**LITERATURE SURVEY**

1. **Secure Ranked Keyword Search over Encrypted Cloud Data**

**AUTHORS:** C. Wang, N. Cao, J. Li, K. Ren, W. Lou.

As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only boolean search, without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest, On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, for the first time we define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). Thorough analysis shows that our proposed solution enjoys ``as-strong-as-possible" security guarantee compared to previous SSE schemes, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.

# Privacy-Preserving Double-Projection Deep Computation Model With Crowd sourcing on Cloud for Big Data Feature Learning

**AUTHORS:** Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Deen.

Recent years have witness a considerable advance of Internet of Things with the tremendous progress of communication theories and sensing technologies. A large number of data, usually referring to big data, have been generated from Internet of Things. In this paper, we present a double-projection deep computation model (DPDCM) for big data feature learning, which projects the raw input into two separate subspaces in the hidden layers to learn interacted features of big data by replacing the hidden layers of the conventional deep computation model (DCM) with double-projection layers. Furthermore, we devise a learning algorithm to train the DPDCM. Cloud computing is used to improve the training efficiency of the learning algorithm by crowdsourcing the data on cloud. To protect the private data, a privacy-preserving DPDCM (PPDPDCM) is proposed based on the BGV encryption scheme. Finally, experiments are carried on Animal-20 and NUS-WIDE-14 to estimate the performance of DPDCM and PPDPDCM by comparing with DCM. Results demonstrate that DPDCM achieves a higher classification accuracy than DCM. More importantly, PPDPDCM can effectively improve the efficiency for training parameters, proving its potential for big data feature learning.

# Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage

**AUTHORS:** R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang

# Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In this paper, we investigate the security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional PEKS framework suffers from an inherent insecurity called inside keyword guessing attack (KGA) launched by the malicious server. To address this security vulnerability, we propose a new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, we define a new variant of the smooth projective hash functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we provide an efficient instantiation of the general framework from a Decision Diffie-Hellman-based LH-SPHF and show that it can achieve the strong security against inside the KGA.

# An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys

**AUTHORS:** X. Liu, R.H. Deng, K.K.R. Choo, J. Weng.

In this paper, we propose a toolkit for efficient and privacy-preserving outsourced calculation under multiple encrypted keys (EPOM). Using EPOM, a large scale of users can securely outsource their data to a cloud server for storage. Moreover, encrypted data belonging to multiple users can be processed without compromising on the security of the individual user's (original) data and the final computed results. To reduce the associated key management cost and private key exposure risk in EPOM, we present a distributed two-trapdoor public-key cryptosystem, the core cryptographic primitive. We also present the toolkit to ensure that the commonly used integer operations can be securely handled across different encrypted domains. We then prove that the proposed EPOM achieves the goal of secure integer number processing without resulting in privacy leakage of data to unauthorized parties. Last, we demonstrate the utility and the efficiency of EPOM using simulations.

1. **Building an encrypted and searchable audit log**

**AUTHORS:** B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters

Audit logs are an important part of any secure system, and they need to be carefully designed in order to give a faithful representation of past system activity. This is especially true in the presence of adversaries who might want to tamper with the audit logs. While it is important that auditors can inspect audit logs to assess past system activity, the content of an audit log may contain sensitive information, and should therefore be protected from unauthorized parties. Protecting the contents of audit logs from unauthorized parties (i.e., encrypting it), while making it efficiently searchable by authorized auditors poses a problem. We describe an approach for constructing searchable encrypted audit logs which can be combined with any number of existing approaches for creating tamper-resistant logs. In particular, we implemented an audit log for database queries that uses hash chains for integrity protection and identitybased encryption with extracted keywords to enable searching on the encrypted log. Our technique for keyword search on encrypted data has wide application beyond searchable audit logs.