A SURVEY ON E-HEALTH RECORDS SECURITY OVER PATIENT CENTRIC DATA IN PUBLIC CLOUD

BIRRU DEVENDER
ResearrchScholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, India.

Dr. SYED ABDUL SATTAR
PhD (ECE), PhD (CS) Director R&D, professor of ECE. Nawab shah Alam Khan college of engineering & Technology, new malakpet, malakpet, Hyderabad. T.S. India.

ABSTRACT

E- Health record service is populated in public cloud for health record exchange between different health domains. It permits health record user to generate, control, and distribute their health record with health domains. In certainty, an E-HR examine is likely to be hosted by third-party cloud service providers in order to improve its interoperability. However, there have been serious privacy concerns about outsourcing patients PHR data to the cloud server. Problem such as threat of privacy publicity, scalability in key organization, flexible admission and efficient user revocation, have continued and most significant confront toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for E-HR service, attribute-based encryption (ABE) techniques is used to encrypt each user E-HR file. In Key policy attribute-based encryption (KP-ABE), a single data owner can encrypt her data and share with multiple endorsed users by distributing keys to them. KP-ABE achieves low amortized overhead. Multiple-authority attribute-based encryption (MA-ABE) has multiple trusted authorities; each governs different subset of the system user attributes.

Keywords:- *Personal health records, cloud computing, data privacy, access control, attribute based encryption*

LITERATURE SURVEY

[Ruixuan Li ; Chenglin Shen ; Heng He ; Zhiyong Xu ; Cheng-Zhong Xu,2017] 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 computational 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.

[Ghassan O. Karame ; Claudio Soriente ; Krzysztof Lichota ; Srdjan Capkun,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 ciphertext 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.

[Fan Zhang ; Majd Sakr ; Kai Hwang ; Samee Khan,2017] Understanding the scalability of MapReduce applications is a challenging problem. The difficulty lies in the distributed mapping of the input big data. The distribution of data and compute resources must match with fluctuating network substrates. User-defined Map and Reduce functions over application parameters further complicate the issue. Therefore, it offers great payoff to use small datasets and limited test runs to reveal the behavior of MapReduce applications over big-data. In this paper, we analyze the scaling effects of server cluster-size over varieties of Map- and Reduce-intensive applications. In our study, we discover specific conditions which lead to the power-law conformity in representative MapReduce applications. We report four major discoveries: (1) Within a range of scaling parameters, MapReduce execution time follows the power-law distribution. (2) Power-law scalability for Map-intensive applications work well even with a small cluster size. (3) Shuffle-intensive applications exhibit power-law behavior starting from larger cluster size. (4) The scaling effects may depart from power-law distribution, if the cloud resources are heavily overprovisioned than the workload demands. The above findings enable users to use bounded test runs to allocate and configure virtual and physical resources in large-scale MapReduce applications. These results can be also applied in generating business models for providing cost-effective cloud computing services.

[He Li ; Kaoru Ota ; Mianxiong Dong ; Athanasios Vasilakos ; Koji Nagano,2017] Graphics processing unit (GPU) accelerated processing performs significant efficiency in many multimedia applications. With the development of GPU cloud computing, more and more cloud providers focus on GPU-accelerated services. Since the high maintenance cost and different speedups for various applications, GPU-accelerated services still need a different pricing strategy. Thus, in this paper, we propose an optimal GPU-accelerated multimedia processing service pricing strategy for maximize the profits of both cloud provider and users. We first analyze the revenues and costs of the cloud provider and users when users adopt GPU-accelerated multimedia processing services then state the profit functions of both the cloud provider and users. With a game theory based method, we find the optimal solutions of both the cloud provider's and users' profit functions. Finally, through large scale simulations, our pricing strategy brings higher profit to the cloud provider and users compared to the

original pricing strategy of GPU cloud services

[Bassem Wanis ; Nancy Samaan ; Ahmed Karmouch,2016] Cloud clients (CCs) of current distributed cloud applications are still not assured of their service quality, in particular, in terms of the experienced latency. Unfortunately, this is mainly attributed to the unpredictability of the communication links among their hosting distributed data centers. To address this problem, this article introduces a novel virtual-network-as-a-service (VNaaS) model to host these applications. In contrast to existing randomly or statically provisioned inter-data centers bandwidth sharing models, the proposed model allows CCs to accurately express their varying network resources needs, demand constraints and tolerance to the cloud latency. In turn, the model maps these requirements to create inter-data centers virtual links hosting each multiple virtual pipes with differentiated service qualities to carry the CC's various traffic flows. To aid the CCs in optimally determining their VNaaS demands, given the budget constraints of their hosted applications, we also develop a novel demand selection scheme based on a two stage-budget allocation mechanism. In the first budgeting stage, the CC calculates an optimal effective service rate for each of its virtual link along with a corresponding link budget and price index. In the second stage, the virtual link budget is distributed to purchase bandwidth for the link's virtual pipes, each with a given service quality and pricing. We then extend the proposed model to allow the CC to enforce any required virtual links' capacity constraints on the effective service rates resulting from the traffic matrix on the VNaaS

[Burak Kantarci ; Hussein T. Mouftah,2016] In the cloud era, data centers consume tremendous power due to their huge computing and storage requirements. Furthermore, allocation and release of resources by numerous cloud customers leads to significant energy consumption at the data centers, which in turn, increases the Operational expenditures (Opex) of the operators. In this article, we combine energy efficiency and Time of Use (ToU)-awareness, and propose a novel virtualization scheme, namely ToU-aware Provisioning (ToUP) for an inter-data center network over an IP over WDM backbone. In ToUP, in addition to the traffic between two backbone nodes, upstream user demands destined to data centers and downstream data center demands originating from many data centers; inter-data center traffic is also considered for workload sharing between the data centers. Initially, we present an MILP formulation to model the optimal behavior of ToUP. Since the inter-data center network needs to be reconfigured in polynomial time, we propose a simulated annealing (SA)-based heuristic. We verify the heuristic by using the MILP solution as the benchmark.

[Sunirmal Khatua ; Preetam Kumar Sur ; Rajib Kumar Das ; Nandini Mukherjee,2016] Cloud service providers (CSPs) adapt different pricing models for their offered services. Some of the models are suitable for short term requirement while others may be suitable for the cloud service user's (CSU) long term requirement. For example, reservation-based pricing model is appropriate for a CSU's long term demand for resources. Finding the optimal amount of

resources to be reserved in advance, to minimize the total cost, needs sufficient research effort. Various algorithms were discussed in the last couple of years to solve the resource reservation problem but most of them are based on integer programming problem (IPP) which is NP in nature. In this paper, we derive some heuristic-based polynomial time algorithms to find some near optimal solution to this problem. We show that the cost for CSU using our approach is comparable to the solution obtained using optimal IPP.

[Zhe Huang ; Danny H. K. Tsang,2106] Consolidating virtual machine workload is a unique feature of cloud computing platforms that greatly reduces the operating cost of the cloud data center. Correctly consolidating VMs' workloads for a large scale cloud computing platform is nontrivial because a shortsighted scheme may save some cost in one aspect but becomes expensive in other aspects being neglected. In this paper, we present a framework that automates the VM consolidation process to improve the VMs and servers assignment whenever such improvement is possible. The proposed VM consolidation framework can achieve a balance among multiple administrative objectives (e.g., power cost, network cost) during the VM consolidation process. The solution method of solving the VM consolidation problem is designed based on the powerful and efficient semi quasi M-convex optimization framework. The proposed algorithm can also produce VM consolidation solutions that require minimal system reconfigurations (e.g., VM migrations, turning on/off servers). More importantly, the proposed algorithm can be implemented distributedly so that the scalability of the proposed framework is greatly improved. As a result, the proposed framework is efficient, scalable and highly practical.

[Yan Yang ; Fei Teng ; Tianrui Li ; Hao Wang ; Hongjun Wang ; Qi,2015] Semi-supervised clustering ensemble has emerged as an important elaboration of classical clustering problem that improves quality and robustness in clustering by combining the results of different clustering components with user provided constraints. MapReduce is a parallel programming model for processing big data using large numbers of distributed computers (nodes). In this paper, we propose a novel semi-supervised multi-ant colonies consensus clustering algorithm and implement the parallelization of this algorithm using MapReduce on Hadoop platform. Our method incorporates pairwise constraints not only in each ant colony clustering process, but also in computing new similarity matrix during the process of the multi-ant colonies ensemble. In addition, it enhances the computational efficiency for big data by adopting a MapReduce Framework. Experimental results demonstrate the effectiveness of the proposed method.

[Liwei Kuang ; Laurence Yang ; Jun Feng ; Mianxiong Dong,2015] As the rapidly growing volume of data are beyond the capabilities of many computing infrastructures, to securely process them on cloud has become a preferred solution which can both utilize the powerful capabilities provided by cloud and protect data privacy. This paper presents an approach to securely decompose a tensor, a mathematical model widely used in data-intensive applications, to a core tensor multiplied with a certain number of truncated orthogonal bases. The

unstructured, semi-structured, and structured data are represented as low-order sub-tensors which are then encrypted using the fully homomorphic encryption scheme. A unified high-order cipher tensor model is constructed by collecting all the cipher sub-tensors and embedding them to a base tensor space. The cipher tensor is decomposed through a proposed secure algorithm, in which the square root operations are eliminated during the Lanczos procedure. Theoretical analyses of the algorithm in terms of time complexity, memory usage, decomposition accuracy, and data security are provided. Experimental results demonstrate that the approach can securely decompose a tensor. With the advancement of fully homomorphic encryption scheme, it can be expected that the secure tensor decomposition approach has the potential to be applied on cloud for privacy-preserving data processing.

[Ting Wang ; Yu Xia ; Jogesh Muppala ; Mounir Hamdi,2015] Today's data center networks are usually over-provisioned for peak workloads. This leads to a great waste of energy since in practice traffic rarely ever hits peak capacity resulting in the links being under-utilized most of the time. Furthermore, the traditional non-traffic-aware routing mechanisms worsen the situation. From the perspective of resource allocation and routing, this paper aims to implement a green data center network and save as much energy as possible. With the benefit of blocking island paradigm, we present a general framework trying to maximize the network power conservation and minimize sacrifices of network performance and reliability. The bandwidth allocation mechanism together with power-aware routing algorithm achieve a bandwidth guaranteed green tighter network. Moreover, our fast efficient heuristics for allocating bandwidth enable the system to scale to large sized data centers. The evaluation result shows that achieving up to more than 50% power savings are feasible while guaranteeing network performance and reliability.

[Fangyuan Chi ; Xiaofei Wang ; Wei Cai ; Victor Leung,2015] As the game industry matures, processing complex game logics in a timely manner is no longer an insurmountable problem. However, current cloud-based mobile gaming solutions are limited by their relatively high requirements on Internet resources. Also, they typically do not consider the geographical locations of nearby mobile users and thus ignore the potential cooperation among them. Therefore, inspired by existing cloud computing techniques, we propose an ad hoc mobilecloudlet- cloud based approach to implement cooperative gaming architecture. In this paper, two modules of the architecture are introduced: 1) progressive game resources download, by which mobile users can adaptively download gaming resources from cloud servers or nearby mobile users, 2) ad-hoc mobile based cooperative task allocation, by which gaming components can be executed dynamically on local devices, nearby devices, stationary cloudlet(s), or cloud servers. The mechanisms of both modules are formulated as optimization problems and algorithms are proposed to solve them. Simulations results based on real mobility traces show that our system's performance

depends highly on the ad-hoc network environment. Our scheme has lower system resource usage while utilizing resources of nearby devices, compared to the cloud-based gaming architecture; and performs better with short on-device task duration compared to code-offloading based architecture.

[Sisi Xiong ; Yanjun Yao ; Shuangjiang Li ; Qing Cao ; Tian He ; Hairong Qi ; Leon Tolbert ; Yilu Liu,2014] As one of the most popular cloud services, data storage has attracted great attention in recent research efforts. Key-value (k-v) stores have emerged as a popular option for storing and querying billions of key-value pairs. So far, existing methods have been deterministic. Providing such accuracy, however, comes at the cost of memory and CPU time. In contrast, we present an approximate k-v storage for cloud-based systems that is more compact than existing methods. The tradeoff is that it may, theoretically, return errors. Its design is based on the probabilistic data structure called "bloom filter", where we extend the classical bloom filter to support key-value operations. We call the resulting design as the kBF (key-value bloom filter). We further develop a distributed version of the kBF (d-kBF) for the unique requirements of cloud computing platforms, where multiple servers cooperate to handle a large volume of queries in a load-balancing manner. Finally, we apply the kBF to a practical problem of implementing a state machine to demonstrate how the kBF can be used as a building block for more complicated software infrastructures.

[Ling Tang ; Hao Chen,2014] In the cloud context, pricing and capacity planning are two important factors to the profit of the Infrastructure-as-a-Service (IaaS) providers. This paper investigates the problem of joint pricing and capacity planning in the IaaS provider market with a set of Software-as-a-Service (SaaS) providers, where each SaaS provider leases the virtual machines (VMs) from the IaaS providers to provide cloud-based application services to its end-users. We study two market models, one with a monopoly IaaS provider market, the other with multiple-IaaS-provider market. For the monopoly IaaS provider market, we first study the SaaS providers' optimal decisions in terms of the amount of end-user requests to admit and the number of VMs to lease, given the resource price charged by the IaaS provider. Based on the best responses of the SaaS providers, we then derive the optimal solution to the problem of joint pricing and capacity planning to maximize the IaaS provider's profit. Next, for the market with multiple IaaS providers, we formulate the pricing and capacity planning competition among the IaaS providers as a three-stage Stackelberg game. We explore the existence and uniqueness of Nash equilibrium, and derive the conditions under which there exists a unique Nash equilibrium. Finally, we develop an iterative algorithm to achieve the Nash equilibrium.

[Xiaoyong Xu ; Maolin Tang,2014] The placement of the mappers and reducers on the machines directly affects the performance and cost of the MapReduce computation in cloud computing. From the computational point of view, the mappers/reducers placement problem is a generalization of the classical bin packing problem, which is NP-complete. Thus, in this paper we propose a new heuristic algorithm for the mappers/reducers placement problem in cloud computing and evaluate it by comparing with some other

heuristics on solution quality and computation time by solving a set of test problems with various characteristics. The computational results show that our heuristic algorithm is much more efficient than the other heuristics. Also, we verify the effectiveness of our heuristic algorithm by comparing the mapper/reducer placement for a benchmark problem generated by our heuristic algorithm with a conventional mapper/reducer placement. The comparison results show that the computation using our mapper/reducer placement is much cheaper while still satisfying the computation deadline.

[Zhen Mo ; Qingjun Xiao ; Yian Zhou ; Shigang Chen,2014] Data security is a major concern in cloud computing. After clients outsource their data to the cloud, will they lose control of the data? Prior research has proposed various schemes for clients to confirm the existence of their data on the cloud servers, and the goal is to ensure data integrity. This paper investigates a complementary problem: When clients delete data, how can they be sure that the deleted data will never resurface in the future if the clients do not perform the actual data removal themselves? How to confirm the non-existence of their data when the data is not in their possession? One obvious solution is to encrypt the outsourced data, but this solution has a significant technical challenge because a huge amount of key materials may have to be maintained if we allow fine-grained deletion. In this paper, we explore the feasibility of relieving clients from such a burden by outsourcing keys (after encryption) to the cloud. We propose a novel multi-layered key structure, called Recursively Encrypted Red-black Key tree (RERK), that ensures no key materials will be leaked, yet the client is able to manipulate keys by performing tree operations in collaboration with the servers. We implement our solution on the Amazon EC2. The experimental results show that our solution can efficiently support the deletion of outsourced data in cloud computing.

[Alexei Karve ; Andrzej Kochut,2013] With multiplicity of Cloud service providers offering geographically distributed Compute Clouds, both providers and customers find it necessary to quickly move virtual machine images between data centers. This is usually accomplished using standard rsync-based transfer which is slow and bandwidth intensive given large size of virtual machine images. This article proposes a mechanism to reconstitute an image on target data center using information about overlap among images and content already available in the target data center. No changes to file system are needed and the approach can immediately be used with traditional libraries storing images as regular files. Moreover, we use a peer-to-peer approach that allows simultaneous retrieval of fragments from multiple data centers. The system and algorithms have been implemented and evaluated on two Compute Cloud environments using three image libraries representative for a typical service provider. The evaluation shows an average 6 times reduction in terms of network transfer volume and time and can result in even larger reductions in case of images with small configuration changes.

[Bharath K. Samanthula ; Wei Jiang,2013] With the growing popularity of data and service outsourcing, where the data resides on remote servers in encrypted form, there remain open questions about what kind

of query operations can be performed on the encrypted data. In this paper, we focus on one such important query operation, namely range query. One of the basic security primitive that can be used to evaluate range queries is secure comparison of encrypted integers. However, the existing secure comparison protocols strongly rely on the encrypted bit-wise representations rather than on pure encrypted integers. Therefore, in this paper, we first propose an efficient method for converting an encrypted integer z into encryptions of the individual bits of z. We then utilize the proposed security primitive to construct a new protocol for secure evaluation of range queries in the cloud computing environment. Furthermore, we empirically show the efficiency gains of using our security primitive over existing method under the range query application.

CONCLUSION:

In this paper taken survey from different authors regarding PHR sharing cloud and various data sharing schemes have been analyzed and compared. Some methods provide better protection against replay attacks without perfect clock synchronization. But it has a disadvantage of handling large number of keys. Provide better sharing of data using less number of per user keys and resist attacks by key sharing methods. Fine grained access control is provided in. Asymmetric proxy re-encryption methods and are also compared.

REFERENCES:

[1] H. Y. Lin and W. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," IEEE Transactions on Parallel and Distributed Systems, vol. 23, pp. 995 – 1003, June 2012.

[2] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," IEEE Transactions on Dependable and Secure Computing, vol. 09, pp. 556–568, July-August 2012.

[3] J.-M. Do, Y.-J. Song, and N. Park, "Attribute based proxy re-encryption for data confidentiality in cloud computing environments," IEEE International Conference on Computers, Networks, Systems, and Industrial Engineering, pp. 248–251, 2011.

[4] P. K. Tysowski and M. A. Hasan, "Re-encryption-based key management towards secure and scalable mobile applications in clouds," IACR Cryptology ePrint Archive, pp. 668–668, 2011.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," IEEE Globecom 2011 proceedings, 2011.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Proceedings of the 14th ACM conference on Computer and communications security, pp. 598–609, 2007.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1–9, July 2009.

[8] G. R. Blakley. Safeguarding cryptographic keys. In Proceedings of the National Computer Conference, 48, pages 313–317. American Federation of Information Processing Societies Proceedings, 1979.

[9] A. Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, November 1979. [10] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. August 1995. Springer-Verlag.

[11] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Advances in Cryptology–EUROCRYPT, 1998.

[12] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In Proceedings of Public Key Cryptography. pp. 112-121.

[13] M. Mambo and E. Okamoto. Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts. In TFECCS, 1997.

[14] Giuseppe Ateniese, Kevin Fu, Matthew Green and S. Hohenberger Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage, ACM Transactions on Information and System Security, Vol. 9, No. 1, February 2006.

[15] D. Chaum. Blind signatures for untraceable payments. In Advances in Cryptology: Proceedings of Crypto'82, pages 199–203, 1983.

[16] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31:469–472, 1985.

[17] Lidong Zhou ; Schneider, F.B. ; Marsh, M.A.; Redz A. Distributed Blinding for Distributed ElGamal Re-encryption, 25th IEEE International Conference on Distributed Computing Systems, 2005.