5-2017

Cryptography and data security in cloud computing

Zheng YAN
Xidian University

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Vijay VARADHARAJAN
Macquarie University

DOI: https://doi.org/10.1016/j.ins.2016.12.034

Editorial

Cryptography and Data Security in Cloud Computing

Cloud computing offers a new way of services by re-arranging various resources and providing them to users based on their demands. It also plays an important role in the next generation mobile networks and services (5G) and Cyber-Physical and Social Computing (CPSC). Storing data in the cloud greatly reduces storage burden of users and brings them access convenience, thus it has become one of the most important cloud services.

However, cloud data security, privacy and trust become a crucial issue that impacts the success of cloud computing and may impede the development of 5G and CPSC. First, storing data at cloud increases the risk of data leakage and unauthorized access. Second, cloud data centers are becoming the targets of attacks and intrusions, which challenge cloud data security. Third, data management operations, such as data storage, backup, migration, deletion, update, search, query and access in the cloud may not be fully trusted by its owners. Data owners should preferably audit the trustworthiness of data management. Any sources of intrusions and attacks should be able to be detected and tracked. The above requirements actually introduce a big security challenge, especially for big data storage and management. Fourth, data process and computation in the cloud could disclose the privacy of data owners or related entities to unauthorized parities. How to authorize cloud data process and protect data processing result is another interesting and significant research topic. Cloud data security, privacy and trust are indeed becoming key issues that impact the success of cloud computing.

Cryptography is widely applied to ensure data security, privacy and trust in cloud computing. But existing solutions are still imperfect and inefficient, thus impractical. Storing encrypted data in the cloud makes it hard to perform auditing on data management although the risk of privacy leakage is greatly reduced. Key management for access control and revocation introduces additional computation and communication costs. In addition, operations such as fusion, aggregation, and mining on encrypted data are still impractical to be deployed due to high computation complexity and inefficiency. Cryptography in cloud computing promises many novel solutions and at the same time, many challenges are yet to be overcome.

This special issue aims to bring together researchers and practitioners to discuss various aspects of cryptography and data security in cloud computing, explore key theories, investigate technology enablers, develop significant applications and innovate new solutions for overcoming major challenges in this exciting research area. This special issue collects 15 articles that cover original unpublished research illustrative of “Cryptography and Data Security in Cloud Computing” from over 60 submissions after a very rigorous review process. We classify them into four categories and briefly introduce them as below.

1. Secure cloud data storage

In the article “Supporting Dynamic Updates in Storage Clouds with the Akl-Taylor Scheme”, Castiglione et al. tried to overcome the applicability problem of hierarchical key assignment schemes for cloud data access control due to the highly dynamic nature of cloud-based storage. They provided new results on the Akl-Taylor scheme, by carefully analyzing its problem of supporting dynamic updates and key replacement operations, considering different key assignment strategies and proving that the proposed schemes are secure with respect to the notion of key recovery.

In the article “Secure Independent-update Concise-expression Access Control for Video on Demand in Cloud”, He et al. proposed a Secure Independent-update Concise-expression Access Control (SICAC) scheme based on Attribute-Based Encryption in the cloud, to provide flexible and efficient authentication and authorization for Video on Demand (VoD) services. The proposed scheme aims to overcome the challenges caused by frequent subscribing/unsubscribing behaviors of a large number of cloud users and numerous categories of videos in the cloud. The authors designed an independent-update Key

Policy ABE (KP-ABE) algorithm that allows users to update their keys separately and a concise-expression access structure that can describe various logic relationships flexibly and efficiently.

The existing schemes for secure exchange of media files between mobile devices and the cloud have limitations in terms of memory support, processing load, battery power, and data size, thus they are not suitable for resource-constrained mobile devices. In the article "Cryptography-Based Secure Data Storage and Sharing Using HEVC and Public Clouds", Usman, Jan, and He proposed a secure, lightweight, energy-efficient and robust scheme in order to solve this problem. The proposed scheme considers High Efficiency Video Coding (HEVC) Intra encoded video streams in unsliced mode as a source for data hiding in order to support real-time processing at resource-starving mobile devices.

Li et al. proposed another kind of secure cloud data storage solution in the article "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing". The authors proposed an intelligent cryptography approach named Security-Aware Efficient Distributed Storage (SA-EDS) model, by which the cloud service operators cannot directly reach partial data. It divides data efficiently and stores them separately in distributed cloud servers.

2. Cloud data privacy protection

In order to preserve privacy of the published data and the interests of subscribers in data publish-subscribe services over the cloud, Yang et al. propose a privacy-preserving Attribute-Keyword based data Publish-Subscribe (AKPS) scheme in the article "Privacy-Preserving Attribute-Keyword Based Data Publish-Subscribe Service on Cloud Platforms". They employed Attribute-Based Encryption with decryption outsourcing to encrypt the published data and proposed a new searchable encryption to enable subscribers to selectively receive interested data. The AKPS is original and different from existing methods because it can support multiple publishers and multiple subscribers, while none of two publishers/subscribers share the same secret keys. Moreover, it smartly ties both access policy and subscription policy by two secrets, thus successfully avoiding bypassing access/subscription policy checking procedure.

In the application of outsourcing high computational complexity Compressive Sensing (CS) reconstruction process to the cloud, data privacy protection and simultaneous maintenance of the image remains challenging. To address this challenge, Hu et al. proposed a novel outsourced image reconstruction and identity authentication scheme in the article "A Compressive Sensing Based Privacy Preserving Outsourcing of Image Storage and Identity Authentication Service in Cloud". The scheme integrates the techniques of signal processing in the CS domain and computation outsourcing. It ensures the cloud to securely reconstruct image without revealing the underlying content for protecting privacy. In addition, it applies identity authentication to provide the reconstruction service.

In order to solve the problem of Secure Approximate k-Nearest Neighbor (SANN) query from an encrypted database and overcome the challenge that processing such a query without ever decrypting the data in the cloud with efficiency, recoverability and non-distinguishability, Peng et al. presented a novel model to remove the above limitations in the article "A Reusable and Single-interactive Model for Secure Approximate k-Nearest Neighbor Query in Cloud". Concretely, they proposed a reusable and single interactive SANN paradigm in Euclidean high-dimensional space. Extensive evaluations based on four datasets demonstrated that the proposed mechanisms provide effective tradeoff between accuracy and security.

Peng et al. considers the privacy issue in Location-Based Services (LBS) over the cloud in the article "Collaborative Trajectory Privacy Preserving Scheme in Location-based Services". They proposed a Collaborative Trajectory Privacy Preserving (CTPP) scheme to obfuscate the actual trajectory of a user by issuing fake queries to confuse the LBS adversary. First, a multi-hop caching-aware cloaking algorithm was proposed to collect valuable information. Then a collaborative privacy preserving querying algorithm was applied to issue a fake query to confuse the location service provider (LSP) in order to ensure user trajectory privacy.

Private Set Intersection (PSI) enables parties to compute the intersection of their input sets privately. But existing server-aided PSI protocols were designed based on loose security assumptions with regard to trust model and key management. In the article "Server-aided Private Set Intersection Based on Reputation", Zhang et al. proposed a two-server-aided PSI protocol under multiple keys, combining symmetric key proxy re-encryption with social reputation system to prevent collusion and encourage cooperation.

Efficient and privacy-preserving content-based image retrieval is a significant research topic to enable image related security services over the cloud. Xia et al. proposed an encrypted Content-Based Image Retrieval (CBIR) scheme in cloud computing in the article "EPCBIR: An Efficient and Privacy-preserving Content-based Image Retrieval Scheme in Cloud Computing". Through image feature vector extraction, pre-filter table construction and a secure k-Nearest Neighbor (kNN) algorithm, the proposed scheme achieves CBIR over encrypted images without revealing any sensitive information to the cloud and meanwhile increases search efficiency.

In order to preserve privacy during friend matching or recommendation process in social networks, Li et al. proposed Small-World in the article "Small-World: Secure Friend Matching over Physical World and Social Networks". It aims to achieve secure friend matching over physical world and social networks simultaneously. The authors designed a physical proximity module, a Katz score-based social strength proximity module, an El Gamal cryptosystem-based solution and its extension to establish a multi-hop (4-hop at most) social connection chain and a weight assigning function to adjust module contributions in order to reach their research goal.

3. Trusted cloud data management

The article "Tell me the Truth: Practically Public Authentication for Outsourced Databases with Multi-User Modification" aims to solve the problem of the integrity verification of outsourced database with multi-user modification and advanced efficiency. The authors proposed a novel signature scheme that allows users to sign the modified data independently and is homomorphically verifiable.

In order to realize data veracity in mobile cloud computing, Lin et al. proposed a category based context aware and recommendation incentive based reputation mechanism (CCRM) in the article "Towards Better Data Veracity in Mobile Cloud Computing: A Context-Aware and Incentive-Based Reputation Mechanism". In this mechanism, data category, context sensing, security relevance evaluation model, and Vickrey-Clark-Groves (VCG) based recommendation incentive scheme are applied to resist internal collusion attacks and bad mouthing attacks.

4. Cryptography related to cloud data security

As one of the most popular public key cryptographic algorithms, RSA algorithm is widely used for securing cloud computing. The security of RSA lies in the difficulty of factoring large integers efficiently. The General Number Field Sieve (GNFS) algorithm is the most efficient algorithm for factoring integers that are longer than 110 digits. The article "Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing" studies the GNFS algorithm in the cloud. It proposes a novel parallel block Wiedemann algorithm to improve execution performance and reduce the communication cost of solving large and sparse linear systems over GF(2), which is one of the most time-consuming steps of the GNFS algorithm.

Order Preserving Encryption (OPE) is a kind of encryption designed to support search on ciphertexts. But existing schemes suffer from the problems of security and ciphertext expansion. In the article "Semi-Order Preserving Encryption", Yang et al. proposed the notation of semi-order preserving encryption (SOPE) as a substitute for OPE. SOPE uses semi-order preserving condition instead of strict order preserving condition to support range query on ciphertexts. SOPE can get a balance between precision, security and ciphertext expansion by adjusting semi-order preserving degree according to concrete conditions.

Editing this special issue has been an advanced experience although its working load is pretty heavy. We would like to thank all authors and reviewers for their tremendous contributions to it. We indeed appreciate the kind help and support from professor Witold Pedrycz, the Editor-in-Chief of Information Sciences, for ensuring the quality of the whole special issue. We believe there are many other significant research questions that are worth special efforts to explore, but unfortunately not covered in this special issue. We believe this special issue can stimulate future research and interests in the field of cloud data security, privacy and trust.

Acknowledgment

This work is sponsored by the National Key Foundational Research and Development on Network and Space Security, China (grant 2016YFB0800704), the NSFC (grants 61672410 and U1536202), the PhD grant of the Ministry of Education, China (grant JY0300130104), the Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), the 111 project (grants B08038 and B16037), and Aalto University.

Guest editors

Zheng Yan
State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
Department of Communications and Networking, Aalto University, Espoo 02150, Finland

Robert H. Deng
School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore 178902

Vijay Varadharajan
Department of Computing, Faculty of Science, Macquarie University, Australia

E-mail addresses: zyan@xidian.edu.cn (Z. Yan), robertdeng@smu.edu.sg (R.H. Deng), vijay.varadharajan@mq.edu.au (V. Varadharajan)