Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A Survey of Security Threats and Security Management in Cloud Computing

S. P. Lalitha
Research scholar, Dept of CSE,
School of Computing
SRM Institute of Science & Technology,
SRM Nagar,Kattankulathur,Chennai,TN-603203.
email address: splalitha1980@gmail.com

Dr. A. Murugan
Professor, Dept. of Data Science & Business Systems,
School of Computing
SRM Institute of Science & Technology,
SRM Nagar, Kattankulathur,Chennai,TN-603203.
email address: murugana@srmist.edu.in

Article Info
Page Number: 4632 - 4638
Publication Issue:
Vol 71 No. 4 (2022)

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

Abstract

The cloud computing is the delivery of computing services which includes the servers, storage, databases, networking, software, analytics, and intelligence over the Internet. The attacks and threats degrade the performance of the cloud computing services. The detection and mitigation of these threats and attacks are very important in all types of cloud services to provide various services to the users through the cloud platform. In this paper, various conventional security methodologies for cloud system are discussed in detail with its limitations and advantages.

Keywords—Cloud, services, detection, mitigation, threats

Acronyms	**Abbreviations**
CC	Cloud Computing
CP	Cloud Providers
MCDM	Multi-criteria Decision Methods
HPE	Hewlett Packard Enterprise
IoT	Internet of Things
PSO	Particle Swarm Optimization
ACO	Ant Colony Optimization

I. INTRODUCTIONS

Cloud Computing (CC) is a platform which uses computer networks for distributing the various services to the required on-demand host sources. The availability of these cloud services can be accessible from anywhere in the work through the internet services. Many companies now as days provides these cloud services to the various types of users depends upon their usage requirement and availability of various utilities. These service providers are known as Cloud Providers (CP). The selection of CP is important for obtaining the service quality. For the effective cloud service, bandwidth is important due to the handling of number of multimedia data from various sender nodes to receiving nodes. There are many CP available today which provides various CC services for the users around the world [13-15]. In this regard, many developing software's or applications are developed to resolve the issues arising in CP. Multi-criteria Decision Methods (MCDM) is the example of these type of application for providing free link failure network for cloud services. The cloud service providers provide different types of services for different types of clouds. The clouds can be categorized into three models as stated below.

- Public cloud;
- Private cloud;
- Hybrid cloud;

Public cloud- Public cloud provides on demand services among the various users and the cloud resources can be maintained by third party. The public cloud can be accessed through the internet. These types of cloud services are available in both free of cost and paid. There is more number of threats in this case of public cloud due to the usage of more number of users on the same cloud platform as illustrated in Fig.1.Microsoft Azure, Oracle web services and Amazon Web Services are the examples of public cloud service providers.

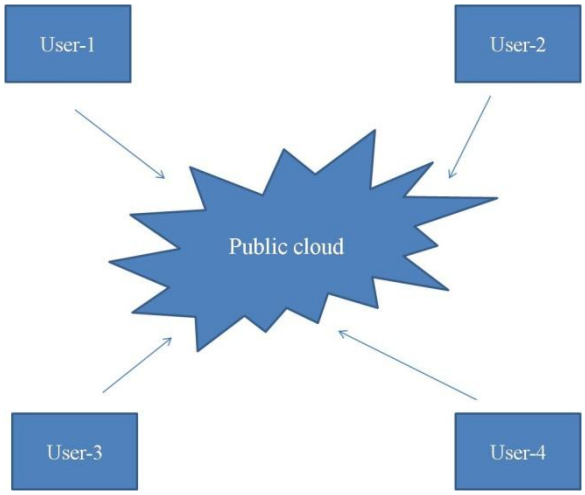

Fig.1. Public cloud illustration

Private cloud- The on-demand cloud infrastructure is provided to the particular company or industry based on their own needs and services, as illustrated in Fig.2. Intranet plays an effective role in private clouds. Microsoft, IBM and CISCO are the examples of private cloud service

providers. Hewlett Packard Enterprise (HPE) is the best private cloud service provider among the various private cloud service providers at present.

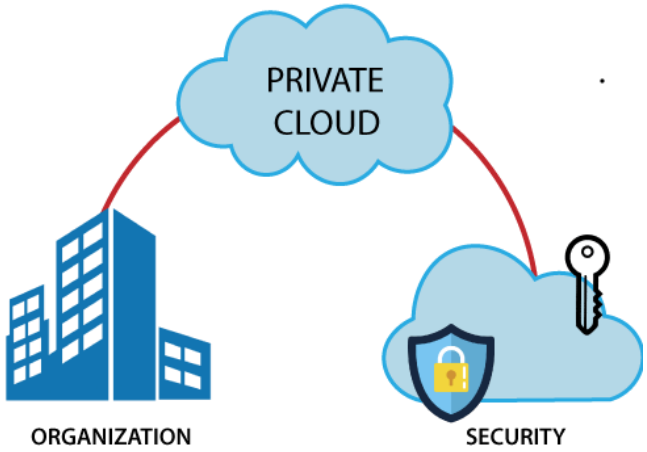

Fig. 2. Private cloud illustrations

Hybrid cloud- It is a computing environment or platform which combines the utilities of private and public clouds. Google, Amazon Web Services and HPE are the examples of hybrid cloud service providers, as illustrated in Fig.3.

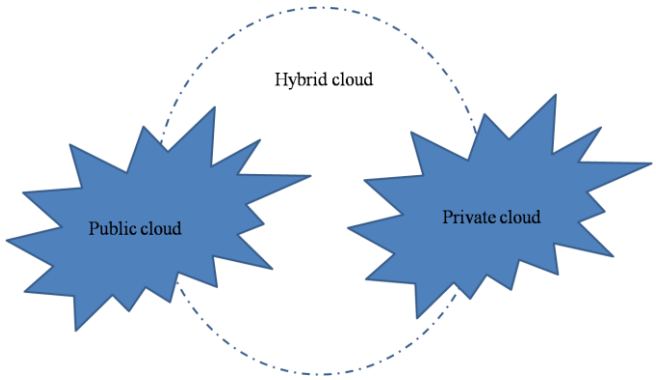

Fig. 3. Hybrid cloud illustrations

In all types of cloud models, the security threats are the common issues which degrade the performance of the utilization of these cloud services [16-18]. These threats in the cloud can be categorized as stated below.

- Insider user threats;
- External threats;
- Data leakage threats;
- Data segregation threats;
- Physical distribution threats;

The detection and mitigation of these threats and attacks are very important in all types of cloud services to provide various services to the users through the cloud platform. In this paper, various conventional security methodologies for cloud system are discussed in detail with its limitations and advantages.

II. Literature Survey

A. Survey based on the cloud storage end

Amr et al. (2021) designed a framework model for providing the security methods for cloud computing systems. Through the developed model, threats and various types of attacks were detected and mitigated in cloud storage. The designed system provided one time password for the user to access the cloud storage to protect the owner's authentication. During logging and uploading the data from the user end to the cloud storage, the generated one time password was checked and verified at every time in order to protect the data from the malicious or unauthorized persons access. Through the developed algorithms, the data in remote cloud storage was secured.

Mehrtak et al. (2021) proposed a model which was used for the security management in health care applications in remote cloud system. The unauthorized access of the remote users was restricted to enter and access the cloud system using bit level programming method. The authors provided and discussed various set of cloud protocols to manage the security system of the cloud environment. The simulation results of the developed proposed security model were tested on various test beds for remote cloud system in order to verify the authentication report.

Tewari et al. (2020) improved the security of the cloud storage system through the Internet of Things (IoT) framework model using security entity methods. The user end to end system was protected from accessing by other nodes in the system architecture. The authors addressed various security protocols which were used and tested in this work. The various attack detection methods were also discussed in this work to enhance the performance of the cloud storage system.

Alsolami et al. (2018) proposed security active methodology for detecting and mitigating the various types of active and passive attacks in cloud storage. The issues arrived in cloud system was also discussed in this work to improve the security enhancement methods on various types of cloud models. The authors estimated the performance efficiency of the developed cloud model using various metrics with respect to conventional state of the art methods in this paper.

Gururaj Ramachandra et al. (2017) discussed various mechanisms for improving the security in cloud computing framework. The main objective of this work was to detect and mitigate the active and passive vulnerabilities in cloud storage. The authors provided various potential console for the detection and mitigation process of the threats in cloud networking storage. The basic and fundamental cloud architecture was analyzed for the effective implementation of threat detection mechanism on cloud networking. Service aggregation and service arbitration of the cloud storage was improved by providing the suitable cloud mechanism in this work. Also, the authors addressed major issues concerned in private, public and hybrid cloud storage systems. End to end encryption methodologies for security enhancement in cloud was also discussed in this work.

B. Survey based on the threats in cloud system

Chimakurthi et al. (2021) provided effective solutions for COVID-19 pandemic emergency using cloud application services for remote devices. During Covid-19 situation, work from home was advised in many of the industries or companies to prevent attack from the deadly virus. In this

situation, maintaining and transferring lot of multimedia data from one device to other devices and one device to remote device was crucial task. Therefore, this paper addressed a solution for this situation by providing a cloud environment system between the multiple users. This also required a lot of security threats due to the lot of access from various devices at a time. In order to protect the data from un-authorized users, this work provided a compact solution for the users of cloud system. This increased the overall production rate of any company which used cloud storage as a platform. The active attacks were mostly affected this type of public cloud devices and they were detected and mitigated using the proposed methodology in this work.

Singh et al. (2021) provided a solution for security enhancement in cloud system users. The DDos attacks and other similar attacks were detected and mitigated by the proposed method in this work. The number of attacks detected by this method was well compared with other conventional cloud attack detection methods with respect to various addressing parameters. The authors analyzed the proposed solution for cloud platform with their enhanced security model in this work.

Demin et al. (2019) designed a solution for the private cloud system with the adaptive infrastructure environment background. In this scenario, the user's ends were also protected by the developed system for enhancing the level of security by the methods provided by this work. The developed and designed model provided an optimum solution for the security attacks and enhanced the level of security rate by mitigating the attack users at any devices.

Hossain et al. (2019) improved the storage capacity of the all types of cloud models for managing the large number of multimedia files in cloud environment. The authors compressed the multimedia data using various compression schemes and then the compressed multimedia data was optimized by several suitable optimization approaches such as Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) algorithm. The pattern or data with optimized logic were now transferred to other networking devices through the cloud storage. The performance of the cloud system was analyzed with respect to compression ratio and optimization models. The simulation results of this compression and optimization model was also analyzed for its effective cloud system management process.

Jeba et al. (2019) proposed a green cloud computing model which used energy minimization algorithm for reducing the energy consumption of the developed cloud model. The cloud centers of the developed model were also analyzed by various set of parameters to validate the effectiveness of the developed model.

Olakanmi et al. (2019) used generic cloud architecture model for the effective management of cloud system for various applications. The authors prevented the untrusted platforms for improving the cloud access rate from various nodes in cloud systems. The authors also addressed the main issues or problems in the cloud storage system. The simulation results of this compression and optimization model was also analyzed for its effective cloud system management process. The authors estimated the performance efficiency of the developed cloud model using various metrics with respect to conventional state of the art methods in this paper.

Jadad et al. (2019) proposed Context-aware prediction model for the effective creation of cloud model solution for many real time applications. The authors developed the system which pertained a logical model with heuristic parameters. The un-trustable users were restricted by using the cloud system through the developed model in this work. The simulation results of the developed proposed security model were tested on various test beds for remote cloud system in order to verify the authentication report.

III. CONCLUSIONS

In this paper, the usage and types of various clouds such as public, private and hybrid clouds are explained with examples. Also, the types of security threats and attacks are also described. The conventional methodologies for improving the security mechanism in cloud system detailed in this paper. The merits and demerits of each conventional method are described. The threats detection methods in each conventional method are elaborated with simulation environment. Based on this survey, the problems in present security mechanism of cloud system are identified and presented in this paper.

REFERENCES

[1] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", Procedia Computer Science 110 (2017) 465–472.
[2] Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish, Mohamed A. Amin, Ismail M. Hagag, "A New Secure Model for Data Protection over Cloud Computing", Computational Intelligence and Neuroscience, vol. 2021, Article ID 8113253, 11 pages, 2021.
[3] Tewari A and B. B. Gupta, "Security, privacy and trust of different layers in internet-of-things (iots) framework," Future Generation Computer Systems, vol. 108, pp. 909–920, 2020.
[4] E. Alsolami, "Security threats and legal issues related to cloud based solutions," *IJCSNS International Journal Of Computer Science And Network Security*, vol. 18, no. 5, 2018.
[5] M. Mehrtak, S. SeyedAlinaghi, M. MohsseniPour et al., "Security challenges and solutions using healthcare cloud computing," Journal of Medicine and Life, vol. 14, no. 4, 2021.
[6] Chimakurthi, V. N. S. S. (2021) "The Future Of Cloud Computing Amidst A Desperate Security Maze: The Impact Of COVID And The Future Challenges", Asian Journal of Humanity, Art and Literature, 8(2), pp. 75-84.
[7] B. Demin, S. Parlati, P. F. Spinnato, and S. Stalio, "U-LITE, A private cloud approach for particle physics computing," International Journal of Cloud Applications and Computing, vol. 9, no. 1, pp. 1–15, 2019.
[8] R. P. Singh, A. Haleem, M. Javaid, and R. Kataria, "Cloud computing in solving problems of COVID-19 pandemic," Journal of Industrial Integration and Management, 2021.
[9] K. Hossain, M. Rahman, and S. Roy, "IoT data compression and optimization techniques in cloud storage," International Journal of Cloud Applications and Computing, vol. 9, no. 2, pp. 43–59, 2019.
[10] J. A. Jeba, S. Roy, M. O. Rashid, S. T. Atik, and M. Whaiduzzaman, "Towards green cloud computing an algorithmic approach for energy minimization in cloud data centers," International Journal of Cloud Applications and Computing, vol. 9, no. 1, pp. 59–81, 2019.
[11] O.Olakanmi and A. Dada, "An efficient privacy-preserving approach for secure verifiable outsourced computing on untrusted platforms," International Journal of Cloud Applications and Computing, vol. 9, no. 2, pp. 79–98, 2019.
[12] H. A. Jadad, A. Touzene, K. Day, N. Alziedi, and B. Arafeh, "Context-aware prediction model for offloading mobile application tasks to mobile cloud environments," *International Journal of Cloud Applications and Computing*, vol. 9, no. 3, pp. 58–74, 2019.
[13] P. Chaudhary, B. B. Gupta, X. Changd, N. Nedjah, and K. TaiChui, "Enhancing big data security through integrating XSS scanner into fog nodes for smes gain," *Technological Forecasting and Social Change*, vol. 168, Article ID 120754, 2021.
[14] P. Prasad, B. Ojha, R. R. Shahi, and R Lal, "3-Dimensional security in cloud computing," in *Proceedings of the 2011 3rd International Conference On Computer Research and Development (ICCRD)*, Shanghai, China, March 2011.

[15] S. Kumar, S. A. Abbas Jafri, N. A. Nigam, N. Gupta, G. Gupta, and S. K. Singh, "A new user identity based authentication, using security and distributed for cloud computing," in *Proceedings of the International Conference on Mechanical and Energy Technologies (ICMET 2019)*, vol. 748, Galgotias College of Engineering and Technology, Greater Noida, UP, India, November 2019.

[16] G. B. Tarekegn, G. Abadi Maru, and H. Zelalem Liyew, "Privacy and security issues IN cloud computing," *International Journal Of Current Research*, vol. 8, no. 7, pp. 34894–34898, 2016.

[17] Y. Harrath and R. Bahlool, "Multi-objective genetic algorithm for tasks allocation in cloud computing," *International Journal of Cloud Applications and Computing*, vol. 9, no. 3, pp. 37–57, 2019.

[18] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, 2021.