Security and Safety, Vol. 4, E2025001 (2025)
https://doi.org/10.1051/sands/2025001
sands.edpsciences.org

Security and Safety of Data in Cloud Computing

Editorial

Open Access

Other Fields

Preface: Security and safety of data in cloud computing

Dengguo Feng[1,*], Jian Ren[2], and Yang Zhang[3]

[1] *Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*
[2] *Department of Electrical and Computer Engineering, Michigan State University, East Lansing 48824-1312, USA*
[3] *CISPA Helmholtz Center for Information Security, Saarbrücken 66123, Germany*

Received: 31 December 2024 / Revised: 31 December 2024 / Accepted: 2 January 2025 / Published online: 31 January 2025

Citation Feng DG, Ren J, and Zhang Y. Preface: Security and safety of data in cloud computing. Security and Safety 2025; **4**: E2025001. https://doi.org/10.1051/sands/2025001

As a technology integrating distributed computing, network computing and virtualization, cloud computing has attracted much attention since its emergence. By offering flexible and reliable resource services, cloud computing has been widely applied in various domains and has also enabled the advancement of transformative IT technologies such as big data and artificial intelligence. However, the extensive use of cloud computing also brings a large number of data security issues such as data theft and privacy inference. Cloud data, especially sensitive data during computation and processing, are increasingly exposed to risks of security and privacy breaches, which pose great challenges to both industry and academia.

This special topic includes 4 papers covering typical approaches to security and privacy of data in cloud computing, namely Fully Homomorphic Encryption (FHE), Searchable Encryption (SE), Membership Inference Attack (MIA), and De-anonymization Attack. The contributions are as follows:

In the survey "Recent advances of privacy-preserving machine learning based on (Fully) Homomorphic Encryption [1]", the author discusses Fully Homomorphic Encryption (FHE), a promising technique for privacy-preserving machine learning (PPML), which enables data manipulation without decryption. Despite FHE's potential, the variety of available schemes and evolving solutions make it challenging to assess the best approach for specific use cases. The article aims to provide an overview of recent advancements in FHE-based PPML, helping users understand the strengths and limitations of different methods, select the most appropriate one for their needs, and evaluate expected efficiency levels. It also outlines the four generations of FHE schemes, ranging from slow to more efficient implementations.

In the survey "Efficient verifiable searchable encryption with search and access pattern privacy [2]", the authors address the challenge of simultaneously achieving search pattern privacy, access pattern privacy, and verifiability of conjunctive keyword search results. Their constructions support random splitting and blinding of index parameters between non-collusive servers and the embedding of random numbers in keyword trapdoor generation for verifying the correctness of search results. The paper provides a formal security analysis and evaluates the performance efficiency improvements in terms of computational cost, communication cost, and storage cost.

In the paper "Advancing membership inference attacks: The present and the future [3]", the authors discuss the privacy risks in machine learning (ML) posed by membership inference attacks (MIAs), which determine whether a specific data sample was part of a model's training set. While ML's success depends on large datasets, these datasets often contain sensitive information, raising privacy concerns. Such as MIAs can reveal whether specific individual data was used for training. The paper reviews the current

* Corresponding author (email: fengdg@263.net)

state of MIAs, examining their principles, threat models, and methodologies, and highlights research challenges, proposing future directions for enhancing model robustness and privacy.

In the paper "Trajectory-user linking via supervised encoding [4]", the authors address the privacy risks posed by Location-Based Services (LBS) and the Trajectory-User Linking (TUL) task, which is a type of De-anonymization attack that links user trajectories to their originators. They introduce TULSE (Trajectory-User Linking via Supervised Encoding), a method that improves TUL by extracting spatial and temporal information through Supervised Spatiotemporal Encoding and uses BiLSTM with multi-head attention to capture bidirectional and multi-topic semantics. The study also proposes a novel metric, Hierarchical Privacy Loss (HPL), to better assess privacy risks in TUL tasks. The extensive numerical results show that TULSE outperforms existing methods on check-in and GPS datasets.

This special topic serves as a platform to exchange advancements in security and privacy of data in cloud computing, offering theoretical insights and practical solutions. We extend our appreciation to all authors, reviewers, and editors for their valuable contributions to this special topic.

References

[1] Hong C. Recent advances of privacy-preserving machine learning based on (Fully) Homomorphic Encryption. Secur Saf 2025; **4**: 2024012. https://doi.org/10.1051/sands/2024012

[2] Wu AX, Feng DG and Zhang M et al. Efficient verifiable searchable encryption with search and access pattern privacy. Secur Saf 2025; **4**: 2024022. https://doi.org/10.1051/sands/2024022

[3] Li Z and Zhang Y. Advancing membership inference attacks: The present and the future. Secur Saf 2025; **4**: 2024017. https://doi.org/10.1051/sands/2024017

[4] Hu CR, Li Z and Wu SY et al. Trajectory-user linking via supervised encoding. Secur Saf 2025; **4**: 2024018. https://doi.org/10.1051/sands/2024018