12-14-2025

Privacy-Preserving Intrusion Detection

Johannes Unruh
German Aerospace Center, johannes.unruh@dlr.de

Oscar Hernan Ramirez Agudelo
German Aerospace Center, oscar.ramirezagudelo@dlr.de

Michael Karl
German Aerospace Center, michael.karl@dlr.de

TREO
Technology, Research, Education, Opinion

Privacy-Preserving Intrusion Detection

Enabling Collaborative AI-based Security without Data Sharing

Johannes Unruh (Johannes.Unruh@dlr.de), Oscar Hernan Ramirez-Agudelo (Oscar.RamirezAgudelo@dlr.de), Michael Karl (Michael.Karl@dlr.de)

The growing complexity of cyberattacks has made intrusion detection systems (IDS) an indispensable component of modern defense strategies. In particular, deep learning-based IDS promise powerful detection capabilities, but their effectiveness relies on access to large and diverse datasets. Such datasets, however, typically contain highly sensitive information about internal network structures, communication patterns, and service usage, which organizations are unwilling or unable to share. This creates a paradox: stronger defenses require collaboration, yet collaboration is hindered by confidentiality and trust concerns.

This research investigates secure multiparty computation (MPC) as a way to resolve this dilemma. MPC allows multiple parties to jointly compute over distributed datasets without revealing their private inputs. Applied to IDS training, this means that organizations can contribute data to a shared model without ever exposing raw traffic records. In our prototype, we employed the MP-SPDZ framework to train a three-layer neural network on the ToN_IoT dataset using replicated secret sharing. The resulting model achieved a test accuracy of about 94%, closely matching the baseline from plaintext training. This demonstrates that collaborative, privacy-preserving IDS is technically feasible with state-of-the-art cryptographic techniques.

At the same time, our experiments underscore the significant challenges of such an approach. MPC protocols introduce high computational and communication costs, which limit scalability and practicality for real-world deployments. Addressing these issues requires optimization of the cryptographic protocols and careful consideration of system design, possibly in combination with complementary approaches such as federated learning or homomorphic encryption.

The broader vision is the development of decentralized and trustworthy cybersecurity infrastructures where organizations collaborate without compromising confidentiality. By enabling the joint training of IDS models across institutional boundaries, MPC can unlock richer datasets, improve the detection of novel and sophisticated attacks, and foster new forms of cross-sector defense collaboration. This work illustrates both the opportunities and the obstacles in translating advanced cryptography into operational security practice, highlighting a path toward collective cyber resilience built on privacy-preserving technologies.

References

Araki, T., Furukawa, J., Lindell, Y., Nof, A., & Ohara, K. (2016). High-throughput semi-honest secure three-party computation with an honest majority. Proceedings of the ACM Conference on Computer and Communications Security (CCS).

Dalskov, A., Escudero, D., & Keller, M. (2021). Fantastic Four: Honest-Majority Four-Party Secure Computation with Malicious Security. Proceedings of the USENIX Security Symposium.

Mohassel, P., & Zhang, Y. (2017). SecureML: A system for scalable privacy-preserving machine learning. Proceedings of the IEEE Symposium on Security and Privacy (S&P).

Mokri, S., et al. (2021). Efficient privacy-preserving collaborative intrusion detection. Computers & Security, 106, 102289.

Nasr, M., Shokri, R., & Houmansadr, A. (2019). Comprehensive privacy analysis of deep learning. Proceedings of the IEEE Symposium on Security and Privacy (S&P).