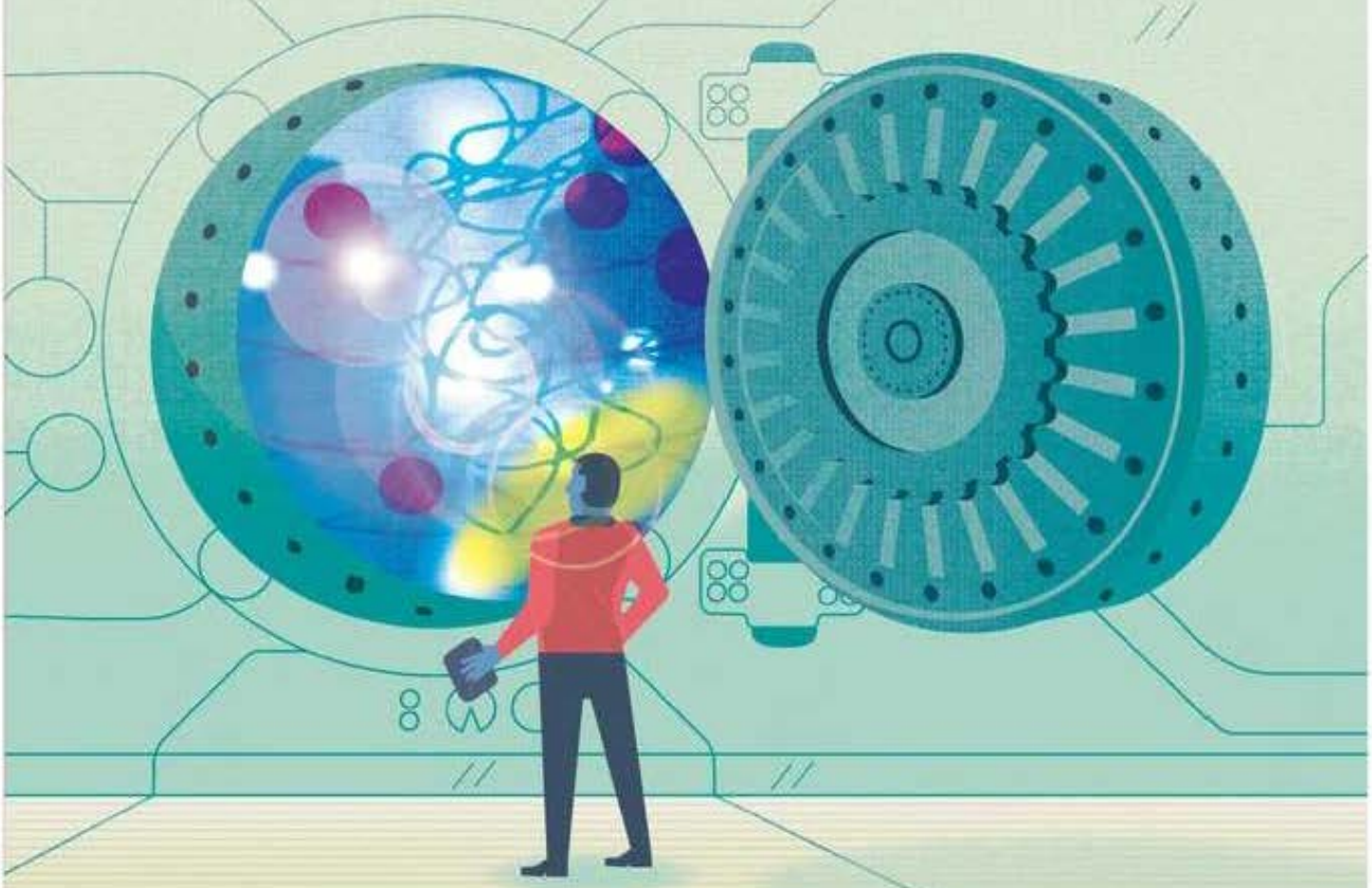
04.25

Computer

SECURE AND INTELLIGENT SYSTEMS



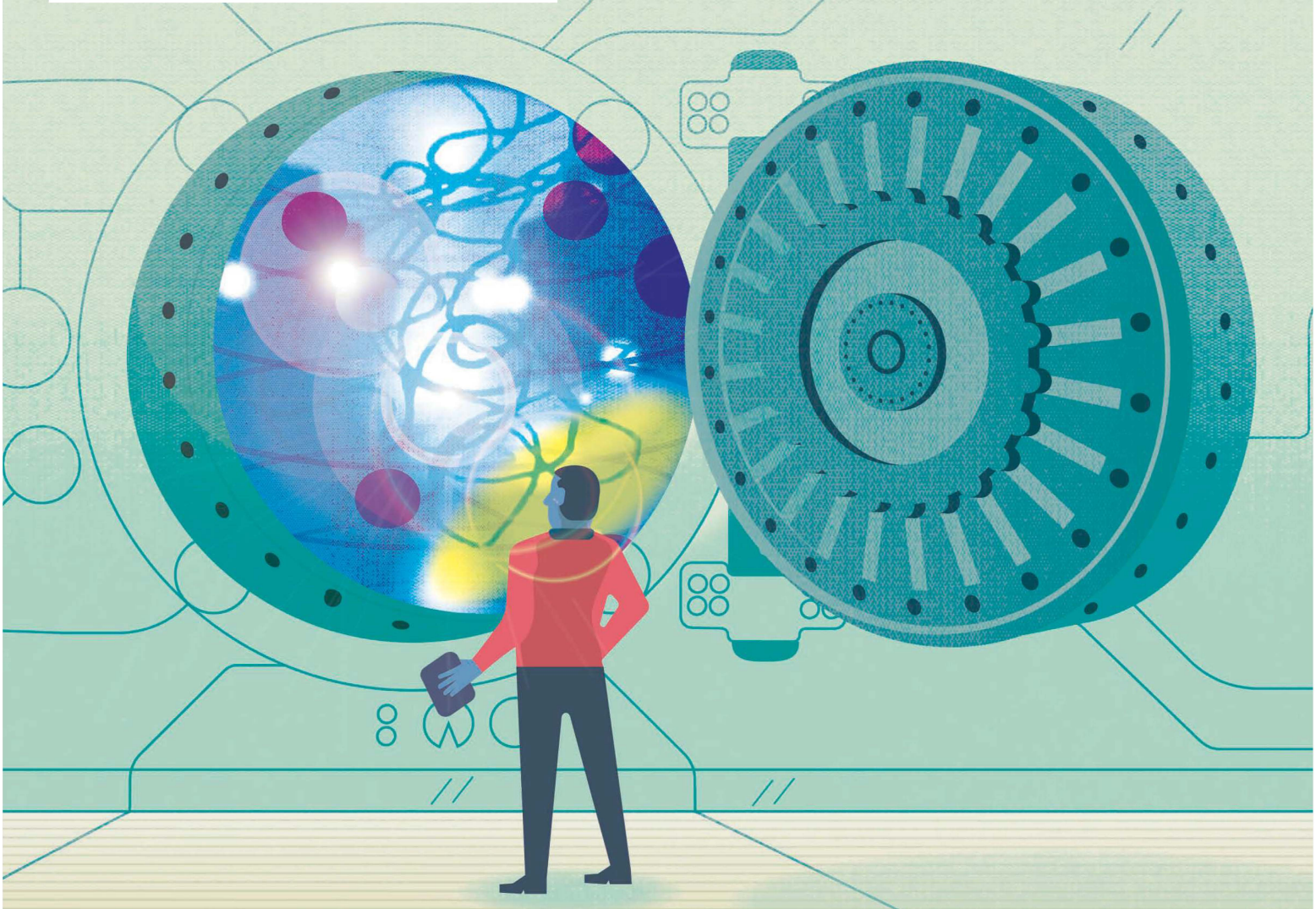
IEEE
IEEE COMPUTER SOCIETY

vol. 58 no. 4

www.computer.org/computer

SECURE AND INTELLIGENT SYSTEMS

D. Frank Hsu, Fordham University
Christina Schweikert, St. John's University



Digital Object Identifier 10.1109/MC.2025.3534447
Date of current version: 27 March 2025

Secure and intelligent systems are those that not only employ methods and technologies such as machine learning, informatics, and artificial intelligence (AI) in decision making but also incorporate robust security measures to protect sensitive data and prevent unauthorized access or adversarial attacks. In essence, a secure and intelligent system combines security and intelligence to function efficiently and effectively while increasing reliability and mitigating risks.

In this issue, we are very pleased to include four articles presenting innovative and timely contributions to secure and intelligent computing.

ABOUT THIS ISSUE

Kuhn et al.[A1] present an insightful method for measuring and visualizing the relative strength of a dataset in machine learning. The authors use a combinatorial method to effectively measure the convergence of interactions between features, an essential consideration in judging data adequacy for training, validation, and testing.

Next, Gavrilova[A2] provides a comprehensive overview of information fusion in the context of innovations in biomimetic multimodal systems. These include unimodal/multimodal system design, deep learning architectures, new behavioral traits based on online social media analytics, and paying attention to the user's data security and privacy.

Then, Nakao et al.[A3] provide a thorough analysis of the escalating complexity and sophistication of cyberattacks within Internet of Things (IoT) environments. It covers detailed case studies

APPENDIX: RELATED ARTICLES

A1. D. R. Kuhn, M S Raunak, and R. N. Kacker, "Measuring and visualizing dataset coverage for machine learning," *Computer*, vol. 58, no. 4, pp. 18–26, Apr. 2025, doi: 10.1109/MC.2025.3527374.

A2. M. L. Gavrilova, "Information fusion: A decade of innovations in biometric multimodal research," *Computer*, vol. 58, no. 4, pp. 27–36, Apr. 2025, doi: 10.1109/MC.2025.3526135.

A3. K. Nakao, D. Inoue, and K. Yoshioka, "Unveiling IoT threats: A case study on darknet and honeypot analysis," *Computer*, vol. 58, no. 4, pp. 37–45, Apr. 2025, doi: 10.1109/MC.2025.3531364.

A4. E. Owusu, M. Mapkar, M. Rahouti, and D. C. Verma, "Robust Intrusion detection with combinatorial fusion and generative artificial intelligence," *Computer*, vol. 58, no. 4, pp. 46–57, Apr. 2025, doi: 10.1109/MC.2024.3524302.

ABOUT THE AUTHORS

D. FRANK HSU is the Clavius Distinguished Professor of Science, a professor of computer and information science, and director of the Laboratory of Informatics and Data Mining, Fordham University, New York, NY 10023 USA. Contact him at hsu@fordham.edu.

CHRISTINA SCHWEIKERT is an associate professor of computer science and the program director for the Master of Science in Data Science program, St. John's University, Queens, NY 11439 USA. Contact her at schweikc@stjohns.edu.

that highlight the vulnerabilities of IoT devices, advanced threat detection, and an analysis of IoT malware, all through the lens of darknet observation and honeypot technologies.

Finally, Owusu et al.[A4] present a novel intrusion detection system that combines combinatorial fusion analysis with generative AI to enhance anomaly detection in intelligent systems. The system addresses challenges in detecting low-profile and evolving threats, in particular for imbalanced datasets.