DOI: https://doi.org/10.36910/6775-2524-0560-2022-48-05
UDC 004[657+005]338.4

Zalialetdzinau Kanstantsin
https://orcid.org/0000000319380122
software engineer Brimit LLC

THEORETICAL AND METHODOLOGICAL ASPECTS OF ASSESSING THE SECURITY OF CLOUD IT COMPONENTS ACCORDING TO THE CRITERIA OF EXISTING STANDARDS

Zalialetdzinau K. Theoretical and methodological aspects of assessing the security of cloud it components according to the criteria of existing standards. Purpose of the study. Computing of clouds provide the admittance to the collection of computational possessions like storage of network and services. These possessions can be resealed and prompt with the minor efforts of the management because they have a scalable and dynamic environment. As a service the cloud computing offers the computing infrastructure, development of the stage as well as software and web applications like the model of pay as you go for the customers. Services are measured as the infrastructures as services (IAAS), Platform as a Service (PAAS), and the service software (SAAS) in diligence. In the research, we deliberate the Assessing the Security of Cloud It Components according to the criterion of obtainable principles. **Methodology.** In the advancement of the cloud computing metrics hierarchy, we covenant with the cloud computing management security with the GQM methodology. The main intention of the hierarchy proposed is to develop index for the security which entirely explained the security level in an estimate computing cloud environment. On the stride of the index for the security, we compute the index for the security to compute the allocation index. This allocation index will help in the management of the priorities set with a strong security prejudice. In this, we elucidate the slant for computingcloud management by use of security as a standard. **Scientific review.** The most enviable prerequisite of the computing of the cloud is to shun waste the underused possessions and mount the point of the response rate in the shortage of resources. In the latest literature in the administration field prioritization provision of the resources, we noticed that algorithm is preferred for the energy proficient management of the computing cloud environments. The metrics for the security use as instrument to provide the status about the information of security. **Conclusion.** In this editorial, we projected a management method for the computingcloud by using the criteria for the security. We accessible the 2 approaches to resource management. These strategies pact with the granularity and scalability in the computing cloud system. The security index covey the level of the security in the cloud computing environment in the modeled with metrics hierarchy. The biggest gain of using this approach is that it ropes the hierarchical decomposition that makes the model more scalable and disseminated.

Key words: computing of clouds, system administrator, computing cloud system, computing cloud environments, cloud computing management security.

Залялетдзінов К. Теоретико-методологічні аспекти оцінки безпеки хмарних it компонентів за критеріями існуючих стандартів. Мета дослідження. Обчислення в хмарах забезпечують доступ до колекції обчислювальних ресурсів, таких як зберігання мережі та послуг. Ці володіння можна повторно запечатати та негайно за допомогою незначних зусиль керівництва, оскільки вони мають масштабоване та динамічне середовище. Як послуга, хмарні обчислення пропонують обчислювальну інфраструктуру, розробку сцени, а також програмне забезпечення та веб-додатки, як модель оплати по ходу роботи для клієнтів. Послуги оцінюються як інфраструктура як послуга (IAAS), платформа як послуга (PAAS) і сервісне програмне забезпечення (SAAS). У дослідженні ми розглядаємо оцінку безпеки компонентів Cloud It за критерієм доступних принципів. **Методологія.** Удосконалюючи ієрархію показників хмарних обчислень, ми дотримуємося умов безпеки керування хмарними обчисленнями за допомогою методології GQM. Основним призначенням запропонованої ієрархії є розробка індексу для безпеки, який повністю пояснює рівень безпеки в оцінюваному обчислювальному хмарному середовищі. По ходу індексу для цінних паперів ми обчислюємо індекс для цінних паперів, щоб обчислити індекс розподілу. Цей індекс розподілу допоможе в управлінні встановленими пріоритетами з серйозним упередженням щодо безпеки. Тут ми пояснюємо напрямок керування обчислювальними хмарами за допомогою безпеки як стандарту. **Наукова рецензія.** Найбільш завидною передумовою обчислень хмари є уникати марнування недовикористаних речей і підвищувати точку відповіді на дефіцит ресурсів. В останній літературі в галузі адміністрування пріоритетів надання ресурсів, ми помітили, що алгоритм є кращим для енергоефективних керування обчислювальними хмарними середовищами. Метрики безпеки використовуються як інструмент для надання статусу інформації про безпеку. **Висновок.** У цій статті ми спроектували метод керування обчислювальною хмарою за допомогою критеріїв безпеки. Нам доступні 2 підходи до управління ресурсами. Ці стратегії узгоджуються з деталізацією та масштабованістю обчислювальної хмарної системи. Індекс безпеки відображає рівень безпеки в середовищі хмарних обчислень у змодельованій ієрархії метрик. Найбільша перевага використання цього підходу полягає в тому, що він використовує ієрархічну декомпозицію, яка робить модель більш масштабованою та поширеною. Ключові слова: обчислення хмар, системний адміністратор, обчислювальна хмарна система, обчислювальні хмарні середовища, безпека управління хмарними обчисленнями.

Ключові слова: хмарні обчислення, системний адміністратор, обчислювальна хмарна система, обчислювальні хмарні середовища, безпека управління хмарними обчисленнями.

Relevance of the problem. Computing of the cloud elaborate the access to computational resources like services, storage space and network. These possessions can be at large with the minor efforts of the management in a scalable or dynamic environment (Daylami, 2015).

The technology that provides the cloud computing services has a different level of risk in comparison with the other information technology environments (Gashi, 2016). Despite its benefits, the main dilemma in cloud computing is security issues.

The developers of the software classify the cloud differently in comparison to the system administrator. The database administrator has its definition. The cloud simply means scalable services that admittance the user via internet connections. A supplier like Microsoft, Amazon and Google and much more supply the different service. In the cloud that users pay through the payment services. The providers provide a broad range of the services of the cloud for example messaging, social service for the computing, CRM and the content administration and identity. Computing of the cloud depend on the sharing of resources. With the use of internet enabled devices forcomputingcloud consent the task for the software application. The wide range of meaning affords under cloud computing. The advantage of sharing resources is that cloud computing can achieve stability and economies of scale. It is also defined in two 2 categories the first one is cloud computing services and the second one is computing of the cloud models of the development.

Analysis of recent research and publications. It permit you to exertion with several jobs with the same document. It merely overcomes the restriction of the traditional computer system. It provides more quickness because it has fast access. The services hosted are further classified into the3 categories like service of the infrastructure (IAAS), Platform as service (PAAS) and lastly the Software as a Service (SAAS). The service of the cloud is used by the client on an hourly basis. It m to flexible like user have the services at the desired point of service and the time of the cloud that observe by the suppliers (Srivastava & Khan, 2018).

There are some threats of the security that exploit by the use of computing of the cloud. The first one is the botnets which will extend the spam and malware in 2010 almost 761 breaches of the data were inspect by the secret of European services and almost 63 per cent transpire in the companies with the fewer rate of 100 employees. And in the other year the 2011 the survey of the security system supplier Symantec corp. have 2000+ small enterprises that show 73 per cent breached by the attack of the cyber.

One of the main features of the computing cloud is paying as you set off with the computing model as resources. The model of the computing enables the organizations to purchase the computing power as many resources without the need for large reserves of the capital in the infrastructure of IT. The advantage of computing cloud is scalability and also raises the suppleness for a relativelyfixed price (Son & Buyya, 2018). It is a new trend in the system if distributed. The user does not need to have facts and a level of expertise in infrastructure control for the cloudsIt also endow with abstraction. The provider of the cloud provide the common online business application in which the admittance from servers from end to end web browsers (Malik, 2018).

Definition of the research goal. Computing of clouds provide the admittance to the collection of computational possessions like storage of network and services. These possessions can be resealed and prompt with the minor efforts of the management because they have a scalable and dynamic environment. As a service the cloud computing offers the computing infrastructure, development of the stage as well as software and web applications like the model of pay as you go for the customers. Services are measured as the infrastructures as services (IAAS), Platform as a Service (PAAS), and the service software (SAAS) in diligence. In the research, we deliberate the Assessing the Security of Cloud It Components according to the criterion of obtainable principles.

Statement of the main material of the research. Cloud computing Modules. Cloud hosting operation models are classified by the proprietorship, size and access. It tells us about the cloud nature. Many organizations willing to realize it since it will minimize the operation cost.

Cloud computing deployment models. Public Cloud. In this type of hosting of the cloud the services of the cloud are delivering over network that is untie for the public use. It is an actual representation hosting of the cloud. In this cloud, the model source grants the services and the infrastructure to diverse consumers. The patrons do have not to direct over the infrastructure location. Instead of the security level, there is no difference in the public or private clouds' structural design. The public clouds are suited for the businesses that require managing load and it is economical in the matter of the cost. The dealers provide the licensing strategy for individual user. In the public cloud the cost share by all the user. It is doing well for the customers economically. Public cloud amenitiesmay be accessible for free like of a community cloud Google (Linthicum, 2017).

Private Cloud. Private cloud is known as the internal cloud and executes on the cloud-based secure environment and defends from the firewall governed by department of IT that fits into the exacting corporate. It is consent to the authorized user and bestows the organization superior power over on data. It is hosted internally as well as externally and provides the resources from the distinct pool to private cloud services. In the type of cloud there is no need for the regulation of the security and limitation of the bandwidth that present in the environment of the public cloud. The providers and the clients have direct on the infrastructure security user access. Eucalyptus system is the example of it (Odun-Ayo, 2018).

Hybrid Cloud. It is an integrated kind of clouding and it constitutes an arrangement for two or more than it for the servers of the cloud that public, private or community cloud. It is proficient in crossing isolation and prevails over the restrictions of the supplier. It is not catalog into public, private or cloud computing. This user has been allowed raise the capacity and the capability by assimilation, aggregation and customization by an additional package of cloud or service (Rao et al., 2015). In a hybrid cloud, the capitals are supervised either in the house or by an outside provider.

Security Issues. The models of the cloud servicesthat provide the different services to the users and it is also reveal the information that add the security and risk issue in the computing cloud system. IAAS is located in the bottom layer and provide the powerful function to the clouds. IAAS enablesthe hackers to execute attacks like forcing of the brute cracking, which want elevated power of computing. The virtual machine is supported by IAAS which offers the platform to the hackers to commence the attacks that entail a large numerical of the instances attacking. In the cloud model, the data loss is also a security risk. Data in the cloud is simply accessed by external hackers and unauthorized internal employees. The internal employee invests the data accidentally or intentionally. The hackers get admittance to database by using hacking techniques. Viruses and Trojan can upload to the system of the cloud and origin harm (Kaur & Singh, 2015). To implement the system it is important to recognize the cloud threats that have better mechanism for the security to protect the computing cloud environments (Polk et. al., 2017).

Malicious attacks. Security threats come about within or outside of the organizations. According to Cyber Security Watch Survey in the 2011, 21 percent of the cyber attacks were cause by the insiders. 33 percent of the respondents’consideration that the attacks of the insiders are more costly and damage to the organizations.

In general, inside attacks were unlawful contact with and use corporate information (63 %), and shoplifting of intellectual property (32%). The users of Malicious can add admittance to specific sensitive data and lead the data contravene Jathanna & Jagli (2017) has discovered malicious attacks by the unofficial client on the victims of the IP address and physical server. The malicious schedule can diverge from stealing of the data. In a cloud scenario, an insider can demolish the complete infrastructure or influence or steal data.

The system depend on the solely on the service of the cloud supplier for the security with the high level of the risk.

Theoretical aspects. According to (Landwehr, 2015), to guard a computer system the enterprise sensitivity of datais requires that manipulated with the application. The security of policies and threat management is part of the security of the computer system. Specific rules set under the security policies like protecting the physical level, disaster recovery and containment, management backup, media preservation and destruction, training of the user, event logging policy use of cryptography and its parameters, system and resource access control, thwart infringement of regulation and beliefs etc. the management of the risk occupy the systematic and continuous appraisal of computer security levels.

The system and application classify intimidation and vulnerabilities for additional modification (Malik, 2018; Wulf et al., 2021).

As pierced in (Lindner et al.,2021), computing of the cloud conveys the option of infrastructure computing, software development and deployment podium, web applications as services, that are accessible to the customers like pay you as go model. In the industry, these services are submitted as Infrastructure as a Service (IAAS), Platform as a Service (PAAS), and Software as a Service (SAAS), respectively.

Studies like (Langum et al., 2021), confer the explanation to the troubles computing allocation resources of the clouds that base on a criteria of the numeral, maximal use of resources, minimizing the response time for the user or reduction of power consumption. The problem is generally define as problem of the knapsack problem, or a specific deviation (Vector Bin Packing) , equally troubles are known to be NP-hard troubles (Lingham et al., 2019).

Security Metrics. These are the dimension from that supervise or balance the level of seclusion and security. It also computes thecurrent status of the security in a environment of computing.By using the metrics of the security we simply encourage transparency, decision making, inevitability and practical preparation. Metric is a purely classify as a standard of measurement that convolutes what is being measured like attribute and how it is measured like the unit of measure). The development of the dimension metric collection that has a pre established rule (Odun-Ayo et al., 2018). Permit the result interpretation. Additional the metrics are catalogued into primitive metrics or sub metrics (Pendleton et. al., 2016).

Any restrictions or controls connecting to the primitives are distinct in the measurement method. A metric can be expressed in one of the following behavior:

- # number is identify as the absolute value of any evaluateaspect;
- % percentageutter a percentage of an part measure the relation to the total number of elements
- Logicvalues articulate Yes or No for an occasion.

In cloud computing security and privacy is most arguetopic in the migration of information evaluate to the traditional system. In Foster & Gannon (2017) the authors classify the definition of the cloud computing and comparing the computational grids and clouds, all the way through the psychiatry of facet of architectures, models of business, management and security. The main problem is also present in computing cloud, that are the need of standardization with solutions of the cloud.

In the new technique the integration of the security policy with Security SLA are accessible by (Berkane et al., 2020; Yahya et al., 2017).

A formal form for the specification for abstract security properties offered by Rahulamathavan et al. (2015), and a formal loom to specification and rigorous analysis of security metrics is presented by Krautsevich et al. (2017). The methodology reviews of the new describes the multilevel security strategyto measure the quality of protection for the in order flow and the risks occupied in the problem of multilevel safety in computer networks is offered by (Berkane, 2020).

Methodology. The methodology for the management of the security in the computing of the cloud is based on the following components is: hierarchy of the security metrics; security index; allocation index; computing cloud management.

The security metrics oh hierarchies are derivative of the GQM methodology. The security index computes from the use of the hierarchy of the security metrics. It allocates the calculations of the index allocation. The scheduler for cloud management is use for the index allocation as an allusion to the allocation resource process. In the area of the management of security, the security metrics hierarchy offered a lateststructure of visualization of the security informationthat collectedfrom the environment of the cloud computing.

Security challenges of service model. In the year of 1970 the GQM Methodology the GQM technique (Goal Question Metric) Yahya et al. (2015) planned to budgetrying for defect of the software from the qualitative and subjective state in empirical model, in which flaw measured alongsidedistinctpurpose and objectives linked with the outcome. This technology elaborates the measurement model into three levels:

1. Conceptual level (goal) it is the main goal due to many reasons like quality of the models that have many views related to specific environment.
2. Operational level (question) a range of question that elaborates the form and concentrate on the objects discriminate the measurementof a definiteobject.
3. Quantitative level (metric) it is a metrics set that base on the representation that linked with each question in sort to answer it in aassessableapproach.

The security metrics hierarchy is generatingstraight from the GQM classificationdevelopment, thefeature of the securityplan to parallel to the security metrics. Table I prove the affiliationamong the GQM methodology and the security metrics hierarchy (SMH).

Conclusions and prospects for further research. In the additional work, the security metrics calculate automatically from the environment but this course wants an expert who will set up the preventive values to ranges. In a simple way that is sculptor is dependent on the interference of the human. Another formulation to analyze the index of the protection that can be take from combining a weight rate for apiece metric, in this every weight value signifies the degree of consequence in the midst of metrics on the way to compile the set of metrics (Monsalve et al., 2015; Chaabane et al., 2019). The security metrics at the superior level are calculated as the weighted standard of the metrics level that instantlyless it. Next, we preparation to broaden the association of the stratagem for the cloud computing managing that presented by (AA and AR), in relative to transparency and performance, for a preface set of 180 metrics that take from the accepted method of GQM.

In this study, we anticipated management methodology for the computing of cloud by using the security criterion. We present the two articles for the resources of the management that deal with scalability and the granularity in the computing cloud. The security index transmits security level measured in the computing cloud environment for the diverse security features modeled hierarchy metrics. In addition, this approach leads to supporting hierarchical decomposition, that permits the model scalable and distributed.

References

1. Berkane, M. L., Boufaida, M., & Bouzerzour, N. E. H. (2020). Modelling elastic scaling of cloud with energy-efficiency: Application to smart-university. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2020.11.025
2. Daylami, N. (2015). The origin and construct of cloud computing. *International Journal of the Academic Business World*, *9*(2), 39-45.
3. Foster, I., & Gannon, D. B. (2017). *Cloud Computing for Science and Engineering*. MIT Press.
4. Gashi, L. (2016). Cloud Computing and Enterprise Data Reliability. In *University for Business and Technology International Conference*. University for Business and Technology. https://doi.org/10.33107/ubt-ic.2016.5
5. Kaur, M., & Singh, H. (2015). A Review of Cloud Computing Security Issues. *International Journal of Education and Management Engineering*, *5*(5), 32–41. https://doi.org/10.5815/ijeme.2015.05.04
6. Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. *International Journal of Advances in Engineering & Technology*, *8*(3), 397.doi.org/10.14257/ijgdc.2015.8.5.21
7. Lingham, G., Mackey, D. A., Lucas, R., & Yazar, S. (2019). How does spending time outdoors protect against myopia? A review. *British Journal of Ophthalmology*, *104*(5), 593–599. https://doi.org/10.1136/bjophthalmol-2019-314675
8. Malik, M. I. (2018). Cloud computing-technologies. *International Journal of Advanced Research in Computer Science*, *9*(2), 379–384. https://doi.org/10.26483/ijarcs.v9i2.5760
9. Monsalve, J., Landwehr, A., & Taufer, M. (2015). Dynamic CPU Resource Allocation in Containerized Cloud Environments. In *2015 IEEE International Conference on Cluster Computing (CLUSTER)*. IEEE. https://doi.org/10.1109/cluster.2015.99
10. Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018). Cloud Computing Architecture: A Critical Analysis. In *2018 18th International Conference on Computational Science and Applications (ICCSA)*. IEEE. https://doi.org/10.1109/iccsa.2018.8439638
11. Pendleton, M., Garcia-Lebron, R., Cho, J. H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, *49*(4), 1-35.
12. Polk, T., Souppaya, M., & Barker, W. C. (2017). Mitigating IoT-Based Automated Distributed Threats. https://www.nccoe.nist.gov/sites/default/files/legacy-files/iot-ddos-project-description-draft.pdf
13. Rao, T. V. N., Naveena, K., David, R., & Narayana, M. S. (2015). A new computing environment using hybrid cloud. *Journal of Information Sciences and Computing Technologies*, *3*(1), 180-185.
14. Son, J., & Buyya, R. (2018). A taxonomy of software-defined networking (SDN)-enabled cloud computing. *ACM computing surveys (CSUR)*, *51*(3), 1-36. https://doi.org/10.1145/3190617
15. Srivastava, P., & Khan, R. (2018). A Review Paper on Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(6), 17. https://doi.org/10.23956/ijarcsse.v8i6.711
16. Wulf, F., Lindner, T., Westner, M., & Strahringer, S. (2021). IaaS, PaaS, or SaaS? The Why of Cloud Computing Delivery Model Selection – Vignettes on the Post-Adoption of Cloud Computing. In *Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2021.758
17. Chaabane, M., Bouassida Rodriguez, I., Colomo-Palacios, R., Gaaloul, W., & Jmaiel, M. (2019). A modeling approach for Systems-of-Systems by adapting ISO/IEC/IEEE 42010 Standard evaluated by Goal-Question-Metric. *Science of Computer Programming*, *184*, 102305. https://doi.org/10.1016/j.scico.2019.102305
18. Yahya, F., Walters, R. J., & Wills, G. B. (2017). Using Goal-Question-Metric (GQM) Approach to Assess Security in Cloud Storage. In *Enterprise Security* (pp. 223–240). Springer International Publishing. https://doi.org/10.1007/978-3-319-54380-2_10
19. Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. *International Journal of Engineering Research and Applications*, *7*(6), 31-38.
20. Rahulamathavan, Y., Rajarajan, M., Rana, O. F., Awan, M. S., Burnap, P., & Das, S. K. (2015). Assessing Data Breach Risk in Cloud Systems. In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. https://doi.org/10.1109/cloudcom.2015.58