

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

A Survey on Attribute Based Access Control (ABAC) with Application in Cloud IAAS

Devendra Prasad, Dr. R.K.Bharti

Ph.D Scholar, Uttarakhand Technical University, Dehradun, Assistant Professor, Poornima University, Jaipur, India

Assistant Professor, BTKIT, Dwarahat, Almora, Uttarakhand, India

ABSTRACT: Recently, attribute based access control (ABAC) has received considerable attention from the security community for its policy flexibility and dynamic decision making capabilities. The general idea of ABAC is to determine the authorization decisions of an access request based on various attributes of the entities involved in the access (e.g., users, subjects, objects, context, etc.). Hence, in an ABAC system, proper assignment of attribute values to different entities is necessary to protect against unauthorized access. There has been considerable prior research for ABAC in various aspects such as formal models, enforcement models, policy composition languages and soon. However, mechanisms for ensuring proper attribute value assignments to entities have not been well studied.

KEYWORDS: Cloud Computing, IaaS, Constraint Aware Scheduling, Attribute Based Access Control, Cloud Scheduling Mechanism.

I. INTRODUCTION

In general, constraints are an important and powerful mechanism for laying out higher-level security policies. For instance, in an organization, constraints can specify higher-level policies to put restriction on the behavior of its employees such as separation of duty constraints in role based access control whereby a particular employee cannot take both 'programmer' and 'tester' roles for the same project. Such a constraint eventually prevents the employee from simultaneously working on both developing and testing code for same project. In this dissertation, we develop constraint specification in attribute based access control (ABAC) and cloud infrastructure-as-a-service (IaaS). Generally, ABAC regulates permissions of users or subjects to access system resources dynamically based on associated authorization rules with a particular permission. A user is able to exercise a permission on an object if the attributes of the user's subject and the object have a configuration satisfying the authorization rule specified for that permission. Hence, proper assignment of attribute values (or simply attribute assignment) to these entities is crucially important in an ABAC system for preventing unintended accesses. In this dissertation, we focus on constraint specification as an high-level policy specification on attributes assignment to entities in an ABAC based system as a mechanism to determine which entity should get which attribute values. By entities, we refer to users, subjects and objects, which are common in access control systems. A user is an abstraction of a human being. A subject is an instantiation of a user and can refer to a particular session much like in role based access control (RBAC) and an object is a resource in the system. While ABAC is policy neutral, it is also complex to manage since its access management not only depends on authorization rules but also assigned attributes to the entities. Imposing constraint on attribute value assignments can mitigate this complexity by imposing centrally designed and configured constraints on the decentralized process by which specific attribute values are assigned to individual entities.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

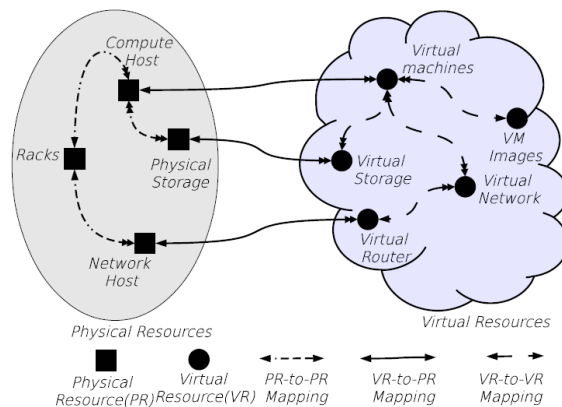


Fig 1. Cloud Resources Mapping Relation

Wang et al [33] in 2004 proposed a framework that models an ABAC system using logic programming with set constraints of a computable set theory. Requesting remote services in an identity-less open system requires that sets of attributes be presented in order to gain accesses to resources. In order to do so, they propose a stratified logic programming based framework to specify ABAC policies where collections of attribute and service options are modeled as sets in a computable hereditarily finite set theory. Their policies are flounder free, consistent and complete. In order to enhance runtime performance, they transform ABAC policies so that rewritten policies have the same runtimes as executing materialized rules. Their ongoing work explore other computable set theories and efficient implementations.

II. LITERATURE SURVEY

Bobroff et al [43] in 2007 Proposed an algorithm that proactively adapts to demand changes and migrates virtual machines between physical hosts. A management algorithm for dynamic allocation of virtual machines to physical servers is presented. Time series forecasting techniques and bin packing heuristic are combined to minimize the number of physical machines required to support a workload. A method for characterizing the gain that a given virtual machine can achieve from dynamic migration is also presented. Experimental studies of the algorithm and its applicability using traces from production data centers are shown. The algorithm achieves significant reduction in resource consumption (up to 50% as compared to the static allocation) and also reduces the number of SLA violations. Vouk et al [12] in 2008 examines the idea of "cloud" figuring, the issues it tries to address, related examination points, and a "cloud" usage in view of VCL (Virtual Computing Laboratory) innovation. It put forward an administration based construction model, lessened data innovation overhead for the end-client, incredible adaptability, and diminished collective expense of proprietorship, on demand administrations.

Wang et al [8] in 2008 brings an overview on the Cloud figuring and gives the cutting edge of Cloud registering innovations. In this paper, the creator endeavor to contribute the thought of Cloud registering: definition, value, usefulness, enabling advancement and normal applications.

M. Zaharia et al [50] in 2008 Motivated by the real-world problem of node heterogeneity, the authors have analyzed the problem of speculative execution in MapReduce. They identified flaws with both the particular threshold-based scheduling algorithm in Hadoop and with progress-rate-based algorithms in general. They designed a simple, robust scheduling algorithm, LATE, which uses estimated finish times to speculatively execute the tasks that hurt the response time the most. LATE performs significantly better than Hadoop's default speculative execution algorithm in real workloads on Amazon's Elastic Compute Cloud.

M. Isard et al [53] in 2009 addresses the problem of scheduling concurrent jobs on clusters where application data is stored on the computing nodes. This setting, in which scheduling computations close to their data is crucial for performance, is increasingly common and arises in systems such as MapReduce, Hadoop, and Dryad as well as many

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

grid-computing environments. The authors argue that data-intensive computation benefits from a fine-grain resource sharing model that differs from the coarser semi-static resource allocations implemented by most existing cluster computing architectures. The problem of scheduling with locality and fairness constraints has not previously been extensively studied under this resource-sharing model. They introduce a powerful and flexible new framework for scheduling concurrent distributed jobs with fine-grain resource sharing. The scheduling problem is mapped to a graph datastructure, where edge weights and capacities encode the competing demands of data locality, fairness, and starvationfreedom, and a standard solver computes the optimal online schedule according to a global cost model. They evaluate their implementation of this framework, which they call Quincy, on a cluster of a few hundred computers using a varied workload of data- and CPU-intensive jobs. They evaluate Quincy against an existing queue-based algorithm and implement several policies for each scheduler, with and without fairness constraints. Quincy gets better fairness when fairness is requested, while substantially improving data locality. The volume of data transferred across the cluster is reduced by up to a factor of 3.9 in our experiments, leading to a throughput increase of up to 40%.

Buyya et al [10] in 2009 highlights the cloud registering and details the architectural planning for the resources for the business sector highlighting the technologies such as the Virtual Machines (VMs). The creator likewise gives experiences on business based asset management methodologies that envelop both client and computational administration to support Service Level Agreement (SLA).

Rimal et al [7]in 2009 has depicted scientific categorization for delineating cloud computing structural engineering and further this scientific categorization is used for looking over a few current cloud computing administrations grew by different ventures all through the world like Google, force.com and Amazon.

Tharam Dillon et al [58] in 2010 discussed the challenges and issues of Cloud computing. The authors articulated the relationships amongst Cloud computing, Service-Oriented Computing and Grid computing. Also analyzed a few challenges on the way towards adopting Cloud computing. The interoperability issue was highlighted and a number of solutions are discussed thereafter for different cloud service deployment models.

Ramgovind S et al [62] in 2010, In their paper key security considerations and challenges which are currently faced in the Cloud computing industry are highlighted. While current offerings explore trail-and error control methods, a great deal of investment must be made in the managing security around this evolving technology. The Cloud Security Alliance is one such organization. It is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud computing, and provide education on the uses of Cloud computing to help secure all other forms of computing. By following guiding principles discussed in this paper, a great deal of insecurities may be easily expelled, saving business owners' valuable time and investment.

Shengmei Luo et al [64] in 2011 first point out some security vulnerabilities in virtualization security and management and analyze the vulnerabilities. Then they propose a virtualization security framework aim at the vulnerabilities. In this framework, VM system architecture can solve the problem of virtualization security effectively, and virtualization security management settles the question that various VM managements bring. Through the combination of these two models, they can effectively solve the risk caused by the current virtualization security and management.

Dudin et al [6] in 2011, The author states that the cloud computing is popular approach for information handling and stockpiling. There is no convincing motivation in buying luxurious programming and gear for the limit of a ton of data. Arutyunov et al [3] in 2012, The historical backdrop of the development, present state, future consultations, favorable circumstances and disservice of cloud computing as one of the advanced imaginative innovations is depicted. It is an approach in which data is for all time put away in servers on the Internet and reserved briefly on customers that incorporate desktop PCs, diversion focuses, table PCs, journals, divider PCs, handheld gadgets, sensors, and screens. The primary models on which cloud computing is working at present time are: framework as a Service, stage as a service, Programming as a Service, information as a Service and work environment as a Service. Speed and expense are the two principle focal points of cloud computing and the most critical weakness of this innovation is security.

Islam et al [5] in 2012, The author highlight the distinctive parts of cloud computing for discovering the reality without bounds era of driving as cloud computing after centralized computer based processing, individualized computing, customer server based registering and web server based figuring.

Jin et al [36] in 2012, Proposed an attribute based access control model in which they provide an authorization policy specification language and formal framework using which DAC, MAC and RBAC policies can be expressed.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

FeiTeng [47] in 2012, This research provides the author a good literature on existing schedulers which are mentioned in this description. The authors main contributes are-1. they solve the resource allocation problem in the user-level of cloud scheduling. 2. They address the task scheduling problem in the systemlevel of cloud scheduling. 3. they settle the evaluation problem for on-line schedulability tests in cloud computing. They also develop a simulator to model MapReduce framework. This simulator offers a simulated environment directly used by MapReduce theoretical researchers. A good survey of all schedulers is given as below-

Bijon et al [30] in 2013, provides a generic framework for risk-aware role based access control where they propose a guideline to incorporate risks around various components of a role based access control system such as user role assignment, role activation, etc. A quantified risk-aware RBAC sessions and role Activation/deactivation framework has been proposed in this paper.

Khalid Zaman Bijon et al [59] in 2013, This paper serves a basis for my research goal. Actually conflicting relations among attributes is an important factor for attribute assignment in ABAC. The author developed ABCL for specifying these constraints on attribute assignments. The gave the ABCL application in banking organization proving its expressiveness for generating various constraints for fulfilling the organization's security requirements. Finally, they have shown ABCL can formally specify constraints in cloud IaaS.

Keiko Hashizume et al[42] in 2013, The authors have presented security issues for cloud models: IaaS, PaaS, and SaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

Zhifeng Xiao et al [65] in 2013, Throughout this paper, the authors have systematically studied the security and privacy issues in cloud computing based on an attribute-driven methodology. They have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preservability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well. They believe this review will help shape the future research directions in the areas of cloud security and privacy.

Kaur et al [4] in 2014, The purpose of this paper is to discuss cloud computing, its characteristics, progression and comparable study with structure enrolling. This survey focuses on significant effect on society and business of cloud computing.

Kataoka et al[11] in 2014, The author focuses their examination on disseminated figuring, and this examination reveals that the specific thought of "structure figuring" and other related thoughts appeared to be as one in the first stage.

Abdulaziz, Almeahmadi[15,16] in 2014, An Intent-based Access Control (IBAC), a novel access control model first proposed by the authors, is an access control system that detects the intention of the user requesting access answering the question "Why?" access is being requested as opposed to current access control systems that asks "Who?" is requesting access. IBAC is designed to prevent the insider threat as opposed to the current access control systems that are designed to prevent the outsider threat. IBAC is a risk-based access control that assesses risk of access based on the detected intent and the motivation level towards executing that intent. IBAC takes advantage of the robustness of P300-based Concealed Information Test to detect intent of access and uses the brain signals to detect the motivation level. The access control system has been used on 30 participants with 100% detected intentions of access and all malintent users being rejected access before they commit their mal-intended action.

Abdulaziz, Almeahmadi [17] in 2014, An Emotion-based Access Control (EBAC), a novel access control model first proposed by the authors, is an access control system that detects the emotion of the user requesting access in order to form an access decision. This form of access control adds the sensibility aspect to access control systems to further analyze the risk of granting an authorized user access. A user who has a high level of anger and might cause damage if granted access. As well as denying a malicious authorized user access can be useful, granting a non-authorized user who have good intentions of access can be useful as well (e.g. granting firefighters access to a facility in order to suppress damage).

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Mina Sedaghat [46] in 2015, The authors tried to formulate the scheduling problem as a multidimensional bin-packing problem, which is a challenging combinatorial NP-hard problem. The scheduling problem becomes more complicated still because different jobs and workloads have different SLA requirements, and may require different ways of bin-packing tasks together. Their scheduler supports constraints placement also.

Khalid Bijon et al [61] in 2015, The authors presented a generalized attribute-based constraint specification framework for virtual resource to physical resource scheduling in IaaS clouds. The mechanism also optimizes the number of physical resources while satisfying the conflicts. This paper gives me the research work based on the potential future work described in this paper is to extend this mechanism to address the limitations. Another future research is to develop a suitable front-end application program interface for specification and management of the conflicts.

R Charanya et al [28] in 2016, This paper discusses survey on access controls Security issues in cloud computing. The existing solutions are role based access control, identification based access control, attribute based access control and hierarchical based access control. Still existing solution are not sufficient to trust the cloud. The future plan is to implement a trust model for secure storage of file.

III. CONCLUSION

In this research, first, we developed a constraints specification language for ABAC. We identified different type of relations among attributes and develop a hierarchical relationship structure. We verified the expressiveness of the language by configuring various separation-of-duty constraints for role based access control and security policies for banking organizations. We also developed constraints specification mechanisms in cloud IaaS. First, we formalized a simple constraints specification mechanism for isolation management at both user level and resource level in the cloud. We also developed a formal administrative model for the management of user privileges. We then presented CVRM, the very first constraints specification process that enables tenants to specify several virtual resource management policies needed for production enterprise applications to run in IaaS clouds. CVRM can be specified as part of a cloud deployment, and would be installed in every cloud service provided by the IaaS providers. We also identified that virtual-resource management policies can be discovered and constructed from log file which is similar to the well-known frequent-itemsets mining problem in database systems. We demonstrated a constraint mining algorithm for CVRM where the algorithm leverages standard Apriori algorithm from the data mining literature. We also analyzed whether the mined constraints preserve semantic meaning with respect to the configuration requirements of the tenant. Finally, we presented a generalized attribute-based constraints specification framework for virtual resource to physical resource scheduling in IaaS clouds. The mechanism also optimizes the number of physical resources while satisfying the conflicts. We developed and analyzed the implementation of this mechanism in OpenStack cloud platform.

REFERENCES

- [1] P.NagendraBabu et al, "A Literature Survey on Cloud Computing" in International Journal of Engineering Trends and Technology (IJETT), 2015, pp. 305-312.
- [2] TahiraMahboob et al, "A Survey – Cloud Computing a Global Perspective" in IEEE Conference on e-Learning, e-Management and e-Services, 2015, pp. 190-195.
- [3] Arutyunov, V. V. (2012). Cloud computing: Its history of development, modern state, and future considerations. Scientific and Technical Information Processing, 39(3), 173–178.
<http://doi.org/10.3103/S0147688212030082>
- [4] Kaur, R., & Kaur, A. (2014). A Review Paper on Evolution of Cloud Computing, its Approaches and Comparison with Grid Computing, 5(5), 6060–6063.
- [5] Islam, S. S., Mollah, M. B., Huq, M. I., & Ullah, M. A. (2012). Cloud computing for future generation of computing technology. 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 129–134.
<http://doi.org/10.1109/CYBER.2012.6392539>
- [6] Dudin, E. B., & Smetanin, Y. G. (2011). A review of cloud computing. Scientific and Technical Information Processing, 38(4), 280–284.
<http://doi.org/10.3103/S0147688211040083>

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

- [7] Rimal, B. P., Choi, E., & Lumb, I. (2009). A taxonomy and survey of cloud computing systems. NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC, 44–51.
<http://doi.org/10.1109/NCM.2009.218>
- [8] Wang, L., Laszewski, G. Von, Kunze, M., & Tao, J. (2008). Cloud computing: A Perspective study. Proceedings of the Grid Computing Environments (GCE) Workshop, 28, 1–11.
Retrieved from <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Cloud+computing:+A+Perspective+study#0>
- [9] Zhang, S. Z. S., Zhang, S. Z. S., Chen, X. C. X., & Huo, X. H. X. (2010). Cloud Computing Research and Development Trend. *Future Networks, 2010. ICFN '10. Second International Conference on*, 93–97. <http://doi.org/10.1109/ICFN.2010.58>
- [10] Buyya, R., Buyya, R., Yeo, C. S., Yeo, C. S., Venugopal, S., Venugopal, S., Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 17. <http://doi.org/10.1016/j.future.2008.12.001>
- [11] Kataoka, R., Ikawa, Y., & Uchihiro, N. (2014). The Evolutionary Process from a Technology Concept to a Service Concept : A Cloud Computing Case Study, (1), 1855–1865.
- [12] Vouk, M. a. (2008). Cloud computing Issues, research and implementations. ITI 2008 - 30th International Conference on Information Technology Interfaces, 235–246. <http://doi.org/10.1109/ITI.2008.4588381>
- [13] Peter Mell and Timothy Grance (September 2011). *The NIST Definition of Cloud Computing* (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145.
- [14] Dieter Gollmann. *Computer Security*, 3rd ed. Wiley Publishing, 2011, p. 387, bottom
- [15] AbdulazizAlmeahmadi and Khalil El-Khatib, "On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC)", *Systems Journal*, IEEE , vol. PP, no. 99, pp. 1, 12, doi: 10.1109/JSYST.2015.2424677 URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7103286&isnumber=4357939>
- [16] Abdulaziz Almeahmadi "Insider Threats Meet Access Control", URL: https://www.amazon.com/gp/aw/d/1539772012/ref=mp_s_a_1_1?ie=UTF8&qid=1477837714&sr=81&pi=AC_SX280_SY350_FMwebp_QL65&keywords=almeahmadi&dpPl=1&dpID=518-g2uTc0L&ref=plSrch
- [17] AbdulazizAlmeahmadi and Khalil El-Khatib. 2013. "Authorized! access denied, unauthorized! access granted". In *Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13)*.
- [18] Jin, Xin, Ram Krishnan, and Ravi Sandhu. "A unified attribute-based access control model covering dac, mac and rbac." *Data and Applications Security and Privacy XXVI*. Springer Berlin Heidelberg, 2012. 41–55.
- [19] Hu, Vincent C.; Ferraiolo, David; Kuhn, Rick; Schnitzer, Adam; Sandlin, Kenneth; Miller, Robert; Scarfone, Karen. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations"
- [20] Ferreira, Ana; Chadwick, David; Farinha, Pedro; Correia, Ricardo; Zao, Gansen; Chiro, Rui; Antunes, Luis (2009). "How to Securely Break into RBAC: The BTG-RBAC Model". *Computer Security Applications Conference (ACSAC)*. IEEE. pp. 23–31. doi:10.1109/ACSAC.2009.12
- [21] Feltus C. (2014). *Aligning Access Rights to Governance Needs with the Responsibility MetaModel (ReMMo) in the Frame of Enterprise Architecture*
- [22] Ballard, Ella Deon (2013). "Identity Management Guide: Managing Identity and Authorization Policies for Linux-Based Infrastructures". Red Hat. Retrieved 2014-01-06. Any PAM service can be identified as to the host-based access control (HBAC) system in IdM.
- [23] "ABAC (Attribute Based Access Control), jerichosystems.com". Retrieved 2016-07-11.
- [24] "SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations" (PDF). NIST. 2014. Retrieved 2015-12-08.
- [25] "Attribute Based Access Control (ABAC), axiomatics.com". Retrieved 2016-07-05.
- [26] "Attribute Based Access Control - Dynamic Authorization, nextlabs.com". Retrieved 201701-13.
- [27] <http://www.prweb.com/releases/2016/10/prweb13771686.htm>
- [28] R Charanya et al, "Survey on Access Control Issues in Cloud Computing" in IEEE, 2016.
- [29] Ravi Sandhu, David Ferraiolo, and Richard Kuhn. The NIST model for role-based access control: Towards a unified standard. In *Proceedings of the Fifth ACM Workshop on Rolebased Access Control*, pages 47–63. ACM, 2000.
- [30] K.Z. Bijon, R. Krishnan, and R. Sandhu. A framework for risk-aware role based access control. In *IEEE Conference on Communications and Network Security (CNS)*, pages 462–469, Oct 2013.
- [31] Dang Nguyen, Jaehong Park, and Ravi Sandhu. Dependency path patterns as the foundation of access control in provenance-aware systems. In *Proceedings of the 4th USENIX conference on Theory and Practice of Provenance*, pages 4–4. USENIX Association, 2012.
- [32] Yuan Cheng, Jaehong Park, and Ravi Sandhu. A user-to-user relationship-based access control model for online social networks. In *Data and applications security and privacy XXVI*, pages 8–24. Springer, 2012.
- [33] Lingyu Wang, Duminda Wijesekera, and Sushil Jajodia. A logic-based framework for attribute based access control. In *Proc. of the ACM FMSE*, 2004.
- [34] Eric Yuan and Jin Tong. Attributed based access control (ABAC) for web services. In *proceedings of the IEEE ICWS*, 2005.
- [35] Bo Lang, Ian Foster, Frank Siebenlist, Rachana Ananthkrishnan, and Tim Freeman. A flexible attribute based access control method for grid computing. *Journal of Grid Computing*, 7(2):169–180, 2009.
- [36] Xin Jin, Ram Krishnan, and Ravi Sandhu. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. In *DBSec*, 2012.
- [37] David D. Clark and David R. Wilson. A Comparison of Commercial and Military Computer Security Policies. In *Proceedings of the IEEE S&P*, 1987.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

- [38] Gail JoonAhn and Ravi Sandhu. Role-based authorization constraints specification. *ACM Trans. Inf. Syst. Secur.*, 3(4):207–226, November 2000.
- [39] Jos B Warmer and Anneke G Kleppe. *The object constraint language: getting your models ready for MDA*. Addison-Wesley Professional, 2003.
- [40] Tyson R Browning and Ali A Yassine. Resource-constrained multi-project scheduling: Priority rule performance revisited. *International Journal of Production Economics*, 126(2):212–228, 2010.
- [41] M. Stillwell, D. Schanzenbach, F. Vivien, and H. Casanova. Resource allocation using virtual clusters. In *Cluster Computing and the Grid, 2009. CCGRID '09. 9th IEEE/ACM International Symposium on*, pages 260–267, May 2009.
- [42] Keiko Hashizume et al. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1):1–13, 2013.
- [43] Norman Bobroff et al. Dynamic placement of virtual machines for managing SLA violations. In *Proceedings of the International Symposium on Integrated Network Management*. IEEE, 2007.
- [44] Nicolò Maria Calcavecchia, Ofer Biran, Erez Hadad, and Yosef Moatti. VM placement strategies for cloud scenarios. In *Proceedings of The International Conference on Cloud Computing*. IEEE, 2012.
- [45] Carlo Mastroianni, Michela Meo, and Giuseppe Papuzzo. Probabilistic consolidation of virtual machines in self-organizing cloud data centers. *IEEE Transactions on Cloud Computing*, 1(2):215–228, 2013.
- [46] Mina Sedaghat. Cluster Scheduling and Management for Large-Scale Compute Clouds. *Ph.D. Thesis*, 2015
- [47] Fei Teng. Resource allocation and scheduling models for cloud computing. *Ph.D. Thesis*, 2012
- [48] R. Buyya, C. Yeo, S. Venugopala, J. Broberg, and I. Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599–616, 2009. 25, 39.
- [49] D. Borthakur. *The Hadoop Distributed File System: Architecture and Design*. The Apache Software Foundation, 2007. 46, 47, 135
- [50] M. Zaharia, A. Konwinski, A. D. Joseph, R. H. Katz, and I. Stoica. Improving mapreduce performance in heterogeneous environments. In R. Draves and R. van Renesse, editors, *Proceedings of Symposium on Operating Systems Design and Implementation*, pages 29–42. USENIX Association, 2008. 47, 131
- [51] M. Zaharia, D. Borthakur, J. Sen Sarma, K. Elmeleegy, S. Shenker, and I. Stoica. Job scheduling for multi-user mapreduce clusters. Technical Report UCB/EECS-2009-55, EECS Department, University of California, Berkeley, Apr 2009. 47, 131
- [52] M. Zaharia, D. Borthakur, J. S. Sarma, K. Elmeleegy, S. Shenker, and I. Stoica. Delay scheduling: a simple technique for achieving locality and fairness in cluster scheduling. In *Proceedings of International Conference on EuroSys*, pages 265–278, 2010. 47
- [53] M. Isard, V. Prabhakaran, J. Currey, U. Wieder, K. Talwar, and A. Goldberg. Quincy: fair scheduling for distributed computing clusters. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*, pages 261–276. ACM, 2009. 48
- [54] J. M. Hyman, J. M. Hyman, A. A. Lazar, A. A. Lazar, G. Pacifici, and G. Pacifici. Real-time scheduling with quality of service constraints. *IEEE Journal on Selected Areas in Communications*, 9:1052–1063, 1991. 52
- [55] H. Tokuda and C. W. Mercer. Arts: a distributed real-time kernel. *SIGOPS Operating Systems Review*, 23:29–53, July 1989. 53
- [56] S. Kato, R. Rajkumar, and Y. Ishikawa. A loadable real-time scheduler suite for multicore platform. Technical Report 12, Carnegie Mellon University, Department of Electrical and Computer Engineering, December, 2009. 53
- [57] Lee Gunho. Resource Allocation and Scheduling in Heterogeneous Cloud Environments, Ph.D. thesis, 2012
- [58] Tharam Dillon et al, “Cloud Computing: Issues and Challenges” in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 27-33.
- [59] Khalid Zaman Bijon et al, “Cloud Constraints Specification in Attribute Based Access Control”, 2013
- [60] Khalid Zaman Bijon et al, “Towards An Attribute Based Constraints Specification Language”, IEEE, 2013, pp. 108-113.
- [61] Khalid Bijon et al, “Mitigating Multi-Tenancy Risks in IaaS Cloud Through Constraints Driven Virtual Resource Scheduling” ACM, 2015, pp. 63-74.
- [62] Ramgovind S et al, “The Management of Security in Cloud Computing”, IEEE, 2010.
- [63] Farzad Sabahi, “Virtualization-Level Security in Cloud Computing” IEEE, 2011, pp. 250254
- [64] Shengmei Luo et al, “Virtualization security for cloud computing service”, IEEE, 2011, pp. 174-179
- [65] Zhifeng Xiao et al, “Security and Privacy in Cloud Computing”, IEEE, 2013, pp. 843-859