Editorial

We release the third issue of the sixteenth volume of the **Journal of Information Security Research** with the following papers.

In the opening paper, "**Impact of Cybersecurity Controls on Attack Success, Financial Loss, and Incident Response: An Empirical Analysis Using Synthetic Enterprise Incident Data**," the authors presented an empirical analysis of enterprise cybersecurity incident data to evaluate the effectiveness of major technical, organizational, and governance controls in reducing cyber risk and improving operational response performance. This work used a synthetic dataset comprising over 100,000 enterprise-level incidents with 50+ features; the authors developed a multi-task machine learning pipeline employing XGBoost, Random Forest, SVM, and statistical baselines across three core tasks: binary attack-success classification and multi-class risk-level prioritisation. The XGBoost model achieves superior performance across all tasks. These findings provide a data-driven blueprint for strategic cybersecurity investments, demonstrating that identity-centric controls, rapid detection and response capabilities, and governance frameworks collectively form the foundation of resilient enterprise security architectures.

In the next paper, "**Graph-Based Threat Classification and Embedding Analysis of Cyber Threat Intelligence,**" the authors proposed a comprehensive, graph-based Cyber Threat Intelligence (CTI) analysis framework that transforms fragmented IOCs into a structured cybersecurity knowledge graph. The authors constructed a heterogeneous graph modeling complex interactions among malware, campaigns, threat actors, and infrastructure. this research establishes a scalable and explainable foundation for automated threat attribution and campaign discovery, bridging the critical gap between isolated indicators and semantic attack behaviors to enhance proactive cyber defense capabilities in modern digital environments.

In the last paper, "**Comprehensive Evaluation of Fake News Detection Models: Calibration, Error Analysis, and Statistical Significance on the TruthSeeker Database**," the authors presented a comprehensive evaluation framework for fake news detection using the large scale TruthSeeker2023 dataset, comparing traditional machine learning models (Logistic Regression, Random Forest, XGBoost) with transformer based architectures. Statistical significance testing (McNemar, bootstrap, DeLong, paired t-test, Wilcoxon) confirms that observed performance improvements are robust and not attributable to random variation. The findings establish that evaluating confidence reliability alongside accuracy provides a more realistic assessment of model suitability for real world misinformation detection.

We hope that these papers reflect current research in information security.

Editors