International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

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

K.Dhivya, K. Pushparaj, B.Vinoth

M.E. CSE, Department of Computer Science and Engineering, Chendhuran College of Engineering and Technology, Lena Vilakku, Pudukkottai, Tamilnadu, India

Assistant Professor, Department of Computer Science and Engineering, Chendhuran College of Engineering and Technology, Lena Vilakku, Pudukkottai, Tamilnadu, India

Head of the Department, Department of Computer Science and Engineering, Chendhuran College of Engineering and Technology, Lena Vilakku, Pudukkottai, Tamilnadu, India

ABSTRACT: The major aims of this method a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un trusted cloud. This scheme is able to support dynamic groups. Efficiently, specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret Keys of the remaining users. The size and computation overhead of encryption are constant and Independent with the number of revoked users. We present a secure and privacy-preserving access control to users, which guarantee any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership.

KEYWORDS*:* Cloud computing, software-defined networking, resource management, software-defined clouds, IaaS, OpenStack, OpenDaylight.

I. INTRODUCTION

his paper presents a Secure Multi owner data sharing scheme, Named Mona, For dynamic groups in the cloud. By Tleveraging group Signature and dynamic broadcast Encryption techniques, any cloud user can anonymously share data with other. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

Several security schemes for data sharing on un trusted servers have been proposed. In these approaches, data owners store the encrypted data files in un trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

Cloud Computing

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. The business model, IT as a service (ITaaS), is used by in-house, enterprise IT organizations that offer any or all of the above services. Using software as a service, users also rent application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run. End users access cloud-based applications through a web browser or a light-weight desktop or mobile app while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.

Cloud computing used in:

Autonomic computing — Computer systems capable of self-management.

Client–server model — Client–server computing refers broadly to any distributed application that distinguishes between service providers (servers) and service requesters (clients).

Grid computing — "A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."

Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as census, industry and consumer statistics, police and secret intelligence services, enterprise resource planning, and financial transaction processing.

Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."

Peer-to-peer — Distributed architecture without the need for central coordination, with participants being at the same time both suppliers and consumers of resources (in contrast to the traditional client–server model).

Cloud gaming — Also called On-demand gaming is a way of delivering to games to computers. The gaming data will be stored in the provider's server, so that gaming will be independent of client computers used to play the game.

Characteristics

- Agility improves with users' ability to re-provision technological infrastructure resources.
- Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.
- Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure.

This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house).The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere. Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another. Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

- Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
- Peak-load capacity increases (users need not engineer for highest possible load-levels)
- Utilization and efficiency improvements for systems that are often only 10–20% utilized.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

- ✓ Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.[30]
- ✓ Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.
- ✓ Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Virtualization

Virtualization (or virtualisation) is the creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system (OS), storage device, or network resources. While a physical computer in the classical sense is clearly a complete and actual machine, both subjectively (from the user's point of view) and objectively (from the hardware system administrator's point of view), a virtual machine is subjectively a complete machine (or very close), but objectively merely a set of files and running programs on an actual, physical machine (which the user need not necessarily be aware of). Virtualization can be viewed as part of an overall trend in enterprise IT that includes autonomic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The usual goal of virtualization is to centralize administrative tasks while improving scalability and overall hardware-resource utilization. With virtualization, several operating systems can be run in parallel on a single central processing unit (CPU). This parallelism tends to reduce overhead costs and differs from multitasking, which involves running several programs on the same OS. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions are:

- A secure multi-owner data sharing scheme. It implies that any user in the group can securely
- It is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.
- To provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource? Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.
- A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead is provided

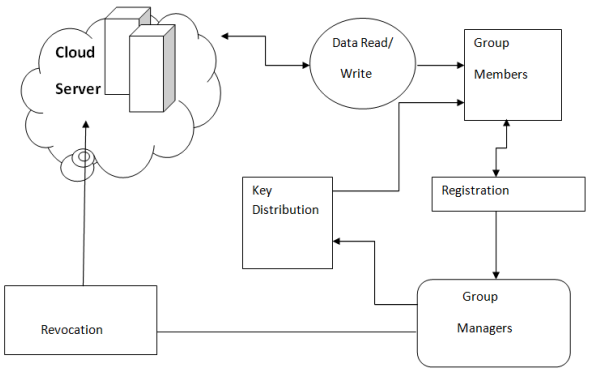

Fig.1 Proposed System Architecture

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

A. Existing System Summary

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data. The data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

II. RELATED WORKS

The authors "Shucheng Yu_, Cong Wang†, Kui Ren, and Wenjing Lou", proposed a paper titled "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", in that they described such as:

Purpose

This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents.

Materials and Methods

Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an un trusted server to authorize file writes. We have built a prototype of Plutus on Open AFS.

Results

We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

In the year of 2003, the author "MaheshSan Francisco, CA, USA" proposed a paper titled "Plutus: Scalable secure file sharing on untrusted storage", in that the author described such as the novel uses of cryptographic primitives applied to the problem of secure storage in the presence of untrusted servers and a desire for owner managed key distribution.

Materials and Methods

Eliminating almost all requirements for server trust (we still require servers not to destroy data – although we can detect if they do) and keeping key distribution (and therefore access control) in the hands of individual data owners provides a basis for a secure storage system that can protect and share data at very large scales and across trust boundaries.

Results

We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an un trusted server to authorize file writes. We have built a prototype of Plutus on Open AFS.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

The authors "Eu-Jin Goh_, Hovav Shacham†, Nagendra Modadugu, Dan Boneh‡" proposed a paper titled "SiRiUS: Securing Remote Untrusted Storage", in that they described such as: SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, OceanStore, and Yahoo! Briefcase.

Methods and Materials

SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server.

The authors "Rongxing Lin, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen" proposed a paper titled "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", in that they described such as the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access,and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

The author "Brent Waters" proposed a paper titled "Ciphertext-Policy Attribute-Based Encryption: An Expressive, E_cient, and Provably Secure Realization", in that the author described such as a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP- ABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. In our most e_cient system, ciphertext size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model.

III. PROPOSED SYSTEM SUMMARY

A secure multi-owner data sharing scheme is provided. It implies that any user in the group can securely share data with others by the un trusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. A secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource, is provided.

Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead. This paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Advantages

- We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.
- We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

IV. RESULTS AND DISCUSSION

The following figure, Fig.2 illustrates the User Login Page view of the proposed system.

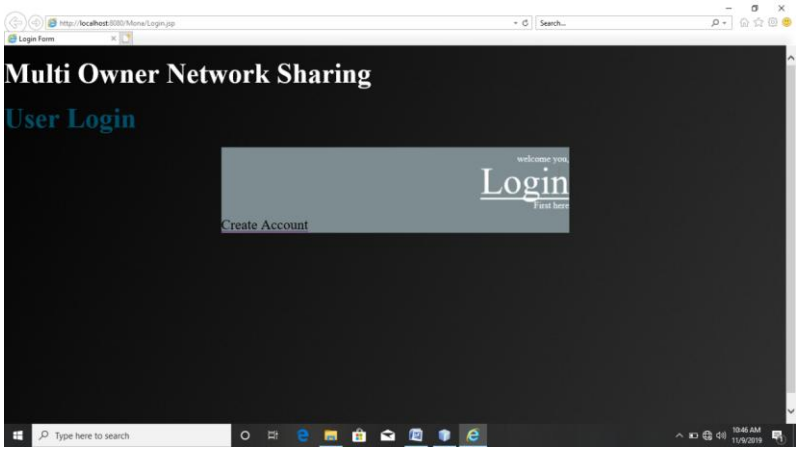

Fig.2 User Login Page

The following figure, Fig.3 illustrates the Administrator Login Page view of the proposed system.

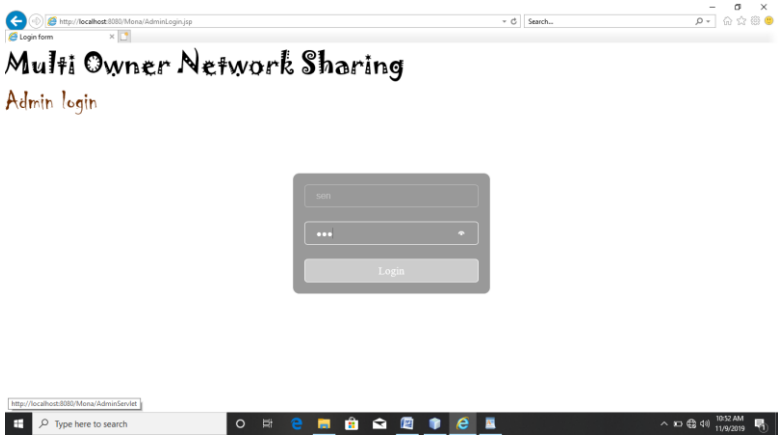

Fig.3 Administrator Login page

The following figure, Fig.4 illustrates the User Registration Page view of the proposed system.

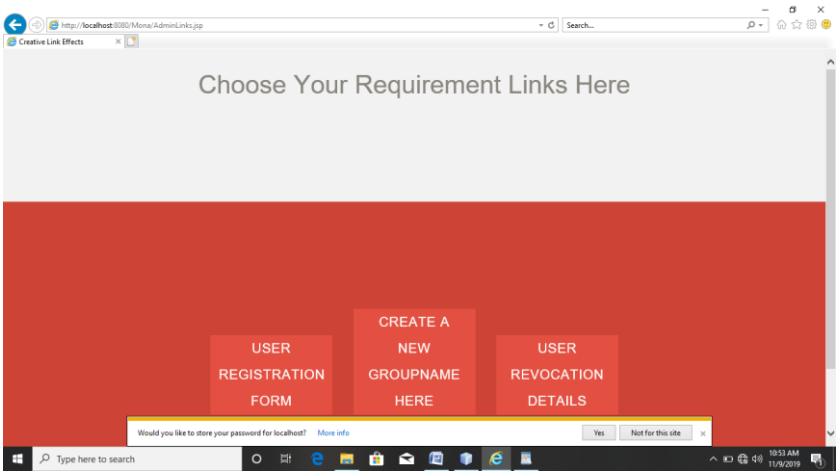

Fig.4 User Registration

The following figure, Fig.5 illustrates the Registration Form view of the proposed system.

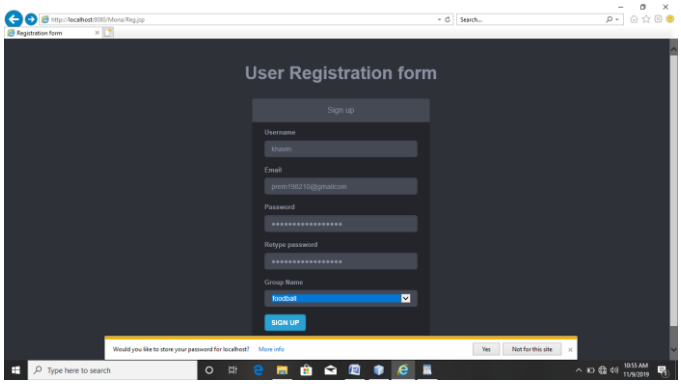

Fig.5 Registration Form

V. CONCLUSION AND FUTURE SCOPE

We design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

Our model can be generalized on the cost structure. The total cost could, for example, be as a multivariate function of created knowledge and cited knowledge, and exhibit convexity on each cost term. This reflects the scenario where knowledge acquisition and creation become increasingly difficult as more knowledge has been incorporated into one's artifact. Based on the formulation above, one may also specify the super-/sub-modularity of the total cost function as appropriate.

REFERENCES

[1] R. Buyya, R. N. Calheiros, J. Son, A. V. Dastjerdi, and Y. Yoon, "Software-defined cloud computing: Architectural elements and open challenges," in Proceedings of the 3rd International Conference on Advances in Computing, Communications and Informatics. IEEE Press, 2014.
[2] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, "Software defined cloud: Survey, system and evaluation," Future Generation Computer Systems, vol. 58, pp. 56– 74, 2016.
[3] H. Jin, T. Cheocherngngarn, D. Levy, A. Smith, D. Pan, J. Liu, and N. Pissinou, "Joint host-network optimization for energyefficient data center networking," in Proceedings of the 2013 IEEE 27th International Symposium on Parallel Distributed Processing, May 2013, pp. 623–634.
[4] J. Son, A. V. Dastjerdi, R. N. Calheiros, and R. Buyya, "SLA-aware and energy-efficient dynamic overbooking in SDN-based cloud data centers," IEEE Transactions on Sustainable Computing, vol. 2, no. 2, pp. 76–89, April 2017.
[5] J. W. Jiang, T. Lan, S. Ha, M. Chen, and M. Chiang, "Joint vm placement and routing for data center traffic engineering," in Proceedings of the 2012 IEEE INFOCOM, March 2012, pp. 2876–2880.
[6] K. Zheng, X. Wang, L. Li, and X. Wang, "Joint power optimization of data center network and servers with correlation analysis," in Proceedings of the 2014 IEEE INFOCOM, April 2014, pp. 2598–2606.
[7] R. Cziva, S. Jout, D. Stapleton, F. P. Tso, and D. P. Pezaros, "SDNbased virtual machine management for cloud data centers," IEEE Transactions on Network and Service Management, vol. 13, no. 2, pp.212–225, June 2016.
[8] K. Zheng, W. Zheng, L. Li, and X. Wang, "PowerNetS: Coordinating data center network with servers and cooling for power optimization," IEEE Transactions on Network and Service Management, vol. 14, no. 3, pp. 661–675, Sept 2017.
[9] J. Son, A. V. Dastjerdi, R. N. Calheiros, X. Ji, Y. Yoon, and R. Buyya, "CloudSimSDN: Modeling and simulation of softwaredefined cloud data centers," in Proceedings of the 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, May 2015, pp. 475–484.
[10] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks," in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. ACM, 2010, p. 19.

[11] C. H. Benet, R. Nasim, K. A. Noghani, and A. Kassler, "Open-StackEmu - a cloud testbed combining network emulation with OpenStack and SDN," in Proceedings of the 2017 14th IEEE Annual Consumer Communications Networking Conference, Jan 2017, pp. 566–568.
[12] B. Martini, D. Adami, A. Sgambelluri, M. Gharbaoui, L. Donatini, S. Giordano, and P. Castoldi, "An SDN orchestrator for resources chaining in cloud data centers," in Proceedings of the 2014 European Conference on Networks and Communications, June 2014, pp. 1–5.
[13] B. Martini, D. Adami, M. Gharbaoui, P. Castoldi, L. Donatini, and S. Giordano, "Design and evaluation of SDN-based orchestration system for cloud data centers," in Proceedings of the 2016 IEEE International Conference on Communications, May 2016, pp. 1–6.
[14] M. Gharbaoui, B. Martini, D. Adami, S. Giordano, and P. Castoldi, "Cloud and network orchestration in SDN data centers: Design principles and performance evaluation," Computer Networks, vol. 108, no. Supplement C, pp. 279 – 295, 2016.
[15] D. Adami, B. Martini, A. Sgambelluri, L. Donatini, M. Gharbaoui, P. Castoldi, and S. Giordano, "An SDN orchestrator for cloud data center: System design and experimental evaluation," Transactions on Emerging Telecommunications Technologies, vol. 28, no. 11, p. e3172, 2017.
[16] J. Tordsson, R. S. Montero, R. Moreno-Vozmediano, and I. M. Llorente, "Cloud brokering mechanisms for optimized placement of virtual machines across multiple providers," Future Generation Computer Systems, vol. 28, no. 2, pp. 358 – 367, 2012.
[17] A. N. Toosi, C. Qu, M. D. de Assuno, and R. Buyya, "Renewable aware geographical load balancing of web applications for sustainable data centers," Journal of Network and Computer Applications, vol. 83, no. Supplement C, pp. 155 – 168, 2017.
[18] A. Beloglazov and R. Buyya, "Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers," Concurrency and Computation: Practice and Experience, vol. 24, no. 13, pp. 1397–1420, 2012.
[19] M. Al-Fares, A. Loukissas, and A. Vahdat, "A scalable, commodity data center network architecture," in Proceedings of the ACM SIG COMM 2008 Conference on Data Communication. New York, NY, USA: ACM, 2008, pp. 63–74.
[20] S. Pelley, D. Meisner, T. F. Wenisch, and J. W. VanGilder, "Understanding and abstracting total data center power," in Workshop on Energy-Efficient Design (WEED), 2009.
[21] X. Wang, Y. Yao, X. Wang, K. Lu, and Q. Cao, "CARPO: Correlation-aware power optimization in data center networks," in Proceedings of the 2012 IEEE INFOCOM, March 2012, pp. 1125– 1133.
[22] J. Kang and S. Park, "Algorithms for the variable sized bin packing problem," European Journal of Operational Research, vol. 147, no. 2, pp. 365 – 372, 2003.
[23] A. Beloglazov, J. Abawajy, and R. Buyya, "Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing," Future Generation Computer Systems, vol. 28, no. 5, pp. 755–768, May 2012.
[24] R. Wang, R. Esteves, L. Shi, J. A. Wickboldt, B. Jennings, and L. Z. Granville, "Network-aware placement of virtual machine ensembles using effective bandwidth estimation," in Proceedings of the 10th International Conference on Network and Service Management (CNSM) and Workshop, Nov 2014, pp. 100–108.
[25] H. E. Egilmez, S. T. Dane, K. T. Bagci, and A. M. Tekalp, "Open- QoS: An OpenFlow controller design for multimedia delivery with end-to-end quality of service over software-defined networks," in Proceedings of the 2012 Asia-Pacific Signal Information Processing Association Annual Summit and Conference, Dec 2012, pp. 1–8.
[26] R. Wang, S. Mangiante, A. Davy, L. Shi, and B. Jennings, "QoSaware multipathing in datacenters using effective bandwidth estimation and SDN," in Proceedings of the 12th International Conference on Network and Service Management (CNSM), Oct 2016, pp. 342–347.
[27] K. Zheng, X. Wang, and J. Liu, "DISCO: Distributed traffic flow consolidation for power efficient data center network," in Proceedings of the 16th International IFIP TC6 Networking Conference, Networking. IFIP Open Digital Library, 2017.
[28] F. P. Tso, D. R. White, S. Jouet, J. Singer, and D. P. Pezaros, "The Glasgow Raspberry Pi cloud: A scale model for cloud computing infrastructures," in Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, July 2013, pp. 108–112.
[29] G. Urdaneta, G. Pierre, and M. van Steen, "Wikipedia workload analysis for decentralized hosting," Elsevier Computer Networks, vol. 53, no. 11, pp. 1830–1845, July 2009.
[30] S. H. Yeganeh, A. Tootoonchian, and Y. Ganjali, "On scalability of software-defined networking," IEEE Communications Magazine, vol. 51, no. 2, pp. 136–141, February 2013.
[31] J. Son and R. Buyya, "Priority-aware VM allocation and network bandwidth provisioning in software-defined networking (SDN)- enabled clouds," IEEE Transactions on Sustainable Computing, 2018. [Online]. Available: http://doi.org/10.1109/TSUSC.2018.2842074.