Survey on Implementation of Security in Cloud

Deepak Garg and Jagpreet Sidhu

Abstract Cloud computing has emerged as one of the next generation computer technologies. It is a model wherein storage, computing facilities, and applications are provided as services on the top of Internet. It permits associations to decrease capital costs, in administration costs, and improve unwavering quality and accessibility by getting administrations and infrastructural assets momentarily in a flexible way utilizing pay-as-you-go demonstrates. These services are provided on resources located at diverse geographical location beneath various service providers. The adjustment of cloud has exchange control of physical assets from potential clients to specialist organizations. This change has offered mount to security dangers and concerns which comes about into absence of certainty of potential clients on distributed computing. The paper displays a short explanatory review on different security issues in distributed computing. It presents a distinct view on classifying various security risks and concerns in cloud computing. A different method of classification varies security frameworks, models, and techniques—selected from latest literature on resources of repute. The paper concludes on realization of some unique cloud security objectives and challenges.

Keywords Cloud · Security · Cloud platforms · Effective citations

1 Introduction

The cloud computing worldview has turned into a standard answer for the arrangement of business procedures and applications, and it is quickly developing. It is giving people in general cloud vision, framework, stage, and programming

D. Garg (✉) · J. Sidhu
Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Patiala, Punjab, India
e-mail: deepak.garg@chitkara.edu.in

J. Sidhu
e-mail: jagpreet.sidhu@chitkara.edu.in

R. Singh et al. (eds.), *Intelligent Communication, Control and Devices*,
Advances in Intelligent Systems and Computing 624,
https://doi.org/10.1007/978-981-10-5903-2_164

administrations to clients and specialist co-ops on a compensation as-you-go premise. It is also modeled for enabling ever-present, suitable, on-demand network accessibility to a pool of configurable computing resources that are sharable and that can be swiftly provisioned and unrestricted by means of least management effort or service contributor interface. But, security is the major thing where we have to look onto it. Cloud Architecture: Depend on client–server services, we can divide cloud computing into three types: First, Platform-as-a-Service (PaaS): Cloud providers provide a platform where clients can run the applications means cloud providers are delivered the applications to the client that they are able to run the application on their own platform. Platforms are managed by the cloud providers. Second, Software-as-a-Service (SaaS): This service includes computing which is provided by cloud servers, consists of OS, coding language, database management, environment of the platform, etc. Without buying the hardware, customers can run the applications by using the resources. Third, Infrastructure-as-a-Service (IaaS): This is a tune-up of pay-as-you-go same as PaaS and SaaS including resources, storage, etc. (Fig. 1).

Cloud computing can be differentiated into four categories, and in all different categories, there are different security issues. Private cloud: Private cloud is used by a big institutes or societies. But this cloud will be restricted only in that organization means others organization can't share that cloud. Public cloud: This cloud is owned by an organization but other organization also can share that cloud. Hybrid cloud: An organization buys a cloud from another cloud services and uses that cloud. After buying the cloud, only the people of those organizations can only access that cloud. So, hybrid cloud consists of personal cloud and open cloud. The public cloud: This cloud is used by other organization (Fig. 2).

Various security dangers are related with cloud information administrations, such as network eavesdropping, side channel attacks, illegal invasion, virtualization vulnerabilities, abuse of cloud, and denial of service attacks. Security issues in cloud computing: The security issues we face in cloud computing can be categorized into three types:

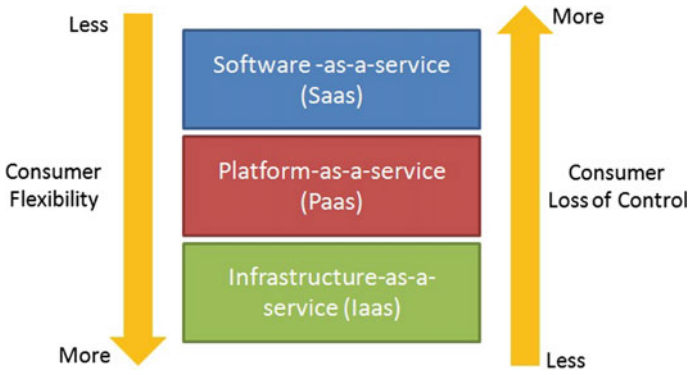

Fig. 1 Cloud deployment model

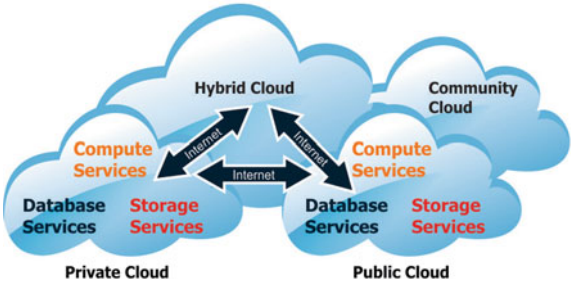

Fig. 2 Types of cloud deployment model

- Conventional security issues
- Availability issues
- Third-party control-related issues.

2 Literature Review

This paper analyzes the previous works of authors done between 2014 and 2016 in order to critically summarize the current knowledge in the area of security, and new algorithms are developed using some important techniques, and also, various outcomes are discussed. Figure 3 represents the different types of techniques used for evaluating or developing new security models.

However, Table 1 describes what type of dataset, Simulators, Parameters has been used to implement various new applications for security. Dataset is corpus on which the developed algorithm is implemented, and the results are observed. Simulator is software that provides a platform to execute an algorithm developed for various security issues or it is software in which algorithm designed to provide a realistic imitation of operation can be implemented. Constraints are boundaries which define the reach of a particular method or algorithm.

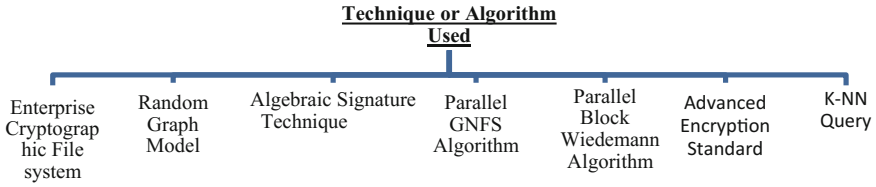

Fig. 3 Techniques or algorithm used

Table 1 Techniques/algorithms used in cloud security

References	Dataset	Simulation	Parameters	Application
[1]	Not discussed	Not discussed	Updated data storage	Created secure record sharing in public storage Outlines a protected and productive stackable framework named Shield
[2]	Not discussed	Actualized utilizing C on a framework with an Intel Core i5-2450 M CPU at 2.5 GHz, and 6 GB RAM	Correspondence cost and computation cost of data auditing and element information refresh	Remote data auditing (RDA) techniques
[3]	MIT reality-mining dataset and Nodobo dataset	Not discussed	Security, cost, and load adjusting in telephone clone provisioning	Developed SWAP a scheme for telephone clones
[4]	Not discussed	Implemented the parallel GNFS algorithm integrated with parallel block Wiedemann algorithm	Not discussed	Not discussed
[5]	Standard HD videos	Not discussed	Not discussed	HEVC encoded video stream
[6]	Not discussed	Not discussed	Improved chaos prediction and suppression methods	CPSS model
[7]	Real datasets (Hong-Kong and SIFT1M) and synthetic datasets (Gaussian64, Gaussian256)	Not discussed	Not discussed	Secure approximate k-nearest neighbor (SANN) query
[8]	Not discussed	There own built simulator	Security and efficiency	Security-aware efficient distributed storage (SA-EDS) model
[9]	TPC-H scale 1.0 dataset	Not discussed	Correctness, security, and theoretical performance	Tree-based order-preserving encryption (OPE) mechanism

(continued)

Table 1 (continued)

References	Dataset	Simulation	Parameters	Application
[10]	Not discussed	Not discussed	Data privacy against CS, key confidentiality against QUs, query privacy against CS and DO, query controllability	Not discussed

3 Findings

In Table 2, we have calculated the effective citations in security domain of cloud computing by using the formula

$$\mathrm{EC}_{\mathrm{sd}j(y)} = \frac{P_{\mathrm{sd}j(y)}}{P_{j(y)}} \times C_{j(y)} \tag{1}$$

where in Eq. (1)

$\mathrm{EC}_{\mathrm{sd}j(y)}$ signifies effective citations in specific domain (i.e., cloud security) journal of year y. Table 2 represents data.

$P_{\mathrm{sd}j(y)}$ signifies total number of publications in specific domain (i.e., cloud security) journal of year y. Table 3 represents data.

Table 2 Effective citations in security domain of cloud computing

	2011	2012	2013	2014	2015
J1	198.47	267.57	511.01	518.18	718.51
J2	0.00	50.66	44.80	253.66	124.27
J3	3.83	48.60	29.74	54.54	35.67
J4	16.95	47.57	121.02	186.35	321.27
J5	38.34	60.86	127.57	154.41	146.69

J1 Future generation computer system
J2 Information sciences
J3 Journal of computer and sciences
J4 Journal of network and computer applications
J5 Journal of parallel and distributed computing

Table 3 Total publications in specific domain journal

	2011	2012	2013	2014	2015
J1	34	40	93	108	76
J2	0	5	5	31	9
J3	1	9	6	12	6
J4	11	14	19	31	33
J5	11	21	32	28	24

Table 4 Total publications in journal of repute

	2011	2012	2013	2014	2015
J1	123	148	188	292	174
J2	360	423	612	871	516
J3	80	65	92	123	109
J4	185	181	157	267	170
J5	136	147	150	136	98

Table 5 Total citations in journal of repute

	2011	2012	2013	2014	2015
J1	718	990	1033	1401	1645
J2	3648	4286	5484	7127	7125
J3	306	351	456	559	648
J4	285	615	1000	1605	1655
J5	474	426	598	750	599

Table 6 Percentage of publications in security domain of cloud computing

	2011	2012	2013	2014	2015
J1	27.64	27.03	49.03	36.99	43.68
J2	0	1.18	0.82	3.56	1.74
J3	1.25	13.85	6.52	9.76	5.5
J4	5.95	7.73	12.1	11.61	19.41
J5	8.09	14.29	21.33	20.59	24.49

$P_{j(y)}$ implies Total Publications in journal of repute. Table 4 represents the data.

$C_{j(y)}$ depicts Total Citations in journal of repute. Table 5 represents data.

In Table 6, we have calculated the percentage of publications in security domain of cloud computing.

Percentage for calculating is

$$\text{Percentage} = \frac{\text{EC}^{\#}}{\text{TC}^{\$}} * 100 \tag{2}$$

The term EC means Effective Citations in security field of cloud computing in the journal of repute.

$ The term TC means Total Number of Effective Citations in security domain of cloud computing in the journal of repute.

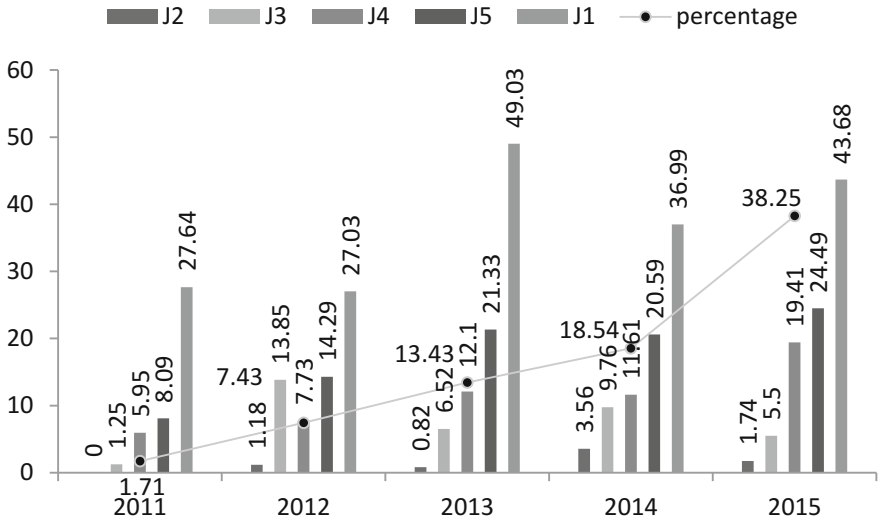

Fig. 4 Journal wise percentage of citations

4 Results

Figure 4 depicts a number of researchers who are citing the works published by Future Generation Computer System journal as it is the prestigious journal in the area of cloud computing.

5 Conclusion

From the above survey, we can conclude that there are various techniques that can be deployed to analyze the results for secured cloud data. Also, to verify results, various datasets are used that are related to user concerns, and security algorithms are proved using that. Before implementing the algorithms onto the data, data cleansing is performed, and this refines the data and makes it ready for analysis. There are also some authors who have not discussed their few parameters. On the basis of this analysis, the above-stated interpretations of result are done. This interpretation of results further provides the outcome of the analysis performed on the gathered data. Graph depicts the number of effective citations to the proportion of total number of citations in relation to a journal of repute.

6 Future Work

We will analyze some more areas where security has to be implemented that are in electronic health records and will be developing some dynamic algorithms that may work at any of the models and also at any of the platform services provided by the cloud providers. Also, we will be using static dataset to prove the results of our developed algorithms.

References

1. Shu, J., Shen, Z., Xue, W.: Shield A stackable secure storage system for file sharing in public storage. Journal of Parallel and Distributed Computing, 74(9), 2872–2883 (2014)
2. Sookhak, M., Gani, A., Khan, M. K., Buyya, R.: Dynamic remote data auditing for securing big data storage in cloud computing. Information Sciences, 380, 101–116 (2017)
3. Vaezpour, S. Y., Zhang, R., Wu, K., Wang, J., Shoja, G. C.: A new approach to mitigating security risks of phone clone co-location over mobile clouds. Journal of Network and Computer Applications, 62, 171–184 (2016)
4. Yang, L. T., Huang, G., Feng, J., Xu, L.: Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing. Information Sciences, 387, 254–265 (2016)
5. Usman, M., Jan, M. A., He, X.: Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds. Information Sciences, 387, 90–102 (2016)
6. Dai, H., Zhao, S., Chen, K.: A chaos-oriented prediction and suppression model to enhance the security for cyber physical power systems. Journal of Parallel and Distributed Computing, 103, 87–95 (2016)
7. Peng, Y., Cui, J., Li, H., Ma, J.: A reusable and single-interactive model for secure approximate k-nearest neighbor query in cloud. Information Sciences, 387, 147–164 (2016)
8. Li, Y., Gai, K., Qiu, L., Qiu, M., Zhao, H.: Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103–115 (2016)
9. Xiang, T., Li, X., Chen, F., Guo, S., Yang, Y.: Processing secure, verifiable and efficient SQL over outsourced database. Information Sciences, 348, 163–178 (2016)
10. Zhu, Y., Huang, Z., Takagi, T.: Secure and controllable k-nn query over encrypted cloud data with key confidentiality. Journal of Parallel and Distributed Computing, 89, 1–12 (2016)