IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol. 9, Issue.3, March 2021 E-ISSN: 2347-2693

# Data Centric Security Approach For Cloud Computing

**Thade Lakshmi Devi[1*], S. Krishna Mohan Rao[2]**

[1,2]Department of computer science and engineering, Mewar University, Rajasthan, India

**Corresponding Author: manu.venni5@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v9i3.4952 | Available online at: www.ijcseonline.org

Received: 20/Mar/2021, Accepted: 25/Mar/2021, Published: 31/Mar/2021

***Abstract*-**The Data Centric Security (DCS) approach is talked about in detail. This approach is the central one utilized as a part of this postulation for upgrading cloud computing security and privacy. The Paper begins with looking into and ordering conceivable security solutions, in light of the DCS ideas in the cloud computing model. 3, at that point expands on these, to shape the applied structure for DCS implementations proposed in this exploration. [6] The normal advantages of applying the DCS way to deal with the cloud computing environments are talked about in. The extent of the application of the DCS way to deal with the cloud computing model for this proposal is recognized in the fundamental security necessities of applying the DCS way to deal with this extension are additionally cleared up. In addition, the accessible innovations that can be utilized to accomplish these necessities are looked into in that section. In light of such audits, appropriateness of these advancements is evaluated to determine a novel solution, which is among the fundamental contributions of this examination. Finally, the outline of this part is quickly introduced. [9]

***Keywords*-** Communication network, 3G, mobile core network, Broadband Router, HNB.

## I. DATA-CENTRIC SECURITY APPROACH [2][11][6]

In distributed computing, clients' information is taken care of generally in virtual stockpiles in a cloud administration provider's cloud foundation. In the public SaaS and DaaS models, clients simply guarantee the set aside information while all the equipment and programming drew in with taking care of and treatment of the information are controlled by the specialist organizations. In various models, for instance, the public IaaS and PaaS models, programming treatment of the information and applications is furthermore controlled by the clients, while the equipment isn't. Thus, from the cloud clients' perspective, the main asset in the cloud climate is their information, especially information that contain delicate data, for instance, government, social protection, and budgetary information. With the benefits. [3][6].

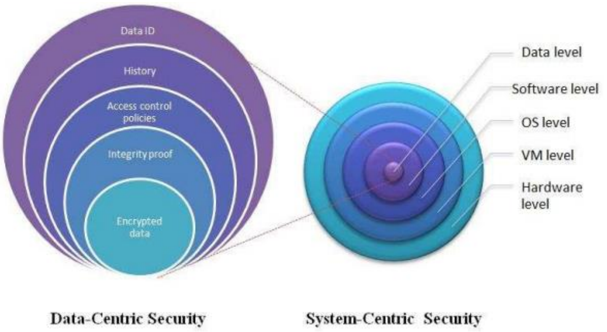
### 1.1 CLASSIFYING SECURITY SOLUTIONS FOR CLOUD COMPUTING

To the extent understanding the DCS thought, information security answers for the distributed computing perspective can be assembled considering two measures: the primary arrangement relies upon which level the security is given at, and the subsequent grouping relies upon who is accountable for giving the security. [6]

On the right-hand side of Figure 2.0, the levels that security capacities can be given at, according to information, are laid out. At the point when everything is said in done, arrangements focusing on giving security from outside the information level are designated framework driven security. If the arrangements revolve around a particular level, they are described by that specific level. For example, arrangements that intend to improve the security confinement between VMs at the VM (hypervisor) level can be named VM-driven security arrangements. On the other hand, arrangements wanting to give information security from inside the actual information, as showed up on the left-hand side of Figure 3.1, are designated information driven security arrangements. The levels showed up in Figure 3.1 are ordinary levels. There can be dynamically or less levels in a sensible framework, considering the genuine requirements and execution. [4]

## II. THERE ARE THREE DUTY LEVELS OF SECURITY: [1][3]

- Service supplier level where security is given and supported by the cloud supplier.
- Trusted Computing level where security is given and supported by an outsider.
- Data-centric security level where security is given and supported by the data proprietor.



2.0 A FIGURE REPRESENT CASE OF THE SECOND CLASSIFICATION

TABLE 2.1 HETEROGENEOUS DESCRIPTIONS OF DATA-CENTRIC SECURITY

| Ref. | Security level | Descriptions |
|---|---|---|
| **(Bilger, O'Connor et al. 2006)** | **Outside data** | "The IBM data-centric security model (DCSM): The spotlight in the DCSM is on inferring the correct security level, in light of a business analysis of the data being dealt with. This data classification at that point drives the properties and access control strategies representing the utilization of data by applications that actualize business forms. Security services and their basic mechanisms can be dreamy into interfaces that specifically bolster data taking care of approaches." |
| **(Jennifer 2009)** | **Outside data** | "Data-centric technology is an important trendy expression that, on the off chance that it develops as indicated by its present vision, could give technology building obstructs that would enable security professionals to name data and confine data access to approved utilize cases." "Data-centric security begins with a hard take a gander at what data the business must ensure and why, or an activity in information classification." |
| **(Ransom and Werner 2009)** | **Inside data** | "The focal point of data-centric security is to give constantly the fitting security level for every datum set, as per its esteem, taking into consideration persistent ideal data security, in any case where the data is conveyed, put away, or utilized. For this reason, every datum set has its security necessities connected to the data." |
| **(Chow, Golle et al. 2009)** | **Inside data** | "We propose moving from shielding data all things considered (system and applications which utilize the data) to shielding data from inside. We call this approach of data and information securing itself information-centric. This self-protection requires insight be placed in the data itself. Data should act naturally depicting and protecting, paying little mind to its environment. Data should be scrambled and bundled with a utilization strategy. Whenever accessed, data ought to counsel its strategy and endeavor to reproduce a secure environment utilizing virtualization and uncover itself just if the environment is checked as trustworthy (utilizing Trusted Computing). Information centric security is a characteristic extension of the pattern toward better, more grounded, and more usable data protection." |

## 2.1 DCS CHARACTERISTICS. [3]

In this part, the DCS approach is analyzed in more detail. A couple of its characteristics are included and analyzed to convey a clearer see about the DCS applied requirements. All of these ascribes is related to protection and security issues in guaranteeing customers' information in distributed computing. Generally, security essentially insinuates keeping an eye on three guideline concerns: mystery, respectability and availability. For the most part, CIA is used as an abbreviation for these three basic security requirements. To the extent information security, the CIA requirements are on information order, information trustworthiness and information openness. In distributed computing or any processing framework, the CIA essentials are in like manner associated with the framework concerning framework protection, framework uprightness and framework openness. [4]

### 2.1.1 THE ACCOMPANYING RUN DOWN FEATURES THE CRITERIA THAT ANY GAVE SECURITY SOLUTION IN VIEW OF THE DCS APPROACH MUST SATISFY: [6][8]

1. Every datum set is self-depicting, self-securing and self-protecting (i.e. secure data set). Accordingly, every datum set's security prerequisites and highlights are given from inside it and don't rely upon offices outside the data set, aside from some essential data dealing with forms.
2. The data protection does not depend on the cloud provider or Trusted Third Party (TTP).[5]
3. Just the data proprietor is in charge of making and dealing with these security necessities and highlights for every datum set from the season of making it until the point when the finish of the data set's lifecycle.
4. All operations identified with access to the ensured data set by approved clients and implementation of the security policies on the data are performed without bargaining the clients' privacy or data confidentiality.

### 2.1.2. THIS APPROACH IS RELIED UPON TO ACCOMPLISH THESE ADVANTAGES: [5][8]

Information privacy is protected. The information are self-guaranteed and the insurance can't be fixed in the cloud or wherever else by any affirmed substance. For example, by keeping the information encoded constantly at the cloud, even the cloud supplier can't unscramble. The information classification is guaranteed whether or not there are security breaks in the cloud. Re-appropriating mixed information to the cloud can be seen as safer even than keeping it decoded in-house. Hence, the data stays secure whether the cloud worker gets haggled either from inside or outside

The multi-layered nature of the security the board is diminished. The security boundaries of each datum set can be undeniably shown self-governing from other informational indexes' or outer security workplaces. For example, changing the security need for a particular informational collection is simply cultivated by changing the security boundaries joined to the informational collection explicitly. [6]

Responsibility and auditability are given from program codes attached to the actual information. Access logs are associated with the information and the logs are gotten against alterations. The logs offer data to the information owner upon request considering predefined design of the associated program.

Straightforwardness of the information use and area of the information in the cloud can be given by data to inescapable observing and following usefulness associated with the information.

Protection of information access arrangements is defended as the admittance to information is approved under the safe strategies concealed inside the information. Access is performed without the need of revealing these arrangements or any fragile data to a cloud supplier or TTP. [8]

Trustworthiness of information is guaranteed all through its lifecycle. Affirmed customers can affirm the uprightness and realness for each datum set only.

Information security and respectability rely upon the nature of the cryptographic strategies used more than on trust of the cloud specialist co-ops and don't need a TTP.

Versatility can be assessed in a couple of points. Since in the DCS approach, each set of information has its own entrance control execution, the informational collection can be moved inside the cloud climate without limitation related to get to control approval. Also, self-guaranteed information empowers the cloud to proper data resources capably with less worry about trust requirements. For example, by virtue of read just resources, numerous copies of prevalence data can be safely made and coursed feasibly among cloud hubs to improve the read execution. [5]

The methodology allows either a customer or a cloud supplier to improve information accessibility by keeping different copies of the information in different geographic areas, for example different information center areas of a comparable supplier or unmistakable suppliers. Thus, this framework will give a more raised measure of transformation to non-basic disappointment since information are available whether or not a worker in one area misses the mark. The DCS approach empowers such a system to be utilized as duplicates of a data set contain the very same self-protection information.

## III. ATTRIBUTES. [8][9] [11]

Before some of the attributes will be defined, the term cloud should be explained. A cloud has been long used in IT, in network diagrams respectively, to represent a sort of black box where the interfaces are well known but the internal routing and processing is not visible to the network users. Key attributes in cloud computing: [9]

- **Service-Based*:*** Consumer concerns are abstracted from provider concerns through service interfaces that are well-defined. The interfaces hide the implementation details and enable a completely automated response by the service provider. The service could be considered "ready to use" or "off the shelf" because it is designed to serve the specific needs of a set of consumers, and the technologies are tailored to that need rather than the service being tailored to how the technology works. The articulation of the service feature is based on service levels and IT outcomes such as availability, response time, performance versus price, and clear and predefined operational processes, rather than technology and its capabilities. In other words, what the service needs to do is more important than how the technologies are used to implement the solution.[9]
- **Scalable and Elastic*:*** The service can scale capacity up or down as the consumer demands at the speed of full automation (from seconds for some services to hours for others). Elasticity is a trait of shared pools of resources. Scalability is a feature of the underlying infrastructure and software platforms. Elasticity is associated with not only scale but also an economic model that enables scaling in both directions in an automated fashion. This means that services scale on demand to add or remove resources as needed. [7]
- **Shared:** Services share a pool of resources to build economies of scale and IT resources are used with maximum efficiency. The underlying infrastructure, software or platforms are shared among the consumers of the service (usually unknown to the consumers). This enables unused resources to serve multiple needs for multiple consumers, all working at the same time.[8]
- **Metered by Use**: Services are tracked with usage metrics to enable multiple payment models. The service provider has a usage accounting model for measuring the use of the services, which could then be used to create different pricing plans and models. These may include pay-as-you go plans, subscriptions, fixed plans and even free plans. The implied payment plans will be based on usage, not on the cost of the equipment. These plans are based on the amount of the service used by the consumers, which may be in terms of hours, data transfers or other use-based attributes delivered.
- **Uses Internet Technologies**: The service is delivered using Internet identifiers, formats and protocols, such as URLs, HTTP, IP and representational state transfer Web-oriented architecture. Many examples of Web technology exist as the foundation for Internet-based services. Google's Gmail, Amazon.com's book buying, eBay's auctions sharing all exhibit the use of Internet and Web technologies and protocols. More details about examples are in the chapter four – Integration [2].

## IV. CLOUD COMPUTING CATEGORIES [8][9]

There are three main categories in CC, Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). All of them are described below in more details

- **Infrastructure as a Service** is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. [8]
- **Software as a Service** is a software distribution model in which applications are hosted by a vendor or service

provider and made available to customers over a network, typically the Internet. It is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture become increasingly available. [9]

- **Platform as a Service** is an outgrowth of Software as a Service (SaaS). It is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. [10]

## V. CONCLUSION

The overall commitment on the hypothesis has both a speculative and a practical viewpoint. A graph of the bleeding edge of safety viewpoints in distributed computing and a bare essential confided in dispatch show for conventional VM dispatch in distributed computing conditions can be named as the speculative commitments. Two practical commitments are joined, to be explicit a separated diagram for the execution of the dispatch show in OpenStack and an advancing execution (the results of which will be represented in a revived form of this report). [9] The point by point execution design can be used as a piece of solicitation to explicitly execute the show in a passed on OpenStack climate. The outcomes of the execution of the show will be given in an invigorated variant of this paper, close by a presentation assessment of the show once the execution stage is done up. A couple of disclosures of the hypothesis should be named. At first, believed figuring can be used to address a part of the security stresses in distributed computing inside the security model of an untrusted cloud specialist organization. In any case, a series of expectations, for instance, for example accessibility of actual admittance to the information center should be fulfilled in order to ensure a believed VM dispatch in a public distributed computing climate. Furthermore, while open source distributed computing frameworks are in powerful progression (something which presents the two challenges and openings), reinforce for confided in registering from broad chip makers, for instance, Intel and AMD, and what's more support for distributed computing stages from open source working framework merchants energizes the use of confided in processing limits into distributed computing. The results of this proposition set forth a safeguard for enlarging the extent of usage cases for confided in processing by applying it to distributed computing conditions. Confided in figuring, when associated successfully with explicit suppositions satisfied, can offer the abilities to safely perform information controls on distant equipment had and kept up by a pariah with an irrelevant peril for information uprightness. While the presentation of a believed VM dispatch show can be seen as a commitment towards an assessment move in the business with respect to confided in processing, it should be enhanced by secure and trust-keeping up executions of other routinely used distributed computing tasks, for instance, VM relocation, suspension and cancellation, information stockpiling, secure capabilities the board, etc. [11]

## REFERENCES

[1] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, ,(2011)“All your clouds are belong to us: security analysis of cloud management interfaces,” in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, CCSW ’11, (New York, NY, USA), pp. 3–14, ACM, 2011.

[2] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, (2009) “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,” in Proceedings of the 16th ACM conference on Computer and communications security, CCS ’09, (New York, NY, USA), pp. 199–212, ACM, 2009.

[3] D. Molnar and S. Schechter, (2010) “Self hosting vs . cloud hosting, : Accounting for the security impact of hosting in the cloud,” in Workshop of the economics of cloud security, pp. 1–18, 2010.

[4] Y. Chen, V. Paxson, and R. Katz, (2010) “The hybrex model for confidentiality and privacy in cloud computing,” Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, January 2010.

[5] N. Santos, K. P. Gummadi, and R. Rodrigues, ( 20009) “Towards trusted cloud computing,” in Proceedings of the 2009 conference on Hot topics in cloud computing, HotCloud’09, (Berkeley, CA, USA), USENIX Association, 2009.

[6] D. Kuhlmann, R. Landfermann, H. V. Ramasamy, M. Schunter, G. Ramunno, and D. Vernizzi, (2006) “An open trusted computing architecture – secure virtual machines enabling user-defined policy enforcement,” Work, pp. 1–14, 2006.

[7] N. Pohlmann and H. Reimer, (2008) “Trusted computing - eine einfA˜ 1 4 hrung,” in Trusted Computing (N. Pohlmann and H. Reimer, eds.), pp. 3–12, Vieweg+Teubner, 2008. 10.1007/978-3-8348-9452- 6 1.

[8] M. Nauman, S. Khan, X. Zhang, and J.-P. Seifert,(2010) “Beyond kernel-level integrity measurement: Enabling remote attestation for the android platform,” in Trust and Trustworthy Computing (A. Acquisti, S. Smith, and A.-R. Sadeghi, eds.), vol. 6101 of Lecture Notes in Computer Science, pp. 1–15, Springer Berlin / Heidelberg, 2010. 10.1007/978-3-642-13869-01.

[9] I. Bente, G. Dreo, B. Hellmann, S. Heuser, J. Vieweg, J. von Helden, and J. Westhuis,(2011) “Towards permission-based attestation for the android platform,” in Trust and Trustworthy Computing (J. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, and Y. Beres, eds.), vol. 6740 of Lecture Notes in Computer Science, pp. 108–115, Springer Berlin / Heidelberg, 2011. 10.1007/978-3-642- 21599-58.

[10] R. Neisse, D. Holling, and A. Pretschner, (2011) “Implementing trust in cloud infrastructures,” in Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on, pp. 524 –533, may 2011.

[11] B. Parno,(2008) “Bootstrapping trust in a ”trusted” platform,” in Proceedings of the 3rd conference on Hot topics in security, (Berkeley, CA, USA), pp. 9:1–9:6, USENIX Association, 2008.