LICENSING OPPORTUNITY: NEXT GENERATION ACCESS CONTROL SYSTEM AND PROCESS FOR CONTROLLING DATABASE ACCESS (REFERRED TO AS NEXT GENERATION ACCESS CONTROL - NDAC)

DESCRIPTION

Problem

Given the sensitivity of much of the data that resides in DBMSs, controlled access in accordance with policy is a fundamental requirement. While policymakers have specified a wide variety of access controls to address real-world security issues, only a small subset of these policies can be enforced in database scenarios. Furthermore, today's approach to access control is by no means standardized, requiring separate configurations of an often-complicated amalgamation of mechanisms, including those that are custom-implemented in applications and specific to DBMS products.

Invention

Provides a universal access control layer between applications and DBMSs, following a standardized ABAC model (NGAC*) that is a) DBMS-agnostic, b) does not require modification of the DBMS software, and c) can enforce types of access policies and at a granularity not typically available in database scenarios with a minimal performance impact. Operationally, users issue untrusted queries, and NDAC only allows authorized queries to be sent to the database.

*Next-Generation Access Control (NGAC) is an ANSI/INCIT standard.

BENEFITS

Commercial Application

- Prevents data breaches: Provides a simplified and standardized means of protecting databases from queries sent from any application.
- Improves data usage: Users issue broad sweeping queries, and NDAC allows access to an optimal set of permissible data per enterprise policies.
- Cost savings: Developers no longer need to implement access control at the software level, which significantly saving time and reducing organizational costs.
- Uniform policy enforcement: Enforces common policy over queries sent to multiple databases.

Competitive Advantage

- Before the fact audit: Can determine DBMS resources (i.e., rows, columns, tables, and fields) that a user is authorized to access in advance of the user issuing a query. It can be used to demonstrate adherence to security and privacy policies.
- One mechanism: In contrast to other middleware approaches, NDAC does not manage and coordinate multiple access control mechanisms to achieve fine-grained access control. That is, it provides cell-level

Contact: licensing@nist.gov

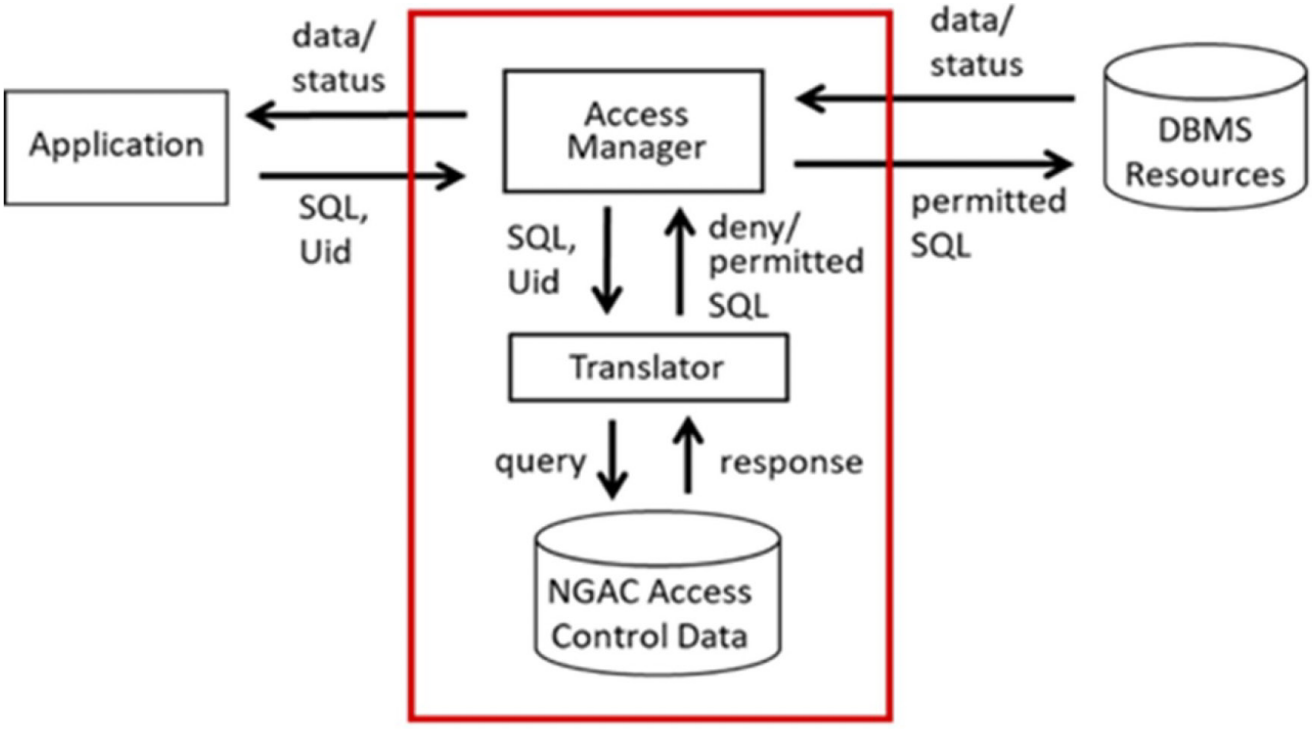
NIST TECHNOLOGY PARTNERSHIPS OFFICE

NIST Technology Partnerships Office
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899-2200

LICENSING OPPORTUNITY: NEXT GENERATION ACCESS CONTROL SYSTEM AND PROCESS FOR CONTROLLING DATABASE ACCESS (REFERRED TO AS NEXT GENERATION ACCESS CONTROL - NDAC)

protection without having to resort to data masking.

- Performance: linear-time algorithms for translating user queries to permitted queries.



1. Access Manager intercepts the SQL statement from an Application user and sends it to the Translator.
2. Translator converts the user's SQL statement into either an access DENY or a SQL permitted statement that is sent back to the Access Manager.
3. Access Manager submits the permitted SQL statement to the database; in the case of a DENY, the Access Manager forwards the indication to the application user.
4. In the case of a Select operation, data extracted from the database is sent back to the Access Manager and forwarded to the Application and user.

Contact: licensing@nist.gov

NIST TECHNOLOGY PARTNERSHIPS OFFICE

NIST Technology Partnerships Office
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899-2200