha generation, improved cybersecurity audits by SMEs and the need for automated preventive and detective controls to counter AAI attacks.

The first paper, entitled 'Secure Captcha Generation with Blockchain Integration: The Case of Historical Gurmukhi Numeral Recognition' is by Harpal Singh, Simpel Rani and Gurpreet Singh Lehal, from India. It focuses on the recognition of numerals in historical Gurmukhi manuscripts and presents a novel application of secure CAPTCHA generation with blockchain integration, offering a promising solution to enhance online security.

In the second paper, 'Observations and Learnings from Cybersecurity Audits of SMEs', the authors Murray E. Jennex, Jeffry Babb and Amjad Abdullatn, from the USA, use student-conducted cybersecurity audits of SMEs to determine if SME cybersecurity behavior has evolved over the last 20 years. The findings indicate a lack of cybersecurity resources in SMEs, both in terms of personnel and knowledge, concluding that all SMEs need to perform cybersecurity audits, using managed service providers, to provide personnel and knowledge resources, and change their pricing practices so that the costs of being cyber secure are recognized.

The third paper is entitled 'Defense-in-depth Model of Countermeasures Against Adversarial AI Attacks: Literature Review and Classification', and is by Pavankumar Mulgund, Raghvendra Singh, Raj Sharman, Manish Gupta and Ameya Shastri Pothukuchi, all from the USA. This paper contributes to bridging that gap in the scholarly discourse about the threat of adversarial artificial intelligence (AAI) attacks by presenting a holistic view of countermeasures against AAI attacks. It presents a systematic classification of identified countermeasures into three categories: preventive, detective, and corrective controls, based on the defense in depth (D-i-D) model. The findings reveal a significant emphasis on the development of automated preventive and detective controls to counter AAI attacks, which is relevant to academics and practitioners alike.

I hope that you enjoy reading this first Issue of 2025.

Gurpreet Dhillon, Editor-in-Chief