STM JOURNALS

Journal of
Multimedia Technology &
Recent Advancements

ISSN: 2349-9028
Volume 10, Issue 2, 2023
DOI (Journal): 10.37591/JoMTRA

http://computers.stmjournals.com/index.php?journal=JoMTRA&page=index

Review JoMTRA

Cloud System Performance and Security Improvements with Multi-Tenancy integration

Meenakshi Saini[1,*], Neha Bathla[2]

Abstract

Cloud computing has emerged as a popular paradigm for delivering scalable and flexible computing resources to businesses and individuals. However, assuring the performance and security of cloud systems continues to be a significant concern. Multiple users or tenants can share the same cloud infrastructure thanks to multi-tenancy, a crucial notion in cloud computing. This dissertation explores the integration of multi-tenancy as a means to enhance the security and performance of cloud systems. The comprehensive review of the existing literature on cloud computing, multi-tenancy, and the associated security and performance challenges. It analyses the benefits and drawbacks of multi-tenancy and identifies the key research gaps that need to be addressed. To address the security concerns, the dissertation investigates various security mechanisms and techniques that can be employed within a multi-tenant cloud environment. It explores access control models, encryption techniques, and secure data isolation methods to ensure the privacy and integrity of tenant data. The dissertation also explores auditing and monitoring mechanisms to detect and mitigate potential security breaches.

Keywords: Cloud computing, multi-tenancy, Metlab, Interface Complexity, security

INTRODUCTION

The phrase "cloud computing" describes the method of gaining access to data and programmes stored on remote servers in various data centres over the Internet. Instead of storing data and applications locally on each user's computer or mobile device, cloud computing stores everything on a centralized server. As with many other modern applications, Facebook can be accessed and updated from any web-enabled device [9]. Cloud computing is rapidly becoming more widespread in the technical sector in today's age of plentiful digital resources. Academic experts, corporate tycoons, government officials, and IT companies have all voiced concerns about the security of cloud computing and the issues it creates in terms of entrance barriers. Protection of private data, accessibility of services, assessment of vendors, and recommendations from satisfied customers all fall under this heading. These challenges have arisen as a result of preexisting issues and newly expressed needs for cloud computing capabilities like as scalability, resource sharing, and virtualization. It's crucial to consider both the type of deployment and the service delivery mechanism when attempting to classify deployments [10]. Transferring data to and from the cloud still leaves digital assets vulnerable to theft. It was emphasized, nevertheless, that more must be done to protect people's privacy and security online.

***Author for Correspondence**
Meenakshi Saini
E-mail: meenakshi.saini1242@gmail.com

[1]Student, Department of Computer Science & Engineering, Yamuna Institute of Engineering & Technology (YIET), Gadholi, Yamuna Nagar, Haryana, India
[2]Assistant Professor, Department of Computer Science & Engineering, Yamuna Institute of Engineering & Technology (YIET), Gadholi, Yamuna Nagar, Haryana, India

Received Date: August 02, 2023
Accepted Date: August 17, 2023
Published Date: September 05, 2023

Citation: Meenakshi Saini, Neha Bathla. Cloud System Performance and Security Improvements with Multi-Tenancy integration. Journal of Multimedia Technology & Recent Advancements. 2023; 10(2): 10–16p.

Research efforts are being concentrated on finding ways to strengthen the safety and efficiency of cloud-based, distant education platforms. Several research studies have looked into how cloud computing might be used in virtual classrooms. Researchers have already established that both the performance and security of the data are inadequate. Information sent over the internet needs to be transferred quickly and safely. Before being delivered across a network, digital content assets should be encrypted and compressed. Researchers implemented a content substitution technique to lessen the size of the transmitted packets [13–15].

CLOUD COMPUTING

To describe a model of service delivery in which consumers obtain on-demand, networked access to configurable computer resources that may be swiftly installed and released with minimal administration effort or contact from the service provider, the phrase "cloud computing" is commonly used. Despite its numerous advantages, cloud computing also poses new difficulties for data centers and business application designers and administrators. In light of the possibility that this novel deployment model possesses characteristics very distinct from those of conventional designs, the efficacy and effectiveness of conventional defensive systems are being reevaluated. A different approach to cloud security adopts the security models used in shared multi-user mainframes and applies them to the cloud. Both public and private cloud services might benefit from having their administration handled by a third party [16–20]. Therefore, cloud service providers have a substantial financial interest in developing and maintaining a safe system for managing their services. Access to sensitive data, data isolation, privacy, bug exploitation, recovery, responsibility, hostile insiders, management console security, account control, and multi-tenancy are just some of the security challenges that have been brought to light. Using several cloud providers, standardizing APIs, and enhancing support for virtual machines are all strategies for safeguarding the cloud in addition to encryption and PKI. This system intends to advance the TDT4 (Topic Detection and Tracking (TDT-2004)) mechanism and the privilege mechanism by combining research from the crypto and IR areas. The goal is to deliver a system architecture that guarantees safety and efficiency [21–25].

ARCHITECTURE OF CLOUD COMPUTING:

Cloud computing architecture [11] consists of the front end and the back end. The front end is the part of the system with which the user has direct contact, while the back end handles all of the processing that occurs on the cloud. While there are many alternative implementations of cloud computing, the most basic or conceptual architecture has just three entities: the end user, the intermediary layer, and the cloud itself. The end user layer contains all the sensors, Smart devices, actuators, etc. that constantly generate data by monitoring their environment. There is a layer of devices in the middle that acts as a bridge between the end consumers and the cloud. The cloud computing infrastructure provides access to digital workstations, data storage, and processing services via the Internet. Figure 1 depicts the overall architecture of cloud computing. With the explosion in the number of Internet of Things devices over the past decade, centralized computing models like parallelism, grids, and clouds have had to give way to the more distributed Fog-assisted cloud computing [12]. Concerns about latency, bandwidth, and security have arisen because of the enormous amount of data being produced by these IoT devices.

LITERATURE REVIEW

Multi-tenant FPGA in the cloud was examined by M. K. Ahmed et al. (2022). FPGAs have advantages in speed, flexibility, and acceleration over more static processing systems like central processing units and graphics processing units because they enable for changes to be made during execution. FPGAs are superior to other computing technologies in optimizing and speeding up massively parallel search operations and signal processing in terms of power consumption, latency, and processing speed. Many of the largest public cloud providers, like as Amazon, have started introducing cloud acceleration services based on field-programmable gate arrays. In cloud applications, FPGAs allow for specialized acceleration with minimal power consumption, however this comes with unexplored security risks. The cloud platform becomes more susceptible to malicious attacks if users are allowed to change the hardware configuration after it has been deployed. Due to safety concerns, public cloud providers have yet to offer multi-tenant FPGA services. This essay looks ahead to future challenges that will need to be handled [1] and explores the dangers associated with using multi-tenant cloud FPGAs.

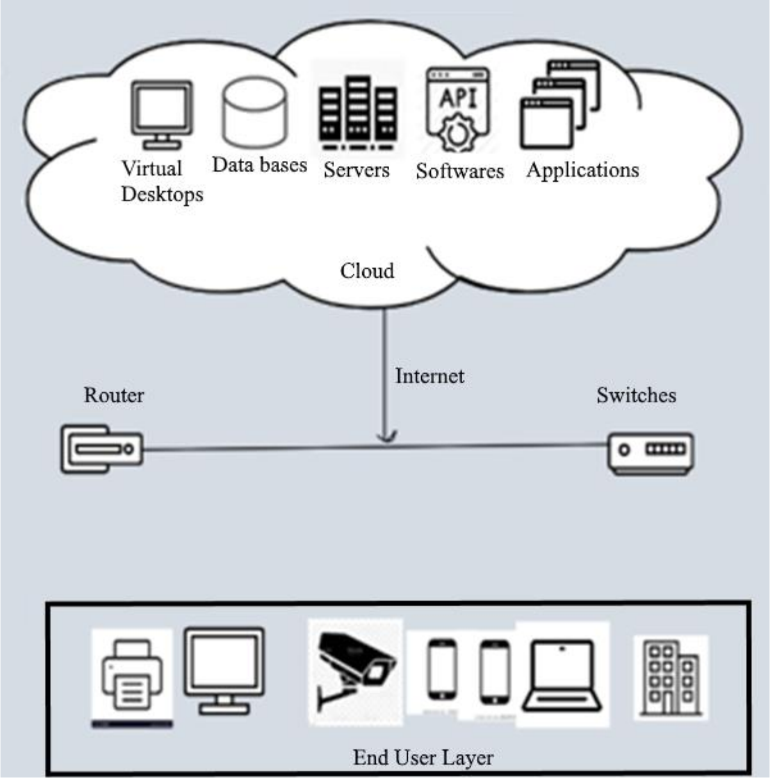

Figure 1. Cloud Computing Architecture.

Engineering software in the cloud, cloud-based network security, and cloud performance measurement were all introduced by R. O. Akor et al. (2020). Modern software engineers are able to more effectively combine the evolution of computer information technology with Internet technology and computer technology to create ground-breaking programmes because of the increased computing power, analysis capabilities of software engineering, and storage capacities made possible by cloud computing. Data gendering security needs constant attention. By drawing parallels between the native engineering that exists outside the realm of internet access and ideas like network speed analysis, uptime, and downtime [2], this article provides a systematic introduction to the concept of cloud-based software engineering as well as its safety and general performance assessment.

Problems, existing solutions, and future challenges in establishing a secure cloud environment were discussed by Y. Alghofaili et al. (2021). Several layers of cloud infrastructure's security are examined in depth in this article. It investigates the top infrastructure issues that could affect the cloud computing business model. It also discusses how various approaches to security issues are currently being addressed in the literature. An overview of the outstanding issues is provided to facilitate their resolution. In-depth analysis of the issues at hand revealed that cloud features like adaptability, elasticity, and multi-tenancy pose new challenges at each tier of the infrastructure. Since multi-tenancy can lead to concerns with availability, misuse, data loss, and privacy violation, it has been shown to have the greatest influence across all layers of infrastructure. Finally, this survey provided recommendations for subsequent research [3].

In 2019, A. S. A. Yancheshmeh et al. analyzed cloud multi-tenancy security. Cloud computing has evolved as the next phase of network computing in a world where everything may be transferred quickly via the Internet. Since cloud computing provides "pay-as-you-go" access to applications, processing, network, and storage resources as on-demand services, it has enabled even the smallest of enterprises to build web and mobile apps for millions of users. Tenants may receive these services via Infrastructure as a Service, Platform as a Service, or Software as a Service. In an effort to keep costs down for their clientele, cloud service providers have begun to experiment with a model called "multi-tenancy" [4].

Resource sharing can be optimised with multi-tenancy and load balancing in the cloud, as demonstrated by the research of S. Q. A.-K. Al-Maliki et al. (2022). Cloud computing has attracted a lot of attention from academics and corporate executives in recent years. Given the cloud's potential to facilitate data sharing and promote cost efficiency, it is likely to maintain a prominent position in the foreseeable future. This article provides a concise overview of how cloud computing might benefit academic and digital libraries through the use of multi-tenant and load-balancing technologies to facilitate the sharing of digital resources. They propose a new paradigm for the sharing of digital resources by augmenting the current user service model with private cloud storage for additional sectors like the medical and financial fields. This research discussed cloud computing and its applications, as well as digital data optimization for service delivery via the internet. This study's findings could be used to pinpoint and create high-quality, multi-tenant cloud service load-balancing solutions [5].

The concept of cloud computing security was first developed by B. Alouffi et al. (2021). Researchers conducted a comprehensive literature study and determined that these 80 papers were the best available options for resolving the issues raised. Based on the findings of this SLR, seven critical security threats to cloud services have been identified. The evaluated literature revealed a preponderance of discussions about data manipulation and leaks. It was understood that there were security concerns with both data storage and data infiltration in the cloud computing environment. Data outsourcing by end users is still an issue for cloud service providers and their clients, as was found in this SLR. We observed that blockchain technology has the potential to be employed as a complementary tool in the fight against safety issues. The SLR concludes with suggestions for follow-up work that could improve data privacy, integrity, and accessibility [6].

In their 2020 study, L. Campanile et al. focused on the effectiveness of security monitoring in shared cloud-based applications. In this paper, the authors present a modelling approach that is well-suited to assisting professionals in planning and evaluating relevant parameters when dealing with new designs or migration projects, particularly with regards to the delays that may affect security monitoring systems in cloud based architecture. The technique depends on modularity and multi formalism methodologies to handle complexity and guide designers through an incremental process, aid in the transfer of technical knowledge into modelling practice, and facilitate the use of simulation. They provide a practical example motivated by a mandated new law for the Italian public sector concerning data centres [7].

The suggested ECC work by S. U. Chandrika et al. (2022) [8] protects the privacy of messages sent over MTC. Our research found a considerable reduction in the time needed to complete all of these studies when compared to established methodologies. The revised ECC was so effective because it required less memory, was faster, had smaller key sizes, generated keys quickly, and saved a lot of resources. The encryption time for the proposed MECC system with a key length of 4096 bits was just 51 ms, which is a significant improvement over the current method (92 ms). Likewise, The proposed methodology requires 159 ms to decrypt a 4096-bit key. When compared to state-of-the-art algorithms like AES, Blow Fish, and Two Fish, the proposed method uses 836 less kilobytes of storage space for the cypher text key. Furthermore, the time needed to generate a key (35 s) appears to be significantly smaller than that of existing methods. Key generation time, encryption/decryption time, and computational complexity are all areas in which the proposed method shows clear advantages over state-of-the-art alternatives.

PROBLEM STATEMENT

Multi-tenancy issues have become increasingly common as the cloud computing market has expanded. In addition, a number of major firms have moved to cloud infrastructure. Cloud computing allows users to access a wide variety of internet services. It makes no difference where you put your data storage device. Information or data may be obtained from the internet. Position is unrelated to where one resides. Cloud service consumers and renters benefit from a number of features, including flexibility and scalability. If a tenant's needs change, they can adjust their resource allotment up or down. Cloud infrastructure maintenance is not the responsibility of tenants or users [26–30]. This is a challenging and potentially deadly issue in multi-tenant cloud computing. There is always a chance that information could be lost, stolen, or hacked. Inadvertently granting access to the database by the administrator leaves the door open for an unauthorized user to get entry. Even while software and cloud computing companies say consumer data is secure than ever on their servers, there are still security weaknesses. SaaS apps may have varying response times due to their distributed nature. In compared to their server-based equivalents, SaaS applications are famously slow and sluggish. This slowness lowers the overall efficiency of the systems. In the increasingly competitive cloud computing market, poor performance is a serious problem for cloud service providers. It's critical that multi-tenancy cloud service providers increase their productivity.

PROPOSED WORK

To achieve these objectives, research is considering the proposed research methodology that involves a systematic review of existing literature, an analysis of the challenges, proposed model along with the evolution of comparison. Present research work has considered research related to cloud computing and security challenges and focus has been made on the factors that is influencing security as shown in Figure 2. In this way proposed work would be capable to enhance security mechanism by integrating Multi-tenancy in cloud. Finally comparison of the performance and security of conventional and proposed work would be made [31–34].

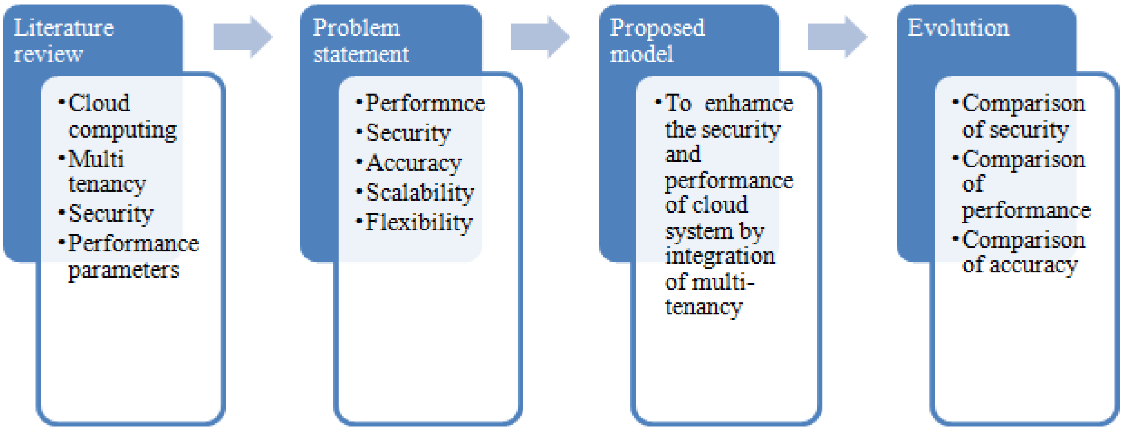

Figure 2. Proposed Research Methodology.

CONCLUSION AND FUTURE SCOPE

Conclusion

Although sophisticated algorithms like DES, AES, and RSA are utilized by conventional data security methods to offer security, these methods are notoriously sluggish to perform. While polynomial encryption is fast and provides some security, Deep Learning's training of the data set necessitated the existence of preceding records in order to effectively teach the computer. Adding deep learning to polynomial encryption is a necessary step towards achieving optimal security. Cloud data storage services that use cutting-edge hybrid, automated security architecture will soon be available to these enterprises.

Future Scope

Multi tenancy describes the practice of allowing multiple tenants to share the same cloud computing service. In the cloud, users are unaware of and unable to communicate with one another, and their data is segregated from that of all other users. With multi-tenancy, cloud data platforms may serve an endless number of customers with the same set of resources without the need for custom application development or the exposure of sensitive data. Multi-tenancy is widely used because it is the foundation of most local data centers, SaaS, and other cloud services. The advantages of multi-tenancy include increased processing capacity at lower cost, improved resource utilization, and reduced maintenance expenses when compared to single-tenancy.

REFERENCES

1. Ahmed MK, Mandebi J, Saha SK, Bobda C. Multi-Tenant Cloud FPGA: A Survey on Security. arXiv preprint arXiv:2209.11158. 2022 Sep 22.
2. R. O. Akor, “Cloud-Based Software Performance Evaluation Engineering, Network Security, and, Performance Evaluation” vol. 4480, no. 5, pp. 64–68, 2020, doi: 10.36349/easjecs.2020.v03i05.002.
3. Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, “Secure cloud infrastructure: A survey on issues, current solutions, and open challenges,” Appl. Sci., vol. 11, no. 19, 2021, doi: 10.3390/app11199005.
4. Ali shokrollahi yancheshmeh, “Multi-Tenancy Security in Cloud Computing,” Degree Proj. Inf. Commun. Technol., pp. 1–73, 2019.
5. S. Q. A.-K. Al-Maliki, “Efficient Cloud-based Resource Sharing Through Multi-tenancy and Load Balancing: An Exploration of Higher Education and Digital Libraries,” pp. 1–16, 2022.
6. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies,” IEEE Access, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.
7. L. Campanile, M. Iacono, S. Marrone, and M. Mastroianni, “On Performance Evaluation of Security Monitoring in Multitenant Cloud Applications,” Electron. Notes Theor. Comput. Sci., vol. 353, pp. 107–127, 2020, doi: 10.1016/j.entcs.2020.09.020.
8. S. U. Chandrika and T. P. Perumal, “Modified ECC for Secure Data Transfer in Multi-Tenant Cloud Computing,” Int. J. Comput. Netw. Inf. Secur., vol. 14, no. 6, pp. 76–88, 2022, doi: 10.5815/ijcnis.2022.06.06.
9. V. Chang, M. Ramachandran, Y. Yao, Y. H. Kuo, and C. S. Li, “A resiliency framework for an enterprise cloud,” Int. J. Inf. Manage., vol. 36, no. 1, pp. 155–166, 2016, doi: 10.1016/j.ijinfomgt.2015.09.008.
10. Y. Cheng, “Design and Implementation of Cloud Computing Network Security Virtual Computing and Defense Technology,” Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/7876199.
11. J. K. Dawson, T. Frimpong, J. B. H. Acquah, and Y. M. Missah, “Reconnoitering Security Algorithms Performance in the Cloud: Systematic Literature Review Based on the Prisma Archetype,” J. Theor. Appl. Inf. Technol., vol. 101, no. 6, pp. 2203–2227, 2023.
12. V. C. Hu, M. Iorga, W. Bao, A. Li, Q. Li, and A. Gouglidis, “General Access Control Guidance for Cloud Systems,” NIST Spec. Publ., 2020, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf
13. M. Kasthuri, “Blockchain based Data Security as a Service in Cloud Platform Security,” Int. J. Cloud Comput. Serv. Archit., vol. 11, no. 6, pp. 1–8, 2021, doi: 10.5121/ijccsa.2021.11601.
14. X. Li, D. Pan, Y. Wang, and R. Ruiz, “Scheduling multi-tenant cloud workflow tasks with resource reliability,” Sci. China Inf. Sci., vol. 65, no. 9, pp. 1–18, 2022, doi: 10.1007/s11432-020-3295-2.
15. S. Mangesh Latekar and R. Ravindran, “Resolving Multi Tenancy Issues Using Cloud Automation,” Int. J. Sci. Res. Eng. Trends, vol. 6, no. 3, pp. 2395–566, 2020.
16. P. M. Mutulu and A. M. Kahonge, “A Multi-Tenancy Cloud Trust Model using Quality of Service Monitoring: A Case of Infrastructure as a Service (IaaS),” Int. J. Comput. Appl., vol. 174, no. 27, pp. 41–46, 2021, doi: 10.5120/ijca2021921175.
17. V. Narasayya and S. Chaudhuri, “Cloud Data Services: Workloads, Architectures and Multi-Tenancy,” Cloud Data Serv. Workload. Archit. Multi-Tenancy, 2021, doi: 10.1561/9781680837759.

18. X. Ou, “Research on data access security agent technology in cloud computing security,” J. Phys. Conf. Ser., vol. 1693, no. 1, 2020, doi: 10.1088/1742-6596/1693/1/012013.
19. M. S. Sabri and R. Kapoor, “Challenges in Cloud Security a Review,” Rev. Artic. SSRN Electron. J., vol. 9, no. 1, pp. 4143–4148, 2021, [Online]. Available: www.ijcrt.org
20. R. J. Victor and M. Singh, “Security analysis in multi-tenant cloud computing healthcare system,” Int. J. Mech. Eng. Technol., vol. 9, no. 3, pp. 71–78, 2018.
21. M.Saraswathi, T.Bhuvaneswari, Multitenancy in Cloud-based Software, as a Service Application, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. l3,issue11, page 1-4,2013
22. JKRSastry, M TrinathBasu, Securing Multi-tenancy systems through multi DB instances and multiple databases on different physical servers, International Journal of Electrical and Computer Engineering (IJECE), Volume 9, Issue 2, Pages 1385-1392, 2019. https://doi.org/10.11591/ijece.v9i2.pp1385-1392
23. JKRSastry, M TrinathBasu, Multi-Factor Authentication through Integration with IMS System, International Journal of Emerging Trends in Engineering Research, Volume 8, No. 1, Page, 88-113, 2020
24. M.Trinath Basu, Dr.JKRSastry, A full security included Cloud Computing Architecture, International Journal of Engineering & Technology, Volume 7, Issue 2.7, Page 807-812, 2018.
25. Satveer Kaur and Amanpreet Singh “The concept ou Cloud Computing and Issues regarding its Privacy and Security” International Journal ou Engineering Research & Technology (IJERT), Vol 1 Issue 3, May 2019.
26. Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues uor Cloud Computing. International Journal ou Inuormation Security and Privacy, 4(2), 39-51. doi: 10.4018/ jisp.2010040103
27. Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conuerence on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ ICCSEE.2018.193
28. Farzad Sabahi “Cloud Computing Security threats and Responses”, 2011 IEEE 3rd International Conuerence on Communication Soutware and Network (ICCSN), pp. 245-249, May 2019.
29. Sekhar R V, Nandini N, Bhanumathy D and Hemalatha M, “Identity based authentication for data stored in cloud” published in International Journal of Advanced Research in Computer Science and Software Engineering, vol.5, 2015, 243-247.
30. King N J and Raja V T, “Protecting the privacy and security of sensitive customer data in the cloud Computer law and Security Review,” vol.28, 2012, 308-319.
31. Khoshkholghi M A, Abdullah A, Latip R, Subramaniam S and Othman M, “Disaster Recovery in Cloud Computing: A Survey Computer and Information Science,” vol.7, 2014, 39-54.
32. D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, “Retaining data control to the client in infrastructure clouds,” Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE. pp. pp. 9–16, 2009.
33. Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks (ICCSN), May 2011.p.245-249.
34. McAfee, 6 Cloud security issues that businesses experience, [Online]. Available: https://www.mcafee.com/blogs/enterprise/cloud-security/6-cloud-security-issues-that-businesses-experience/. Last Visit Nov 17, 2020.
35. A. Singh and K. Chatterjee. (2017). “Cloud security issues and challenges: A survey,” Journal of Network and Computer Applications, vol. 79, no. 5, pp. 88–115.