JAVA/J2EE PROJECT ABSTRACTS

(Big Data, Cloud Computing, Networking, Network-Security, Mobile Computing, Wireless Sensor Network, Datamining, Webmining, Artificial Intelligence, Vanet, Ad-Hoc Network)

IEEE 2016 / 2015 / 2014 / 2013 Papers

1. **Anonymous Authentication for Secure Data Stored on Cloud with Decentralized Access Control**
Decentralized storage system for accessing data with anonymous authentication provides more secure user authentication, user revocation and prevents replay attacks. Access control is processed on decentralized KDCs it is being more secure for data encryption. Generated decentralized KDC's are then grouped by (KGC). Our system provides authentication for the user, in which only system authorized users are able to decrypt, view the stored information. User validations and access control scheme are introduced in decentralized, which is useful for preventing replay attacks and supports modification of data stored in the cloud. The access control scheme is gaining more attention because it is important that only approved users have access to valid examine. Our scheme prevents supports creation, replay attacks, reading and modify data stored in the cloud. We also address user revocation. The problems of validation, access control, privacy protection should be solved simultaneously.

2. **Deleting Secret Data with Public Verifiability.**
Existing software-based data erasure programs can be summarized as following the same one-bit-return protocol: the deletion program performs data erasure and returns either success or failure. However, such a onebit- return protocol turns the data deletion system into a black box – the user has to trust the outcome but cannot easily verify it. This is especially problematic when the deletion program is encapsulated within a Trusted Platform Module (TPM), and the user has no access to the code inside. In this paper, we present a cryptographic solution that aims to make the data deletion process more transparent and verifiable. In contrast to the conventional black/white assumptions about TPM (i.e., either completely trust or distrust), we introduce a third assumption that sits in between: namely, "trust-but-verify". Our solution enables a user to verify the correct implementation of two important operations inside a TPM without accessing its source code: i.e., the correct encryption of data and the faithful deletion of the key. Finally, we present a proof-of-concept implementation of the SSE system on a resource-constrained Java card to demonstrate its practical feasibility. To our knowledge, this is the first systematic solution to the secure data deletion problem based on a "trust-but-verify" paradigm, together with a concrete prototype implementation.

3. **Secure Cloud Storage Meets with Secure Network Coding**

This paper reveals an intrinsic relationship between secure cloud storage and secure network coding for the first time. Secure cloud storage was proposed only recently while secure network coding has been studied for more than ten years. Although the two areas are quite different in their nature and are studied independently, we show how to construct a secure cloud storage protocol given any secure network coding protocol. This gives rise to a systematic way to construct secure cloud storage protocols. Our construction is secure under a definition which captures the real world usage of the cloud storage. Furthermore, we propose two specific secure cloud storage protocols based on two recent secure network coding protocols. In particular, we obtain the first publicly verifiable secure cloud storage protocol in the standard model. We also enhance the proposed generic construction to support user anonymity and third-party public auditing, which both have received considerable attention recently. Finally, we prototype the newly proposed protocol and evaluate its performance. Experimental results validate the effectiveness of the protocol

4. **Multi-Objective Tasks Scheduling Algorithm for Cloud Computing Throughput Optimization**

In cloud computing datacentersexert server unification to enhance the efficiency of resources. Many Vms (virtual machine) are running on each datacenter to utilize the resources efficiently. Most of the time cloud resources are underutilized due to poor scheduling of task (or application) in datacenter. In this paper, we propose a multi-objective task scheduling algorithm formappingtasks to a Vms in order to improve the throughput of the datacenter and reduce the cost without violating the SLA (Service Level Agreement) for an application in cloud SaaS environment. The proposed algorithm provides an optimal scheduling method. Most of the algorithms schedule tasks based on single criteria (i.e execution time). But in cloud environment it is required to consider various criteria like execution time, cost, bandwidth of user etc. This algorithm is simulated using CloudSim simulator and the result shows better performance and improved throughput.

5. **Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption**

Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user’s authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

6. **Secure and Efficient Cloud Computing Framework**

Cloud computing is a very useful solution to many individual users and organizations. It can provide many services based on different needs and requirements. However, there are many issues related to the user data that need to be addressed when using cloud computing. Among the most important issues are: data ownership, data privacy, and storage. The users might be satisfied by the services provided by the cloud computing service providers, since they need not worry about the maintenance and storage of their data. On the other hand, they might be worried about unauthorized access to their private data. Some solutions to these issues were proposed in the literature, but they mainly increase the cost and processing time since they depend on encrypting the whole data. In this paper, we are introducing a cloud computing framework that classifies the data based on their importance. In other words, more important data will be encrypted with more secure encryption algorithm and larger key sizes, while less important data might even not be encrypted. This approach is very helpful in reducing the processing cost and complexity of data storage and manipulation since we do not need to apply the same sophisticated encryption techniques to the entire users data. The results of applying the proposed framework show improvement and efficiency over other existing frameworks.

7. **Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing**

With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. Furthermore, PRMSM supports efficient data user revocation.Extensive experiments on real-world datasets confirm the efficacy and efficiency of PRMSM.

8. A Hybrid Cloud Approach for Secure Authorized Deduplication

Data deduplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing.To better protect data security, this paper makes the first attempt to formally address the problem of authorized data deduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. We also present several new deduplication constructions supporting authorized duplicate check in a hybrid cloud architecture. Security analysis demonstrates that our scheme is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement a prototype of our proposed authorized duplicate check scheme and conduct testbed experiments using our prototype. We show that our proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

9. On the Security ofDataAccess Control for Multiauthority CloudStorageSystems

Data access control has becoming a challenging issue in cloud storage systems. Some techniques have been proposed to achieve the secure data access control in a semitrusted cloud storage system. Recently, K.Yang *et al.*proposed a basic data access control scheme for multiauthoritycloud storage system (DAC-MACS) and an extensive data access control scheme (EDAC-MACS). They claimed that the DAC-MACS could achieve efficient decryption and immediate revocation and the EDAC-MACS could also achieve these goals even thoughnonrevoked users reveal their Key Update Keys to the revoked user. However, through our cryptanalysis, the revocation security of both schemes cannot be guaranteed. In this paper, we first give two attacks on the two schemes. By the first attack, the revoked user can eavesdrop to obtain other users’ Key Update Keys to update its Secret Key, and then it can obtain proper Token to decrypt any secret information as a nonrevoked user. In addition, by the second attack, the revoked user can intercept Ciphertext Update Key to retrieve its ability to decrypt any secret information as a nonrevoked user. Secondly, we propose a new extensive DAC-MACS scheme (NEDAC-MACS) to withstand the above two attacks so as to guarantee more secure attribute revocation. Then, formal cryptanalysis of NEDAC-MACS is presented to prove the security goals of the scheme. Finally, the performance comparison among NEDAC-MACS and related schemesisgivento demonstrate that the performance of NEDAC-MACS is superior to that of DACC, and relatively same as that of DAC-MACS.

10. Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to reauthenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

11. Implementation OF DNA cryptography in cloud computing and using socket programming

Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services and etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services provider's servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters

12. Task Scheduling in Cloud Computing

Wireless Cloud computing delivers the data and computing resources through the internet, on a pay for usage basis. By using this, we can automatically update our software. We can use only the space required for the server, which reduces the carbon footprint. Task scheduling is the main problem in cloud computing which reduces the system performance. To improve system performance, there is need of an efficient task-scheduling algorithm. Existing task-scheduling algorithms focus on taskresource requirements, CPU memory, execution time and execution cost. However, these do not consider network bandwidth. In this paper, we introduce an efficient taskscheduling algorithm, which presents divisible task scheduling by considering network bandwidth. By this, we can allocate the workflow based on the availability of network bandwidth. Our proposed task-scheduling algorithm uses a nonlinear programming model for divisible task scheduling, which assigns the correct number of tasks to each virtual machine. Based on the allocation, we design an algorithm for divisible load scheduling by considering the network bandwidth.

13. An Optimized Task Scheduling Algorithm in CloudComputing

Cloud provides convenient and on demand network access for computing resources available over internet. Individuals and organizations can access the software and hardware such as network, storage, server and applications which are located remotely easily with the help of Cloud Service. The tasks/jobs submitted to this cloud environment needs to be executed on time using the resources available so as to achieve proper resource utilization, efficiency and lesser makespan which in turn requires efficient task scheduling algorithm for proper task allocation. In this paper, we have introduced an Optimized Task Scheduling Algorithm which adapts the advantages of various other existing algorithms according to thesituation while considering the distribution and scalability characteristics of cloud resources.

14. Attribute-Based Access Control for Multi-Authority with constant size ciphertext in cloud Computing

In most existing CP-ABE schemes, there is only one authority in the system and all the public keys and private keys are issued by this authority, which incurs ciphertext size and computation costs in the encryption and decryption operations that depend at least linearly on the number of attributes involved in the access policy. We propose an efficient multi-authority CP-ABE scheme in which the authorities need not interact to generate public information during the system initialization phase. Our scheme has constant ciphertext length and a constant number of pairing computations. Our scheme can be proven CPA-secure in random oracle model under the decision q-BDHE assumption. When user's attributes revocation occurs, the scheme transfers most re-encryption work to the cloud service provider, reducing the data owner's computational cost on the premise of security. Finally the analysis and simulation result show that the schemes proposed in this thesis ensure the privacy and secure access of sensitive data stored in the cloud server, and be able to cope with the dynamic changes of users' access privileges in large-scale systems. Besides, the multi-authority ABE eliminates the key escrow problem, achieves the length of ciphertext optimization and enhances the efficiency of the encryption and decryption operations

15. A Study on Secure Intrusion Detection System in Wireless MANETs to Increase the Performance of Eaack

Mobile Ad hoc Network (MANET) has been pervasive in many applications, including some procedures such as security in critical applications has been a major threats in MANETs. This exceptional characteristic of MANETs, anticipation methodologies lonely cannot able to be secure the data. In this circumstance secure acknowledgment of each data should have a defensive force before the attackers violate the system. The mechanism of Intrusion Detection System (IDS) is normally used to protect the wireless networks for security purposes in MANETs. In case of MANETs, intrusion detection system is favored since the first day of their invention. Communication is restricted to the transmitters within a radio frequency range. Owing to the superior technology that reduces the cost of infrastructure services to gain more importance in autonomous topology of mobile nodes. A novel IDS, EAACK is mainly a secure authentication method using acknowledgment for MANETs to transmit packets in mobility nodes. In this case, out of range in mobile nodes cases security issues while transmitting data from source to destination nodes. This results that the communication of each mobility nodes takes place in radio frequency range and the out of range in communication leads the parties to relay data transmissions to reach the destination node.

16. Privacy-Preserving Detection of Sensitive Data Exposure

Statistics from security firms, research institutions and government organizations show that the number of data-leak instances have grown rapidly in recent years. Among various data-leak cases, human mistakes are one of the main causes of data loss. There exist solutions detecting inadvertent sensitive data leaks caused by human mistakes and to provide alerts for organizations. A common approach is to screen content in storage and transmission for exposed sensitive information. Such an approach usually requires the detection operation to be conducted in secrecy. However, this secrecy requirement is challenging to satisfy in practice, as detection servers may be compromised or outsourced. In this paper, we present a privacy- preserving data-leak detection (DLD) solution to solve the issue where a special set of sensitive data digests is used in detection.The advantage of our method is that it enables the data owner to safely delegate the detection operation to a semihonest provider without revealing the sensitive data to the provider. We describe how Internet service providers can offer their customers DLD as an add-on service with strong privacy guarantees. The evaluation results show that our method can support accurate detectionwith very small number of false alarms under various data-leakscenarios.

17. A Secure Client Side Deduplication Scheme in Cloud Storage Environments

Recent years have witnessed the trend of leveraging cloud-based services for large scale content storage, processing, and distribution. Security and privacy are among top concerns for the public cloud environments. Towards these security challenges, we propose and implement, on Open Stack Swift, a new client-side de duplication scheme for securely storing and sharing outsourced data via the public cloud. The originality of our proposal is twofold. First, it ensures better confidentiality towards unauthorized users. That is, every client computes a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by integrating access rights in metadata file, an authorized user can decipher an encrypted file only with his private key.

18. Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

19. On the Security of a Public Auditing Mechanism for Shared Cloud Data Service

Recently, a public auditing protocol for shared data called Panda (IEEE Transactions on Services Computing, doi:10.1109/TSC.2013.2295611) was proposed to ensure the correctness of the outsourced data. A distinctive feature of Panda is the support of data sharing and user revocation. Unfortunately, in this letter, we show that Panda is insecure in the sense that a cloud server can hide data loss without being detected. Specifically, we show that even some stored file blocks have been lost, the server is able to generate a valid proof by replacing a pair of lost data block and its signature with another block and signature pair. We also provide a solution to the problem while preserving all the desirable features of the original protocol

20. Secure Auditing and Deduplicating Data in Cloud

As the cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. In this work, we study the problem of integrity auditing and secure deduplication on cloud data. Specifically, aiming at achieving both data integrity and deduplication in cloud, we propose two secure systems, namely SecCloud and SecCloud+. SecCloud introduces an auditing entity with a maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is designed motivated by the fact that customers always want to encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data.

21. An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration

Induced by incorporating the powerful data storage and data processing abilities of cloud computing (CC) as well as ubiquitous data gathering capability of wireless sensor networks (WSNs), CC-WSN integration received a lot of attention from both academia and industry. However, authentication as well as trust and reputation calculation and management of cloud service providers (CSPs) and sensor network providers (SNPs) are two very critical and barely explored issues for this new paradigm. To fill the gap, this paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Considering the authenticity of CSP and SNP, the attribute requirement of cloud service user (CSU) and CSP, the cost, trust, and reputation of the service of CSP and SNP, the proposed ATRCM system achieves the following three functions: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP. Detailed analysis and design as well as further functionality evaluation results are presented to demonstrate the effectiveness of ATRCM, followed with system security analysis.

22. Truthful Greedy Mechanisms for Dynamic Virtual Machine Provisioning and Allocation in Clouds

A major challenging problem for cloud providers is designing efficient mechanisms for virtual machine (VM) provisioning and allocation. Such mechanisms enable the cloud providers to effectively utilize their available resources and obtain higher profits. Recently, cloud providers have introduced auction-based models for VM provisioning and allocation which allow users to submit bids for their requested VMs. We formulate the dynamic VM provisioning and allocation problem for the auction-based model as an integer program considering multiple types of resources. We then design truthful greedy and optimal mechanisms for the problem such that the cloud provider provisions VMs based on the requests of the winning users and determines their payments. We show that the proposed mechanisms are truthful, that is, the users do not have incentives to manipulate the system by lying about their requested bundles of VM instances and their valuations. We perform extensive experiments using real workload traces in order to investigate the performance of the proposed mechanisms. Our proposed mechanisms achieve promising results in terms of revenue for the cloud provider.

23. DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

24. Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems

Storage-as-a-service offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their sensitive data to be stored on remote servers. In this paper, we propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: 1) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append, 2) it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the utsourced data, 3) it enables indirect mutual trust between the owner and the CSP, and 4) it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and a prototype implementation on Amazon cloud platform to evaluate storage, communication, and computation overheads.

25. EasySMS: A Protocol for End-to-End Secure Transmission of SMS

Nowadays, short message service (SMS) is being used in many daily life applications, including healthcare monitoring, mobile banking, mobile commerce, and so on. But when we send an SMS from one mobile phone to another, the information contained in the SMS transmit as plain text. Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission. In this paper, we propose an efficient and secure protocol called EasySMS, which provides end-to-end secure communication through SMS between end users. The working of the protocol is presented by considering two different scenarios. The analysis of the proposed protocol shows that this protocol is able to prevent various attacks, including SMS disclosure, over the air modification, replay attack,man-in-the middle attack, and impersonation attack. The EasySMS protocol generates minimum communication and computation overheads as compared with existing SMSSec and PK-SIM protocols. On an average, the EasySMS protocol reduces 51% and 31% of the bandwidth consumption and reduces 62% and 45% of message exchanged during the authentication process in comparison to SMSSec and PK-SIM protocols respectively. Authors claim that EasySMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of cellular network.

26. Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing

Cloud computing is emerging as a prevalent data interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose ashared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing, is attractive for multi-user collaborative cloud applications.

27. CloudMoV: Cloud-based Mobile Social TV

The rapidly increasing power of personal mobile devices (smartphones, tablets, etc.) is providing much richer contents and social interactions to users on the move. This trend however is throttled by the limited battery lifetime of mobile devices and unstable wireless connectivity, making the highest possible quality of service experienced by mobile users not feasible. The recent cloud computing technology, with its rich resources to compensate for the limitations of mobile devices and connections, can potentially provide an ideal platform to support the desired mobile services. Tough challenges arise on how to effectively exploit cloud resources to facilitate mobile services, especially those with stringent interaction delay requirements. In this paper, we propose the design of a Cloud-based, novel Mobile sOcial tV system (CloudMoV). The system effectively utilizes both PaaS (Platform-as-a-Service) and IaaS (Infrastructure-as-a-Service) cloud services to offer the living-room experience of video watching to a group of disparate mobile users who can interact socially while sharing the video. To guarantee good streaming quality as experienced by the mobile users with time-varying wireless connectivity, we employ a surrogate for each user in the IaaS cloud for video downloading and social exchanges on behalf of the user. The surrogate performs efficient stream transcoding that matches the current connectivity quality of the mobile user. Given the battery life as a key performance bottleneck, we advocate the use of burst transmission from the surrogates to the mobile users, and carefully decide the burst size which can lead to high energy efficiency and streaming quality. Social interactions among the users, in terms of spontaneous textual exchanges, are effectively achieved by efficient designs of data storage with BigTable and dynamic handling of large volumes of concurrent messages in a typical PaaS cloud. These various designs for flexible transcoding c- pabilities, battery efficiency of mobile devices and spontaneous social interactivity together provide an ideal platform for mobile social TV services. We have implemented CloudMoV on Amazon EC2 and Google App Engine and verified its superior performance based on real-world experiments.

28. A packet marking approach to protect cloud environment against DDoS attacks

Cloud computing uses internet and remote servers for maintaining data and applications. It offers through internet the dynamic virtualized resources, bandwidth and on-demand software's to consumers and promises the distribution of many economical benefits among its adapters. It helps the consumers to reduce the usage of hardware, software license and system maintenance. Simple Object Access Protocol (SOAP) is the system that allows the communications interaction between different web services. SOAP messages are constructed using either HyperText Transport Protocol (HTTP) and/or Extensible Mark-up Language (XML). The new form of Distributed Denial of Service (DDoS) attacks that could potentially bring down a cloud web services through the use of HTTP and XML. Cloud computing suffers from major security threat problem by HTTP and XML Denial of Service (DoS) attacks. HX-DoS attack is a combination of HTTP and XML messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider. To address the problem of HX-DoS attacks against cloud web services there is a need to distinguish between the legitimate and illegitimate messages. This can be done by using the rule set based detection, called CLASSIE and modulo marking method is used to avoid the spoofing attack. Reconstruct and Drop method is used to make decision and drop the packets on the victim side. It enables us to improve the reduction of false positive rate and increase the detection and filtering of DDoS attacks.

29. Load Balancing for Privacy-Preserving Access to Big Data in Cloud

In the era of big data, many users and companies start to move their data to cloud storage to simplify data management and reduce data maintenance cost. However, security and privacy issues become major concerns because third-party cloud service providers are not always trusty. Although data contents can be protected by encryption, the access patterns that contain important information are still exposed to clouds or malicious attackers. In this paper, we apply the ORAM algorithm to enable privacy-preserving access to big data that are deployed in distributed file systems built upon hundreds or thousands of servers in a single or multiple geo-distribu ted cloud sites. Since the ORAM algorithm would lead to serious access load unbalance among storage servers, we study a data placement problem to achieve a load balanced storage system with improved availability and responsiveness. Due to the NP-hardness of this problem, we propose a low-complexity algorithm that can deal with large-scale problem size with respect to big data. Extensive simulations are conducted to show that our proposed algorithm finds results close to the optimal solution, and significantly outperforms a random data placement algorithm.

30. Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage

The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease security concerns over inadvertent data leaks in the cloud. A key challenge to designing such encryption schemes lies in the efficient management of encryption keys. The desired flexibility of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents. However, this also implies the necessity of securely distributing to users a large number of keys for both encryption and search, and those users will have to securely store the received keys, and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data. The implied need for secure communication, storage, and complexity clearly renders the approach impractical. In this paper, we address this practical problem, which is largely neglected in the literature, by proposing the novel concept of keyaggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.

31. Enabling Efficient Access Control with Dynamic Policy Updating for Big Data in the Cloud

Due to the high volume and velocity of big data, it is an effective option to store big data in the cloud, because the cloud has capabilities of storing big data and processing high volume of user access requests. Attribute-Based Encryption (ABE) is a promising technique to ensure the end-to-end security of big data in the cloud. However, the policy updating has always been a challenging issue when ABE is used to construct access control schemes. A trivial implementation is to let data owners retrieve the data and re-encrypt it under the new access policy, and then send it back to the cloud. This method incurs a high communication overhead and heavy computation burden on data owners. In this paper, we propose a novel scheme that enabling efficient access control with dynamic policy updating for big data in the cloud. We focus on developing an outsourced policy updating method for ABE systems. Our method can avoid the transmission of encrypted data and minimize the computation work of data owners, by making use of the previously encrypted data with old access policies. Moreover, we also design policy updating algorithms for different types of access policies. The analysis show that our scheme is correct, complete, secure and efficient.

32. Toward Efficient and Privacy-Preserving Computing in Big Data Era

Big data, because it can mine new knowledge for economic growth and technical innovation, has recently received considerable attention, and many research efforts have been directed to big data processing due to its high volume, velocity, and variety (referred to as “3V”) challenges. However, in addition to the 3V challenges, the flourishing of big data also hinges on fully understanding and managing newly arising security and privacy challenges. If data are not authentic, new mined knowledge will be unconvincing; while if privacy is not well addressed, people may be reluctant to share their data. Because security has been investigated as a new dimension, “veracity,” in big data, in this article, we aim to exploit new challenges of big data in terms of privacy, and devote our attention toward efficient and privacy-preserving computing in the big data era. Specifically, we first formalize the general architecture of big data analytics, identify the corresponding privacy requirements, and introduce an efficient and privacy-preserving cosine similarity computing protocol as an example in response to data mining’s efficiency and privacy requirements in the big data era.

33. Privacy Preserving Data Analytics for Smart Homes

A framework for maintaining security & preserving privacy for analysis of sensor data from smart homes, without compromising on data utility is presented. Storing the personally identifiable data as hashed values withholds identifiable information from any computing nodes. However the very nature of smart home data analytics is establishing preventive care. Data processing results should be identifiable to certain users responsible for direct care. Through a separate encrypted identifier dictionary with hashed and actual values of all unique sets of identifiers, we suggest re-identification of any data processing results. However the level of re-identification needs to be controlled, depending on the type of user accessing the results. Generalization and suppression on identifiers from the identifier dictionary before re-introduction could achieve different levels of privacy preservation. In this paper we propose an approach to achieve data security & privacy through out the complete data lifecycle:data generation/collection, transfer, storage, processing and sharing.

34. KASR: A Keyword-Aware Service Recommendation Method on MapReduce for Big Data

Applications Service recommender systems have been shown as valuable tools for providing appropriate recommendations to users. In the last decade, the amount of customers, services and online information has grown rapidly, yielding the big data analysis problem for service recommender systems. Consequently, traditional service recommender systems often suffer from scalability and inefficien-cy problems when processing or analysing such large-scale data. Moreover, most of existing service recommender systems present the same ratings and rankings of services to different users without considering diverse users' preferences, and therefore fails to meet users' personalized requirements. In this paper, we propose a Keyword-Aware Service Recommendation method, named KASR, to address the above challenges. It aims at presenting a personalized service recommendation list and recommending the most appro-priate services to the users effectively. Specifically, keywords are used to indicate users' preferences, and a user-based Collaborative Filtering algorithm is adopted to generate appropriate recommendations. To improve its scalability and efficiency in big data environ-ment, KASR is implemented on Hadoop, a widely-adopted distributed computing platform using the MapReduce parallel processing paradigm. Finally, extensive experiments are conducted on real-world data sets, and results demonstrate that KASR significantly im-proves the accuracy and scalability of service recommender systems over existing approaches.

35. Cost Minimization for Big Data Processing in Geo-Distributed Data Centers

The explosive growth of demands on big data processing imposes a heavy burden on computation, storage, and communication in data centers, which hence incurs considerable operational expenditure to data center providers. Therefore, cost minimization has become an emergent issue for the upcoming big data era. Different from conventional cloud services, one of the main features of big data services is the tight coupling between data and computation as computation tasks can be conducted only when the corresponding data is available. As a result, three factors, i.e., task assignment, data placement and data movement, deeply influence the operational expenditure of data centers. In this paper, we are motivated to study the cost minimization problem via a joint optimization of these three factors for big data services in geo-distributed data centers. To describe the task completion time with the consideration of both data transmission and computation, we propose a two-dimensional Markov chain and derive the average task completion time in closed-form. Furthermore, we model the problem as a mixed-integer non-linear programming (MINLP) and propose an efficient solution to linearize it. The high efficiency of our proposal is validated by extensive simulation based studies.

36. Dache: A Data Aware Caching for Big-Data Applications Using the MapReduce Framework

The buzz-word big-data refers to the large-scale distributed data processing applications that operate onexceptionally large amounts of data. Google’s MapReduce and Apache’s Hadoop, its open-source implementation,are the defacto software systems for big-data applications. An observation of the MapReduce framework is that the framework generates a large amount of intermediate data. Such abundant information is thrown away after the tasks finish, because MapReduce is unable to utilize them. In this paper, we propose Dache, a data-aware cache framework for big-data applications. In Dache, tasks submit their intermediate results to the cache manager. A task queries the cache manager before executing the actual computing work. A novel cache description scheme and a cache request and reply protocol are designed. We implement Dache by extending Hadoop. Testbed experiment results demonstrate that Dache significantly improves the completion time of MapReduce jobs

37. A Load Balancing Model Based on Cloud Partitioning

Load balancing in the cloud computing environment has an important impact on the performance. Good load balancing makes cloud computing more efficient and improves user satisfaction. This article introduces a better load balance model for the public cloud based on the cloud partitioning concept with a switch mechanism to choose different strategies for different situations. The algorithm applies the game theory to the load balancing strategy to improve the efficiency in the public cloud environment.

38. ClubCF: A Clustering-based Collaborative Filtering Approach for Big Data Application

Spurred by service computing and cloud computing, an increasing number of services are emerging on the Internet. As a result, service-relevant data become too big to be effectively processed by traditional approaches. In view of this challenge, a Clustering-based Collaborative Filtering approach (ClubCF) is proposed in this paper, which aims at recruiting similar services in the same clusters to recommend services collaboratively. Technically, this approach is enacted around two stages. In the first stage, the available services are divided into small-scale clusters, in logic, for further processing. At the second stage, a collaborative filtering algorithm is imposed on one of the clusters. Since the number of the services in a cluster is much less than the total number of the services available on the web, it is expected to reduce the online execution time of collaborative filtering. At last, several experiments are conducted to verify the availability of the approach, on a real dataset of 6,225 mashup services collected from ProgrammableWeb.

39. Identity-Based Encryption with Outsourced Revocation in Cloud Computing

Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

40. An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments

The increasing spread of mobile cloud computing paradigm is changing the traditional mobile communication infrastructure. Today, smartphones can rely on virtual (software) “clones” in the cloud, offering backup/recovery solutions as well as the possibility to offload computations. As a result, clones increase the communication and computation capabilities of smartphones, making their limited batteries last longer. Unfortunately, mobile cloud introduces new privacy risks, since personal information of the communicating users is distributed among several parties (e.g., cellular network operator, cloud provider). In this paper, we propose a solution implementing an end-to-end anonymous communication protocol between two users in the network, which leverages properties of social networks and ad hoc wireless networks. We consider an adversary model where each party observing a portion of the communication possibly colludes with others to uncover the identity of communicating users. We then extensively analyse the security of our protocol and the anonymity preserved against the above adversaries. Most importantly, we assess the performance of our solution by comparing it to Tor on a real tested of 36 smartphones and relative clones running on Amazon EC2 platform.

41. Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification

The advent of the cloud computing makes storage outsourcing become a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research consider the problemof secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation in practical cloud storage system. In this paper, we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the our scheme definition. Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, countability and traceability of secure group user revocation. Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

42. Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates

Cloud computing opens a new era in IT as it can provide various elastic and scalable IT services in a pay-as you-go fashion, where its users can reduce the huge capital investments in their own IT infrastructure. In this philosophy, users of cloud storage services no longer physically maintain direct control over their data, which makes data security one of the major concerns of using cloud. Existing research work already allows data integrity to be verified without possession of the actual data file.

When the verification is done by a trusted third party, this verification process is also called data auditing, and this third party is called an auditor. However, such schemes in existence suffer from several common drawbacks. First, a necessary authorization/authentication process is missing between the auditor and cloud service provider, i.e., anyone can challenge the cloud service provider for a proof of integrity of certain file, which potentially puts the quality of the so-called 'auditing-as-a-service' at risk; Second, although some of the recent work based on BLS signature can already support fully dynamic data updates over fixed-size data blocks, they only support updates with fixed-sized blocks as basic unit, which we call coarse-grained updates. As a result, every small update will cause re-computation and updating of the authenticator for an entire file block,which in turn causes higher storage and communication overheads. In this paper, we provide a formal analysis for possible types of fine-grained data updates and propose a scheme that can fully support authorized auditing and fine-grained update requests. Based on our scheme,we also propose an enhancement that can dramatically reduce communication overheads for verifying small updates. Theoretical analysis and experimental results demonstrate that our scheme can offer not only enhanced security and flexibility, but also significantly lower overhead for big data applications with a large number of frequent small updates, such as applications in social media and business transactions.

43. A Secure Client Side Deduplication Scheme in Cloud Storage Environments

Recent years have witnessed the trend of leveraging cloud-based services for large scale content storage, processing, and distribution. Security and privacy are among top concerns for the public cloud environments. Towards these security challenges, we propose and implement, on OpenStack Swift, a new client-side deduplication scheme for securely storing and sharing outsourced data via the public cloud. The originality of our proposal is twofold. First, it ensures better confidentiality towards unauthorized users. That is, every client computes a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by integrating access rights in metadata file, an authorized user can decipher an encrypted file only with his private key.

44. A Framework For Selection Of Best Cloud Service Provider Using Ranked Voting Method

Cloud computing provides computing resources on demand. It is a promising solution for utility computing. Increasing number of cloud service providers having similar functionality poses a problem to cloud users of its selection. To assist the users, for selection of a best service provider as per user's requirement, it is necessary to create a solution. User may provide its QoS expectation and service providers may also express the offers. Experience of existing users may also be beneficial in selection of best cloud service provider. This paper identifies QoS metrics and defines it in such a way that user and provider both can express their expectation and offers respectively into quantified form. A dynamic and flexible framework using Ranked Voting Method is proposed which takes requirement of user as an input and provides a best provider as output.

45. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability

Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose to build privacy into mobile healthcare systems with the help of the private cloud. Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and auditability for misusing health data. Specifically, we propose to integrate key management from pseudorandom number generator for unlinkability, a secure indexing method for privacypreserving keyword searchwhich hides both search and access patterns based on redundancy, and integrate the concept of attributebased encryption with threshold signing for providing role-based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.

46. iFarm: Development of Cloud-based System of Cultivation Management for Precision Agriculture

Precision agriculture is aimed at optimizing farming management and it requires records of agricultural work. Farmers conventionally write records on paper but it is difficult and tedious to check past agricultural-work data and control the cost of agricultural products. A system of cultivation management, iFarm, is proposed, which was developed to support efficient farming management. The system consists of smartphone applications, Web browsers and a cloud server. Farmers on farmland can easily refer to work plans, enter field data into the cloud system, and share them with head office in real time by using smartphones. Farmers at head office can analyze data in the cloud system with a Web browser and estimate farming costs and form work plans based on their analyses

47. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of “coordinate matching,” i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use “inner product similarity” to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

48. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information—identity privacy—to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity

49. Load Rebalancing for Distributed File Systems in Clouds

Distributed file systems are key building blocks for cloud computing applications based on the MapReduce programming paradigm. In such file systems, nodes simultaneously serve computing and storage functions; a file is partitioned into a number of chunks allocated in distinct nodes so that MapReduce tasks can be performed in parallel over the nodes. However, in a cloud computing environment, failure is the norm, and nodes may be upgraded, replaced, and added in the system. Files can also be dynamically created, deleted, and appended. This results in load imbalance in a distributed file system; that is, the file chunks are not distributed as uniformly as possible among the nodes. Emerging distributed file systems in production systems strongly depend on a central node for chunk reallocation. This dependence is clearly inadequate in a large-scale, failure-prone environment because the central load balancer is put under considerable workload that is linearly scaled with the system size, and may thus become the performance bottleneck and the single point of failure. In this paper, a fully distributed load rebalancing algorithm is presented to cope with the load imbalance problem. Our algorithm is compared against a centralized approach in a production system and a competing distributed solution presented in the literature. The simulation results indicate that our proposal is comparable with the existing centralized approach and considerably outperforms the prior distributed algorithm in terms of load imbalance factor, movement cost, and algorithmic overhead. The performance of our proposal implemented in the Hadoop distributed file system is further investigated in a cluster environment.

50. Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation

The advent of the cloud computing makes storage outsourcing become a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research consider the problemof secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation in practical cloud storage system. In this paper, we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the our scheme definition. Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, countability and traceability of secure group user revocation. Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

51. Optimizing Cloud Resources for Delivering IPTV Services Through Virtualization

Virtualized cloud-based services can take advantage of statistical multiplexing across applications to yield significant cost savings. However, achieving similar savings with real-time services can be a challenge. In this paper, we seek to lower a provider's costs for real-time IPTV services through a virtualized IPTV architecture and through intelligent time-shifting of selected services. Using Live TV and Video-on-Demand (VoD) as examples, we show that we can take advantage of the different deadlines associated with each service to effectively multiplex these services. We provide a generalized framework for computing the amount of resources needed to support multiple services, without missing the deadline for any service. We construct the problem as an optimization formulation that uses a generic cost function. We consider multiple forms for the cost function (e.g., maximum, convex and concave functions) reflecting the cost of providing the service. The solution to this formulation gives the number of servers needed at different time instants to support these services. We implement a simple mechanism for time-shifting scheduled jobs in a simulator and study the reduction in server load using real traces from an operational IPTV network. Our results show that we are able to reduce the load by ~ 24% (compared to a possible ~ 31%). We also show that there are interesting open problems in designing mechanisms that allow time-shifting of load in such environments.

52. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

53. Secure Logging As a Service—Delegating Log Management to the Cloud

Securely maintaining log records over extended periods of time is very important to the proper functioning of any organization. Integrity of the log files and that of the logging process need to be ensured at all times. In addition, as log files often contain sensitive information, confidentiality and privacy of log records are equally important. However, deploying a secure logging infrastructure involves substantial capital expenses that many organizations may find overwhelming. Delegating log management to the cloud appears to be a viable cost saving measure. In this paper, we identify the challenges for a secure cloud-based log management service and propose a framework for doing the same.

54. Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing

Cloud computing is an Internet-based computing. Computing services, such as data, storage, software, computing,and application, are delivered to local devices through Internet. The major security issue of cloud computing is that the cloud provider must ensure that their infrastructure is secure, and that prevent illegal data accesses from outsiders, other clients, or even the unauthorized cloud employees. In this paper, we deal with cloud security services including key agreement and authentication. By using Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing, we design the secure cloud computing (SCC). Two types of SCC are proposed. One requires a trusted third party (TTP), and the other does not need a TTP. Also, our SCC can be extended to multi-server SCC (MSCC) to fit an environment, where each multi-server system contains multiple servers to collaborate for serving applications. Due to the strong security and operation efficiency, the proposed SCC and MSCC are extremely suitable for use in cloud computing.

55. A cloud computing based telemedicine service

Health is the greatest invention of technology in medicine. Earlier slow and erroneous processes are replaced by precise and faultless methods involving fast internet services. These techniques allow real-time data accessibility with proper authentication. The idea is based on cloud-computing and real time streaming of videos. The information is made available on the WEB in a suitable format, from where, it can be accessed by authorized medical staff. Cloud computing has a revolutionary effect on telemedicine. Many medical professionals are already using advance telehealth application of cloud computing. According to various specialists and researchers, cloud computing can improve healthcare services to an undoubtedly large extent. This paper discusses the advancement in utilization of cloud computing in field of telehealth. It can contribute to improve health scenario all over the world.

56. Privacy-Preserving Public Auditing for Secure Cloud Storage

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance.However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

57. CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring

Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy reencryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

58. Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing

In cloud computing, data generated in electronic form are large in amount. To maintain this data efficiently, there is a necessity of data recovery services. To cater this, in this paper we propose a smart remote data backup algorithm, Seed Block Algorithm (SBA). The objective of proposed algorithm is twofold; first it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process. Proposed SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques.

59. An Improved Mutual Authentication Framework for Cloud Computing

In this paper, wehave propose a user authentication scheme for cloud computing. The proposed framework providesmutual authentication and session key agreement in cloud computing environment. The scheme executesin three phases such as server initialization phase, registration phase, authentication phase. Detailed security analyses have been made to validate the efficiency of the scheme. Further, the scheme has the resistance to possible attacks in cloud computing.

60. Innovative Schemes for Resource Allocation in the Cloud for Media Streaming Applications

Media streaming applications have recently attracted a large number of users in the Internet. With the advent of these bandwidth-intensive applications, it is economically inefficient to provide streaming distribution with guaranteed QoS relying only on central resources at a media content provider. Cloud computing offers an elastic infrastructure that media content providers (e.g., Video on Demand (VoD) providers) can use to obtain streaming resources that match the demand. Media content providers are charged for the amount of resources allocated (reserved) in the cloud. Most of the existing cloud providers employ a pricing model for the reserved resources that is based on non-linear time-discount tariffs (e.g., Amazon CloudFront and Amazon EC2). Such a pricing scheme offers discount rates depending non-linearly on the period of time during which the resources are reserved in the cloud. In this case, an open problem is to decide on both the right amount of resources reserved in the cloud, and their reservation time such that the financial cost on the media content provider is minimized.We propose a simple - easy to implement - algorithm for resource reservation that maximally exploits discounted rates offered in the tariffs, while ensuring that sufficient resources are reserved in the cloud. Based on the prediction of demand for streaming capacity, our algorithm is carefully designed to reduce the risk of making wrong resource allocation decisions. The results of our numerical evaluations and simulations show that the proposed algorithm significantly reduces the monetary cost of resource allocations in the cloud as compared to other conventional schemes.

61. NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds

To provide fault tolerance for cloud storage, recent studies propose to stripe data across multiple cloud vendors. However, if a cloud suffers from a permanent failure and loses all its data, we need to repair the lost data with the help of the other surviving clouds to preserve data redundancy. We present a proxy-based storage system for fault-tolerant multiple-cloud storage called NCCloud, which achieves cost-effective repair for a permanent single-cloud failure. NCCloud is built on top of a network-coding-based storage scheme called the functional minimum-storage regenerating (FMSR) codes, which maintain the same fault tolerance and data redundancy as in traditional erasure codes (e.g., RAID-6), but use less repair traffic and, hence, incur less monetary cost due to data transfer. One key design feature of our FMSR codes is that we relax the encoding requirement of storage nodes during repair, while preserving the benefits of network coding in repair. We implement a proof-of-concept prototype of NCCloud and deploy it atop both local and commercial clouds. We validate that FMSR codes provide significant monetary cost savings in repair over RAID-6 codes, while having comparable response time performance in normal cloud storage operations such as upload/download.

62. Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

63. Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing

Cloud computing is a new approach in the field of information technology and development of computer technologies based on the World Wide Web. One of the most important challenges in this area is the security of cloud computing. On the other hand the security of access to critical and confidential information in banks, institutions and etc is extremely essential. Sometimes even with the enormous costs, it is not fully guaranteed and it is compromised by the attackers. In this paper by providing a novel method, we improve the security of data access in cloud computing for a company or any other specific locations using the location-based encryption.

64. C-MART: Benchmarking the Cloud Parallel and Distributed Systems

Cloud computing environments provide on-demand resource provisioning, allowing applications to elastically scale. However, application benchmarks currently being used to test cloud management systems are not designed for this purpose. This results in resource underprovisioning and quality-of-service (QoS) violations when systems tested using these benchmarks are deployed in production environments. We present C-MART, a benchmark designed to emulate a modern web application running in a cloud computing environment. It is designed using the cloud computing paradigm of elastic scalability at every application tier and utilizes modern web-based technologies such as HTML5, AJAX, jQuery, and SQLite. C-MART consists of a web application, client emulator, deployment server, and scaling API. The deployment server automatically deploys and configures the test environment in orders of magnitude less time than current benchmarks. The scaling API allows users to define and provision their own customized datacenter. The client emulator generates the web workload for the application by emulating complex and varied client behaviors, including decisions based on page content and prior history. We show that C-MART can detect problems in management systems that previous benchmarks fail to identify, such as an increase from 4.4 to 50 percent error in predicting server CPU utilization and resource underprovisioning in 22 percent of QoS measurements.

65. Pre-emptive scheduling of on-line real time services with task migration for cloud computing

This paper presents a new scheduling approach to focus on providing a solution for online scheduling problem of real-time tasks using “Infrastructure as a Service” model offered by cloud computing. The real time tasks are scheduled pre-emptively with the intent of maximizing the total utility and efficiency. In traditional approach, the task is scheduled non- pre-emptively with two different types of Time Utility Functions (TUFs) - a profit time utility function and a penalty time utility function. The task with highest expected gain is executed. When a new task arrives with highest priority then it cannot be taken for execution until it completes the currently running task. Therefore the higher priority task is waiting for a longer time. This scheduling method sensibly aborts the task when it misses its deadline. Note that, before a task is aborted, it consumes system resources including network bandwidth, storage space and processing power. This leads to affect the overall system performance and response time of a task. In our approach, a preemptive online scheduling with task migration algorithm for cloud computing environment is proposed in order to minimize the response time and to improve the efficiency of the tasks. Whenever a task misses its deadline, it will be migrated the task to another virtual machine. This improves the overall system performance and maximizes the total utility. Our simulation results outperform the traditional scheduling algorithms such as the Earliest Deadline First (EDF) and an earlier scheduling approach based on the similar model.

66. Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data

Cloud computing has emerging as a promising pattern for data outsourcing and high-quality data services. However, concerns of sensitive information on cloud potentially causes privacy problems. Data encryption protects data security to some extent, but at the cost of compromised efficiency. Searchable symmetric encryption (SSE) allows retrieval of encrypted data over cloud. In this paper, we focus on addressing data privacy issues using SSE. For the first time, we formulate the privacy issue from the aspect of similarity relevance and scheme robustness. We observe that server-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-(k) multikeyword retrieval. In TRSE, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext. As a result, information leakage can be eliminated and data security is ensured. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency.

67. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.