NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 7, July. -2021

REVIEW ON DISTRIBUTED DATABASE SYSTEMS

Mateo Santiago
University of Valladolid- Spain
Rafael Campbell- Polytechnic Institute of Guarda
(Instituto Politécnico da Guarda) , Portugal

INTRODUCTION

Distributed database system refers to a pool of databases incorporated and integrated physically across various sites in a computer network. The topic of the research paper will be anchored on A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security. On top of this, the study will establish how social media, the Internet of Things (IoT), and self-driving automobiles integrate distributed database systems in their models.

The chosen research topic would provide a unique opportunity to explore and analyze the study's most critical issues. In addition, the topic will provide room whereby areas in distributed database systems will be identified for future research. It would be crucial that I spend time reading about the identified topic for this study. Consequently, I would develop accurate, credible, and well-researched findings that would widen my scope and understanding. In addition, my research on distributed database systems would be used in future studies as a reference.

Selected paper anchored on the topic of A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security

The importance of access control models in enhancing data security and safety cannot be understated. It was evident that companies, government institutions, businesses, and organizations worldwide utilize the access control models from the topic. Consequently, these models aid in examining who the employees are, the digital resources they have access to, and performance processes. In addition, the topic explains the challenge and difficulty of access control models to be implemented successfully in distributed data systems. It is vital to note that the selected topic sought to automatically establish permissions, authenticity and access levels of users utilizing computer and network devices installed with distributed database systems.

In addition, the topic was anchored on determining the type of devices users would utilize and preventing access to data that is not needed. The topic added that the access control models were used in real-life scenarios, such as education and health. Consequently, this model has enhanced scalability and the accuracy levels of the distributed database systems. The topic takes note of the ever-increasing risks of malicious viruses, and unwarranted intruders pose to information systems and other digital infrastructure, for example, computer and network systems.

However, there have been crucial efforts to mitigate such threats, as explained by the topic in the paper. It is vital to note that whereas some systems violations due to breach occur deliberately, thus making the systems inaccessible, others often happen due to accidental or hardware challenges. From this perspective, the topic further adds that either by malice or accidental, security breaches and violations impact negatively on the operations and reliability of an organization, business or company.

Backdoor access control, intentional and accidental breaches are the leading causes of unauthenticated surfing behaviors' and malicious attacks. When an individual intentionally interchanges computer and systems network data, they infringe the integrity principle of enhancing data security. In addition, this would raise the need for adequate access control models proposed in the topic. It is vital to note that good access models are often designed concerning the organization's confidential access rights and scalability. Moreover, the topic further highlights the technique of establishing access levels and permission of users anchored on the distributed database systems. Consequently, this would aid in minimizing and preventing access to crucial data not needed in real-time.

In addition, the topic of the study extended by examining how access control models play a vital role in enhancing measures that would mitigate unwarranted access. Further, access control models used in distributed data systems are today unable to meet the demands of the ever-increasing number of systems. Consequently, this has increased the complexity of effectively enhancing data security in organizations that

utilize distributed data systems. On the other hand, the topic also examines the challenges experienced by a firm or individual that uses distributed database system. Consequently, understanding the challenges and gaps. All would aid in coming up with recommendations for future research founded on DDBS. First, distributed database systems have the potential to be complex. In addition, this would make it hard for a user utilizing a server network or computer device to navigate through the database. The multiple distributions of databases across various locations cause complexity in the system.

Companies and individuals using DDBS often argue that it is an expensive database system due to its complexity, thus making it hard to sustain and maintain. Data integrity is another vital challenge surrounding the use of the distributed database system. The storage of data in different or multiple locations raises the question of how it would have been utilized. Consequently, this crucial data may fall into the hands of unwarranted third parties who might negatively interfere with the data. It would require a highly skilled labour force to manage and sustain such a system.

Companies like Amazon, Facebook, Sound Cloud, eBay, etc., would have to invest most of their financial resources in hiring such a specialized system. The challenge here is that small and emerging companies in the information technology industry would find it hard to incorporate and integrate distributed database systems into the organizational structure. It is vital to note that users of distributed database systems often remotely access such systems. Increased network traffic would lead to a system failure or crash. Companies find it hard to optimize a distributed database system making it a big challenge. It is vital to note that I picked the topic anchored on understanding the new scalable and expandable access control model for distributed database systems. In addition, this is because of the existence of few research work or studies that have been done based on it. Secondly, I was interested in understanding how companies benefit from utilizing such a platform and its challenges. Thirdly, I chose this topic to stimulate more studies on distributed database systems and access control models. From the topic, I learned that distributed database systems could be integrated with a new access control model to enhance data security (Guclu, 2020).

A snapshot of one beneficial insight from the study is how companies in the IT industry and social media use distributed database systems to enable their users to access the latest features in their platforms, thus enhancing functionality and efficiency. One profound challenge I noted from this system is that it is complex and expensive to manage and sustain. The research was meaningful because I identified past research work anchored on distributed database systems. Secondly, I understood how users and companies thrive under the benefits and challenges of using such a system. In terms of improving the topic discussed, more studies need to be done regarding this topic. I foresee a future where there would be intensified use of access control models in distributed database systems.

CONCLUSION

To sum up, more research work must be conducted regarding how access control modes would be sued in distributed database systems to enhance companies' data security.

REFERENCES

1) Guclu, M., Bakir, C., & Hakkoymaz, V. (2020). A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security. Scientific Programming, 2020.
2) Dheeba, J., Singh, N. A., & Selvi, S. T. (2014). Computer-aided detection of breast cancer on mammograms: A swarm intelligence optimized wavelet neural network approach. Journal of biomedical informatics, 49, 45–52.
3) Shen, R., Yan, K., Tian, K., Jiang, C., & Zhou, K. (2019). Breast mass detection from the digitized x-ray mammograms based on the combination of deep active learning and self-paced learning. Future Generation Computer Systems, 101, 668–679.
4) Qi, X., Zhang, L., Chen, Y., Pi, Y., Chen, Y., Lv, Q., & Yi, Z. (2019). Automated diagnosis of breast ultrasonography images using deep neural networks. Medical image analysis, 52, 185–198.
5) Wilkinson, I., & Graves, M. (). Magnetic resonance imaging: In: Adam a, dixon ak, gillard jh, schaeferprokop cm, eds. Grainger & Allison's Diagnostic Radiology: A Textbook of Medical Imaging.
6) Hossam, A., Harb, H. M., & Abd El Kader, H. M. (2018). Automatic image segmentation method for breast cancer analysis using thermography. Journal of Engineering Sciences, 46, 12–32.

7) R Alugubelli, "DATA MINING AND ANALYTICS FRAMEWORK FOR HEALTHCARE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.534-546, February 2018, Available at:http://www.ijcrt.org/papers/IJCRT1134096.pdf.