Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200145

Web Based Application for Cloud Security and Compliance

Priyanka K[a,1], and Priya R[b]
[a,b]*Asst. Prof, Panimalar Engineering College, Chennai, India*

Abstract. cloud computing service is the most important services for many of the organizations. The service providers must ensure of their security and protection techniques to guarantee to protect the client data. There are some cloud security guidelines that supports the cloud data security are need to be followed by the vendors. Despite the fact, the vendors are facing the mess of security and protection controls and eventually leads to an confusion among the consumers on concerning the safety efforts and whether their measures satisfies the security measures. An inclusive report to survey the risk and security issues faced by cloud consumers have depicted to control the hazards. In light of this investigation, an ontology describing the cloud security controls, threats and compliances framed. a web based cloud application is designed to recommend the cloud security policies from the ontology such that it also helps the existing cloud providers. Security strategies can also be planned by the consumers by utilizing the web application that describing the ontology

Keywords. Ontology, web-application, security, Datacenter

1. Introduction

Cloud based storage and services are the appealing for the money savings and quick accessible/scaling or protection of cloud information stays a worry for optimum clients and a key barrier in appropriation of the cloud. In contemporary years, distinct cloud protection gauges are proposed or being created via way of measures bodies like Cloud Security Alliance (CSA), International Organization for Standards (ISO), National Institute for Standards and Technology (NIST), and so forth. Most cloud groups are executing a huge wide variety of safety and protection controls. This has induced perplexity and fear amongst customers with apprehend to what protection efforts they want to count on from the cloud administrations and what compliance guidelines to embody for their mission statistics on the cloud. This paintings makes three key commitments. Initially, we've directed an in depth report to audit the capability risks appeared thru cloud customers and decided the consistence fashions and safety controls that need to be set up to deal with the threat. It proposes, given the threats an agency faces, right cloud protection arrangements and companies that help them. This software arranges the security issues faced by the cloud consumers and its solutions that need to be derived when the security issues occurs. This utility also suggests the cloud providers that aids for the safety regulations. The focal aspect of ths paper is at the primary and 1/three commitments. In segment III, the study of the one-of-a-type cloud protection control models, consistence fashions and threats. The

[1] Priyanka K, Asst. Prof, Panimalar Engineering College, Chennai, India;
Email: priyankamecs.24@gmail.com

metaphysics we've got created for cloud security compliances and security norms are quick shrouded in phase IV, and is not a focus of this paper. the idea utility of the application is depicted in the chapter V and the future additional security policies is also inclusive.

2. Related work

cloud computing enables storage potentiality to store and process the data in third party network data servers [1]. the companies and institutions use cloud in various models such as private, public, hybrid, and community [2]. Security concerns related with cloud computing fall into two general classifications: security issues faced by cloud providers such as the organization providing software-, platform-, or infrastructure-as-a-service by means of the cloud and security issues faced by their customers and the organizations who have applications or store information on the cloud[3]. The cloud providers must be sure that their organization providing the cloud resources is secured and the client must also take the measures to protect their data and applications. when an organization plans to store the information or plans to run their application on the public cloud, the ability to access the physical access to the servers will be denied. Thus possibly the sensitive data is in risk. as it has been stated by the Cloud Security Alliance Report insider hit are the 6th greatest risk in cloud computing[4]. As a result the carrier carriers want to ensure that verifications aqr led for representatives who've physical get right of entry to to the servers within the statistics middle. And also the carriers have to have a look on data centres for any distrustful movements. So as to keep property, reduce fees, and appearance after productiveness, cloud professional co-ops frequently shop multiple purchaser's statistics on a comparable server. In the cloud assets, the priivate facts may be visible by exclusive clients and to cope with such situations the providers ought to seperate the records and consistent stockpiling segregation.[2].The extensive utilization of virtualization in executing cloud foundation brings one among a type safety issues for clients or inhabitants of an public cloud service.[5] Virtualization adjusts the relationship among the OS and simple device –processing, garage or maybe networking. This gives an extra layer – virtualization – that itself must be accurately configured, managed and secured.[6] .While those concerns are to a outstanding quantity hypothetical, they do exist. [7] For instance, a destroy in the director pc with the management programming of the virtualization programming can purpose the whole datacenter to head down.

3. Security threat and control models

3.1. Compliance Standards and cloud security controls.

Analyzing the security threats identified in some articles and from some other documents, for predicting and to analyze the threats faced by the consumers and that they are:

3.1.1. Data Breach

Poor access the board of object stockpiling containers and information stores cause touchy data to be made open, which has been one of the significant reasons for information ruptures on the cloud.

3.1.2. Denial Of Service (DoS)

Another attack for cloud security data is a Denial of Service (DoS) attack will sealup the cloud services and leads to inaccessible of data. simply it can be possible by flooding the framework with traffic such that it will leads to server crash.

3.1.3. Account Hijacking

Regardless of whether your workers aren't utilizing default, insecure passwords, programmers despite everything can " guess " the qualifications, access your cloud utilizing your staffs' records, and, subsequently, take or control your information or damage your business forms when all is said in done. This is designated, "account seizing" as well as account hijacking.

3.1.4. Insecure APIs

Regardless of whether your own frameworks are sheltered, there are frequently outsider administrations that can present extra cloud security dangers. To be specific, IoT arrangements are ordinarily viewed as a risk to information protection: gadgets, for example, associated vehicles, wellbeing screens, and home machines, gather and transmit huge amounts of delicate information progressively. Thus, interlopers can commandeer your information by hacking your APIs, not simply the cloud.

3.1.5. Insider Threats

In cloud computing apart from the outsider threats the insider threats are very dangerous such that representatives also can cause the security breach. additionally they can also fill the malware in the server and also utilize the gadgets for business purpose.

3.2. Shield from threats by utilizing security consistence models

The following are the cloud security best practices:

3.2.1. Data encryption, key management

Security management technique that protects the data and it can be accessed only via the user encrypted key. An encryption key management system includes generation, exchange, storage, use, destruction and replacement of encryption keys.

3.2.2. Media protection

Media Protection Policy is to guarantee the security of the Criminal Justice Information (CJI) until such time as the data is either discharged to the open by means of approved spread.

3.2.3. Classification and verification

Approving the client assets such as key and passwords is the significant method of improving the control of security. by the level up, the suppliers also have to provide the control to the authorized clients.

3.2.4. Portability and interoperability

it is the ability of the designed framework to integrate and share data among the other data framework without violating the security policies.

3.2.5. Application security

simply it can be stated as the security of the application that runs on the cloud server.

4. Surveillance for security and formulating ontology

The framed ontology depicts the security issues that in the cloud with the control methods. The ontology is used for describing the security issues and the supporting security controlling methods. security policies act as the shield from the issues and policies for recommending the cloud data protection. Enhancing the security applications to the assessing the risk management are the parts of cloud security control models that controls the data loss and insecurities and the insider threats. The ontology can be framed from analyzing the properties of the security threats and cloud compliance model.

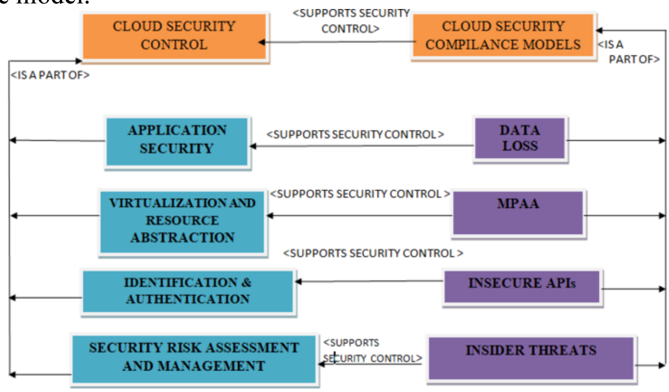

Figure 1. Illustration of ontology

5. Conclusion

A review of the comprehensive study for the latent threats that faced by the cloud data service purchaser and planned to manage the risk by designing an ontology. The ontology is used to frame the security enhancing methods. Cloud users who are hesitating to include and run their data in cloud may use this application that recommends the cloud security policies. other IT compliance models are being analyzed as so to increase the security features by incorporating it to application in future. various rules were developing in order that reasons for the ontology to match with the complaint providers.

References

[1] Haghighat, M.; Zonouz, S.; Abdel-Mottaleb, M. (2015). "CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification". Expert Systems with Applications. 42(21): 7905–7916. doi:10.1016/j.eswa.2015.06.025.

[2] Srinivasan, Madhan (2012). State-of-the-art cloud computing security taxonomies.'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. ACM ICACCI'. p. 470. doi:10.1145/2345396.2345474. ISBN 9781450311960

[3] Winkler, Vic. Cloud Computing: Virtual Cloud Security Concerns. Technet Magazine, Microsoft. Retrieved 12 February 2012.

[4] Hickey, Kathleen. Dark Cloud: Study finds security risks in virtualization. Government Security News. Retrieved 12 February 2012.

[5] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. p. 59. ISBN 978-1-59749-592-9. Archived from the original on 2012-07-29. Retrieved 2012-02-12.

[6] Cloud Security Alliance ,2013, The Notorious Nine: Cloud Computing Top Threats in 2013, p8-p21.

[7] NIST, NIST Cloud Computing Reference Architecture, 2011

[8] Privacy and data protection,Vol 7 Issue 4, IT compliance and IT security-Part 1, Dr. Jörg Hladjk, p 3-4

[9] SSAE16, The SSAE16 Auditing Standard ,http://www.ssae-16.com/

[10] FedRAMP, http://www.gsa.gov/portal/category/102375

[11] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Volume 34, Issue 1, January 2011, Pages 1–11

[12] Ramgovind, S.; Eloff, M.M.; Smith, E., The management of security in Cloud computing, Information Security for South Africa (ISSA), 2010 , vol., no., pp.1,7, 2- 4 Aug. 2010

[13] T. Mather, S.Kumarswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009

[14] CSA, Diana Kelley ,Understanding Cloud Controls Matrix v1.4.xls [10] CSA , Nov 14 2014, CSA security Guidance v3, [11] Mell, P. & Grance, t. (2011) The NIST Definition of Cloud Computing, (Special Publication 800-145).

[15] V. D. Ambeth Kumar; V. D. Ashok Kumar; H. Divakar; R. Gokul, “ Cloud enabled media streaming using Amazon Web Services”, IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Pages: 195 – 198, 2-4 Aug. 2017, Vel Tech University, Chennai, India (DOI: 10.1109/icstm.2017.8089150)