Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.750 – 754

A Study on Various Security Aspects in Policy Oriented Cloud Architecture

Vaishali Balhara[1], Dr. Vandana[2]

[1]Asstt. Prof., PG Dept. of Computer Science, All India Jat Heroes Memorial College, MDU, Rohtak
[2]Asstt. Prof., Comp. Sc. Dept., PT. N.R.S. Govt. College, MDU, Rohtak
[1] vaishali_leo@rediffmail.com; [2] vandanamukeshmalik@gmail.com

Abstract— As the information is stored or communicated in the global environment, the foremost challenge is the security of data. The information safety is the primary requirement to achieve the reliable communication. Different constraints, firewalls and agents are appointed to maintain the system integrity and security. In this paper, different security aspects are presented in the form of associated policies. These policies are framed as the rules between two parties involved in the communication. Based on the application, parties and environment, there is requirement of different security policies. In this paper, policy constraint observations are provided to improve the storage and communication integrity of cloud environment.

Keywords— Architecture, Security, Policy

I. INTRODUCTION

A cloud[1][2][3][4][5] is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Hybrid clouds offer more flexibility than both public and private clouds. Specifically, they provide tighter control and security over application data compared to public clouds, while still facilitating on-demand service expansion and contraction. On the down side, designing a hybrid cloud requires carefully determining the best split between public and private cloud components.

Clouds have five essential characteristics:

1. On-demand self-service
2. Broad network access,
3. Database pooling,
4. Rapid elasticity

Cloud computing is one of the distributed system that offers the products and services globally. Scalability and dynamic infrastructure are the core features of Cloud computing. Cloud Computing offer its services for the public environment that is available to all the web users either publicly or privately. Main objective of cloud computing is to share the product and services with organization so that lot of economic benefits will be achieved by adopters. There are different kind of clouds exist respective the clients and the services such as public cloud, private cloud etc. According to the type of resources, the complete cloud computing architecture is divided in number of layers. The bottom most layer of cloud computing defines the core components such as memory, CPU, storage etc. This layer is also called infrastructure layer of cloud computing and it is denoted by IaaS (Infrastructure-as-a-Service). Second layer of cloud computing architecture provides the platform oriented services and represented by Platform-as-a-Service (PaaS). This layer of cloud system deal with the hosting environment and the distribution of the services to different clients via this platform. The actual deployment and the execution of the service are done at this layer.

A) Cloud Storage

Through storage as a service, users can outsource their data storage requirements to the cloud. All processing is performed on the user's PC, which may have only a solid state drive (e.g., flash-based solid-state storage), and the user's primary data storage is in the cloud. Data files may include documents, photographs, or videos. Files stored in the cloud can be accessed from any computer with an Internet connection at any time. How-ever, to make a modification to a file, it must first be downloaded, edited using the user's PC and then the modified file uploaded back to the cloud. The cloud service provider ensures there is sufficient free space in the cloud and also manages the backup of data. In addition, after a user uploads a file to the cloud, the user can grant read and/or modification privileges to other users

B. Cloud Processing

Processing as a service[4][5][6][7] provides users with the resources of a powerful server for specific large computational task. The majority of tasks, which are not computationally demanding, are carried out on the user's PC. More demanding computing tasks are uploaded to the cloud, processed in the cloud, and the results are returned to the user. Similar to the storage service, the processing service can be accessed from any computer connected to the Internet. One example of processing as a service is the Amazon Elastic Compute Cloud service.

In this paper, a study work on policy specification in cloud environment is presented. As the cloud communication is formed, two parties are always involved. These parties are collaborated with some policy agreement based on the application and the domain specification. In this paper these policy constraints and requirements are explored. In this section, the cloud system architecture is defined with specification of different process layers. The cloud system storage and the processing architecture is also defined in the environment. In section II, the work defined by earlier researchers is discussed. In section III, different security policies integrated in the environment are also discussed. In section IV, the conclusion of work is defined.

II. RELATED WORK

Cloud Security is always the main concern for any distributed network. In a shared cloud system, the security requires at different levels, because of which the complete architecture is drawn under policies specification. Different researchers have presented different security policies and architectures to improve the reliability and authenticity of cloud communication. In this section, the work defined by earlier researchers is discussed. Author[1] provided the work on policy driven protocols to improve the confidentiality. A trust framed protocol in scalable network is provided along with key management and storage services improvement. Author designed a methodology driven network to control these security policies and provided the energy effective communication under security feature specification. Author[2] provided the work on dynamic secure cloud network with specification of organizational constraints. The trust perception and the policy measure are applied to achieve the reliable communication. The requirement frame data management is provided by the author to ensure the secure information sharing. Author[3] has provided work on security evaluation for data management in cloud system. Author provided the sensitive information communication with secure data storage on cloud center. A user centric secure data management is provided to achieve the secure communication. Author[4] provided a generalized security policy template for satisfying the security demands of cloud users. The infrastructure driven security requirement computation is applied with required security features to improve the security aspect in cloud system. Author[5] provided a security framework to handle different attacks through expressive policy. Author provided the data management and secure communication on robust platform. The preventive method was provided by the author against DDOS attack for reliable data transition.

Author[6] provided a study based work on security policies for cloud system. A discussion is provided on security context driven access control methods for cloud system. The control policies are analyzed with design time security framework. Author discussed the PaaS as the security model for the distribution of sensitive information. Author[7] provided a security feature based analysis on cloud system and also provided the secure methods to improve the network communication. Author evaluated the associated risk for public and private cloud and other feature vectors based on which the security requirement can be estimated. The work model is discussed for public and private cloud in various application domains. Author[8] provided a security architecture for IaaS based cloud security system. The customized support at domain level is provided to control the secure access. The privacy based retrieval and the single sign based communication method is provided to improve the secure network aspect. The performance criteria based efficient model is provided by author for commercial cloud system. The domain access based communication at higher security level is distributed for identification of such security threat. Author[9] provided a comprehensive study on different security control models and features by considering various risk vectors. Author defined a structural analysis under threats and compliances analysis to achieve the secure policy control in cloud system. Author provided the policy driven measure for secure communication in cloud environment. Incorporation to the security rule specification is provided for reliable communication in distributed environment. Author[10] provided a work on security requirement at infrastructure level and applied the joint responsibility observation at service level distribution. The layered security method is provided for business cloud and achieves the application level, infrastructure level and communication level security. The secure information based sensitive data communication is provided to achieve the high rate communication in real time network.

Author[11] has provided an inter-cloud communication environment for public and private cloud to provide the requirement level observation for secure communication. The functional security aspects are discussed by the author to achieve the security management and to provide the inter cloud communication. Author provided the security fulfillment with range requirement specification. Author applied the feature requirement observation improve the reliability strength for inter-cloud communication. Author[12] presented a comparative analysis on different security methods and models for cloud system. Author provided the security aspect driven analysis on cloud system with specification of enforcement features. The cloud servers deal with attack specification is discussed for protected systems. Author applied the security capabilities driven analysis for layered communication in cloud environment. The security method with memorization is provided for reliable communication in real environment. Author[13] provided the security assurance at infrastructure level to provide the protected application driven communication. Author provided the analysis on various security aspects including confidentiality, integrity, accountability and authorization. Author applied the attack driven observation for secure and reliable communication with infrastructure distribution. The security layer is incorporated to the cloud system to improve the security measures. Author[14] presented an algorithm to achieve the client level trust for cloud system. Author included the encryption algorithm with trust enhancement with secure key distribution. The storage level and transmission level security features are discussed by the author. The secure profile driven security is provided by the author to improve the reliability aspects in real environment. Author[15] provided the security as the integrated polity in cloud system to achieve access control . The requirement level analysis is achieved in cloud system environment with specification of policy rules and to achieve the service driven communication. Author provided the framework for component control and polity control.

III.CLOUD SECURITY POLICY CHARACTERIZATION

One of the major requirements of cloud system integration and evolution is the security[5][6][7][8][9][12] constraint. A cloud system must be capable to provide the security integration in the environment. The system distribution and localization are the major requirement while accessing the data and services in the environment. Cloud system is capable to provide these services at public and private level. The local data security is one of the major challenges in this distributed global environment. Some of the major security constraints, aspects and challenges associated to the cloud environment are listed in this section.

A. *Privacy Policy*

The profile specific service access is the major requirement of cloud environment. It provides the personalized information storage in global environment. The extensive requirement of this environment is to provide the restricted feature access based on intelligent profile observation. The role identification and based on it the availability of the services of the feature access can be controlled. The cloud system architecture is one of difficult architecture which is able to provide the relative jurisdiction in the global versatile environment. The service level commitment and privacy driven access in public domain can be provided in open environment. To achieve the access of private services, the user registration is required. The authorization and the authentication aspects can be merged to gain the cloud system access under privacy control mechanism.

B. *Jurisdiction Policy*

Another requirement of cloud system is to analyze the location driven observation in global environment. The national and state regulatory analysis is required at this stage to achieve the private access in global environment. The specification of these security features with licence specification is required for any global client. The security constraint with commitment to the country and state is applied to achieve high support to security features in organization and service level access. Some of the available services are bounded in some particular geographical area. The security control is required to observe the client location and avail only the allowed services.

C. Data Retention Policy

The cloud system is capable to distribute a product or the service in the distributed environment with specification of business rule or the model. The legal specification of product utilization is also integrated here with. The server access characterization can be applied to control the access activity on cloud system with verified data storage and retrieval. The service activity analysis with security level specification is required to control the operational aspect and define the vender end based service access in the global environment. The specification can be applied to gain the control for overall environment.

D. *Verification Policy*

The activity level definition with specification of cloud access by the client can be controlled with rule specification. The secure process execution with auditing rules is also applied to generate the verified security policy specification. The security policy is required for each vendor who want to establish as a server or the cluster data to distribute the services as the raw product. The policy rules are framed here in the form of certificates and the process access control is also defined. The technical aspects are also formulated to achieve the verification of process execution. The high level consideration is required with security rule specification to control the behaviour of the process respective to the determined policies.

E. *Multi-Tenancy*

Another security policy integrated in the hadoop environment is Multi-Tenancy. This policy is defined in integration to the share information specification and the security rule specification. The key aspects of resource sharing between two parties are based on the deal. The deal must be formulated with specification of parties, time, terms and the criteria. The risk association while applying this deal is also formulated so that the client and the vendor level risk will be controlled.

F. Security Assessment

The cloud system environment is dynamic in different aspects, because of which there is the requirement of setting of some dynamic communication control constraints. These policy constraints include capacity, continuity, maximum delay, maximum failure rate observation etc. The server level agreement is defined to control the load, failure rate and migrations on different servers. The requirement analysis for the security feature can be applied with dynamic assessment. The configuration level map and the assessment at the lower level can be applied to derive these policies. The system can integrate these assessment policies so that the responsible access level discovery and security constraints can be applied on client and server dynamically.

G. Screening Policy

The security screening is the another policy defined at organization level which actually reflects the contracts between the organization and the employees. The exception driven analysis and the investigation observation is analyzed at this stage. The risk observation of appointing a new employee or a new contracter is observed. The background check, execution policy, licence check, government collaboration observations are applied to define screen policy so that the future access to the system will be reliable.

IV. CONCLUSIONS

The paper has presented the cloud security requirement and challenges in the form of policies. The cloud communication is performed between two different parties belong to some different domain, locations and constraints. Some policy agreement is requirement to provide the feature access and to gain the access. The paper has explored some of such policies framed over the cloud system.

REFERENCES

[1] W. Itani, A. Kayssi and A. Chehab, "Policy-based security channels for protecting network communication in mobile cloud computing," Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on, Seville, Spain, 2011, pp. 450-456.

[2] S. J. De and A. K. Pal, "A Policy-Based Security Framework for Storage and Computation on Enterprise Data in the Cloud," System Sciences (HICSS), 2014 47th Hawaii International Conference on, Waikoloa, HI, 2014, pp. 4986-4997.

[3] R. Shuanglin, "Data security policy in the cloud computing," Computer Science & Education (ICCSE), 2012 7th International Conference on, Melbourne, VIC, 2012, pp. 222-225.

[4] M. Rudolph, R. Schwarz and C. Jung, "Security policy specification templates for critical infrastructure services in the cloud," Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for, London, 2014, pp. 61-66.

[5] C. Basescu, A. Carpen-Amarie, C. Leordeanu, A. Costan and G. Antoniu, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies," Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, Biopolis, 2011, pp. 459-466.

[6] Y. Verginadis, G. Mentzas, S. Veloudis and I. Paraskakis, "A Survey on Context Security Policies in the Cloud," 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), Limassol, 2015, pp. 589-594.

[7] H. Lv and Y. Hu, "Analysis and Research about Cloud Computing Security Protect Policy," Intelligence Science and Information Engineering (ISIE), 2011 International Conference on, Wuhan, 2011, pp. 214-216.

[8] I. Gul, A. ur Rehman and M. H. Islam, "Cloud computing security auditing," Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on, Gyeongju, 2011, pp. 143-148.

[9] Y. Fairweather and D. Shin, "Towards multi-policy support for IaaS clouds to secure data sharing," Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on, Austin, TX, 2013, pp. 31-39.

[10] A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on, New York City, NY, 2015, pp. 1081-1084.

[11] F. S. Al-Anzi, S. K. Yadav and J. Soni, "Cloud computing: Security model comprising governance, risk management and compliance," Data Mining and Intelligent Computing (ICDMIC), 2014 International Conference on, New Delhi, 2014, pp. 1-6.

[12] M. Kretzschmar, M. Golling and S. Hanigk, "Security Management Areas in the Inter-cloud," Cloud Computing (CLOUD), 2011 IEEE International Conference on, Washington, DC, 2011, pp. 762-763.

[13] D. Devkota, P. Ghimire, J. Burris and I. Alkadi, "Comparison of security algorithms in cloud computing," Aerospace Conference, 2015 IEEE, Big Sky, MT, 2015, pp. 1-7.

[14] Patil Madhubala R., "Survey on security concerns in Cloud computing," Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, Noida, 2015, pp. 1458-1462.

[15] S. Parida and S. C. Nayak, "An algorithm that earning users' trust on cloud," Advanced Computing (ICoAC), 2013 Fifth International Conference on, Chennai, 2013, pp. 576-584.

[16] H. Takabi and J. B. D. Joshi, "Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment," System Science (HICSS), 2012 45th Hawaii International Conference on, Maui, HI, 2012, pp. 5500-5508.