IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

CCPs - Cloud Computing Policies: A Systematic Review

Md. Mahmudul Hasan[1], Subir Saha[2]

Lecturer, Dept of Computer Science and Engg, Pabna University of Science and Technology, Pabna, Bangladesh [1, 2]

Abstract: Cloud service providers and cloud consumers are tightened together via cloud services that are managed under certain constraints and must be abided by cloud consumers. These rules and regulations are referred to as policies that govern the whole process of accessing, storing and sharing data over cloud. Many publications have dealt with various ranges of policies in cloud computing but there is no in-depth exploration of studies that brings a consolidation of factors and requirements involved in cloud policies. Changes and additions in of cloud policies may lead a better success to govern the system in better ways. In this paper, we aim to conduct a systematic review to address these contexts. From the review, we identified seven major classes of policies; they are investigated more than other minor policies. We also found some policies that are relevant to other policies that may carry new policies towards the betterment of cloud computing paradigm.

Keywords: cloud policy; policy classifications; systematic review; policy requirements.

I. INTRODUCTION

Cloud computing requires agreements from cloud consumers for accessing, transferring cloud resources to the platforms delivered by the cloud service providers (CSPs). Consumers need to allow some or full control to the CSPs in order to receive the services. However, companies and individual consumers are worried about the confidentiality and integrity of the sensitive data they store in the CSPs server. Some honest-but-curious CSPs may view the data that might be harmful for the consumers. For example, giant public email services such a Gmail and Yahoo Mail have millions of users who store, share and access sensitive information including original identity, wealth properties, transaction histories and many more. Nobody can guarantee that these sensitive information are hidden from the CSPs. Such context concerns that the practitioners and researchers must address this issue which in turn become the Cloud Computing Policies (CCPs).

The term policies are high-level specifications that requires how access is controlled and who, under what circumstances, may access what information [1]. In other words, policies are rules that are a collection of allowed actions along with individual rules applied together to address a particular contract or agreement [5]. In every diverse domains of cloud computing a set of rules are placed in order to keep the property unaltered and prevent from any misuse. Researchers already taken this into consideration and many studies have been conducted in diverse domains of cloud computing, and making of policies are growing.

Policy from one domain may affect other policies in different domains. For example, security, access and privacy are related concepts and they appear together in many scenarios. Understanding policies of each of them can assist the research community to understand the relevancy among them and open the ideas for future researches. Till date no consolidation of such articles are made for the future investigation of CCPs. In this paper, we conduct a Systematic Review (SR) to obtain a collection of research articles that embraces major policies consolidated into one place for future researchers to begin from.

In the remainder of this paper, we describe the SR method in section II by presenting the research questions that we aim to investigate in this study. In section III, we categorize major CCPs, describe their meaning, factors and requirements followed by an overall discussion on the found outcomes in section IV. We explain the limitations and recommendations of this study in section V and conclude the paper in section VI.

II. REVIEW METHOD

In this SR, we consider four Research Questions (RQs) for determining the content and the structure of the study, for selecting primary studies, and identifying important factors and characteristics relevant to CCPs. In this section, we also set the scope of the literature reviewed and boundaries of our study. The RQs are following-

RQ1. How CCP can be defined?
RQ2. What are the major types of CCPs in the literature?
RQ3. What factors or characteristics are involved in each type of CCPs?
RQ4. What are the requirements for implementing CCPs?

We select five of the major sources for searching initial studies relevant to the RQs: ACM Digital Library,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

IEEExplorer, Springer, ScienceDirect, and Google Scholar. The search string applied for each of the sources is 'Cloud Computing Policy' in the article title, abstracts and keywords. The aim was to investigate what literature says about available policies, identify important characteristics and consolidate them into one place for quick assessment by the future researchers so that they know what is already progressed.

We set the boundaries by limiting the search to only journal and conference proceedings. From the initial search, we obtained 69 ACM, 61 IEEExplorer, 55 Springer, and 89 ScienceDirect relevant journal and conference papers. Google scholar found more than 300 relevant search results. In this study, we found most duplicates in Google Scholar with other major sources as Google Scholar indexes most of the research articles; only 23 research articles are found that are not identical to other sources. Based on these 297 papers we conduct further investigation. We review each of the identified articles manually in article title, abstract and author keywords; 116 relevant research articles are obtained for further review as a result. At this stage, two different criteria are applied to confine the search towards the aim of the findings on the basis on RQs.

A. Inclusion Criteria

This refers to the criteria considered for survival of articles for further inquiry: 1) cloud computing policy is major topic to include in the investigation, 2) For similar kind of studies we keep the most recent version of the concept.

B. Exclusion Criteria

In this study, we focus on the unique policies related to cloud computing that are not biased or motivated by other policies directly or partially. We set the following criteria to exclude the articles: 1) policy based management and techniques, 2) guidelines for the policy makers, 3) business policy, 4) policy models and frameworks, 5) policies are analogous to techniques, 6) policy that solve other raw policies (e.g., privacy policy may guide security policy), and 7) research articles that has no open access are excluded.

After cautious review and critical evaluation based on the above two criteria, we obtain 18 research articles where we can address the RQs. The identifying process along with the number of articles found is shown in Table I.

TABLE I OVERVIEW OF RESEARCH ARTICLES FINDINGS

Sources	Primary Search	Initial Review	Applying Criteria
ACM DL	69	29	8
IEEExplorer	61	43	4
Springer	55	09	1
ScienceDirect	89	30	4
Google Scholar	23	05	1
Total	**297**	**116**	**18**

From the progression of the identified papers it can be noted that the number of articles has significantly dropped due the inclusion and exclusion criteria. That means many of the CCPs are related to the techniques, models, frameworks and used to implement other policies. We are now set to move with 18 identified articles to the next step of this study.

III.POLICY TAXONOMIES IN CLOUD COMPUTING

To serve the purpose of the RQs we considered 116 research articles where we classified all categories of policies exist. By dividing the policy requirements into different groups, it is easy for the researchers to understand the areas the research can be conducted on. The taxonomy of the major CCPs is presented in Fig. 1.

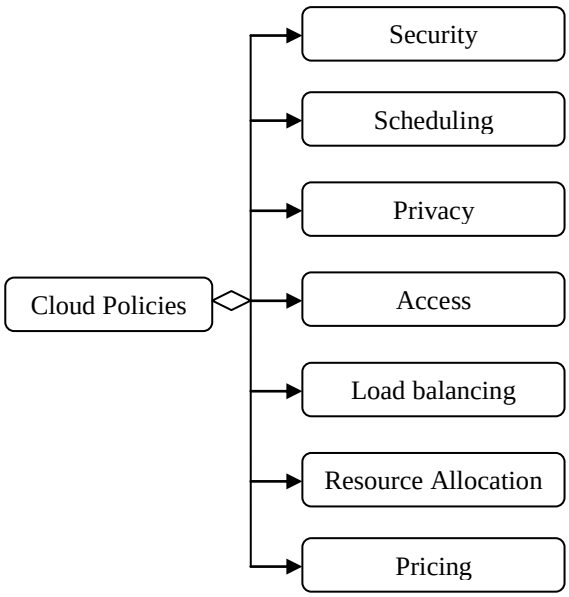

Fig. 1 The taxonomy of the major cloud policies

It is noted that 7 CCPs are identified in the investigation that came more frequently than others: security policies, scheduling policies, privacy policies, access policies, load balancing policies, resource allocation and provisioning policies, and pricing policies. Other minor policies are taken as 'others': QoS (Quality of Service) policies, data backup policies, economic policies, SLA, leasing, dispatching policies and so on.

A. Security Policy

Security policy involves rules for people and data to be protected and unaltered from outside threat. The rules consist of by the role of individual's characters such as data user behaviour, system administrator's responsibilities, the authority access, and personnel concerned to the security [1]. More security can be coped up with the restriction of the access to the system by continuous monitoring of the computer systems by security managers and only other IT authorized persons

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

[3]. The knowledge adequacy for the security personnel are also a matter of concern.
The loss of data integrity and confidentiality are increasing in cloud computing. Data backup and recovery option must be addressed to provide a secured environment in cloud. Any access to user data must be logged [3] and must track the data validity by applying third party audits [2] in compliance with regulations and legislation [1].

B. Scheduling Policy
This policy involves a management or technique that maximizes the system outcome based on the various relevant parameters in competitive environments. The parameters may include CPU rates, task priority, budget, profit, and task length etc [4].
Depending on such various factors some policies have been considered in previous studies. A typical scheduler is first-come-first-serve that is popular and identical in many systems where tasks are queued for future processing.

Another policy for the scheduling is assigning the priority to the smallest job to be completed with the highest priority. In cloud computing concept, this policy avails the faster processing of any task in the list and allow the fairness to use the resources available for every tasks.
The task length is another factor for which the scheduling policy can be implemented. The optimal length based on predefined budget can be considered as the first priority when the profit maximization is a matter of concern.
It has a chance to fall down the slowest tasks to be completed at the end of the list. In such a case, a policy involved to assignment of the highest priority to this kind of tasks may improve the experience of the scheduler [4].

C. Privacy Policy
One of the important and widely concerning policies is setting rules for protecting legal requirements of user information. People tend to share and store their sensitive data to third party agencies and experience serious violation over their data. So, policy with privacy must be required to prevent a lot of community who are taking advantages from the interconnected world [5].

An effective privacy policy for every user can be implemented by enforcing the provider with individual customer's own requirements. Every user specifies their own requirements and based on this specification providers can create their privacy rules.
Another concern about privacy is that if the cloud providers reveal their intention to access customer data and use it for advertising that may lead a serious issue. Google Doc has such serious privacy risks as they take the agreement with the users available for advertising that are directly related where it is applicable [6][7]. This can be overcome by authenticating and verifying the state of the remote platform that everyone has to pass before accessing any kind of information [8]. A fair information principal among users and providers can also be built to provide comfort and security to the users [9].

D. Access Policy
Access policy ensures the process of accessing data is secured and available any time for the data owner. It restricts curious cloud providers to access user data without any permission. It is always expected and trusted that providers never access data and share them for marketing purposes. However, the data could be tampered by them or other third party attacks can be occurred [10]. Time, attribute and location based dynamic access policy is often popular and commonly used in cloud computing [11] [12].

One way of the policy can be implemented by building an encryption process on data channel. Role-based system management policy restricts unauthorized access of data [13]. Another but rather a technical policy is to access data via a query element selection process [10].

E. Load Balancing Policy
The policy that involves load balancing is mainly the methods or techniques for measuring insufficient resources against the requests from users and provides sufficient resources to the specific user or network. The periodic policies using different agents and distributing the load information across data centers reduces the traffic overhead and better scaling [14] that can be implemented in cloud computing.

F. Resource Allocation Policy
This policy involves the process and methods of allocating cloud resources to the desired place. Initially, resources are allocated to the new system where necessary. Later, depending on the resources availability or deficiency VMs (Virtual Machines) are allocated to the necessary node. Two broad classes of policies can be defined for allocation policies: static and dynamic. Static policies are applicable to the places or nodes where the allocation is initiated for the first time. Dynamic provisioning policies follow three criteria for deciding when the policies are used: the current size of the queue, the accumulated execution time of the queued jobs, and the total waiting time among queued jobs [15]

The allocation policy can be implemented by the traditional first-come-first-serve (FCFS) manner. This policy assign tasks to resources as the tasks come into the queue. Another policy can solve the waiting time in FCFS method and implement the method for providing resources to the system. This method conducts a round-robin scheduling for all the jobs running in previous VMs that has been conducting other.

Shortest job is executing first is another resource allocation policy where longer jobs may go for starvation. That is certainly not expected and as a result two queued resources technique is beneficial as shorter and longer jobs have their own queue [15] [16]. Also there are space-shared allocation policy and time-shared allocation policy [17] useful for cloud computing.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

G. Pricing Policy

Pricing policy is the contractual rules that are set by the cloud providers, and users at the front end agree and use the services. The concept of cloud computing ensures cost-effectiveness, and cloud provider always compete each other by specifying various pricing plans. When users take services from cloud providers the pricing policy has bounded and continued until the service time is not expired or user stopped the service forcefully. For example, the Amazon Web Services (AWS) provides possible pricing policy based on the actual price list of Amazon Web Services (AWS) [18].

These are the major CCPs that are identified through the SR. In Table 2, we put a summary of the consolidated view of major policies related to RQs. The tick mark (✓) refers that the corresponding RQ is discussed in that research article. The cross mark (×) indicates that the relevant RQ is not or partially discussed.

TABLE III SUMMARY OF THE CLOUD COMPUTING POLICIES AND AVAILABILITY IN LITERATURE

References	Policy	RQ 1	RQ 2	RQ 3	RQ 4
[1]	Security	✓	✓	✓	✓
[2]	Security	×	×	✓	×
[3]	Security	×	×	✓	✓
[4]	Scheduling	✓	✓	✓	✓
[5]	Privacy	✓	✓	×	✓
[6]	Privacy	✓	×	✓	✓
[7]	Privacy	✓	✓	✓	✓
[8]	Privacy	✓	✓	✓	×
[9]	Privacy	✓	✓	✓	×
[10]	Access	✓	×	✓	✓
[11]	Access	×	×	✓	×
[12]	Access	✓	✓	×	×
[13]	Access	✓	×	×	×
[14]	Load Balancing	✓	×	×	✓
[15]	Resource Allocation	✓	×	✓	✓
[16]	Resource Allocation	×	×	✓	✓
[17]	Resource Allocation	×	×	×	✓
[18]	Pricing	✓	×	×	×

IV. DISCUSSION

The overall task has been challenging to identify the appropriate research articles and categorize them into major policies. We see that the security, privacy and access policies are the most important areas where the researcher provided the most concentration. In a sense of factors that are related to these three areas are very common. They seem one is dependent to other policies. Providing the privacy and access constraints to the user data means that the integrity, confidentiality and data availability on time are ensured. Security policies on top of privacy and access embrace the entire policies.

Scheduling, resource allocation and load balancing are related to performance measurement of the system. Though the resource allocation policies have come more frequently than other twos, they are not ineffective. Rather more concerns are required in these areas. The requirements of the load balancing policies bias the necessity of resource allocation policies. For example, handling overloaded requests from the network must be maintained by allowing proper resource provisioning and allocation. Along with these two, scheduling policies maintain the resources and requests as tasks and execute efficiently in order to obtain the maximum throughput.

Pricing policies came relatively less frequently than other major classes. Since the cost is related to the types of service and internal policies of the service providers because of profit factor, it varies without any pattern. The research articles relating to pricing policies are mostly excluded because it is not often related to the users concern though service providers analyze markets and user behaviour before providing the pricing options. Pricing models that are dynamic is very difficult to deal with.

Other minor CCPs such as QoS policy, admission control policy, migration policy, ciphertext-policy (sub area of security policy) are appeared very less frequently which also require attention to be studied. However, they are not within the scope of this study. One interesting matter can be noted that the identified research articles for CCPs are very recent; almost lies within 6 years of span (2010-2016). One article is yet to be published in 2017. So, the area is still rising and has promising scope to conduct research in CCPs.

V. LIMITATIONS AND FUTURE RESEARCH

The main limitation of our study is the criteria selected for exclusion of the research articles. We choose 5 major sources for the initial search; other sources may include more important articles about the CCPs but they should be few. The appropriateness of the search string could be problematic and additional text in search string may find additional search results. For example, policies related to cloud service models (SaaS, IaaS and PaaS) may be extended in search string whether they are related to policies. Moreover, exclusion of the paid research articles can add more values to our SR. However, articles are not always accessible and written in different languages sometimes. So, further treatments on these areas are necessary.

Another limitation of this study is that we considered the research articles that speak about the policy itself for governing the process, not is used to implement policies for other classes. This certainly limits the policies that are

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

relevant to each other and if has dependencies. A broader search of mapping among multiple areas of policies shall be significant for researchers who use multiple policies from multiple domains in their research.

In our study, we excluded minor categories of policies which may be significant in few cases and more valuable when they are related to other policies. So, search string can be built using two or more minor categories to find the relevance and significance of available research articles. Finally, we can say that CCPs has better scope in future research.

VI. CONCLUSION

Computing as a service has enlightened the use of modern technologies to users. The mutual benefits among cloud users (Service Providers and Service Consumers) are expanding through the mutual acceptance of terms of services and governing rules. From data transfer to data access, in performance measurement and resource distribution, we need to specify appropriate policies for secure information access. Many studies have conducted on a broad range of policies but a consolidation of such vital matter has never been considered. In this paper, we aimed to conduct a SR to identify major policies that were mostly evaluated and devised in literatures, and merge them to one place for future researchers to proceed from this point.

According to the literatures we reviewed, the policy can be defined broadly as the set of rules that governs the whole process under the domain (e.g., security, access, privacy etc) that is in the context. For example, the security policy is defined by the rules of accessing data, the encryption method and transferring information through secure networks. The scheduling policies involve task length, task priority, and cost-effectiveness. This presents the answer of the RQ1. Answering to the RQ2, we found seven major classes of policies and some minor policies as well. Domain policies are prepared based on factors relevant to that particular domain. Based on that we also identified factors and requirements for each policies explained in section III that addresses RQ3 and RQ4. Finally, we evaluated each paper carefully, presented the limitation of the study and suggested future possible works.

REFERENCES

[1] P. A. Boampong and L. A. Wahsheh, "Different facets of security in the cloud," in Proceedings of the 15th Communications and Networking Simulation Symposium. Society for Computer Simulation International, pp. 5, Mar 6, 2012.
[2] S. Rizvi, K. Karpinski, B. Kelly and T. Walker, "Utilizing third party auditing to manage trust in the cloud," Procedia Computer Science, vol. 61, pp. 191-197, 2015.
[3] P. M. El-Kafrawy, A. A. Abdo and A. F. Shawish, "Security Issues Over Some Cloud Models," Procedia Computer Science, vol. 65, pp. 853-858, 2015.
[4] S. Di, D. Kondo and C. L. Wang, "Optimization of composite cloud service processing with virtual machines," IEEE Transactions on Computers, vol. 64, no.6, pp. 1755-1768, 2015.
[5] M. Henze, J. Hiller, S. Schmerling and J. H. Ziegeldorf, "CPPL: Compact Privacy Policy Language," in Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, pp. 99-110, 2016.
[6] M. N. Bashir, J. P. Kesan and C. M. Hayes, "Privacy in the cloud: going beyond the contractarian paradigm," Proceedings of the 2011 workshop on governance of technology, information, and policies, pp. 21-27, 2011.
[7] D. Svantesson and R. Clarke, "Privacy and consumer risks in cloud computing," Computer Law & Security Review, vol. 26, no. 4, pp. 391-397, 2010.
[8] K. Ramachandran, "Trust based Privacy Policy Enforcement in Cloud Computing," Diss., The University of Western Ontario, 2015.
[9] A. Asadullah, I. O. Oyefolahan and M. A. Bawazir, "Factors Influencing Users' Willingness to Use Cloud Computing Services: An Empirical Study," Recent Advances in Information and Communication Technology, vol. 361, pp. 227-236, 2015.
[10] K. Jünemann and J. Köhler, "Data outsourcing simplified: Generating data connectors from confidentiality and access policies," in 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 923-930, May 13-16, 2012.
[11] S. Zickau, D. Thatmann and T Ermakova, "Enabling location-based policies in a healthcare cloud computing environment," in IEEE 3rd International Conference on Cloud Networking (CloudNet), pp. 333-338, 2014.
[12] X, Liu, Q. Liu, T. Peng and J. Wu, "Dynamic access policy in cloud-based personal health record (PHR) systems," Information Sciences, vol. 379, pp. 62-81, 2017.
[13] L. Zhou, V. Varadharajan and M. Hitchens, "Secure administration of cryptographic role-based access control for large-scale cloud storage systems," Journal of Computer and System Sciences, vol. 80, no.8, pp. 1518-1533, 2014.
[14] A. Bhadani, and S. Chaudhary, "Performance evaluation of web servers using central load balancing policy over virtual machines on cloud," in Proceedings of the Third Annual ACM Bangalore Conference, 2010.
[15] D. Villegas, A. Antoniou and S. M. Sadjadi, "An analysis of provisioning and allocation policies for infrastructure-as-a-service clouds," In 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2012.
[16] Y. Han, J. Chan, T. Alpcan and C. Leckie, "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing," 2015.
[17] S. Mehmi, H. K. Verma, A. L. Sangal, "Simulation modeling of cloud computing for smart grid using CloudSim," Journal of Electrical Systems and Information Technology, 2016.
[18] R. Atar, I. Cidon and M. Shifrin, "MDP based optimal pricing for a cloud computing queueing model," Performance Evaluation, vol. 78, pp. 1-6, 2014.

BIOGRAPHY

Md Mahmudul Hasan is currently holding the position of Lecturer at Department of Computer Science and Engineering in Pabna University of Science and Technology, Bangladesh. He received his Bachelor degree in Computer Science and Engineering from Rajshahi University of Engineering and Technology, in 2008 and his Master degree in Computer Science from the University of New South Wales, Canberra, Australia in 2014. He hold the position of Software Engineer in a leading software development firm in Bangladesh from 2008 to 2012. His research interests include Cloud Computing, Software Engineering, Bioinformatics, and Machine Learning.