ASSIGNMENT – 5
DATA WAREHOUSING AND MANAGEMENT

SUBMITTED TO: PROF. SAURABH DEY
SUBMITTED BY: DHRUV DOSHI
MAIL: dh722257@dal.ca

MULTI-TENANT DATABASE ACCESS CONTROL

This research paper proposes a different and more workable model for implementing a multi-user database using a self-created database schema called Elastic Extension Table (EET). They also gave a proposal for an algorithm which allows users to access permitted data more quickly and efficiently. The researcher chose the database sharing mode, in which Tenent ID was the column which was used for the data isolation between tenants. The Elastic Extension Table (EET) consists of several sub-tables, which build the complete structure of the model:

1. Common Tenant Tables: Shared between all the tenant and tenant Info.
2. Virtual Extension Tables: Used to expand the business domain and provide relationships.
3. Extension Tables: used to create the data architecture of the system. These tables have various sub tables which completes the whole structure and have minute details such as storing rows, columns, relationships etc.

The paper includes the previous work related to access control in security domain which was started way back in 1960, came up with various principles for access control like, Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). The paper also provides information regarding Siebel Systems, IBM DB2, and Salceforce.

In paper they have proposed a proxy service which helps us in getting the data out of the tables which is identical to select queries, relationship and joins with many more things. They are so powerful that they automatically retrieves the output in desired format and the tenet would not require to write the queries. This will make the system more easily accessible and robust on our end.

There are several access control lists that determine which data can be accessed by which part of users. Several tables represent a single entity, such as users and tenants, while some also represent multiple or plural entities, such as group tables, role tables, etc. Other miscellaneous information.
Hierarchical access to data, where users decide which group and what role they have, and then verify which columns and rows they can access, so special data blocks are provided according to users. consult.

Various algorithms have been demonstrated using Pseudo code, which demonstrates the work of various functions in obtaining user roles and the columns the user has access to.

The output produced by these algorithms becomes the input of a SELECT query with a WHERE clause.

Finally, a general experiment was carried out and the results showed that accessing the data by querying users with higher roles instead of users with lower roles would cost more and take longer to access the data. Basically it said that the user with higher number of columns in would take more time and computing power to execute and get the desired output. And the another experiment also gave the similar results.

Continuing this I found several research papers and website which could be further referred to advance in this domain,

[1] Q. Zuo, M. Xie, G. Qi, and H. Zhu, "Tenant-based access control model for multi-tenancy and sub-tenancy architecture in Software-as-a-Service," *Frontiers of Computer Science*, vol. 11, no. 3, pp. 465–484, Jun. 2017, doi: 10.1007/s11704-016-5081-x. [Online]. Available: https://link.springer.com/article/10.1007/s11704-016-5081-x. [Accessed: 31-Jul-2021]

[2] "Access Control for Multi-tenant and SaaS applications (ASP.NET, WCF/Silverlight, etc.)," *Visual-guard.com*, 2020. [Online]. Available: https://www.visual-guard.com/EN/net-powerbuilder-application-security-authentication-permission-access-control-rbac/secure-saas-and-multi-tenant-apps-with-asp-net-or-wcf-Silverlight.html. [Accessed: 31-Jul-2021]

[3] H. Yaish and M. Goyal, "Multi-tenant Database Access Control," *2013 IEEE 16th International Conference on Computational Science and Engineering*, Dec. 2013, doi: 10.1109/cse.2013.131. [Online]. Available: https://ieeexplore.ieee.org/document/6755311. [Accessed: 31-Jul-2021]