ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 12, Issue, 10, pp.14235-14240, October, 2020

DOI: https://doi.org/10.24941/ijcr.39941.10.2020

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

APPLYING AUTOMATED ROW LEVEL SECURITY METHOD FOR DATA AND ANALYTIC SOLUTIONS

***Farhana Sethi**

United States of America

ARTICLE INFO

Article History:
Received 19th July, 2020
Received in revised form
27th August, 2020
Accepted 14th September, 2020
Published online 30th October, 2020

Key Words:
Database Management, Security, integrity, and protection, Database design, modeling and Management, Access methods.

ABSTRACT

Row-level security (RLS) with data and analytics application, when provide as a turnkey service, can be used to restrict data access for specified users using Filters restriction on the data access using Attribute-based access control. Row level security is the feature accessible to filter content based on a user's precise requirement, thus decreasing the database exposure to unapproved disclosure of individual or business confidential data. Row-Level security defines the security rule to limit access to objects based on specific rights.RLS or Row-Level Security as the name advocates is a security mechanism that restricts the records from data based on the authorization framework of the current user that is logged in. In other words, the records from the database tables are displayed based on who the user is and to which records do the user has access to. The paper examines the use of Row-level security (RLS) and customization of the solution for large organizations. The paper focused on Attribute-based access control (ABAC), design and implement a standard method that can be used on large scale at the organization level.

Citation: ***Farhana Sethi,*** **2020.** "Applying automated Row Level Security method for Data and Analytic Solutions", *International Journal of Current Research*, 12, (10), 14235-14240.

INTRODUCTION

RLS or Row-Level Security as the name advocates is a security mechanism that restricts the records from data based on the authorization framework of the current user that is logged in. In other words, the records from the database tables are displayed based on who the user is and to which records do the user has access to. This is usually required to privilege specific users to have access to their data only without authorization to view other user's data. Organizations own data to the employees of that organization can assist as an interference to their main job and duties. A typical example is payroll- Payroll information is classified as Confidential Personal information. No one in the organization should be able to see the Payroll information for other employees with exception of payroll and HR administrators. As per The General Data Protection Regulation (GDPR), an organization must limit the purpose, data visibility and consider Privacy by Design for the data classified as Personal (Personal data means any information relating to a recognized or distinguishable single). Another example is sales data for an organization.

Corresponding author:* **Farhana Sethi,
United States of America.

It is beneficial for everyone to know how the company overall is performing so that objectives can be accustomed as needed. Conversely, accessing sales performance data particular to a specific salesman or area classified as Confidential and disclose compensation figures for individuals, which is just as profound as payroll data. Customized Row-level security model gives individuals in the organization the information required to make cognizant decisions, but it restricts access to information the organization ruminates sensitive. For instance, supervisors required date of birth from employee private information on their direct employees, but those direct employees do not want that figures for their colleagues. Superiors do not need required the details of employee personal detail for other subdivisions at their same level within the business, but they might need aggregated level data across the organization useful as a means to recruit and preserve experienced workers. The paper examines the use of Row-level security (RLS) and customization of the solution for large organizations. Through a real business case study in the oil and gas industry, an assessment of the method is provided for the data and analytics application

Explanation of Concept: To explain the model of row level security, we will refer to the example of pay roll data. Complete dataset for compensation on the personnel of a

business is kept in the same table(s) within the data warehouse. Otherwise would significantly complicate the execution of producing the paychecks on continuous intervals. Usually, in a normalized catalogue, some column within this table can be utilized to identify employee's connotation, for example their Organization unit, region (Geomarket) and product line. From the payroll example, an employee ID number usually recognizes the insightful benefit data. A map to a distinct employee information table (called master data with the information of Geomarket and Product line), which contains non-compensation related information such as organization unit, would include the department detail. Essentially when the payroll data join with Organization master data, a decision can be made on the row level security within roles. Filters restriction can be applied and data visualization can be limited within data and analytic application.

As you can see in Figure 1, the first set of visualization depicts the entire dataset. A master or global user may be able to view all the records. However, when a specific user logs in, the Row-Level Security in data table blocks the view of data based on the employee ID. For example, when the user "Jon" logs in he can see only 1 record that belong to him. Similarly, when "Kev" logs in, he can only view data that is relevant to him. However when "An", the Manager of the team log-in, can visualize data for both (John and Kev).

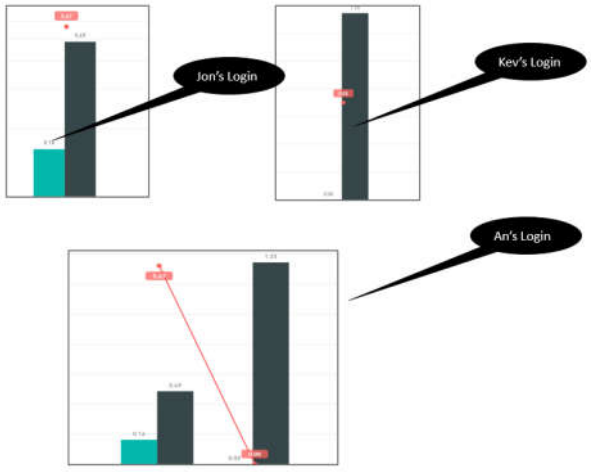

Figure 1. Row-Level Security example from Power BI report visualization

Approach: Data security can be generally achieved using one of the following approaches.

Network segmentation: Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of traffic between subnets based on granular policies. However, in this paper network segmentation is out of scope.
Commercial Software

Software and Database: In our study we are focusing on achieving the desired result by using Software and database approach.

Background and concept: Access control is a security measure which is put in place to regulate the individuals that can view, use, or have access to a restricted environment. Various access control examples can be found in the security systems in our doors, key locks, fences, biometric systems, motion detectors, badge system, and so forth. The purpose of an access control system is to provide quick, convenient access to those persons who are authorized, while at the same time, restricting access to unauthorized people. In application security, there are three types of access control:

Access control lists (ACL): Access control lists are permission-based systems that assign people in an organization different levels of access to files and information.

Role-based access control (RBAC): Role-based access control (RBAC) is a policy-neutral access-control mechanism defined around roles and privileges. In other words, it is not who you are but rather what role(s) you represent. For example, anindividual might be allowed to open a door. That right (or permission) is approved because that person has the role employee, not because of who they are.

Attribute-based access control (ABAC): Attribute based access control (ABAC) is a different approach to access control in which access rights are granted through the use of policies made up of attributes working together. ABAC uses attributes as the building blocks to define feature-rich access control rules and access requests. With ABAC, you can mix and match attributes to define extremely targeted (fine-grained) rules e.g. employees can open the door between 9AM and 10AM or close the door after 5PM if and only if the employee belongs to the 'door opener' group. In our research, we are using organization level widely used attributes to identify user role, e.g. their assigned location, HR Organization unit, department and/or product line. The primary difference between RBAC and ABAC is RBAC provides access to resources or information based on user roles, while ABAC provides access rights based on user, environment, or resource attributes. In this research have focused on Attribute-based access control (ABAC), design and implement a standard method that can be used on large scale at the organization level.

Related work

Many research have focused on finding the right design, implementation, and evaluation of an automated access control policy specification tool. There is an extensive list of challenges related to Attribute-based access control (ABAC) systems. The majority of these difficulties arise from the increased complexity attribute and policy-based access control introduces for the sake of increasing the flexibility and generality of access control policies. In the research paper, Servos et al outlines the most common problems identified and discussed in the recent literature is the lack of an agreed upon reference and/or foundational model of Attribute-based access control (ABAC).They also described the lack of hierarchical and inheritance in Attribute-based access control (ABAC) that presents in Role-based access control (RBAC).The role hierarchy allows for roles to be related in a way that more closely resembles that of actual organizations. Another challenge is the scalability. An Attribute-based access control (ABAC) system requires complex interactions between access control components that

may be distributed among different resources. Another important aspect of access control for both legal and security reasons is to provide audit reports and the ability to easily determine the set of users who have access to a given resource or the set of resources a given user may have access to .

METHODOLOGY

In this paper, we are combining Fine-grained authorization approach with Microsoft Power BI service, a data and analytics application to apply the deployment of Row level security using Attribute-based access control (ABAC). "Fine-grained authorization enables object level security" [1].We have designed a custom and innovative fine-grained access control model based on authorization views that allows authorization translucent querying. However, Power BI Service is a cloud-based service hosted by Microsoft is a place where Power BI desktop files get publish to. As described in Figure 2. The 4 major building blocks of Power BI are dashboards, reports, workbooks, and dataset. All major component are structured into a workspace. Reports: Basic visualization from Power BI Desktop, it may contain multiple tabs or multiple charts in one tab.

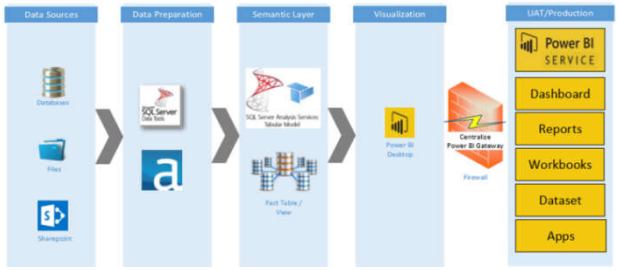

Figure 2. Power BI service high level architecture

Dashboard: A place where you can pin (associate) multiple reports into one single dashboard.

Workbooks: A special type of dataset where it store spreadsheet workbook on Power BI service.

Datasets: A repository of all the data sources used to build the Power BI report. Power BI will generate all the data source in the report in the "Datasets" tab when you publish it to the Power BI service. For Row level security Dataset component will be used to develop the method.

There are four main security types identified in the study of various security mechanisms of data and analytics application. 1) Row Level, 2) Row Level - Workbook Level, 3) Workbook Level and 4) Organization internal Public. As described in Table 1, we are emphasizing Security type 1 and 2 in this studies.

A technique and mechanism are provided for accessing data using Fine-grained authorization in this research. According to one characteristic, a session between a Power BI user client and a database server is started. Values are kept for a set of context attributes associated with the session. The values will be stored in server-side memory that is allocated precisely for that particular Power BI session. The database system includes an attribute set mechanism that selectively limits access to the set of context attributes based on a rule.

Table 1 Key security types categorization and its usage in various security considerations

Security Type	Workbook Permission	Row Level Security	Access Method	Explanation
1) Row Level	No	Yes	RLS	This is when there are access restrictions by Geographical or Product Line in the data, but no specific permission setup for the workbook. When a user goes into the dashboard, they can only see their Geographical or Product Line. People without access can still open the workbook but see a blank dashboard.
2) Row Level - Workbook Level	Yes	Yes	RLS	This is when there are access restrictions by Geographical or Product Line in the data, AND specific permission setup for the workbook. When a user goes into the dashboard, they can only see their Geographical or Product Line. People without access to the workbook will not able to find the workbook.
3) Workbook Level	Yes	No	Group Level	This is when there are specific permission setup for the workbook but no restriction in the data. When a user goes into the dashboard, they can only Global information. People without access to the workbook will not able to find the workbook. RLS is not needed as any access request will be maintained through group subscription.
4) Organization internal Public	No	No	Group Level	This is when all users can see the workbook and Global information in dashboard. RLS is not needed as any access request will be maintained through group subscription.

The rule that state that certain context attributes cannot be set by the client, that certain other context attributes agreed only to certain values by the client, and that certain other context attributes are generously set to any values by the client. For example, the database system detects that a query is issued against a database object via Power BI services. Before executing the query, a policy function associated with the database object is invoked. The policy function creates a modified query by selectively adding zero or more predicates to the query based on a policy associated with the database object. The modified query is then executed.

By means of above approach, User level access not only restricted to the required access level but also in the event of users internal movement from one department to another, their security access will 'seamlessly' transferred and reflected as per their current job role. People who are associated to Oil and gas industry are well versed and familiar with the employee's frequent movement from one job/region or product line to another. The automated RLS technique reduced a significant amount of 'IT Support' ticket and bring the accuracy of data security level to the near of perfection.

Data Preparation: To prepare data for Row level security a dimension master table needs to be created. That contains all the region (Geomarket), product lines and Organization unit. This dimension table should map with the Organization directory database to map all users with their correspondent Organization Unit, Product line and region. In the dimension table that contains the Geomarket and Product Line codes, create a field GMPL Key which will be a concatenation of Geomarket and Product Line codes. This dimension table is a common dataset being used to apply Row level security for various visualization solutions. However, fact table is unique for each visualization solution. Solution has been designed to apply row level security on multiple Power BI reports that share the organization data using common product line and organization unit. As described in Figure -3, it is important to note that this dimension table needs to have a relationship with the fact table with measures that require row-level

security. In case if the data model doesn't have proper Dim and Fact tables, a new field GMPL Key required to be added to any table requiring row-level security.

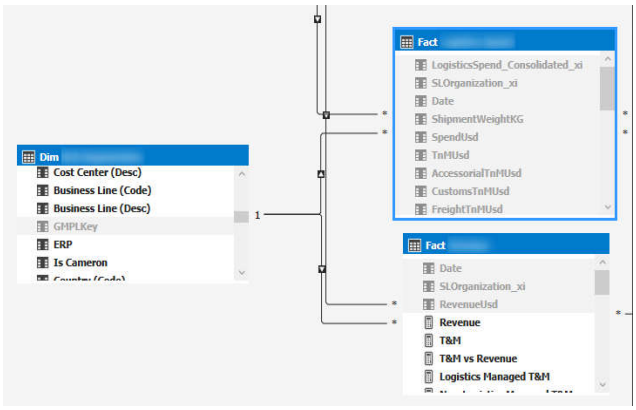

Figure 3. Illustration of Dimension master table with the fact table for RLS

RESULTS

This paper provides a basic introduction to Attribute-based access control(ABAC) and a comprehensive review of recent research efforts toward developing formal models of ABAC using Row level security. The solution focused on to overcome the identified challenges of model foundation, hierarchal visibility, Scalability and auditing.

DISCUSSION

This research has focused on addressing the key challenges Servos et al have described in the previous related work.

Foundational model: The section data preparation described the essence of dimension master table. That information is standard across whole organization and can be used at the backbone for all the needs of Attribute-based access control (ABAC).

Hierarchy: The dimension master table is a transformed table mapped with Organization directory to get the hierarchy of the employees, their Role, Manager and organization unit. This approach overcomes the need of Role-based access control (RBAC) that lacks in out of the box Attribute-based access control (ABAC) system.

Scalability: Since dimension master table is standard and shared across any Fact table provided that it has Geomarket and Product line information. This method can be used for any dataset within organization.

Auditing: Microsoft Power BI Activity Log API for auditing is out of the box service available that we are using to enable audits for the security logging purpose.

Row Level Security procedures: Generally, when access is provided to users to access record definition using a query, they have access to all the records of data in the table built using the associated record definition. For row level access mechanism, we need to control users from seeing some of those data rows.

Row level security is used for tables that hold sensitive data. For row-level security, users can truly have access toa table without having access to all rows on that table. Row level security allows you to store data for many users in a single database and table, while at the same time restricting row-level access based on a user's uniqueness, role, or execution context. Once fact and dimension dataset mapped together as described in Data Preparation section, we bring the output to visualization layer in Power BI. In this case study, we have used two approaches to apply Row Level Security.

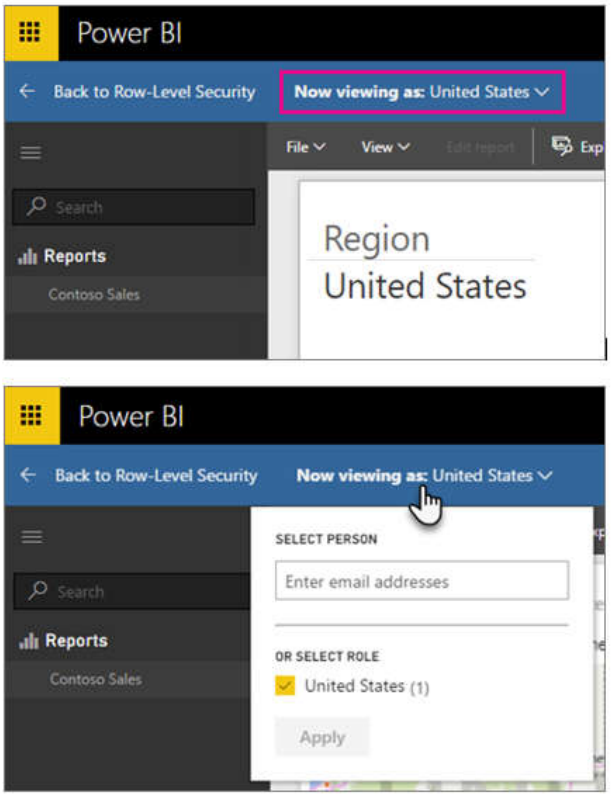

Figure 4. Validation of Row Level security using Power BI.

Row level Security technique for live data connection: Analysis Services is an analytical data engine (Vertipaq) used in decision provision and business analytics. It provides enterprise level semantic data model competencies for business intelligence, data analysis, and reporting applications such as Power BI, Excel, Reporting Services, and other data visualization tools. When Power BI connect to live data with Microsoft Cloud AAS (Azure Analytic service) Manage Roles cannot be implemented due to the limitation in the Power BI tool, the security option will not show up for live connection datasets. Hence, this is required to be implemented in the Analysis Services model by creating new Roles using Microsoft Visual Studio. Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows and web services. To define security roles, Direct Query connection required to be configures and 'Manage Roles' from Data Modeling.

Row level Security technique for Data import: Roles and rules can be defined using Power BI Desktop. When a report distribute to Power BI environment, it also distributes the role definitions. To configure Row Level Security in Power BI Desktop, we have used DAX formulas. DAX stands for Data Analysis Expressions. DAX is a formula language and

is a group of functions, operators, and constants in Microsoft Power BI. Roles can be created using Table filter DAX expression. Users can be assigns to a role from power BI Service. In this study, we enabled dynamic security and practice user principal name () DAX functions. Relationships in Power BI are slightly altered from other database management systems. The direction of a relationship in Power BI means Filtering. Whatever direction of the relationship is, that describes how Power BI filters the data. By default, row-level security filtering uses single-directional filters, we changed and enabled bi-directional filter with row-level security by picking the association. With bidirectional cross-filtering, report designers and data modelers have better mechanism over how they can apply filters when working with related tables. In Microsoft Windows Active Directory, a User Principal Name (UPN) is login name, separator (the @ symbol), and domain name in an email format.

For instance: jon@domain.com After Roles creation, results of the roles can be tested within Power BI Desktop from the Modeling 'View as Roles'. As described in Figure 4, we validated other roles, or grouping of roles, by choosing 'Now viewing' as. We can select to view data as a particular person, or pick a grouping of accessible roles to confirm they are operational.

Citation

- Database fine-grained access control byLei; Chon Hei (San Leandro, CA), McMahon; Douglas James (Redwood City, CA);https://patents.google.com/patent/US6487552B1/en;(10) Patent No.: US 6,487,552 B1;Lei et al. (45) Date of Patent: Nov. 26, 2002
- Servos, Daniel & Osborn, Sylvia. (2017). Current Research and Open Problems in Attribute-Based Access Control. ACM Computing Surveys. 49. 10.1145/3007204.

Compliance with Ethical Standards

Farhana Sethi has no conflict of interest

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Future Scope

"Attribute-based access control (ABAC) is a promising alternative to traditional models of access control (i.e., discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC)) that is drawing attention in both recent academic literature and industry application. However, formalization of a foundational model of ABAC and large scale adoption is still in its infancy. The relatively recent emergence of ABAC still leaves a number of problems unexplored. Issues like delegation, administration, auditability, scalability, hierarchical representations, and the like, have been largely ignored or left to future work"[2]

Conclusion

In this paper, we demonstrate how Row level security can be implemented in data and analytic solutions. It streamlines the strategy and coding of security in the Power BI application. RLS benefits to device boundaries on data row access. The access constraint logic is positioned in the database level rather than in the application level using Attribute-based access control (ABAC). The developed scripts can be implemented in real time or near real time in any large organization.

Abbreviations

- RLS: Row Level Security
- DAX: Data Analysis Expressions
- GDPR: The General Data Protection Regulation
- UPN: User Principal Name
- username(): User Principal Name
- userprincipalname (): User Principal Name
- Direct Query: Direct Query is a direct connection to data source
- ACL: Access control lists
- RBAC: Role-based access control
- ABAC: Attribute-based access control

Declarations

- Ethics approval and consent to participate: Yes
- Consent for publication: Yes
- Availability of data and materials: Cannot provide data and material due to General Data Protection Regulation (GDPR) policy on the data at organization level.
- Competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.
- Funding: Will be provided
- Authors' contributions: Main researcher and implementation lead for the research and Project
- Acknowledgements: The author would like to thank the technical support from the department of IT in the Schlumberger Oil industry to gain the information and data gathering for program development.
- Authors' information: Farhana Sethi Global Data & Analytics Business Intelligence - Quality & Governance Manager with Schlumberger Oilfield, Texas, Houston since 2006. Bachelors in Engineering - Electrical & Computers. Microsoft Certified Architect (Azure Solution Architect. Professional Certification in Reservoir Geomechanics from Stanford University - United States, California. Professional Certification in Internet of Things from Stanford University - United States, California. Professional certification in Data Science: Machine Learning from Harvard University - United States, Massachusetts

REFERENCES

1. Analyzing and Visualizing Data with Power BI- Power BI Training course from EDX: URL : https://www.edx.org/course/analyzing-and-visualizing-data-with-power-bi-2

2. Get started building with Power BI: The Power BI course from Microsoft Virtual Academy: URL: https://docs.microsoft.com/en-us/learn/#!orderby=relevance&prodv=Power%20BI%20for%20Office%20365&lang=1033;
3. Power BI learning guide from Microsoft; URL: https://docs.microsoft.com/en-us/learn/modules/get-started-with-power-bi
4. Video share from Office | Power BI Video channel: URL: https://web.microsoftstream.com/group/3e58477a-6cb5-4498-816b-ab27a040a564
5. Schlumberger Training slide and materials shared by Studio Team: URL: https://slb001.sharepoint.com/sites/office365powerbi24/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2Foffice365powerbi24%2FShared%20Documents%2FIntroduction%20to%20Power%20BI%20Webinar
6. Microsoft Power BI Desktop: Version: Version: 2.79.5768.721 64-bit (March 2020); PBIDesk-topSetup_x64.exe;URL: https://www.microsoft.com/en-us/download/details.aspx?id=58494
7. Microsoft Visual Studio Community 2019: Version 16.5.5; URL: https://visualstudio.microsoft.com/downloads/
8. Microsoft Azure Portal: To build, manage, and monitor all the apps in Microsoft Azure Portal. A single, unified hub built for the teams and projects. :https://portal.azure.com
9. Schlumberger Enterprise data warehouse: glbbirptsqlsvrdev.database.windows.net
10. Schlumberger Azure Analysis Server: asazure://westeurope.asazure.windows.net
11. Schlumberger application: Power BI pathway on De-greed : https://degreed.com/paths?path=getting-started-with-power-bi-enterprise-data-models&id=147477&orgsso=schlumberger
12. Schlumberger application: LDAP: LDAP (LDAP Search): Search company directory (LDAP) from mobile device, one touch call and texting. Organization chart and location information. Business Owner
13. (aka BPM, Product Owner, BPSM): Ahmed Salar; http://ldap.slb.com/
14. Schlumberger application: SL Org: SL Org (SLB Organization); Master Data Management (MDM)The Schlumberger Organization as defined by executive management.URL: https://slb001.sharepoint.com/sites/Dataservices/LegacyMDM/SitePages/Home.aspx
15. Schlumberger Azure Data warehouse: BDT DataPond: To consume data into Tableau/PowerBI for Power BI reporting: Business Owner (aka BPM, Product Owner, BPSM): Rodrigo Patrianova

****