ELYSIUMPRO

INSPIRING THE LEADING EDGE TECHNOLOGIES

ELYSIUMPRO

A UNIT OF ELYSIUM GROUPS

FINAL YEAR PROJECT

CLOUD COMPUTING 2019-2020

TITLES WITH ABSTRACTS

CALL US @

(+91) 9944 7933 98 | (+91) 452 - 424 2842, 424 2843

20 Years of Experience | Automated Services | 24/7 Help Desk Support
Advanced Technologies and Tools | Legitimate Members of all Journals
Quality Project Training | Industry Exposure

ELYSIUM GROUPS

ELYSIUMPRO

INSPIRING THE LEADING EDGE TECHNOLOGIES

www.elysiumpro.in

#227, Elysium Campus, Church Road, Anna Nagar,
Madurai - 625020, Tamil Nadu, India

CALL US @

(+91) 9944 7933 98 | (+91) 452 - 424 2842, 424 2843

/ElysiumPro Project Center / ElysiumPro / ElysiumPro

ELYSIUM GROUPS

EPRO CLD - 001	Energy Efficient Dynamic Offloading in Mobile Edge Computing for Internet of Things

With proliferation of computation-intensive Internet of Things (IoT) applications, the limited capacity of end devices can deteriorate service performance. To address this issue, computation tasks can be offloaded to the Mobile Edge Computing (MEC) for processing. However, it consumes considerable energy to transmit and process these tasks. In this paper, we study the energy efficient task offloading in MEC. Specifically, we formulate it as a stochastic optimization problem, with the objective of minimizing the energy consumption of task offloading while guaranteeing the average queue length. Solving this offloading optimization problem faces many technical challenges due to the uncertainty and dynamics of wireless channel state and task arrival process, and the large scale of solution space. To tackle these challenges, we apply stochastic optimization techniques to transform the original stochastic problem into a deterministic optimization problem, and propose an energy efficient dynamic offloading algorithm called EEDOA. EEDOA can be implemented in an online way to make the task offloading decisions with polynomial time complexity. Theoretical analysis is given to demonstrate that EEDOA can approximate the minimal transmission energy consumption while still bounding the queue length. Experiments results are presented which shows the EEDOA's effectiveness.

EPRO CLD - 002	Online Multi-Workflow Scheduling under Uncertain Task Execution Time in IaaS Clouds

Cloud has become an important platform for executing numerous deadline-constrained scientific applications generally represented by workflow models. It provides a simple and cost-efficient method of running workflows on their rental Virtual Machines (VMs) anytime and anywhere. Since pay-as-you-go is a dominating pricing solution in clouds, extensive research efforts have been devoted to minimizing the monetary cost of executing workflows by designing tailored VM allocation mechanisms. However, most of them assume that the task execution time in clouds is static and can be estimated in advance, which is impractical in real scenarios due to performance fluctuation of VMs. In this paper, we propose an onliNe multi-workflOw Scheduling Framework, named NOSF, to schedule deadline-constrained workflows with random arrivals and uncertain task execution time. In NOSF, workflow scheduling process consists of three phases, including workflow preprocessing, VM allocation and feedback process. Built upon the new framework, a deadline-aware heuristic algorithm is then developed to elastically provision suitable VMs for workflow execution, with the objective of minimizing the rental cost and improving resource utilization. Simulation results demonstrate that the proposed algorithm significantly outperforms two state-of-the-art algorithms in terms of reducing VM rental costs and deadline violation probability, as well as improving resource utilization efficiency.

EPRO CLD - 003	Heterogeneity Aware Workload Management in Distributed Sustainable Datacenters

The tremendous growth of cloud computing and large-scale data analytics highlight the importance of reducing datacenter power consumption and environmental impact of brown energy. While many Internet service operators have at least partially powered their datacenters by green energy, it is challenging to effectively utilize green energy due to the intermittency of renewable sources, such as solar or wind. We find that the geographical diversity of internet-scale services can be carefully scheduled to improve the efficiency of applying green energy in datacenters. In this paper, we propose a holistic heterogeneity-aware cloud workload management approach, sCloud, that aims to maximize the system good put in distributed self-sustainable datacenters. sCloud adaptively places the transactional workload to distributed datacenters, allocates the available resource to heterogeneous workloads in each datacenter, and migrates batch jobs across datacenters, while taking into account the green power availability and QoS requirements. We formulate the transactional workload placement as a constrained optimization problem that can be solved by nonlinear programming. Then, we propose a batch job migration algorithm to further improve the system goodput when the green power supply varies widely at different locations. Finally, we extend sCloud by integrating a flexible batch job manager to dynamically control the job execution progress without violating the deadlines. We have implemented sCloud in a university cloud testbed with real-world weather conditions and workload traces.

EPRO CLD - 004	A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services

Searchable encryption has received a significant attention from the research community with various constructions being proposed, each achieving asymptotically optimal complexity for specific metrics (e.g., search, update). Despite their elegance, the recent attacks and deployment efforts have shown that the optimal asymptotic complexity might not always imply practical performance, especially if the application demands a high privacy. In this article, we introduce a novel Dynamic Searchable Symmetric Encryption (DSSE) framework called Incidence Matrix (IM)-DSSE, which achieves a high level of privacy, efficient search/update, and low client storage with actual deployments on real cloud settings. We harness an incidence matrix along with two hash tables to create an encrypted index, on which both search and update operations can be performed effectively with minimal information leakage. This simple set of data structures surprisingly offers a high level of DSSE security while achieving practical performance. Specifically, IM-DSSE achieves forward-privacy, backward-privacy and size-obliviousness simultaneously. We also create several DSSE variants, each offering different trade-offs that are suitable for different cloud applications and infrastructures. We fully implemented our framework and evaluated its performance on a real cloud system (Amazon EC2). We have released IM-DSSE as an open-source library for wide development and adaptation.

EPRO CLD - 005	Dynamic Cloud Resource Allocation Considering Demand Uncertainty

Cloud computing provisions scalable resources for high performance industrial applications. Cloud providers usually offer two types of usage plans: reserved and on-demand. Reserved plans offer cheaper resources for long-term contracts while on-demand plans are available for short or long periods but are more expensive. To satisfy incoming user demands with reasonable costs, cloud resources should be allocated efficiently. Most existing works focus on either cheaper solutions with reserved resources that may lead to under-provisioning or over-provisioning, or costly solutions with on-demand resources. Since inefficiency of allocating cloud resources can cause huge provisioning costs and fluctuation in cloud demand, resource allocation becomes a highly challenging problem. In this paper, we propose a hybrid method to allocate cloud resources according to the dynamic user demands. This method is developed as a two-phase algorithm that consists of reservation and dynamic provision phases. In this way, we minimize the total deployment cost by formulating each phase as an optimization problem while satisfying quality of service. Due to the uncertain nature of cloud demands, we develop a stochastic optimization approach by modeling user demands as random variables. Our algorithm is evaluated using different experiments and the results show its efficiency in dynamically allocating cloud resources.

EPRO CLD - 006	Dynamic Demand Prediction and Allocation in Cloud Service Brokerage

To maximize its own profit, cloud service brokerage (CSB) aims to distribute tenant demands to reserved servers such that the total reservation cost is minimized with the tenants' service level agreement (SLA) being satisfied. The demand allocation problem for CSB is non-trivial to solve due to uncertainty of tenants' behavior. To avoid possible violations among demands, existing schemes allocate additional padding resources on the predicted demands, which leads to under-utilization of reserved resources. Accordingly, we propose a Probabilistic Demand Allocation (PDA) system to address the demand allocation problem for CSB. In PDA, we not only predict tenants' demands based on their historical records, but also estimate the probability distribution of prediction errors. As over- and under-estimation are equally likely to happen with our prediction method, when allocating demands to a single server, their errors are possibly offset. Hence, it is unnecessary to allocate additional resource to each demand for violation prevention. Given the predication results, we formulate the demand allocation problem by probabilistic optimization, of which the objective is to minimize the overall cost from reserved servers while satisfying tenants' SLA with high probability. Both simulation and real-world experimental results demonstrate the superiority of PDA in reducing servers' reservation cost.

EPRO CLD - 007	Provable Data Possession with Outsourced Data Transfer

With the rapid development of cloud computing, more and more enterprises would like to upload and store their data in the public cloud. When the parts of the business of an enterprise are purchased by another enterprise, the corresponding data will be transferred to the acquiring enterprise. For the usual case, how to outsource the computation cost of data transfer to the cloud How to ensure the remote purchased data integrity Thus, it is important to study provable data possession with outsourced data transfer (DT-PDP). In this paper, for the first time, we propose the novel concept: DT-PDP. By taking use of DT-PDP, the following three security requirements can be satisfied: (1) the other un-purchased data security of acquired enterprise can be ensured; (2) the purchased data integrity and privacy can be ensured; (3) the data transferability's computation can be outsourced to the public cloud servers. For the security concept of DT-PDP, we give its motivation, system model and security model. Then, we design a concrete DT-PDP scheme based on the bilinear pairings. At last, we analyze the security, efficiency and flexibility of the concrete DT-PDP scheme. It shows that our scheme is provably secure and efficient.

EPRO CLD - 008	Scalable Discovery of Hybrid Process Models in a Cloud Computing Environment

Process descriptions are used to create products and deliver services. To lead better processes and services, the first step is to learn a process model. Process discovery is such a technique which can automatically extract process models from event logs. Although various discovery techniques have been proposed, they focus on either constructing formal models which are very powerful but complex, or creating informal models which are intuitive but lack semantics. In this work, we introduce a novel method that returns hybrid process models to bridge this gap. Moreover, to cope with today's big event logs, we propose an efficient method, called f-HMD, aims at scalable hybrid model discovery in a cloud computing environment. We present the detailed implementation of our approach over the Spark framework, and our experimental results demonstrate that the proposed method is efficient and scalable.

EPRO CLD - 009	A Two-Stage Auction Mechanism for Cloud Resource Allocation

The contemporary literature on cloud resource allocation is mostly focused on studying the interactions between customers and cloud managers. Nevertheless, the recent growth in the customers? demands and the emergence of private cloud providers (CPs) entice the cloud managers to rent extra resources from the CPs so as to handle their backlogged tasks and attract more customers. This also renders the interactions between the cloud managers and the CPs an important problem to study. In this paper, we investigate both interactions through a two-stage auction mechanism. For the interactions between customers and cloud managers, we adopt the options-based sequential auctions (OBSAs) to design the cloud resource allocation paradigm. As compared to existing works, our framework can handle customers with heterogeneous demands, provide truthfulness as the dominant strategy, enjoy a simple winner determination procedure, and preclude the delayed entrance issue. We also provide the performance analysis of the OBSAs, which is among the first in literature. Regarding the interactions between cloud managers and CPs, we propose two parallel markets for resource gathering. We capture the selfishness of the CPs by their offered prices. We conduct a comprehensive analysis of the two markets and identify the bidding strategies of the cloud managers.

EPRO CLD - 010	Comments on "SEPDP: Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage"

Provable Data Possession is viewed as an important technique to check the integrity of the data stored in remote servers. Recently, a new provable data possession scheme [Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage, IEEE Transactions on Services Computing, (2018) Doi: 10.1109/TSC.2018.2820713] was proposed. The authors claimed this scheme can guarantee the storage correction. In this paper, we show this scheme cannot satisfy this fundamental security. Specifically, we demonstrate the malicious cloud can generate a proof to pass the third party auditor's verification even if it does not store the user's whole file.

EPRO CLD - 011	Energy-Efficient Fair Cooperation Fog Computing in Mobile Edge Networks for Smart City

Smart City as a new paradigm for future city development leads to a large amount of computing workload and high network latency especially with artificial intelligence (AI) algorithms. Fog computing as one of Mobile Edge Computing (MEC) paradigms deploys some servers at the edge of mobile networks to solve these problems. However, it still remains a challenging issue how to obtain the energy-effective cooperation policy among fog nodes to enhance the users' quality of experience (QoE) under fairness, where the fairness ensures that fog nodes are willing to take part in cooperations. Therefore, we first build up a cooperative fog computing system to process offloading workload on the entire Fog layer by data forwarding. Then we formulate a joint optimization problem of QoE and energy in integrated fog computing process with fairness. After that, we prove the convexity of the optimization problem and design a Fairness Cooperation Algorithm (FCA) to obtain the optimal fairness cooperation policy of all fog nodes. Finally, numerical results show that our FCA can quickly converge to its solution compared with three traditional convex optimization approaches, and FCA can effectively reduce the time overhead and the energy consumption compared to baseline algorithm (BA) and distributed optimization algorithm (DOA).

EPRO CLD – 012	Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing

With the rapid development of cloud services, huge volume of data is shared via cloud computing. Although cryptographic techniques have been utilized to provide data confidentiality in cloud computing, current mechanisms cannot enforce privacy concerns over ciphertext associated with multiple owners, which makes co-owners unable to appropriately control whether data disseminators can actually disseminate their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the ciphertext. We further present a multiparty access control mechanism over the disseminated ciphertext, in which the data co-owners can append new access policies to the ciphertext due to their privacy preferences. Moreover, three policy aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

EPRO CLD - 013	Auction-based VM Allocation for Deadline-Sensitive Tasks in Distributed Edge Cloud

Edge cloud computing is a new paradigm in which the computation and storage services of remote cloud data centers are moved to Edge Cloud Nodes (ECNs) in network edges. Compared to traditional cloud data centers, ECNs are geographically close to mobile users so the communication latency is significantly reduced. In this paper, we study the problem of allocating Virtual Machine (VM) resources in geo-distributed ECNs to mobile users by using the auction theory. First, we treat mobile users and ECNs as the buyers and sellers of the VM resource auction, respectively. Then, we model the VM resource allocation problem as an n-to-one weighted bipartite graph matching problem with 0-1 knapsack constraints. Since this problem is NP-hard, we design a greedy approximation algorithm to determine the winners of the auction, based on which we propose a truthful Auction-based VM resource Allocation (AVA) mechanism to solve the problem. Moreover, we prove that the AVA mechanism not only achieves an approximately optimal solution for winner selection, but also has the properties of truthfulness, individual rationality, and computational efficiency. Finally, we conduct extensive simulations on real traces to verify the significant performances of the proposed AVA mechanism.

EPRO CLD - 014	Cost-Effective Cloud Server Provisioning for Predictable Performance of Big Data Analytics

Cloud datacenters are underutilized due to server over-provisioning. To increase datacenter utilization, cloud providers offer users an option to run workloads such as big data analytics on the underutilized resources, in the form of cheap yet revocable transient servers (e.g., EC2 spot instances, GCE preemptible instances). Though at highly reduced prices, deploying big data analytics on the unstable cloud transient servers can severely degrade the job performance due to instance revocations. To tackle this issue, this paper proposes iSpot, a cost-effective transient server provisioning framework for achieving predictable performance in the cloud, by focusing on Spark as a representative Directed Acyclic Graph (DAG)-style big data analytics workload. It first identifies the stable cloud transient servers during the job execution by devising an accurate Long Short-Term Memory (LSTM)-based price prediction method. Leveraging automatic job profiling and the acquired DAG information of stages, we further build an analytical performance model and present a lightweight critical data checkpointing mechanism for Spark, to enable our design of iSpot provisioning strategy for guaranteeing the job performance on stable transient servers. Extensive prototype experiments on both EC2 spot instances and GCE preemptible instances demonstrate that, iSpot is able to guarantee the performance of big data analytics running on cloud transient servers while reducing the job budget by up to 83.8 percent in comparison to the state-of-the-art server provisioning strategies, yet with acceptable runtime overhead.

EPRO CLD - 015	CHARON: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data

We present CHARON, a cloud-backed storage system capable of storing and sharing big data in a secure, reliable, and efficient way using multiple cloud providers and storage repositories to comply with the legal requirements of sensitive personal data. CHARON implements three distinguishing features: (1) it does not require trust on any single entity, (2) it does not require any client-managed server, and (3) it efficiently deals with large files over a set of geo-dispersed storage services. Besides that, we developed a novel Byzantine-resilient data-centric leasing protocol to avoid write-write conflicts between clients accessing shared repositories. We evaluate CHARON using micro and application-based benchmarks simulating representative workflows from bioinformatics, a prominent big data domain. The results show that our unique design is not only feasible but also presents an end-to-end performance of up to 2.5x better than other cloud-backed solutions.

EPRO CLD - 016	Cost-Efficient Resource Provisioning for Dynamic Requests in Cloud Assisted Mobile Edge Computing

Mobile edge computing is emerging as a new computing paradigm that provides enhanced experience to mobile users via low latency connections and augmented computation capacity. As the amount of user requests is time-varying, while the computation capacity of edge hosts is limited, the Cloud Assisted Mobile Edge (CAME) computing framework is introduced to improve the scalability of the edge platform. By outsourcing mobile requests to clouds with various types of instances, the CAME framework can accommodate dynamic mobile requests with diverse quality of service requirements. In order to provide guaranteed services at minimal system cost, the edge resource provisioning and cloud outsourcing of the CAME framework should be carefully designed in a cost-efficient manner. Specifically, two fundamental problems should be answered: (1) What is the optimal edge computation capacity configuration? (2) What types of cloud instances should be tenanted and what is the amount of each type? To solve these issues, we formulate the resource provisioning in CAME framework as an optimization problem. By exploiting the piecewise convex property of this problem, the Optimal Resource Provisioning (ORP) algorithms with different instances are developed, so as to optimize the computation capacity of edge hosts and meanwhile dynamically adjust the cloud tenancy strategy. The proposed algorithms are proved to be with polynomial computational complexity. To evaluate the performance of the ORP algorithms, extensive simulations and experiments are conducted based on both widely-used traffic models and Google cluster usage tracelogs, respectively.

EPRO CLD - 017	LAMANCO: A Lightweight Anonymous Mutual Authentication Scheme for N-times Computing Offloading in IoT

Nowadays in many application scenarios of IoT, low latency is achieved at the cost of computing-complexity which is beyond the capabilities of IoT devices. Offloading the computing intensive tasks to more powerful edge devices is expected to provide new generation computing-intensive and delay-sensitive services. In the three hierarchy architecture User/IoT-Edge-Cloud, private and secure mutual authentication are necessary between user, IoT device and edge device. However, in the emerging computing paradigms such as mobile transparent computing, edge computing and fog computing, several threats such as edge device compromise, privacy leaking and denial of service (DoS) might crash the security of the system. Here we propose LAMANCO: A Lightweight Anonymous Mutual Authentication scheme for n-times Computing Offloading in IoT. In our novel scheme, through a smartcard as token and an edge device as a security proxy, a user is able to subscribe or renew n-times computing offloading service and consume it securely in daily use. Moreover, both IoT and edge devices authenticate each other anonymously without leaking user's sensitive information, which will preserve the privacy even when an edge device is comprised. Finally, our scheme is based on lightweight one-way hash function and MAC function, therefore the adversary is not able to perform a DoS attack. To evaluate the solution, a security analysis and a performance analysis are presented. Compared with similar schemes, our approach achieves all designed security features and achieves a 1.66 times and 2.87 times of computing speed on IoT and edge devices, respectably.

EPRO CLD - 018	Key Management Scheme for Secure Channel Establishment in Fog Computing

Fog computing is a promising extension of cloud computing, and enables computing directly at the edge of the network. Due to the decentralized and distributed nature of fog nodes, secure communication channels have to be supported in fog computing, which are generally realized through secure keys. Key management schemes are usually employed to generate, distribute and maintain the secret keys. In this paper, we propose a key management scheme called dynamic contributory broadcast encryption (DConBE) for secure channel establishment in fog computing. It allows a group of fog nodes that want to establish a fog system to negotiate a public encryption key and each node's decryption key in one round without a trusted dealer. Any end user may encrypt messages under the public encryption key with short ciphertexts to any subset of the fog nodes in the system. Only selected fog nodes in the system can decrypt the encrypted messages using their respective decryption key. Our new key management scheme also achieves the properties of fog node dynamics, fully collusion-resistant and stateless.

EPRO CLD - 019	Block chain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors

The deployment of cloud storage services has significant benefits in managing data for users. However, it also causes many security concerns, and one of them is data integrity. Public verification techniques can enable a user to employ a third-party auditor to verify the data integrity on behalf of her/him, whereas existing public verification schemes are vulnerable to procrastinating auditors who may not perform verifications on time. Furthermore, most of public verification schemes are constructed on the public key infrastructure (PKI), and thereby suffer from certificate management problem. In this paper, we propose the first certificateless public verification scheme against procrastinating auditors (CPVPA) by using blockchain technology. The key idea is to require auditors to record each verification result into a blockchain as a transaction. Since transactions on the blockchain are time-sensitive, the verification can be time-stamped after the corresponding transaction is recorded into the blockchain, which enables users to check whether auditors perform the verifications at the prescribed time. Moreover, CPVPA is built on certificateless cryptography, and is free from the certificate management problem. We present rigorous security proofs to demonstrate the security of CPVPA, and conduct a comprehensive performance evaluation to show that CPVPA is efficient.

EPRO CLD – 020	Privacy Preserving Searchable Encryption with Fine-grained Access Control

Searchable encryption facilitates cloud server to search over encrypted data without decrypting the data. Single keyword based searchable encryption enables a user to access only a subset of documents, which contains the keyword of the user's interest. In this paper we present a single keyword based searchable encryption scheme for the applications where multiple data owners upload their data and multiple users access the data. We use attribute based encryption scheme that allows user to access the selective subset of data from cloud without revealing his/her access rights to the cloud server. The proposed scheme is proven adaptively secure against chosen-keyword attack in the random oracle model. We have implemented the scheme on Google cloud instance and the performance of the scheme found feasible in real-world applications.

EPRO CLD - 021	A User-Centric Data Protection Method for Cloud Storage Based on Invertible DWT

Protection on end users' data stored in Cloud servers becomes an important issue in today's Cloud environments. In this paper, we present a novel data protection method combining Selective Encryption (SE) concept with fragmentation and dispersion on storage. Our method is based on the invertible Discrete Wavelet Transform (DWT) to divide agnostic data into three fragments with three different levels of protection. Then, these three fragments can be dispersed over different storage areas with different levels of trustworthiness to protect end users' data by resisting possible leaks in Clouds. Thus, our method optimizes the storage cost by saving expensive, private, and secure storage spaces and utilizing cheap but low trustworthy storage space. We have intensive security analysis performed to verify the high protection level of our method. Additionally, the efficiency is proved by implementation of deploying tasks between CPU and General Purpose Graphic Processing Unit (GPGPU) in an optimized manner.

EPRO CLD - 022	Enabling Strong Privacy Preservation and Accurate Task Allocation for Mobile Crowd sensing

Mobile crowdsensing engages a crowd of individuals to use their mobile devices to cooperatively collect data about social events and phenomena for special interest customers. It can reduce the cost on sensor deployment and improve data quality with human intelligence. To enhance data trustworthiness, it is critical for service provider to recruit reliable mobile users based on their personal features, e.g., mobility pattern and reputation, but unfortunately it could lead to privacy leakage of mobile users. It becomes challenging to resolve the contradiction between user privacy and task allocation in mobile crowdsensing. To address the issue, we propose SPOON, a strong privacy-preserving mobile crowdsensing scheme supporting accurate task allocation from geographic information and credit points of mobile users. Specifically, service providers can recruit mobile users based on their locations, and select proper sensing reports according to their trust levels but without invading user privacy. By utilizing proxy re-encryption and BBS+ signature, sensing tasks are protected and reports are anonymized to prevent privacy leakage. In addition, a privacy-preserving credit management mechanism is introduced to achieve decentralized trust management and secure credit proof for mobile users. Finally, we show the security properties of SPOON and demonstrate its efficiency on computation and communication.

EPRO CLD - 023	Comment on "Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing"

In 2018, Yang et al. proposed a decentralized multi-authority attribute-based encryption scheme for cloud computing applications and proved its security using the dual system encryption technique. In this comment paper, we show that Yang et al.'s scheme does not achieve encryption one-wayness under the key-only attack and the user collusion attack, respectively. In the key-only attack, with the knowledge of public parameters only, an adversary can impersonate the attribute authorities to forge user attribute secret keys. In the user collusion attack, malicious users can collude by sharing their secret keys to unauthorizedly decrypt a ciphertext. In order to fix the scheme, we suggest to adopt a pairing-based proof of knowledge protocol and the decryption algorithm from Lewko and Water's ABE [2] scheme.

EPRO CLD - 024	Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of personal health record (PHR). The traditional ciphertext-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: 1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited and 2) the cost of decryption is especially high since the access policy is embedded in the ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show that the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

EPRO CLD - 025	CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme

Searchable encryption provides an effective mechanism that achieves secure search over encrypted data. A popular application model of searchable encryption is that a data owner stores encrypted data to a server and the server can effectively perform keyword-based search over encrypted data according to a query trapdoor submitted by a data user, where the owner's data and the user's queries are kept secret in the server. Recently, many searchable encryptions have been proposed to achieve better security and performance, provide secure data updatable feature (dynamics), and search results verifiable capability (verifiability). However, most of the existing works endow the data user an unlimited search capacities and do not consider a data user's search permissions. In practical application, granting search privileges for data users is a very important measure to enforce data access control. In this paper, we propose an attribute-based searchable encryption scheme by leveraging the ciphertext-policy attribute-based encryption technique. Our scheme allows the data owner to conduct a fine-grained search authorization for a data user. The main idea is that a data owner encrypts an index keyword under a specified access policy, if and only if, a data user's attributes satisfy the access policy, the data user can perform search over the encrypted index keyword.

EPRO CLD - 026	Profit Maximization for Cloud Brokers in Cloud Computing

Along with the development of cloud computing, more and more applications are migrated into the cloud. An important feature of cloud computing is pay-as-you-go. However, most users always should pay more than their actual usage due to the one-hour billing cycle. In addition, most cloud service providers provide a certain discount for long-term users, but short-term users with small computing demands cannot enjoy this discount. To reduce the cost of cloud users, we introduce a new role, which is cloud broker. A cloud broker is an intermediary agent between cloud providers and cloud users. It rents a number of reserved VMs from cloud providers with a good price and offers them to users on an on-demand basis at a cheaper price than that provided by cloud providers. Besides, the cloud broker adopts a shorter billing cycle compared with cloud providers. By doing this, the cloud broker can reduce a great amount of cost for user. In addition to reduce the user cost, the cloud broker also could earn the difference in prices between on-demand and reserved VMs. In this paper, we focus on how to configure a cloud broker and how to price its VMs such that its profit can be maximized on the premise of saving costs for users. Profit of a cloud broker is affected by many factors such as the user demands, the purchase price and the sales price of VMs, the scale of the cloud broker, etc. Moreover, these factors are affected mutually, which makes the analysis on profit more complicated. In this paper, we first give a synthetically analysis on all the affecting factors, and define an optimal multiserver configuration and VM pricing problem which is modeled as a profit maximization problem. Second, combining the partial derivative and bisection search method.

EPRO CLD - 027	Efficient Real-Time Integrity Auditing With Privacy-Preserving Arbitration for Images in Cloud Storage System

Cloud storage provides an inexpensive and effective means for the storage and management of images, which in turn occupy a huge proportion and are usually stored in an archived mode. Considering the security and efficiency requirements of cloud images, an efficient real-time integrity audit scheme is in urgent need. However, existing solutions cannot be directly applied since they do not take the characteristics of cloud images into account and thus take enormous computations, communications, and storage to generate, transfer, and store authentication data. Moreover, the result of auditing cannot be used as evidence to prove the guilt of cloud service provider since the verifier whom is specified by the client may hide its misbehavior. Reversible watermarking is a potential way to achieve lightweight real-time audit for cloud images without introducing permanent distortion. Nevertheless, existing algorithms cannot provide stable capacity for authentication data of fixed length. In addition, it entails security problems once it is used to solve the fairness problem. This paper proposes an efficient real-time integrity audit scheme specific to cloud images with fair arbitration support. The scheme is based on the presented adaptive reversible watermarking algorithm which provides a fixed embedding capacity for images to embed authentication data. To address fairness problem under the proposed mechanism, we adopt Diffie-Hellman key exchange scheme to design a new challenge-response protocol under the established simplified consensus mechanism, so that replay attack resistance and privacy-preserving fair arbitration are achieved.

EPRO CLD - 028	Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage

Public cloud storage is a fundamental cloud computing service. Currently, most owners of large data outsource their data to cloud storage services—even high-profile owners such as governments. However, public cloud storage services are not optimal for ensuring the possession and integrity of the outsourced data, a situation that has given rise to many proposed provable data possession check schemes (PDP). A PDP scheme allows data owners to efficiently, periodically, and securely verify that a cloud storage provider possesses the outsourced data. Most of the currently available provable data possession check schemes make selective (i.e., probabilistic) checks using random data blocks to verify data integrity rather than checking the entire dataset. Therefore, these schemes are considered inadequate by critical infrastructure sectors that involve highly sensitive data (critical data). In this paper, a new and efficient deterministic data integrity check scheme called cryptographic-accumulator provable data possession (CAPDP) is proposed. The CAPDP surpasses the common limitations exhibited by other currently proposed schemes. The underlying scheme of the CAPDP is based on a modified RSA-based cryptographic accumulator that has the following advantages: 1) it allows the data owner to perform an unlimited number of data integrity checks; 2) it supports data dynamics; 3) it is efficient in terms of communication, computation and storage costs for both the data owner and the cloud storage provider

EPRO CLD - 029	A Lightweight Auditing Service for Shared Data with Secure User Revocation in Cloud Storage

As data sharing has become one of the most popular services offered by cloud storage, designing public auditing mechanisms for integrity of shared data becomes more important. Two problems which arise in shared data auditing include preserving user's identity and collusion resistant revocation of users. When data stored at the cloud is shared among a group of users, different users may modify and sign different data blocks which leaks signer identities to the public verifier. Also, when a user is revoked from the group, signatures generated by this user should be re-signed by the cloud server using re-signature keys. In addition, collusion of cloud server and the revoked user should leak no information about the private key of other users. In this paper, by employing a new proxy re-signature scheme, we propose a public shared data auditing mechanism that provides identity privacy and collusion resistant user revocation, simultaneously. The proposed protocol requires only lightweight computations at the user side for signing data blocks in real-time online phase. Moreover, our protocol supports large dynamic group of users, batch auditing and dynamic data operations. Experimental results demonstrate excellent efficiency of our scheme in comparison to the state of the art.

EPRO CLD - 030	Efficient Attribute-based Access Control with Authorized Search in Cloud Storage

Attribute-based encryption has been widely employed to achieve data confidentiality and fine-grained access control in cloud storage. To enable users to identify accessible data in numerous dataset, clear attributes should be appended to the ciphertext, which results in the exposure of attribute privacy. In this paper, we propose an efficient attribute-based access control with authorized search scheme (EACAS) in cloud storage by extending the anonymous key-policy attribute-based encryption (AKP-ABE) to support fine-grained data retrieval with attribute privacy preservation. Specifically, by integrating the key delegation technique into AKP-ABE, EACAS enables data users to customize search policies based on their access policies, and generate the corresponding trapdoor using the secret key granted by the data owner to retrieve their interested data. In addition, a virtual attribute with no semantic meaning is utilized in data encryption and trapdoor generation to empower the cloud to perform attribute-based search on the outsourced ciphertext without knowing the underlying attributes or outsourced data. The data owners can achieve fine-grained access control on their outsourced data, and the data users are flexible to search their interested data based on protected attributes through customizing the search policies. Finally, we demonstrate that EACAS is more efficient than existing solutions on computation and storage overheads.

EPRO CLD - 031	Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage

In attribute-based searchable encryption (ABSE) scheme, data owners can encrypt their data with access policy for security consideration, and encrypt keywords to obtain keyword index for privacy keyword search, and data users can search interesting keyword on keyword indexes by keyword search trapdoor. However, many existing searchable encryption schemes only support single keyword search and most of the existing attribute-based encryption (ABE) schemes have high computational costs at user client. These problems significantly limit the application of attribute-based searchable encryption schemes in practice. In this paper, we propose a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme for cloud storage, in our new scheme, multi-keyword can be searched and the search privacy is protected. That is, the cloud server can search the multi-keyword with keyword search trapdoor but it does not know any information about the keywords searched. In the proposed scheme, many computing tasks are outsourced to the cloud proxy server, which greatly reduces the computing burden at the user client. Besides, the scheme also supports the verification of the correctness of the outsourced private key. The proposed scheme is proved secure that the keyword index is indistinguishable under the adaptive keyword attacks in the general group model, and the ciphertext is selective secure under selective plaintext attacks in the random oracle model. The security and experimental results show that our scheme is suitable for practicability.

EPRO CLD - 032	A Practical Attribute-Based Document Collection Hierarchical Encryption Scheme in Cloud Computing

Ciphertext-policy attribute-based encryption can provide fine-grained access control and secure data sharing to the data users in cloud computing. However, the encryption/decryption efficiency of existing schemes can be further improved when encrypting a large document collection. In this paper, we propose a practical Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme named CP-ABHE. By practical, we mean that CP-ABHE is more efficient in both computation and storage space without sacrificing data security. In CP-ABHE, we first construct a set of integrated access trees based on the documents' attribute sets. We employ the greedy strategy to build the trees incrementally and grow the trees dynamically by combining the small ones. Then, all the documents on an integrated access tree are encrypted together. Different to existing schemes, the leaves in different access trees with the same attribute share the same secret number, which is employed to encrypt the documents. This greatly improves the performance of CP-ABHE. The security of our scheme is theoretically proved based on the decisional bilinear Diffie-Hellman assumption. The simulation results illustrate that CP-ABHE performs very well in terms of security, efficiency, and the storage size of the ciphertext.

EPRO CLD - 033	Block chain for Secure EHRs Sharing of Mobile Cloud based E-health System

Recent years have witnessed a paradigm shift in storage of Electronic Health Records (EHRs) on mobile cloud environments where mobile devices are integrated with cloud computing to facilitate medical data exchanges among patients and healthcare providers. This advanced model enables healthcare services with low operational cost, high flexibility and EHRs availability. However, this new paradigm also raises concerns about data privacy and network security for e-health systems. How to reliably share EHRs among mobile users while guaranteeing high security levels in mobile cloud is a challenging issue. In this paper, we propose a novel EHRs sharing framework that combines blockchain and the decentralized interplanetary file system (IPFS) on a mobile cloud platform. Particularly, we design a trustworthy access control mechanism using smart contracts to achieve secure EHRs sharing among different patients and medical providers. We present a prototype implementation using Ethereum blockchain in a real data sharing scenario on a mobile app with Amazon cloud computing. Empirical results show that our proposal provides an effective solution for reliable data exchanges on mobile clouds while preserving sensitive health information against potential threats. The system evaluation and security analysis also demonstrate performance improvements in lightweight access control design, minimum network latency with high security and data privacy levels, compared to existing data sharing models.

EPRO CLD - 034	Public-Key Encryption with Keyword Search via Obfuscation

Public-key encryption with keyword search (PEKS) enables users to search on encrypted data, which is applicable to the scenario of sharing data in the cloud storage. In this paper, we focus on how to construct a PEKS scheme via obfuscation. Our basic scheme is built on the differing-inputs obfuscation (diO) and can be considered as an initial attempt to apply diO in the PEKS field. The scheme supports searching on encrypted data by providing to the cloud server an obfuscated simple “decrypt-then-compare” circuit with the secret key and the queried keyword hardwired in it. More interestingly, the scheme can be simply improved to resist off-line keyword guessing attacks (KGAs) as the standard PEKS scheme rather than a designated tester one. For complex search conditions, our scheme can be easily extended to multiple functionalities, such as conjunctive and fuzzy keyword search. Furthermore, it can be extended to the PEKS scheme in the multi-user setting.

EPRO CLD - 035	Co-operative Resource Allocation: Building an Open Cloud Market using Shared Infrastructure

In this paper we present DRIVE, a distributed service-based system designed to facilitate an open economic market for federating Cloud providers. To address the challenges associated with market ownership and operation we propose the use of a co-operative (co-op) infrastructure in which the services that make up DRIVE are hosted across participants' resources. To prevent malicious behavior we use cryptographic, secure and privacy preserving allocation protocols as a means of establishing trust in the allocation infrastructure. We investigate through simulation the effect of different strategies, pricing functions, and penalty models on allocation performance and revenue, and show that the overhead of running DRIVE's services on commodity infrastructure is modest.

EPRO CLD - 036	Repair Strategies for Mobile Storage Systems

We study the data reliability problem for devices forming a dynamic distributed storage system. Such systems are commonplace in traditional cloud storage applications where storage node failures and updates are frequent. We consider the application of regenerating codes for file maintenance. Such codes require lower bandwidth to regenerate lost data fragments compared to file replication or reconstruction. We investigate threshold-based repair strategies where data repair is initiated after a threshold number of data fragments have been lost. We show that at a low departure-to-repair rate regime, in which repairs are initiated after several nodes have left the system outperforms if repairs are initiated after a single node departure. This optimality is reversed when the node turnover is high. We further compare distributed and centralized repair strategies and derive the optimal repair threshold for minimizing the average repair cost per unit of time. In addition, we examine cooperative repair strategies and show performance improvements. We investigate several models for the time needed for node repair including a simple fixed time model and a more realistic model that takes into account the number of repaired nodes. Finally, an extended model where additional failures are allowed during the repair process is investigated.

EPRO CLD - 037	Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storage

Cloud storage enables users to outsource data to storage servers and retrieve target data efficiently. Some of the outsourced data are very sensitive and should be prevented for any leakage. Generally, if users conventionally encrypt the data, searching is impeded. Public-key encryption with keyword search (PEKS) resolves this tension. Whereas, it is vulnerable to keyword guessing attacks (KGA), since keywords are low-entropy. In this paper, we present a secure PEKS scheme called SEPSE against KGA, where users encrypt keywords with the aid of dedicated key servers via a threshold and oblivious way. SEPSE supports key renewal to periodically replace an existing key with a new one on each key server to thwart the key compromise. Furthermore, SEPSE can efficiently resist online KGA, where each keyword request made by a user is integrated into a transaction on a public blockchain (e.g., Ethereum), which allows key servers to learn the number of keyword requests made by the user without requiring a synchronization between them for per-user rate limiting. Security analysis and performance evaluation demonstrate that SEPSE provides a stronger security guarantee compared with existing schemes, at the expense of acceptable computational costs.

ELYSIUMPRO

A UNIT OF ELYSIUM GROUPS

THANK YOU!