ANSPRO TECHNOLOGIES

IEEE 2018-19 PROJECT LIST(JAVA)

CLOUD COMPUTING AND MOBILE CLOUD COMPUTING

CODE	TITLE AND ABSTRACT
19ANSP-CC-001	**Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing** ***Abstract*** — Cloud computing and social networks are changing the way of healthcare by providing real-time data sharing in a cost-effective manner. However, data security issue is one of the main obstacles to the wide application of mobile healthcare social networks (MHSNs), since health information is considered to be highly sensitive. In this paper, we introduce a secure data sharing and profile matching scheme for the MHSN in cloud computing. The patients can outsource their encrypted health records to cloud storage with an identity-based broadcast encryption technique, and share them with a group of doctors in a secure and efficient manner. We then present an attribute-based conditional data re-encryption construction which permits the doctors who satisfy the pre-defined conditions in the ciphertext to authorize the cloud platform to convert a ciphertext into a new ciphertext of an identity-based encryption scheme for specialist without leaking any sensitive information. Furthermore, we provide a profile matching mechanism in the MHSN based on identity-based encryption with an equality test, which helps patients to find friends in a privacy-preserving way and achieves flexible authorization on the encrypted health records with resisting the keywords guessing attack. Moreover, this mechanism reduces the computation cost on the patient side. The security analysis and experimental evaluation show that our scheme is practical for protecting the data security and privacy in the MHSN.
19ANSP-CC-002	**Security Analysis of Smartphone and Cloud Computing Authentication Frameworks and Protocols** ***Abstract*** — We live in a digital world where every detail of our information is being transferred from one smart device to another via cross-platform, third-party cloud services. Smart technologies, such as,

	smartphones are playing dynamic roles in order to successfully complete our daily routines and official tasks that require access to all types of critical data. Before the advent of these smart technologies, securing critical information was quite a challenge. However, after the advent and global adoption of such technologies, information security has become one of the primary and most fundamental task for security professionals. The integration of social media has made this task even more challenging to undertake successfully. To this day, there are plentiful studies in which numerous authentication and security techniques were proposed and developed for smartphone and cloud computing technologies. These studies have successfully addressed multiple authentication threats and other related issues in existing the smartphone and cloud computing technologies. However, to the best of our understanding and knowledge, these studies lack many aspects in terms of authentication attacks, logical authentication analysis, and the absence of authentication implementation scenarios. Due to these authentication anomalies and ambiguities, such studies cannot be fully considered for successful implementation. Therefore, in this paper, we have performed a comprehensive security analysis and review of various smartphone and cloud computing authentication frameworks and protocols to outline up-to-date authentication threats and issues in the literature. These authentication challenges are further summarized and presented in the form of different graphs to illustrate where the research is currently heading. Finally, based on those outcomes, we identify the latest and existing authentication uncertainties, threats, and other related issues to address future directions and open research issues in the domain of the smartphone and cloud-computing authentication.
19ANSP-CC-003	**Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing** ***Abstract***—EVCE computing is an attractive network paradigm involving seamless connections among heterogeneous vehicular contexts. It will be a trend along with EVs becoming popular in V2X. The EVs act as potential resource infrastructures referring to both information and energy interactions, and there are serious security challenges for such hybrid cloud and edge computing. Context-aware vehicular applications are identified according to the perspectives of information and energy interactions. Blockchain-inspired data coins and energy coins are proposed based on distributed consensus, in which data contribution frequency and energy contribution amount are applied to achieve the

	proof of work. Security solutions are presented for securing vehicular interactions in EVCE computing.
19ANSP-CC-004	**Collaborative Security in Vehicular Cloud Computing: A Game Theoretic View** ***Abstract***— Connected vehicular cloud computing (CVCC) is a promising paradigm that utilizes the rich resources of connected cars. However, it also introduces new cyber-attack surfaces that may compromise the security or privacy of the vehicles. In reality, security in vehicular cloud computing lies in the willingness of vehicle owners who are concerned with their vehicles' protection from various threats. Increasing the participation of vehicles will improve the security in vehicular cloud computing as a whole. Therefore, for a CVCC service provider, it is very critical to encourage vehicle owners to invest in their own security for achieving deeper security of CVCC systems. In this article, we first present a CVCC architecture and its applications. Then we study several security issues in vehicular cloud computing. Afterward, we model a CVCC network by a two-phase heterogeneous public good game, and then investigate the influence of different incentive mechanisms and the structure of a complex network describing the vehicles' connectivity on the vehicles' investment rate. Finally, we present our conclusion.
19ANSP-CC-005	**Secure and Efficient Privacy-Preserving Ciphertext Retrieval in Connected Vehicular Cloud Computing** **ABSTRACT** As vehicular equipment is becoming more and more intelligent, the vehicular information service, as the main means of capturing information, has been far from able to meet the needs of occupants. Cloud computing, with its powerful computing and storage capabilities, convenient network access, energy saving and excellent scalability, reliability, availability, and other advantages, can be an effective solution to the limitations of existing automotive information services. Connected vehicular cloud computing, which combines cloud computing and VANETs, has the characteristics of both a cloud platform and a mobile ad hoc network, including autonomy and no fixed structure, good scalability, and so on. However, during the information retrieval, high-density node distribution and high-speed mobile nodes may directly affect the information transmission capacity of a VANET by information tampering, transmission delay, and other issues. In this article, we propose a ciphertext-based search system that exploits RSUs as super peers for connected vehicular cloud computing. The proposed system supports ciphertext retrieval for related documents. In the proposed

	system, all the computations and retrieval operations are handled by super stationary peers, while documents are stored in the cloud to achieve high efficiency and security of the index structure. We can also reduce the impact of vehicle dynamics on the information retrieval process in this way. In our system, the indexing efficiency is also improved by utilizing a hybrid indexing structure in which binary trees are nested in a B+ tree. Through security analysis and performance evaluation, we demonstrate that our proposal can achieve acceptable security and efficiency.
19ANSP-CC-006	**Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing** **ABSTRACT** VCC leverages the underutilized storage and computing resources of vehicles to collaboratively provide traffic management, road safety, and infotainment services to end users, such as drivers and passengers. It is a hybrid technology that improves the resource utilization on vehicles and is able to perform complex computing tasks that cannot be handled by a single vehicle. Despite the appealing advantages, security and privacy threats are severe in VCC due to the sharing of resources among unfamiliar vehicles. In this article, we identify security goals for the interoperability with VCC and provide an AKA framework for VCC. Specifically, we first present the research challenges and open problems for designing a reliable AKA with strong security guarantees for VCC. Then we propose an integrated AKA framework that integrates the single-server 3-factor AKA protocol and the non-interactive identity-based key establishment protocol, and evaluate its performance based on a simulated experimental platform. Finally, several interesting issues are discussed to light up the further research directions on AKA for VCC.
19ANSP-CC-007	**Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing** **ABSTRACT** Decentralizing multi-authority attribute-based encryption (ABE) has been adopted for solving problems arising from sharing confidential corporate data in cloud computing. For decentralizing multiauthority ABE systems that do not rely on a central authority, collusion resistance can be achieved using a global identifier. Therefore, identity needs to be managed globally, which results in the crucial problems of privacy and security. A scheme is developed that does not use a central authority to manage users and keys, and only simple trust

	relations need to be formed by sharing the public key between each attribute authority (AA). User identities are unique by combining a user's identity with the identity of the AA where the user is located. Once a key request needs to be made to an authority outside the domain, the request needs to be performed by the authority in the current domain rather than by the users, so, user identities remain private to the AA outside the domain, which will enhance privacy and security. In addition, the key issuing protocol between AA is simple as the result of the trust relationship of AA. Moreover, extensibility for authorities is also supported by the scheme presented in this paper. The scheme is based on composite order bilinear groups. A proof of security is presented that uses the dual system encryption methodology.
19ANSP-CC-008	**An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing** **ABSTRACT** Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which, however, brings potential threats to users' privacy. In this paper, we propose an efficient and privacy-preserving biometric identification outsourcing scheme. Specifically, the biometric to execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over the encrypted database and returns the result to the database owner. A thorough security analysis indicates that the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with previous protocols, experimental results show that the proposed scheme achieves a better performance in both preparation and identification procedures.
19ANSP-CC-009	**Semantic-Aware Searching Over Encrypted Data for Cloud Computing** ***Abstract*—**With the increasing adoption of cloud computing, a growing number of users outsource their datasets to cloud. To preserve privacy, the datasets are usually encrypted before outsourcing. However, the common practice of encryption makes the effective utilization of the data difficult. For example, it is difficult to search the given keywords in encrypted datasets. Many schemes are proposed to make encrypted data searchable based on keywords. However, keyword-based search schemes ignore the semantic representation information of users' retrieval, and

	cannot completely meet with users search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, we propose ECSED, a novel semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. ECSED uses two cloud servers. One is used to store the outsourced datasets and return the ranked results to data users. The other one is used to compute the similarity scores between the documents and the query and send the scores to the first server. To further improve the search efficiency, we utilize a tree-based index structure to organize all the document index vectors. We employ the multikey word ranked search over encrypted cloud data as our basic frame to propose two secure schemes. The experiment results based on the real-world datasets show that the scheme is more efficient than previous schemes. We also prove that our schemes are secure under the known ciphertext model and the known background model.
19ANSP-CC-010	**Secure and Efficient Product Information Retrieval in Cloud Computing** **ABSTRACT** Cloud computing is a promising information technique (IT) that can organize a large amount of IT resources in an efficient and flexible manner. Increasingly numerous companies plan to move their local data management systems to the cloud and store and manage their product information on cloud servers. An accompanying challenge is how to protect the security of the commercially confidential data, while maintaining the ability to search the data. In this paper, a privacy-preserving data search scheme is proposed, that can support both the identifier-based and feature-based product searches. Specifically, two novel index trees are constructed and encrypted, that can be searched without knowing the plaintext data. Analysis and simulation results demonstrate the security and efficiency of our scheme.
19ANSP-CC-011	**Privacy Protection Smartcard Authentication Scheme in Cloud Computing** **Abstract —** Cloud computing provides users with a great deal of flexibility and convenience. However, cloud computing also brings very serious security problems, especially for enterprise data security stored in the cloud. Once the data is outsourced to a third party, the data privacy has become a major problem, such as user authentication, integrity of data *etc*. and needs to be addressed very effectively. A mutual authentication scheme based on smartcard for cloud computing is proposed to solve the

	problem of which the illegal users access the resource of cloud servers and the legal users access the illegal cloud server. The scheme achieves mutual authentication by using hash functions to protect user privacy. Performance comparison shows that the proposed scheme is an efficient one.
19ANSP-CC-012	**Fast and Parallel Trust Computing Scheme Based on Big Data Analysis for Collaboration Cloud Service** ***Abstract*—**Providing high trustworthy service is the most fundamental task for any cloud computing platform. Users are willing to deliver their computing tasks and the most sensitive data to cloud data centers, which is based on the trust relationship established between users and cloud service providers. However, with the development of collaboration cloud computing, how to provider fast response for a large number of users' service requests becomes a challenging problem. In order to quickly provide highly trustworthy services, the service platform must efficiently and quickly reply tens of millions of service requests, and automatically match-make tens of thousands of service resources. In this context, lightweight and fast (high-speed, low overhead) trust computing schemes become the fundamental demand for implementing a trustworthy and collaborative cloud service. In this paper, we propose an innovative and parallel trust computing scheme based on big data analysis for the trustworthy cloud service environment. First, a distributed and modular perceiving architecture for large-scale virtual machines' service behavior is proposed relying on distributed monitoring agents. Then, an adaptive, lightweight, and parallel trust computing scheme is proposed for big monitored data. To the best of our knowledge, this paper is the first to use a blocked and parallel computing mechanism, the speed of trust calculation is greatly accelerated, which makes this trust computing scheme very suitable for a large-scale cloud computing environment. Performance analysis and experimental results verify feasibility and effectiveness of the proposed scheme.
19ANSP-CC-013	**EACS: An Efficient Access Control Scheme for Electronic Publishing in Cloud Computing** **Abstract** — To guarantee that electronic publications are accessible only to the authorized users via cloud, we propose an Efficient access control scheme (EACS) based on Attribute-based encryption (ABE), which is suitable for fine-grained access control. Compared with existing stateof-the-art schemes, EACS is more practical by following functions. Considering the factor that the user membership may change frequently,

	EACS has the capability of coping with dynamic membership efficiently. Arbitrary-State is also supported to facilitate the system management and improve efficiency. Besides, we prove in the standard model that the security of EACS is based on the Decisional Bilinear Diffie-Hellman assumption. To evaluate the practicality of EACS, we provide a detailed theoretical performance analysis and a simulation comparison with existing schemes. Both the theoretical analysis and the experimental results show that our proposal is efficient and practical for electronic publishing under cloud environment.
19ANSP-CC-014	**Block-Stream as a Service: A More Secure, Nimble, and Dynamically Balanced Cloud Service Model for Ambient Computing** **ABSTRACT** Cloud computing has become mainstream in the last few years. Diverse services based on IaaS, PaaS, SaaS, and app store models have been widely available to millions of users worldwide. At the same time, transparent computing (TC) has also gained strong interest in China. With the rapid development of IoT, increasing IoT devices will be deployed to provide information services for end users. As we are heading into the era of ambient computing, where end users are immersed in seamless computing devices and services, the boundary between cloud and devices is getting blurry, and more devices and services need to be securely managed. The existing service models that are defined for user-cloud interaction should be extended to serve more diverse and lightweight devices with nimble and fluid services. With this evolution trend, it is paramount for both cloud service providers and IoT service operators to manage the security and integrity of these services. In this article, we propose a new cloud service model, named block-stream as a service (BaaS), based on our previous study on TC. BaaS is nimbler than SaaS and has better security management than an app store. It is expected that this new cloud service model has great potential to support the vision of ambient computing and securely manage diverse applications on lightweight IoT devices.
19ANSP-CC-015	**A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing** ***Abstract*—**Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud servers. In other words, users lose their right of control on data and face privacy

	leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. In order to solve this problem, we propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Besides, Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.
19ANSP-CC-016	**Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment** **ABSTRACT** A centralized infrastructure system carries out existing data analytics and decision-making processes from our current highly virtualized platform of wireless networks and the Internet of Things (IoT) applications. There is a high possibility that these existing methods will encounter more challenges and issues in relation to network dynamics, resulting in a high overhead in the network response time, leading to latency and traffic. In order to avoid these problems in the network and achieve an optimum level of resource utilization, a new paradigm called edge computing (EC) is proposed to pave the way for the evolution of new age applications and services. With the integration of EC, the processing capabilities are pushed to the edge of network devices such as smart phones, sensor nodes, wearables, and on-board units, where data analytics and knowledge generation are performed which removes the necessity for a centralized system. Many IoT applications, such as smart cities, the smart grid, smart traffic lights, and smart vehicles, are rapidly upgrading their applications with EC, significantly improving response time as well as conserving network resources. Irrespective of the fact that EC shifts the workload from a centralized cloud to the edge, the analogy between EC and the cloud pertaining to factors such as resource management and computation optimization are still open to research studies. Hence, this paper aims to validate the efficiency and resourcefulness of EC. We extensively survey the edge systems and

	present a comparative study of cloud computing systems. After analyzing the different network properties in the system, the results show that EC systems perform better than cloud computing systems. Finally, the research challenges in implementing an EC system and future research directions are discussed.
19ANSP-CC-017	**Cloud Computing Fitness for E-Government Implementation: Importance-Performance Analysis** **ABSTRACT** The means through which governments deliver services and the way they operate may be considerably enhanced through cloud computing. It can help to address e-government implementation challenges and revolutionize e-government systems in terms of cost savings and the professional use of resources. The aim of this paper is to analyze the importance and performance of the factors that influence the fitness of cloud computing for e-government implementation. This paper integrates the task technology fit model with the diffusion of innovation theory to address this issue. Yemeni public institutions were identified as sources for data collection and 292 information technology employees participated as sample respondents for a structured questionnaire. Security, compatibility, relative advantage, and tasks were the variables found to affect the fitness of cloud computing for e-government activities. However, no impact was seen from the standpoints of trialability and complexity of the technology. In terms of assessing the fitness of cloud computing for e-government services, a greater understanding among policy formulators was sought through the importance-performance matrix analysis (IPMA). The results of IPMA can help identifying areas for strategic focus to assess cloud computing as an alternative technology to implement e-government services.
19ANSP-CC-018	**MAGA: A Mobility-Aware Computation Offloading Decision for Distributed Mobile Cloud Computing** ***Abstract*—**Distributed mobile cloud computing (MCC) is the new paradigm for providing ubiquitous cloud resources to mobile users with low latency. Mobility is an important factor in distributed MCC which may incur intermittent connectivity and consequently fail computation offloading requests. Latest researches on human mobility show that mobility of users present inherent patterns, periodicity, and predictability. This motivates us to propose a mobile access prediction algorithm based on tail matching subsequence, whose effectiveness and accuracy is validated by experiments using reality mobility dataset. Then MAGA, a mobility-aware offloading decision method for distributed MCC is

	proposed in this paper for single-job, multicomponent, and multisite offloading scenario. The proposed mobile access prediction is used in MAGA for cloudlet reliability estimation. An integer encoding-based adaptive genetic algorithm is used for offloading decision. Experiment results show the performance advantages of MAGA.
19ANSP-CC-019	**Anonymous and Traceable Group Data Sharing in Cloud Computing** ***Abstract*—**Group data sharing in cloud environments has become a hot topic in recent decades. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. In addition, how to achieve both anonymity and traceability is also a challenge in the cloud for data sharing. This paper focuses on enabling data sharing and storage for the same group in the cloud with high security and efficiency in an anonymous manner. By leveraging the key agreement and the group signature, a novel traceable group data sharing scheme is proposed to support anonymous multiple users in public clouds. On the one hand, group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary. On the other hand, a common conference key is derived based on the key agreement to enable group members to share and store their data securely. Note that a symmetric balanced incomplete block design is utilized for key generation, which substantially reduces the burden on members to derive a common conference key. Both theoretical and experimental analyses demonstrate that the proposed scheme is secure and efficient for group data sharing in cloud computing.
19ANSP-CC-020	**Auditable σ-Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing** ***Abstract*—**As a sophisticated mechanism for secure fine-grained access control over encrypted data, ciphertext-policy attribute-based encryption (CP-ABE) is one of the highly promising candidates for cloud computing applications. However, there exist two main long-lasting open problems of CP-ABE that may limit its wide deployment in commercial applications. One is that decryption yields expensive pairing cost which often grows with the increase of access policy size. The other is that one is granted access privilege for unlimited times as long as his attribute set satisfies the access policy of a given ciphertext. Such powerful access rights, which are provided by CP-ABE, may be undesirable in real-world applications (e.g., pay-as-you use). To address the above drawbacks, in

	this paper, we propose a new notion called *auditable σ -time outsourced CP-ABE*, which is believed to be applicable to cloud computing. In our notion, expensive pairing operation incurred by decryption is offloaded to cloud and meanwhile, the correctness of the operation can be audited efficiently. Moreover, the notion provides *σ -time fine-grained access control*. The cloud service provider may limit a particular set of users to enjoy access privilege for at most *σ* times within a specified period. As of independent interest, the notion also captures *key-leakage resistance*. The leakage of a user's decryption key does not help a malicious third party in decrypting the ciphertexts belonging to the user. We design a concrete construction (satisfying our notion) in the key encapsulation mechanism setting based on Rouselakis and Waters (prime order) CP-ABE, and further present security and extensive experimental analysis to highlight the scalability and efficiency of our construction.
19ANSP-CC-021	**A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing** **Abstract—**With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computationally intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program-based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.
19ANSP-CC-022	**Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services** ***Abstract*—**With the exponential increase of the mobile devices and the fast development of cloud computing, a new computing paradigm called

	mobile cloud computing (MCC) is put forward to solve the limitation of the mobile device's storage, communication, and computation. Through mobile devices, users can enjoy various cloud computing services during their mobility. However, it is difficult to ensure security and protect privacy due to the openness of wireless communication in the new computing paradigm. Recently, Tsai and Lo proposed a privacy-aware authentication (PAA) scheme to solve the identification problem in MCC services and proved that their scheme was able to resist many kinds of existing attacks. Unfortunately, we found that Tsai and Lo's scheme cannot resist the service provider impersonation attack, i.e., an adversary can impersonate the service provider to the user. Also, the adversary can extract the user's real identity during executing the service provider impersonation attack. To address the above problems, in this paper, we construct a new PAA scheme for MCC services by using an identity-based signature scheme. Security analysis shows that the proposed PAA scheme is able to address the serious security problems existing in Tsai and Lo's scheme and can meet security requirements for MCC services. The performance evaluation shows that the proposed PAA scheme has less computation and communication costs compared with Tsai and Lo's PAA scheme.
19ANSP-CC-023	**Supporting Mobile Cloud Computing in Smart Cities via Randomized Algorithms** ***Abstract*—**Smart cities represent rich and dynamic environments in which a multitude of smart mobile devices (SMDs) interact among them by sharing data. SMDs require from fast access to online services, but they offer limited computing capabilities and battery lifetime. SMDs make frequent use of computation offloading, delegating computing-intensive tasks to the cloud instead of performing them locally. In such a large-scale and dynamic environment, there might be thousands of SMDs simultaneously executing processes and, therefore, competing for the allotment of remote resources. This arises the need for a smart allocation of these resources. Accordingly, this paper proposes a biased-randomized algorithm to support efficient and fast link selection. This algorithm is able to provide "real-time" near-optimal solutions that outperform solutions obtained through existing greedy heuristics. Furthermore, it overcomes the responsiveness limitations of exact optimization methods.
19ANSP-CC-024	**Fair Resource Allocation for Data-Intensive Computing in the Cloud**

Abstract—To address the computing challenge of 'big data', a number of data-intensive computing frameworks (e.g., MapReduce, Dryad, Storm and Spark) have emerged and become popular. YARN is a de facto resource management platform that enables these frameworks running together in a shared system. However, we observe that, in cloud computing environment, the fair resource allocation policy implemented in YARN is not suitable because of its memoryless resource allocation fashion leading to violations of a number of good properties in shared computing systems. This paper attempts to address these problems for YARN. Both single-level and hierarchical resource allocations are considered. For single-level resource allocation, we propose a novel fair resource allocation mechanism called Long-Term Resource Fairness (LTRF) for such computing. For hierarchical resource allocation, we propose Hierarchical Long-Term Resource Fairness (H-LTRF) by extending LTRF. We show that both LTRF and H LTRF can address these fairness problems of current resource allocation policy and are thus suitable for cloud computing. Finally, we have developed LTYARN by implementing LTRF and H-LTRF in YARN, and our experiments show that it leads to a better resource fairness than existing fair schedulers of YARN.