International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 6.340, Volume 04, No. 01(I), January - March, 2022, pp.56-60

NOVEL CONCEPT OF MULTI CRITERIA DECISION SYSTEM FOR CLOUD DATA PRIVACY

Pramesh Chandra Srivastava[*]
Dr. Manimala Puri[**]

ABSTRACT

In this modern world of high age of technological access, these all details whether personal or official are available online and can be accessed in any point of time and from anywhere. In such an environment, the data privacy becomes are critical issue. Due to such reasons the cloud management and privacy requirement are changing from day to day, creating a rapid need for a regular update in data privacy respect. Seeing the need of the data privacy in cloud environment, we have proposed the two models in this respect which are based on the following of parameters which includes, Access Control, Identity Based Control and also the authorisation control. This paper works on the proposal of the model which is based on AHP method for the purpose of computation of results. The results which are obtained using this approach founds that the model has its advantages over the current models in terms of costs, and other respects. The research analysis shows that the proposed model fits the current need of enterprises in regard of data privacy.

Keywords: *Access Control, Identity Control, Authorization Control, Data Privacy, Cloud Environment.*

Introduction

Security in cloud processing is a main issue. Data in cloud ought to be put away in encoded structure. To confine customer from accessing the common data straightforwardly, intermediary and business administrations ought to be utilized. Cloud security, otherwise called cloud figuring security, comprises of a bunch of approaches, controls, methodology and innovations that cooperate to ensure cloud-based frameworks, data, and foundation. These security measures are designed to ensure cloud data, support administrative consistence and secure clients' protection just as setting verification rules for individual clients and gadgets. From verifying access to separating traffic, cloud security can be designed to the specific requirements of the business. What's more in light of the fact that these guidelines can be designed and overseen in one spot, organization overheads are decreased and IT groups enabled to zero in on different region of the business. [1] The manner in which cloud security is conveyed will rely upon the singular cloud supplier or the cloud security arrangements set up. Notwithstanding, execution of cloud security cycles ought to be a joint liability between the entrepreneur and arrangement supplier. For organizations making the change to the cloud, vigorous cloud security is basic. Security dangers are continually developing and turning out to be more modern, and cloud registering is no less in danger than an on-premise climate. Therefore, it is crucial for work with a cloud supplier that offers top tier security that has been redone for your foundation.[1]

Cloud security offers many advantages, including:

- **Concentrated security:** Just as cloud processing brings together applications and data, cloud security unifies assurance. Cloud-based business networks comprise of various gadgets and endpoints that can be hard to oversee when managing shadow IT or BYOD. Dealing with these elements halfway improves traffic examination and web separating, smoothes out the checking of organization occasions and results in less programming and strategy refreshes. Debacle recuperation plans can likewise be carried out and actioned effectively when they are overseen in one spot.[2]

[G] Research Scholar, Department of Computer Science and Engineering, Dr. K.N. Modi University, Rajasthan, India.

[**] Professor, Department of Computer Science and Engineering, Dr. K.N. Modi University, Rajasthan, India.

- **Diminished expenses:** One of the advantages of using cloud stockpiling and security is that it disposes of the need to put resources into devoted equipment. In addition to the fact that this reduces capital use, however it additionally diminishes authoritative overheads. Where when IT groups were firefighting security issues responsively, cloud security conveys proactive security includes that offer assurance all day, every day with practically no human intercession. [2]
- **Diminished Administration:** When you pick a trustworthy cloud administrations supplier or cloud security stage, you can say farewell to manual security arrangements and practically steady security refreshes. These assignments can have a gigantic channel on assets, yet when you move them to the cloud, all security organization occurs in one spot and is completely overseen for your sake.
- **Unwavering quality**: Cloud processing administrations offer a definitive in trustworthiness. With the right cloud security measures set up, clients can securely access data and applications inside the cloud regardless of where they are for sure gadget they are utilizing.

An ever increasing number of associations are understanding the numerous business advantages of moving their frameworks to the cloud. Cloud figuring permits associations to work at scale, decrease innovation expenses and utilize coordinated frameworks that give them the upper hand. In any case, it is fundamental that associations have total trust in their cloud figuring security and that all data, frameworks and applications are shielded from data robbery, spillage, debasement and erasure. [2]

All cloud models are defenseless to dangers. IT divisions are normally mindful with regards to moving crucial frameworks to the cloud and it is fundamental the right security arrangements are set up, regardless of whether you are running a local cloud, hybrid or on-premise climate. Cloud security offers all the usefulness of customary IT security, and permits organizations to tackle the many benefits of cloud figuring while at the same time staying secure and furthermore guarantee that data protection and consistence prerequisites are met. [3]

Literature Survey

A. Sun, et.al 2018 [4] Whatever one public cloud, private cloud or a blended cloud, the clients absence of successful security quantifiable assessment techniques to get a handle on the security circumstance of its own information framework overall. This paper gives a quantifiable security assessment framework for various clouds that can be accessed by steady API. The assessment framework incorporates security checking motor, security recuperation motor, security quantifiable assessment model, visual showcase module and so on The security assessment model makes out of a bunch of assessment components comparing various fields, like processing, stockpiling, organization, upkeep, application security and so forth Every component is doled out a three tuple on weaknesses, score and fix technique. The framework embraces "One vote rejected" instrument for one field to count its score and includes the synopsis as the complete score, and to make one security view. We execute the quantifiable assessment for various cloud clients in light of our G-Cloud stage. It shows the powerful security checking score for one or different clouds with visual diagrams and directed clients to change setup, further develop activity and fix weaknesses, to work on the security of their cloud assets.

J. Koo, et.al 2019 [5] With the advancement of cloud processing innovation, created nations including the U.S. are playing out the effectiveness of public safeguard and public area, public development, and development of the foundation for cloud registering climate through the approaches that apply cloud processing. Korea Military is additionally thinking about that apply the cloud processing innovation into its public guard order control framework. Notwithstanding, just existing security prerequisites for public protection information framework can't take care of the issue related security weaknesses of cloud registering. To tackle this issue, it is important to plan the solid security design of public safeguard order control framework considering security necessities connected with cloud processing. This review examine the security necessities required when the U.S. military apply the cloud registering framework. It additionally break down existing security necessities for Korea public guard information framework and security prerequisites for cloud figuring framework and draw the security prerequisites expected to Korea public protection information framework in view of cloud registering.

W. Nie, et.al 2018 [6] For the web-based training, distant schooling assets sharing and asset combination issues? according to the cloud registering innovation, the instruction cloud is broadly utilized. With the far reaching utilization of instruction cloud, the security issues are likewise increasingly conspicuous, like data misfortune. By utilizing the device of Loadrunner and the instrument of AppScan, the paper investigations the information security of the training cloud stage framework in Longgang

District, Shenzhen City, subsequent to dissecting the security issues, we adjust high-hazard security issues in the schooling cloud application framework; the security issues of instruction cloud stage can be tackled. This will ensure the individual security issues of different schooling divisions and instructors and understudies and further develop showing quality in Longgang District, Shenzhen City.

T. Halabi, et.al 2018 [7] Cloud alliances permit Cloud Service Providers (CSPs) to convey more productive service execution by interconnecting their Cloud surroundings and sharing their assets. Be that as it may, the security of the united Cloud service could be compromised assuming the assets are imparted to somewhat shaky and temperamental CSPs. In this paper, we propose a Cloud league development model that considers the security hazard levels of CSPs. We start by measuring the security hazard of CSPs as per clear cut assessment standards connected with security hazard aversion and relief, then, at that point, we model the Cloud league development process as an indulgent coalitional game with an inclination connection that depends on the security hazard levels and notorieties of CSPs. We propose an organization arrangement calculation that empowers CSPs to participate while considering the security hazard acquainted with their foundations, and forgo helping out unwanted CSPs. As indicated by the strength based arrangement ideas that we use to assess the game, the model shows that CSPs will actually want to frame satisfactory leagues on the fly to service approaching asset provisioning demands at whatever point required.

Proposed Model

This model is Cloud Prediction model. In this model, AHP is utilized to choose a best cloud data security model in view of the cloud space. The proposed model is enlightened in figure 1 and further table 1 is utilized to show the significant level and low level data security control.

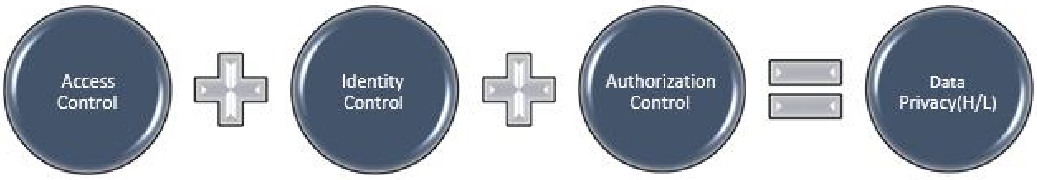

Figure 1 Proposed Model for High and Low data Privacy control

Table 1 Criteria for designing model development data privacy model

Criteria for model task assessment	Model type	
Access Control	High Risk data privacy model	
Identity Control		
Authorization Control		
Access Control	Low Risk data privacy model	
Identity Control		
Authorization Control		

Here we will utilize The Analytic Hierarchy Process (AHP), this was a theory made by Thomas Saaty that aides in assessing indistinct parts through joined assessments using choices from a 1 to 3 essential scale and achieving needs for the components.

It will in general be applied to both actual resources and intangibles and is used for dynamic by getting sorted out an ever-evolving model with a goal, rules (sub-measures), and choices by then settling on pair-wise relationship choices about the strength of get-togethers of parts in a level underneath concerning the part from which they are related in the level above. In the end the necessities of the obvious huge number of parts are mixed to rank different choices. These fundamental moderate frameworks can be contacted stunned decision models with hierarchies of benefits, openings, costs and risks. The AHP has been applied in various zones including resource assignment and compromise.

There are different intangibles that have unprecedented impact that we ought to at first check before we can fuse them as variables. What is most essential is that intangibles should be assessed through ace judgment and only similar with the targets of worry in a situation. The AHP methodology looks at the issue in three areas that are portrayed beneath:

- Stage 1: Alternatives Defining

The AHP cycle begins by portraying the choices that ought to be surveyed. These choices could be the different principles that courses of action should be evaluated against

- Stage 2: Criteria, Problem Definition

The accompanying stage is to exhibit the issue. As demonstrated by AHP strategy, an issue is an associated plan of sub issues. The AHP strategy thusly relies upon breaking the issue into a request for more unobtrusive issues. During the time spent isolating the sub-issue, measures to evaluate the plans create.

- Stage 3: Build up Priority among Criteria Using Pair-wise Comparison

The AHP methodology uses pair-wise relationship with make a structure. For example the firm will be requested to measure the general importance from protection from debasement versus liquidity.

- Stage 4: Checking of the consistency

This movement is inbuilt in most programming gadgets that assist with dealing with AHP issues. For instance in case I express that liquidity is two times as critical as protection from rout and in the accompanying framework I express that security from ruin is half pretty much as huge as probability of thankfulness, by then the going with situation creates:

- Stage 5: Getting of Relative Weights

The item instrument will run the mathematical count reliant upon the data and consign relative weights to the principles. At the point when the condition is ready with weighted measures, one can survey the decisions to get the best plan that facilitates their necessities.

Table 2: Preference between Different Criteria

	5	**3**	**1**	**3**	**5**	
Access Control	Extremely High Level Privacy	Moderate Privacy	Normal	Moderate Privacy	Extremely High Level Privacy	Identity Control
Identity Control	Extremely High Level Privacy	Moderate Privacy	Normal	Moderate Privacy	Extremely High-Level Privacy	Authorization Control
Authorization Control	Extremely High Level Privacy	Moderate Privacy	Normal	Moderate Privacy	Extremely High Level Privacy	Access Control

Here in the table 2 for every boundary that is classification, accessibility and trustworthiness are set on various degree of protection so we can pass judgment on these in view of matched examination and made four mix.

Intensity of Importance	**Definition**	**Explanation**
1	Equal importance	Two exercises contribute similarly to the goal
3	Moderate importance	Experience and judgment marginally favor one activity over another
5	Strong importance	Experience and judgment strongly strongly support one activity out of the two
7	Very strong or demonstrated importance	An activity dominates over the other
9	Extreme importance	Verification to prefer one activity to another is the most significant conceivable request confirmation

Table 3: Full Matrix based on Paired Comparisons

Criterion	Access Control	Identity Control	Control
Access Control	1	1/3	1/5
Identity Control	3	1	1/3
Authorization Control	5	3	1

Conclusion

In this paper, we have made the case that assuming a cloud framework can deal with these protection boundaries, Access Control, Identity Control, and Authorization Control, than certainly, we will actually want to anticipate the high security for the cloud climate. Here have made two kinds of models one for prediction High level Privacy utilizing previously mentioned boundary and one more for low level protection utilizing the previously mentioned boundaries. For this, we have utilized Analytical Hierarchical Processing (AHP) techniques to demonstrate our case. Besides, results show that our case is valid.

References

1. S. Sharma, U.S. Tim, J. Wong, S. Gadia, S. Sharma, “A Brief Review on Leading Big Data Models”, Data Science Journal, 13(0), 138-157, 2014
2. S. Sharma, U.S. Tim, J. Wong, S. Gaida, R. Shandilya, S. K. Peddoju, “Classification and Comparison of NoSQL big data models,” International Journal of Big Data Intelligence, Vol. 2 No.3, 2015
3. S. Sharma, R. Shandilya, S. Patnaik, A. Mahapatra, “Leading NoSQL models for handling Big Data: a brief review”, International Journal of Business Information Systems,Inderscience, 2015.
4. G.W. Van Blarkom, J. B. (2003). Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents. Retrieved from e-Europe: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15263-00-2005-Apr.pdf
5. A.Sun, G. Gao, T. Ji and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD), 2018, pp. 197-201.
6. J. Koo, Y. Kim and S. Lee, "Security Requirements for Cloud-based C4I Security Architecture," 2019 International Conference on Platform Technology and Service (PlatCon), 2019, pp. 1-4.
7. W. Nie, X. Xiao, Z. Wu, Y. Wu, F. Shen and X. Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018, pp. 185-189.
8. T. Halabi, M. Bellaiche and A. Abusitta, "A Cooperative Game for Online Cloud Federation Formation Based on Security Risk Assessment," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018, pp. 83-88.
9. Dove, E. S, Y. Joly, A. M. Tasse, P.P.P. in Genomics, S.P.I.S. Committee, I.C.G.C.I. Ethics, P. Committee and B. M. Knoppers, “Genomics, cloud computing: legal and ethical points to consider”, European Journal of Human Genetics, August 2014.
10. E. Ayday, J. Raisaro, U. Hengartner, A. Molyneaux, and J.-P. Hubaux, “Privacy-preserving processing of raw genomic data,” in Data Privacy Management and Autonomous Spontaneous Security (J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, eds.), vol. 8247 of Lecture Notes in Computer Science, pp. 133147, Springer Berlin Heidelberg, 2014.
11. Y. Huang and I. Goldberg, “Outsourced private information retrieval,” in Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society, WPES ’13, (New York, NY, USA), pp. 119–130, ACM, 2013.
12. K. Lauter, A. Lopez-Alt, and M. Naehrig, “Private computation on encrypted genomic data,” Tech. Rep. MSR-TR-2014-93, June 2014.