WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

TIME BASED ACCESS CONTROL FOR DATA SECURITY TO AVOID THREATS IN CLOUD ENVIRONMENT

Akash[1], Ameen Marzook[2], Manimaran[3], Prof Rajesh[4]

[1]*EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: akashuthaya22@gmail.com
[2]*EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: ameenmarzook5@gmail.com
[3]*EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: manimaran6274@gmail.com
[4]*Assistant professor, EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
E-Mail: rajesh@egspec.org

A B S T R A C T

Existing security risk assessment draws near (e.g., resource based) don't think about unambiguous security necessities of person distributed computing clients in the security risk assessment. In this paper, we propose a danger explicit gamble assessment approach that purposes different security ascribes of the cloud (e.g., weakness data, the likelihood of an assault, and the effect of each assault related with the recognized threat(s)) as well as the client-explicit security prerequisites in the cloud. Our methodology permits a security executive of the cloud supplier to go with fine-grained choices for choosing relief techniques to safeguard the rethought figuring resources of individual clients in view of their particular security against explicit dangers. This is not the same as the current resource based approaches where they don't have the functionalities to give the security assessment of the cloud concerning explicit dangers. Then again, the proposed approach empowers security managers to figure a scope of more successful client-explicit countermeasures regarding the significance of safety necessities and dangers. The preliminary evaluation results show that convincing security plans shift in view of unequivocal risks zeroed in on by different clients for an application in the cloud. Further, the proposed approach isn't restricted to just the cloud-based frameworks, yet can undoubtedly be taken on to other organized frameworks. We have likewise fostered a product instrument to help proposed approach.

Keywords: Cloud Computing, Security Requirements, security Risk Evaluation

INTRODUCTION

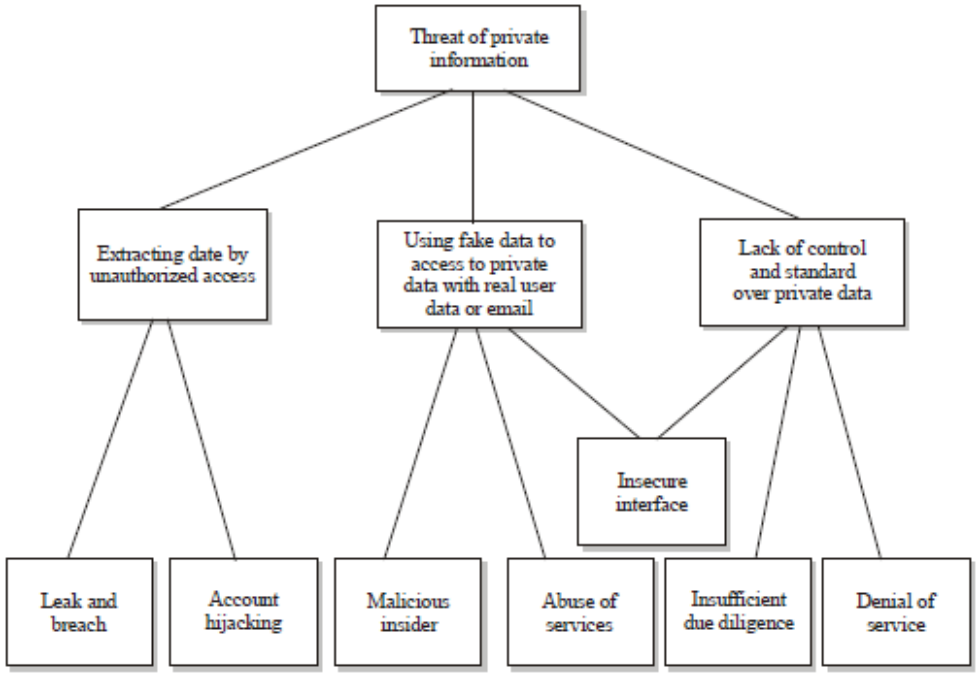
Circulated figuring empowers clients, for instance, organizations, states, and people, to re-fitting their enlisting necessities (programming, equipment, limit, etc.,) for expanded flexibility and better administration of their working out resources and data .It likewise draws in a wide degree of various cyberattacks. The sorts of attacks on circulated processing vary dependent upon the security objectives that aggressors expect to exploit, such assets accessible to compromise, and the risks they present. In a multi-occupant dispersed processing circumstance, a 'one-size-fits-all' security attestation model may not be satisfactory to satisfy various clients with their varying security necessities and prerequisites. Different affiliations have different unequivocal security essentials while using the typical resources of appropriated processing. For example, organization openness is a security need of a client X that should be ensured by the cloud provider. In this current situation, the cloud master local area shouldn't let cyberattacks abuse the accessibility. Another client, Y, could have data trustworthiness as its essential security essential for comparative data amassing applications. The cloud expert association is then to protect the client's data set aside in the cloud system from adjusting. The possibility of each and every client's assets and what is to be protected coordinates the client's security requirements. In this model, client X frequently ponders availability than various requirements.

*M*ETHODOLOGY

The proposed philosophy for security across the board in distributed computing depends on the accompanying parts. I) a progressive safety measurement system; II) a security file; III) a record of allocations; and IV) executive distributed computing A security measurement order is gotten from the methodology. A security list will be registered using the security measurements order progression, which takes into account the estimation of the distribution file. Finally, the cloud board scheduler will utilise the assignment record as a source of perspective for the asset portion process. With regards to the existence pattern of safety executives (Fig. 1), a security measurements pecking order is introduced as another type of perception of safety-related data that is gathered from the distributed computing climate.

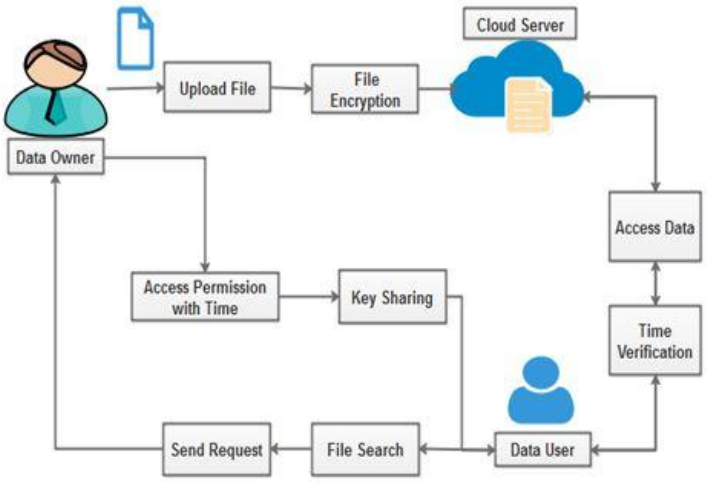
GQM technique The GQM strategy (Goal-Question-Metric) was developed in the 1970s to shift programming abandonment testing from a subjective and emotional state to an anempirical model in which deformities would be estimated against characterised objectives and targets that could then be linked to results. The GQM system identifies an estimation model on three levels. I) Conceptual level (objective)-an objective is characterised for an article for an assortment of reasons, concerning various models of value, according to a few perspectives and within a specific climate; ii) Operational level (question)-a bunch of inquiries are utilised to characterise models of the item under consideration and, afterward, consideration is centred around that item to describe the appraisal or accomplishment of a particular objective; iii) Quantitative level (metric)-a bunch of measurements, in view of the models, are related to answer it in a quantifiable manner. In our approach, the security measurements progressive system is created straightforwardly from the GQM definition process, during which stage security features are intended to analyze security measurements. Table I shows the association between the GQM procedure and the security estimations request (SMH).

MODELING AND ANALYSIS



RESULTS AND DISCUSSION

We have proposed another security risk evaluation approach considering various kinds of dangers by utilising the STRIDE danger model. Our proposed approach can evaluate the bet related with decided perils fine and dandy, which gives an even more fine-grain appraisal of the risks in the cloud. In this segment, we further talk about certain restrictions and future work. The unsafe express security risk assessment results and the recommendation appear to veer from the standard security risk assessments. That's what the contention is qualified. The risk unequivocal philosophy game plan is similar with the picked clients' security necessities. In this way, the suggestion is the ideal arrangement in comparison with the security prerequisites we thought about in the assessment. Regardless, it would benefit from supporting the goodness of the idea to ensure that the picked security game plan achieves the ordinary security prerequisites. Exploring this will be finished in our future work.



Architecture Diagram

CONCLUSION

We showed in this paper that current resource based risk appraisal approaches might result in insufficient risk moderation systems in light of the fact that the countermeasures picked are probably going to be coarse-grained (i.e., not well defined for a danger presented to the security necessities of a particular distributed computing client). Conversely, the proposed danger explicit gamble appraisal can assess and recognize more viable, fine-grained countermeasures, considering client indicated dangers. Furthermore, the proposed approach can also be applied in other networked-based computing environments. We demonstrated the applicability, feasibility, and usability of our proposed approach through experimental evaluation via simulations. The result showed that taking into account different threats yielded a different security solution compared to considering all threats (i.e., the existing asset-based risk assessment). In addition, we were able to identify the fine-grain changes in the risk with respect to different types of threats.

REFERENCES

[1] P. Mell and T. Grance, "SP 800-145. The NIST Definition of Cloud Computing," NIST, Gaithersburg, MD, United States, Tech. Rep., 2011.
[2] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing," in Proc. of the Interna- tional Conference on Intelligent Semantic Web-Services and Applications (ISWSA 2011), 2011, pp. 1–6.
[3] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," The Journal of Supercomputing, vol. 63, no. 2, pp. 561– 592, 2013.
[4] D. Sgandurra and E. Lupu, "Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems," ACM Computing Surveys, vol. 48, no. 3, pp. 1–38, 2016.
[5] K. Khan, A. Erradi, and S. Alhazbi, "Addressing Security Compatibility for Multi-Tenant Cloud Services," International Journal of Computer Applications in Technology, vol. 47, no. 4, pp. 370–378, 2013.
[6] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Com- puting Environments: A Survey, Some Research Issues, and Challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602–622, 2016.
[7] A. A. Almutairi and A. Ghafoor, "Risk-Aware Virtual Resource Manage- ment for Multitenant Cloud Datacenters," IEEE Transactions on Cloud Computing, vol. 1, no. 3, pp. 34–44, 2014.
[8] A. Rao, N. Carreon, R. Lysecky, and J. Rozenblit, "Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems," IEEE Software, vol. 35, no. 1, pp. 38–43, 2018.
[9] A. Almutairi, M. I. Sarfraz, and A. Ghafoor, "Risk-Aware Management of Virtual Resources in Access Controlled Service-Oriented Cloud Dat- acenters," IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 168–181, 2018.
[10] A. Sen and S. Madria, "Risk Assessment in a Sensor Cloud Frame- work Using Attack Graphs," IEEE Transactions on Services Computing, vol. 10, no. 6, pp. 942–955, 2017.
[11] J. Lv and J. Rong, "Virtualisation Security Risk Assessment for En- terprise Cloud Services Based on Stochastic Game Nets Model," IET Information Security, vol. 12, no. 1, pp. 7–14, 2018.
[12] S. Islam, M. Ouedraogo, C. Kalloniatis, H. Mouratidis, and S. Gritzalis, "Assurance of Security and Privacy Requirements for Cloud Deployment Model," IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 387– 400, 2017.