A Comparative Study of Cloud Computing Techniques in respect to Security Challenges and different approaches to protect cloud premise

Dr. Dhanashri S. Kulkarni
Research Scholar (JJTU) & Assistant Professor, Computer Science Department Indira College of Commerce and Science, Pune Maharashtra, India.

Badshaha Gulab Nadaf
Assistant Professor, Computer Application Department
Indira College of Commerce and Science, Pune Maharashtra, India.

DOI: 10.29322/IJSRP.16.02.2026.p17033
https://dx.doi.org/10.29322/IJSRP.16.02.2026.p17033

Paper Received Date: 7th January 2026
Paper Acceptance Date: 8th February 2026
Paper Publication Date: 12th February 2026

Abstract

Cloud is nothing but accessing all the services available worldwide. Cloud is specifically used for storage different resources and worldwide databases and also have access to utmost all the software's across the world. The pre-requisite of cloud is an "Internet". Earlier they was many challenges to access required resources physically at available location so the concepts of cloud has been introduced for all that users who want to access their required resources at their own location. This research work presents comparative study of different cloud techniques with respect to their architecture, security constrain and output producing speed performance. This study will definitely help all companies in selecting cloud for their industrial need.

Keywords: Internet, VPN**,** Infrastructure as a Service (IAAS), Platform as a Service (PaaS), Cloud Security, Google Cloud, AWS.

1. Introduction

Before entering into the world of cloud, there were many challenges faced by the almost all companies. That time, there was not access of data properly in case of data needed to any of an employee if that employee was not at office and don't have any other option to access the data remotely. Many employees use to take all company data in their local drivers like pen drive and or any physical drive. But again security was also one of the major factor so many companies dined to access the company's data in any local drive. Almost all the task were in pending mode due to the non-access of the data. Major issue was the security. Many companies are failed to protect their data from the hackers and scammers. After viewing many challenges, one of the scientist and research Mark Benioff has introduced the concept of cloud along with his team to the outside world aiming easy access of the company data all the world. With the help of cloud, company can access all the applications from that organization worldwide with the help of Internet Instead of access the data using hardware drive or any local server.

In cloud computing concept, there were many components introduced like Fat client and thin client and later it is renamed with front end concept and Backend platforms like available servers and storage of the data. Also many network models introduced in cloud like cloud based delivery and network introduced like Internet, Intranet and Inter cloud. Internet has access all over the world but concept like Intranet don't have any access over the world and this is very small network that is installed inside the small or big organization and can access all the data inside that area only. In this intranet, all the devices like office laptop, personal laptops and phones are connected with the company servers and data sharing is done in that organization only. In Intranet, security issues are also handle with utmost care like firewalls are installed and data is accessed using Virtual Private network. VPN is also important in cloud and that is used to convert all the public network via private network where data is converted to encrypted form to the destination and later same data is decrypted by the end to access the original data. With the help of VPN, company can create tunnel and is used to send data packets via this tunnel.

In cloud front end, there is direct access to the user to see the interface and to interact with the system. UI in cloud is used to create User Interface and UX in cloud is used to keep user experience smooth. Cloud font end is used to keep the user engage always. Cloud back end is used to keep many servers at the same place and is used to store the data. After storing data at the back end, user can process that data by applying well defined techniques and after processing, this is used to decision on cleaned data. Cloud back end mainly consists of applications that company is using so cloud is used to give access to such kind of application worldwide.

In cloud mainly the major issues to access the application so for this cloud consists of mainly Internet, Intranet and Inter cloud. Inter cloud is the concept introduced due to which, two clouds can also interact with each other. The main advantage of Cloud is to on demand self-access of data. Company employee can get required data on the spot without location barrier and with asking data to the admin person

2. Literature Review

In our study we have reviewed 3 papers from Journal of Object Technology with the title “Cloud Computing: Today and Tomorrow” and published this paper by ETH Zurish with vol 8, number 1 the authors won kim and Suwon Korea focused a light on status and adaption issues and technical issues with cloud computing and also provides a glimpses on the future enhancement in the sector of cloud. According to them , Amazon S3 suffered exactly 2 outages in the year 2008 which was like 2 hours in February and 8 hours in August and same happen with the google that google Gmail was also not available for 2 hour in the month of august and the most dangerous thing was RIM’s Blackberry services were unavailable for complete 18 hours and finally they concluded that cloud computing is not able to provide 100 percent services unless and until we will not provide a very strong and suitable architecture for the cloud environment. With this adaptation problem, they focused on security problem and stated that it is impossible to give hundred percent security and privacy in all source of violation including inevitable software bugs and growing sophistication of hackers so finally they concluded cloud vendors must adopt most sophisticated and up to date tools to give better protection to all the applications on premises.

In our second literature study, we gone through the second research paper published by researcher Badar Alouffi , Muhammad hasan and Muhammad Ayaz with the title “Cloud Computing Security: Threats and Mitigation Strategies” where they focused on Cloud Intrusion. Intrusion is nothing but the access on the cloud with no authorization. According to them, this is also one of the major concern of cloud in which care should be taken. They said that the cloud service manager who works as a cloud provider must follow service level agreements and confirm technical standards. Cloud Services must have Intrusion detection system that will identify all the unauthorized users and will send alert message to the service admin to take a strict action against that hackers. Cloud service manager must not allow these hackers if they tried to enter inside cloud environment and only authorized user will get access to data files in premises and also in remote area. Data encryption and data decryption approach must be at the both the end of client and server and to understand anomaly behaviour of the hackers, Intrusion detection system must observe variety of patterns to analyse large number of data files. The information should be accessed through features of HTTP only and on the basis of frequency of the access, the users should be allowed inside premises

The researcher followed three ways of Intrusion detection system where first they introduced the concept of data at rest where the system will scan any kind of data from cloud data storage source then and then only encrypt that data and immediately remove the unauthorized and non-trusted data. In the second way of protection data, they have suggested “Data in Motion” where according to them the data of an organization will be hacked by the hackers with the help of instant messaging and using email also. One more technique hackers will be used is the stenography where the hackers or any employee who want to hack company data will save the data in another file that means if any data want to store to the specific location then instead of store that that in designated folder, what hackers will do is that they wil store the data in some other files. This is called as stenography. One more technique hackers can use is that they will create any image or any random image for the specific text where that text will represent by that image and same image will be transferred to outside premises where no one can judge that image is gone outside and can’t find any text behind that image.

In the third way of security concern, the researchers introduced the concept of “Data in Use” where the actual data of any organization will be accessed through hardware devices. They said that all the computes are connected with the USB ports, printers or any other external devices like CD and by this way they can send confidential information through these hardware devices.

In our third literature review study, we gone through third research paper written by Kire Jakimoski who is working as a faculty of Informatics, FON university, Skopje, Republic of Mecedonia with the title of the research “Security Techniques for data protection in cloud computing” and this paper got published in International journal of Grid and Distributed computing with volume 9 and no 1. According to them security is the main concern for all cloud networks and hackers can hack any data available in cloud environment with the help of available user names and password already stored inside cloud premises. Many times It may happen that an employee from any organization get connected with the cloud environment using given credentials given to them and they used to access all the resources with the same credentials and many time it may happen that they forget to get sign off from that connected environment and user name and password remains active for a long time and they are is a very high risk for that company and risk of getting hacked this data is very strong.

3. Comparative analysis

Ref. No	Author name and volume	Year	Discussed security points	Objectives
35	ETH Zurish with vol 8, number 1	2008	This paper discussed adaption issues and technical issues of cloud enviornment	The objective of this paper was to recommend very strong cloud infrastructure to protect the data in cloud environment
36	Badar Alouffi, Muhammad Hada, Muhammad Ayaz	2011	The paper that provide an overview cloud Computing security: Threats and Mitigation Strategies	The main objective of this Paper is to keep the data in the encrypted and decrypted format at both the end of client and server and
37	Kire Jakimoski	2018	This paper provides an overview on available or stored credentials inside cloud premises	The main objective of this paper is to keep cloud environment safe from employees credentials and not to store any use name and password inside cloud environment and always use new credentials while installing any new app

4. Research Gap analysis

The literature review is highlighting major gaps in cloud security research. These 3 studies focus on technical issues and adaptation challenges, but practical implementation strategies for cloud premises are lacking. There's also a huge gap in addressing emerging threats and proposing countermeasures. Stored credentials in cloud premises need better protection, but effective management solutions are underexplored. Research tends to identify issues rather than propose actionable solutions, and there's limited work on implementing security measures in real-world cloud scenarios. Username and password protection in cloud premises isn't clearly defined, and studies often overlook how organizational policies impact cloud security. Addressing these gaps can significantly enhance cloud security, and more research is needed on practical implementation strategies, solution-oriented approaches, and effective credential management.

5. Conclusion

Identifying research gaps in cloud premises can significantly improve overall cloud computing security. By addressing practical adaptation challenges, technical issues, emerging threats, and implementing effective credential protection measures, organizations can ensure robust cloud security. This multifaceted approach will not only safeguard sensitive data but also facilitate secure cloud adoption, benefiting businesses and users alike. As organizations increasingly rely on cloud infrastructure, prioritizing these security aspects will create a secure environment that supports seamless operations, protects critical assets, and fosters trust in cloud services. Ultimately, bridging these gaps will drive innovation, efficiency, and reliability in cloud ecosystems, creating a win-win for all stakeholders involved.

References

1. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.
2. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.
3. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A & Zaharia, M. (2010). A view of cloud computing.

Communications of the ACM, 53(4), 50-58. 💻

4. Gupta, P., & Kumar, A. (2013). Comparative study of cloud computing technologies. International Journal of Advanced Research in Computer Science and Software Engineering, 3(7), 227-232.
5. Srinivasan, S. (2014). Cloud computing: A comparative study. International Journal of Computer Applications, 96(16), 1-6.
6. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616.
7. Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.
8. Ranjan, R., Benatallah, B., Dustdar, S., & Papazoglou, M. P. (2015). Cloud resource orchestration: A data-centric approach. Computer, 48(7), 48-55.
9. Gong, C., Liu, J., Zhang, Q., Chen, H. T., & Gong, Z. (2010). The characteristics of cloud computing. 2010 39th International Conference on Parallel Processing Workshops, 275-279.
10. Kumar, K., & Lu, Y. H. (2010). Cloud computing for mobile users: Can offloading computation save energy? Computer, 43(4), 51-56.
11. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.
12. Sriram, I., & Khajeh-Hosseini, A. (2010). Research agenda in cloud technologies. Proceedings of the 1st ACM Symposium on Cloud Computing, 1-6.
13. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.
14. Jadeja, Y., & Modi, K. (2012). Cloud computing - concepts, architecture and challenges. 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 877-880.
15. Bashir, A., & Parthasarathy, V. (2018). Cloud computing: A comparative study of security issues and challenges. 2018 2nd International Conference on Inventive Systems and Control (ICISC), 1-6.

10.29322/IJSRP.16.02.2026.p17033