



SPECTRUM SOLUTIONS

Pondicherry, India

Approved by Indian Government under Section 21

S.NO	TITLE	YEAR	ABSTRACT
1	A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data	2016	<p>Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF_IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results . Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.</p>
2	An Efficient Privacy-Preserving Ranked Keyword Search Method	2016	<p>Cloud data owners prefer to outsource documents in an encrypted form for the purpose of privacy preserving. Therefore it is essential to develop efficient and reliable ciphertext search techniques. One challenge is that the relationship between documents will be normally concealed in the process of encryption, which will lead to significant search accuracy performance degradation. Also the volume of data in data centers has experienced a dramatic growth. This will make it even more challenging to design ciphertext search schemes</p>

			<p>that can provide efficient and reliable online information retrieval on large volume of encrypted data. In this paper, a hierarchical clustering method is proposed to support more search semantics and also to meet the demand for fast ciphertext search within a big data environment. The proposed hierarchical approach clusters the documents based on the minimum relevance threshold, and then partitions the resulting clusters into sub-clusters until the constraint on the maximum size of cluster is reached. In the search phase, this approach can reach a linear computational complexity against an exponential size increase of document collection. In order to verify the authenticity of search results, a structure called minimum hash sub-tree is designed in this paper. Experiments have been conducted using the collection set built from the IEEE Xplore. The results show that with a sharp increase of documents in the dataset the search time of the proposed method increases linearly whereas the search time of the traditional method increases exponentially. Furthermore, the proposed method has an advantage over the traditional method in the rank privacy and relevance of retrieved documents.</p>
3	<p>Dynamic and Public Auditing with Fair Arbitration for Cloud Data</p>	2016	<p>Cloud users no longer physically possess their data, so how to ensure the integrity of their outsourced data becomes a challenging task. Recently proposed schemes such as “provable data possession” and “proofs of retrievability” are designed to address this problem, but they are designed to audit static archive data and therefore lack of data dynamics support. Moreover, threat models in these schemes usually assume an honest data owner and focus on detecting a dishonest cloud service provider despite the fact that clients may also misbehave. This paper proposes a public auditing scheme with data dynamics support and fairness arbitration of potential disputes. In particular, we design an index switcher to eliminate the limitation of index usage in tag computation in current schemes and achieve efficient handling of data dynamics. To address the fairness</p>

			<p>problem so that no party can misbehave without being detected, we further extend existing threat models and adopt signature exchange idea to design fair arbitration protocols, so that any possible dispute can be fairly settled. The security analysis shows our scheme is provably secure, and the performance evaluation demonstrates the overhead of data dynamics and dispute arbitration are reasonable.</p>
4	Fine-grained Two-factor Access Control for Web-based Cloud Computing Services	2016	<p>In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a lightweight security device. As a user cannot access the system if s/he does not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.</p>
5	CloudArmor: Supporting Reputation-based Trust Management for Cloud Services	2016	<p>Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability of the trust management service is another</p>

			<p>significant challenge because of the dynamic nature of cloud environments. In this article, we describe the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks and preserve users' privacy, ii) an adaptive and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to compare the trustworthiness of cloud services, and iii) an availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services</p>
6	<p>Identity-Based Encryption with Cloud Revocation Authority and Its Applications</p>	2016	<p>Abstract—Identity-based encryption (IBE) is a public key cryptosystem and eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li <i>et al.</i> proposed a revocable IBE scheme with a key-update cloud service provider (KU-CSP). However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user. In the article, we propose a new revocable IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings, namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH)</p>

			assumption. Finally, we extend the proposed revocable IBE scheme to present a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services
7	Geometric Range Search on Encrypted Spatial Data	2016	Geometric range search is a fundamental primitive for spatial data analysis in SQL and NoSQL databases. It has extensive applications in Location-Based Services, computer-aided design and computational geometry. Due to the dramatic increase of data size, it is necessary for companies and organizations to outsource their spatial datasets to third-party cloud services (e.g. Amazon) in order to reduce storage and query processing costs, but meanwhile with the promise of no privacy leakage to the third party. Searchable encryption is a technique to perform meaningful queries on encrypted data without revealing privacy. However, geometric range search on spatial data has not been fully investigated nor supported by existing searchable encryption schemes. In this paper, we design a symmetric-key searchable encryption scheme that can support geometric range queries on encrypted spatial data. One of our major contributions is that our design is a <i>general</i> approach, which can support different types of geometric range queries. In other words, our design on encrypted data is <i>independent</i> from the shapes of geometric range queries. Moreover, we further extend our scheme with the additional use of tree structures to achieve search complexity that is <i>faster than linear</i> . We formally define and prove the security of our scheme with indistinguishability under Selective Chosen-Plaintext Attacks (IND-SCPA), and demonstrate the performance of our scheme with experiments in a real cloud platform (Amazon EC2).
8	An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing	2016	Ciphertext-policy attribute-based encryption (CPABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy,

			<p>particularly in the area of healthcare and the military. However, the hierarchy structure of shared files hasn't been explored in CP-ABE. In this paper, an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. The ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.</p>
9	<p>Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing</p>	2016	<p>Abstract—In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the task of the decryption to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of</p>

			<p>the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.</p>
10	<p>Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud Email</p>	2016	<p>Recently, a number of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), Identity-Based PRE (IPRE) and Broadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a versatile primitive referred to as Conditional Identity-based Broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple receivers by specifying these receivers' identities, and the sender can delegate a re-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, the re-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows the original sender to enforce access control over his remote ciphertexts in a fine-grained manner. We propose an efficient CIBPRE scheme with provable security. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption key are all in constant size, and the parameters to generate a re-encryption key is independent of the original receivers of any initial ciphertext. Finally, we show an application of our CIBPRE to secure cloud email system advantageous over existing secure email systems based on Pretty Good Privacy protocol or Identity-Based Encryption.</p>
11	<p>Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-encryption Function for E-health Clouds</p>	2016	<p>Electronic health (e-health) record system is a novel application that will bring great convenience in healthcare. The privacy and security of the sensitive personal information is the major concern of the users, which could hinder further development and widely adoption of the systems. The searchable</p>

			<p>encryption (SE) scheme is a technology to incorporate security protection and favorable operability functions together, which can play an important role in the e-health record system. In this paper, we introduce a novel cryptographic primitive named as conjunctive keyword search with designated tester and timing enabled proxy re-encryption function (Re-dtPECK), which is a kind of time-dependent searchable encryption scheme. It could enable patients to delegate partial access rights to others to operate search functions over their records in a limited time period. The length of the time period for the delegatee to search and decrypt the delegator's encrypted documents can be controlled. Moreover, the delegatee could be automatically deprived of the access and search authority after a specified period of effective time. It can also support the conjunctive keywords search and resist the keyword guessing (KG) attacks. By the solution, only the designated tester is able to test the existence of certain keywords. We formulate a system model and a security model for the proposed Re-dtPECK scheme to show that it is an efficient scheme proved secure in the standard model. The comparison and extensive simulations demonstrate that it has a low computation and storage overhead.</p>
12	Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates	2016	<p>Key-exposure resistance has always been an important issue for in-depth cyber defence in many security applications. Recently, how to deal with the key exposure problem in the settings of cloud storage auditing has been proposed and studied. To address the challenge, existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local burdens to the client, especially those with limited computation resources such as mobile phones. In this paper, we focus on how to make the key updates as transparent as possible for the client and propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this paradigm, key updates can be safely outsourced to some authorized party,</p>

			<p>and thus the key-update burden on the client will be kept minimal. Specifically, we leverage the third party auditor (TPA) in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key, while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. We formalize the definition and the security model of this paradigm. The security proof and the performance simulation show that our detailed design instantiations are secure and efficient.</p>
13	<p>Online Resource Scheduling under Concave Pricing for Cloud Computing</p>	2016	<p>With the booming cloud computing industry, computational resources are readily and elastically available to the customers. In order to attract customers with various demands, most Infrastructure-as-a-service (IaaS) cloud service providers offer several pricing strategies such as pay as you go, pay less per unit when you use more (so called volume discount), and pay even less when you reserve. The diverse pricing schemes among different IaaS service providers or even in the same provider form a complex economic landscape that nurtures the market of cloud brokers. By strategically scheduling multiple customers' resource requests, a cloud broker can fully take advantage of the discounts offered by cloud service providers. In this paper, we focus on how a broker can help a group of customers to fully utilize the volume discount pricing strategy offered by cloud service providers through cost-efficient online resource scheduling. We present a randomized online stack-centric scheduling algorithm</p>

			(ROSA) and theoretically prove the lower bound of its competitive ratio. Three special cases of the offline concave cost scheduling problem and the corresponding optimal algorithms are introduced. Our simulation shows that ROSA achieves a competitive ratio close to the theoretical lower bound under the special cases. Trace-driven simulation using Google cluster data demonstrates that ROSA is superior to the conventional online scheduling algorithms in terms of cost saving.
14	Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption	2016	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
15	A Modified Hierarchical Attribute-Based Encryption Access Control Method for	2016	Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices ondemand. Its

	Mobile Cloud Computing	<p>an emerging but promising paradigm to integrating mobile devices into cloud computing, and the integration performs in the cloud based hierarchical multi-user data-shared environment. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system, and it is concerned as the main constraints to the developments of mobile cloud computing. In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this paper. In a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms.</p>
--	------------------------	--