JAVA IEEE Projects Titles – 2017-2018

S.NO	TITLES	YEAR	ABSTRACT
1	A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing	2017	Ciphertext policy attribute-based encryption (CP-ABE) is a promising cryptographic technique for fine-grained access control of outsourced data in the cloud. However, some drawbacks of key management hinder the popularity of its application. One drawback in urgent need of solution is the key escrow problem. We indicate that front-end devices of clients like smart phones generally have limited privacy protection, so if private keys are entirely held by them, clients risk key exposure that is hardly noticed but inherently existed in previous research. Furthermore, enormous client decryption overhead limits the practical use of ABE. In this work, we propose a collaborative key management protocol in CP-ABE (CKM-CP-ABE). Our construction realizes distributed generation, issue and storage of private keys without adding any extra infrastructure. A fine-grained and immediate attribute revocation is provided for key update. The proposed collaborative mechanism effectively solves not only key escrow problem but also key exposure. Meanwhile, it helps markedly reduce client decryption overhead. A comparison with other representative CP-ABE schemes demonstrates that our scheme has somewhat better performance in terms of cloud-based outsourced data sharing on mobile devices. Finally, we provide proof of security for the proposed protocol.
2	Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud	2017	Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing specific credentials (or attributes). However, the standard ABE system does not support secure deduplication, which is crucial for eliminating duplicate copies of identical data in order to save

			storage space and network bandwidth. In this paper, we present an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data deduplication systems, our system has two advantages. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion. In addition, we put forth a methodology to modify a ciphertext over one access policy into ciphertexts of the same plaintext but under other access policies without revealing the underlying plaintex
3	Customer-Satisfaction-Aware Optimal Multiserver Configuration for Profit Maximization in Cloud Computing	2017	Along with the development of cloud computing, an increasing number of enterprises start to adopt cloud service, which promotes the emergence of many cloud service providers. For cloud service providers, how to configure their cloud service platforms to obtain the maximum profit becomes increasingly the focus that they pay attention to. In this paper, we take customer satisfaction into consideration to address this problem. Customer satisfaction affects the profit of cloud service providers in two ways. On one hand, the cloud configuration affects the quality of service which is an important factor affecting customer satisfaction. On the other hand, the customer satisfaction affects the request arrival rate of a cloud service provider. However, few existing works take customer satisfaction into consideration in solving profit maximization problem, or the existing works considering customer satisfaction do not give a proper formalized definition for it. Hence, we firstly refer to the definition of customer satisfaction in economics and develop a formula for measuring customer satisfaction in cloud computing. And then, an analysis is given in detail on how the customer satisfaction affects the profit. Lastly, taking into consideration customer satisfaction, service-

			level agreement, renting price, energy consumption and so forth, a profit maximization problem is formulated and solved to get the optimal configuration such that the profit is maximized
4	Fast Phrase Search for Encrypted Cloud Storage	2017	Cloud computing has generated much interest in the research community in recent years for its many advantages, but has also raise security and privacy concerns. The storage and access of confidential documents have been identified as one of the central problems in the area. In particular, many researchers investigated solutions to search over encrypted documents stored on remote cloud servers. While many schemes have been proposed to perform conjunctive keyword search, less attention has been noted on more specialized searching techniques. In this paper, we present a phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost. Our technique uses a series of n-gram filters to support the functionality. The scheme exhibits a trade-off between storage and false positive rate, and is adaptable to defend against inclusion-relation attacks. A design approach based on an application's target false positive rate is also described
5	Securing Cloud Data under Key Exposure	2017	Recent news reveal a powerful attacker which breaks data confidentiality by acquiring cryptographic keys, by means of coercion or backdoors in cryptographic software. Once the encryption key is exposed, the only viable measure to preserve data confidentiality is to limit the attacker's access to the ciphertext. This may be achieved, for example, by spreading ciphertext blocks across servers in multiple administrative domains—thus assuming that the adversary cannot compromise all of them. Nevertheless, if data is encrypted with existing schemes, an adversary equipped with the encryption key, can still Compromise a single server and decrypt the ciphertext blocks stored therein. In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the ciphertext blocks. To

			this end, we propose Bastion, a novel and efficient scheme that guarantees data confidentiality even if the encryption key is leaked and the adversary has access to almost all cipher text blocks. We analyze the security of Bastion, and we evaluate its performance by means of a prototype implementation. We also discuss practical insights with respect to the integration of Bastion in commercial dispersed storage systems. Our evaluation results suggest that Bastion is well-suited for integration in existing systems since it incurs less than 5% overhead compared to existing semantically secure encryption modes.
6	A New Service Mechanism for Profit Optimizations of a Cloud Provider and Its Users	2017	In this paper, we try to design a service mechanism for profit optimizations of both a cloud provider and its multiple users. We consider the problem from a game theoretic perspective and characterize the relationship between the cloud provider and its multiple users as a Stackelberg game, in which the strategies of all users are subject to that of the cloud provider. The cloud provider tries to select and provision appropriate servers and configure a proper request allocation strategy to reduce energy cost while satisfying its cloud users at the same time. We approximate its servers selection space by adding a controlling parameter and configure an optimal request allocation strategy. For each user, we design a utility function which combines the net profit with time efficiency and try to maximize its value under the strategy of the cloud provider. We formulate the competitions among all users as a generalized Nash equilibrium problem (GNEP). We solve the problem by employing variational inequality (VI) theory and prove that there exists a generalized Nash equilibrium solution set for the formulated GNEP. Finally, we propose an iterative algorithm (IA), which characterizes the whole process of our proposed service mechanism. We conduct some numerical calculations to verify our theoretical analyses. The experimental results show that our IA algorithm can benefit both of a cloud provider and its multiple users by configuring proper strategies.

7	Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Smart Grid	2017	Cloud-supported Internet of Things (Cloud-IoT) has been broadly deployed in smart grid systems. The IoT front-ends are responsible for data acquisition and status supervision, while the substantial amount of data is stored and managed in the cloud server. Achieving data security and system efficiency in the data acquisition and transmission process are of great significance and challenging, because the power grid-related data is sensitive and in huge amount. In this paper, we present an efficient and secure data acquisition scheme based on CP-ABE (Ciphertext Policy Attribute Based Encryption). Data acquired from the terminals will be partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and data transmission can be processed in parallel. Furthermore, we protect the information about the access tree with threshold secret sharing method, which can preserve the data privacy and integrity from users with the unauthorized sets of attributes. The formal analysis demonstrates that the proposed scheme can fulfill the security Requirements of the Cloud-supported IoT in smart grid. The numerical analysis and experimental results indicate that our Scheme can effectively reduce the time cost compared with other popular approaches.
8	Achieving secure, universal, and fine grained query results verification for secure search scheme over encrypted cloud data	2017	Secure search techniques over encrypted cloud data allow an authorized user to query data files of interest by submitting encrypted query keywords to the cloud server in a privacy-preserving manner. However, in practice, the returned query results may be incorrect or incomplete in the dishonest cloud environment. For example, the cloud server may intentionally omit some qualified results to save computational resources and communication overhead. Thus, a well-functioning secure query system should provide a query results verification mechanism that allows the data user to verify results. In this paper, we design a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the

			correctness of each data file in the set but also can further check how many or which qualified data files are not returned if the set is incomplete before decryption. The verification scheme is loose-coupling to concrete secure search techniques and can be very easily integrated into any secure query scheme. We achieve the goal by constructing secure verification object for encrypted cloud data. Furthermore, a short signature technique with extremely small storage cost is proposed to guarantee the authenticity of verification object and a verification object request technique is presented to allow the query user to securely obtain the desired verification object. Performance evaluation shows that the proposed schemes are practical and efficient.