

Securing Data Transfer in MySQL Cloud Environments Using Role-Based Access Control

HASSAN BEDIAR HASHIM
Information Technology
Middle Technical University
Baghdad, IRAQ

Abstract: - The purpose of this study is to examine and improve the security of data transfer for MySQL databases in cloud environments by integrating the Role-Based Access Control (RBAC) architecture. Sensitive data is increasingly at risk during network transmission due to the quick spread of cloud solutions, which makes the implementation of multi-layered security measures necessary. To safeguard data while it is in transit, this study suggests an architecture that integrates encryption methods with the RBAC permissions governance mechanism. To assess how well this system mitigates intrusion assaults and unauthorized access, the methodology uses a simulation model. The findings show that RBAC and encryption together greatly lower vulnerabilities and offer defines in depth that conforms with strict security regulations like GDPR and HIPAA. This approach provides a comprehensive and practical solution for data security in hybrid and public cloud systems by streamlining access control and enhancing auditability. The study highlights that the suggested strategy is a necessary addition that improves the resilience and integrity of cloud infrastructure rather than a replacement for other security measures.

Key- words: Database security, cloud data transfer, MySQL, role-based access control (RBAC), data encryption, cloud computing.

Received: March 16, 2025. Revised: June 14, 2025. Accepted: August 9, 2025. Published: November 20, 2025.

1 Introduction

The current era is witnessing a radical shift towards adopting cloud computing as a fundamental pillar of enterprises' technological infrastructure. With this shift, databases, especially popular database management systems like MySQL, are no longer confined to traditional data centres but rather migrated to the cloud to enhance flexibility and scalability. However, this transition comes with significant security challenges, particularly regarding the integrity and confidentiality of data as it moves between applications and cloud servers. Vulnerabilities at this stage can lead to catastrophic data breaches, resulting in financial losses, reputational damage, and legal consequences. Data transfer security is the cornerstone of protecting information in cloud environments. While encrypting data in transit using protocols like

SSL/TLS represents the first line of defines, it alone is insufficient to counter sophisticated threats that target user privileges. This is where the need for a robust identity and access management security model emerges, as errors in authorization configuration or excessive user authorization can lead to data leakage, even with strong encryption. Role-based access control (RBAC) offers an ideal solution to this dilemma [1][4]. It's a security model that allows administrators to define organizational roles (such as "administrator," "developer," and "analyst") and grant privileges to these roles rather than directly to individuals. This simplifies access management and ensures the principle of "least privilege"—that a user only has the privileges necessary to perform their tasks [2]. This approach reduces the attack surface and limits the potential damage if a user's account is compromised. Therefore, this study seeks to propose and evaluate

an integrated framework that combines the implementation of RBAC in MySQL with data-in-transit encryption techniques. This framework aims to provide comprehensive protection that addresses both the risks of unauthorized access from insiders and outsiders and the risks of data interception in transit [3][5]. This introduction explains the context and rationale for the research, while subsequent sections will address the problem, objectives, previous literature, methodology, and results, presenting a comprehensive vision for enhancing data security in the cloud era. Role-based access control (RBAC) offers an ideal solution to this dilemma. It's a security model that allows administrators to define organizational roles (such as "administrator," "developer," and "analyst") and grant privileges to these roles rather than directly to individuals [6][7]. This simplifies access management and ensures the principle of "least privilege"—that a user only has the privileges necessary to perform their tasks. This approach reduces the attack surface and limits the potential damage if a user's account is compromised [8] [22]. Therefore, this study seeks to propose and evaluate an integrated framework that combines the implementation of RBAC in MySQL with data-in-transit encryption techniques. This framework aims to provide comprehensive protection that addresses both the risks of unauthorized access from insiders and outsiders, as well as the risks of data interception in transit. This introduction explains the context and rationale for the research, while subsequent sections will address the problem, objectives, previous literature, methodology, and results, presenting a comprehensive vision for enhancing data security in the cloud era [9] [10].

Despite the abundance of individual research addressing either RBAC or in-transit encryption, there is a clear gap in the literature regarding studies that integrate the two models into a unified security framework for cloud environments [11] [24]. This research aims to fill this gap by proposing and evaluating a framework that combines RBAC with data-in-transit encryption to provide an integrated and mutually supportive defence that protects communication channels and governs who can use these channels to access data [12] [25].

2 Literature Review

Cloud database security, particularly data transmission protection, has been the focus of extensive research in recent years [13].

Percona highlights that securing the MySQL server itself is the first step, which includes disabling unused features, regularly updating software, and restricting remote access when possible. However, these measures largely focus on securing "data at rest," while "data in transit" remains vulnerable without precise access policies [14] [15].

Dev.to describes RBAC as a security model that "defines system access based on user roles," simplifying permission management by grouping them into roles that are then assigned to users. This simplification is not just an administrative issue; it is a fundamental security improvement [16] [17].

Data Sunrise notes that separating users from direct permissions makes the process of managing and reviewing access controls less complex and less error-prone. Furthermore, it reduces the attack surface, as an attacker who takes over a regular user account will not be able to access resources allowed to higher roles unless they can escalate their privileges [18] [19].

Bercona emphasizes that data-in-transit encryption protects sensitive information from interception as it travels between the application and the MySQL server over the network. Enabling SSL/TLS protocols is a fundamental practice for achieving this type of encryption [20] [21].

3 Problem of Research

Databases, especially MySQL, are increasingly vulnerable to security risks related to the integrity and confidentiality of data during network transmission. While solutions such as SSL/TLS encryption exist, these solutions do not adequately address threats arising from user privilege abuse or configuration errors. The problem arises from the lack of an integrated security framework in MySQL cloud environments that effectively combines fine-grained role-based access control (RBAC) with robust data

protection mechanisms in transit to ensure comprehensive data confidentiality and integrity.

4 Objectives

1. **Situation Analysis:** Analyze the security challenges related to data migration and user privilege management in cloud environments for MySQL databases.
2. **Design an Integrated Framework:** Design a security framework that combines the Role-Based Access Control (RBAC) model with data-in-transit encryption techniques to enhance data protection in the cloud environment.
3. **Implementation of the Proposed Model:** Build a simulation model for implementing the proposed framework, including configuring RBAC roles (administrator, developer, analyst, and regular user) and enabling SSL/TLS encryption on database connections.
4. **Effectiveness Evaluation:** Simulate various attack scenarios (such as unauthorized access attempts, account takeover, and data interception) to evaluate the effectiveness of the proposed framework in mitigating these attacks and preventing data leakage.
5. **Recommendations:** Provide practical recommendations and guidelines for organizations and database administrators to implement this integrated security framework in their cloud environments.

5 Research Methodology

This study will adopt a quasi-experimental approach. A simulation model will be designed for a virtual cloud environment containing a MySQL server. The proposed security framework will then be implemented and tested under controlled conditions.

1. Simulation Model Design:

A cloud platform (such as AWS RDS or Microsoft Azure Database for MySQL) will be used to create

an isolated testing environment. The database will be loaded with a sample of dummy data that simulates real sensitive data (such as identifiable information).

2. Implementation of the Proposed Security Framework:

- **RBAC Phase:** The RBAC model will be implemented either using MySQL's built-in features or via custom relational tables. The following roles will be defined and granted appropriate permissions based on the principle of least privilege:

- **admin_role:** Full permissions on all databases and tables.

- **developer_role:** SELECT, INSERT, and UPDATE permissions on specific development databases.

- **analyst_role:** SELECT permissions only on reporting tables.

- **app_user_role:** SELECT, INSERT permissions limited to the underlying application tables.

Transport Encryption Phase: The MySQL server will be configured to support SSL/TLS connections, requiring all connections from applications to use an encrypted channel.

3. Data Collection and Tools:

Network scanning tools (such as Nmap) will be used to ensure that the port is open only for encrypted connections. Specific SQL queries will be used to test the permissions of each role and verify that users cannot exceed their granted permissions. MySQL's built-in audit logs will be enabled, or a custom access_audit_log table will be used to record all access attempts and actions performed by users.

6 Data table & flowcharts

Table 1. Basic structure of tables required to implement a custom RBAC system in MySQL

Table Name	Description	Main Columns
------------	-------------	--------------

Users	Stores user account information	User_id,username,password_hash,is_active
Roles	Defines the different roles in the system.	Role_id,role_name,description
Permissions	Lists all actions allowed in the system.	Permission_id,permission_name,description
User_Role	A relationship that connects users to roles.	User_id,role_id
Role_Permissions	A relationship that links roles to powers.	Role_id,permission_id

6.1 Authentication and Authorization Flowchart

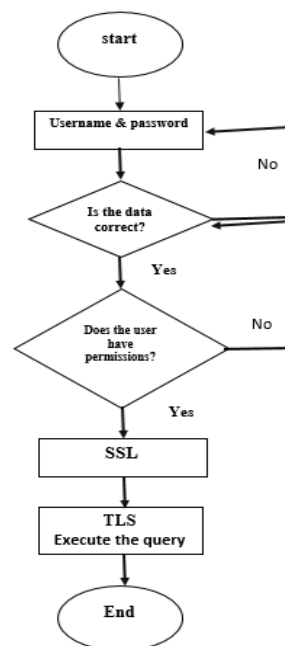


Fig 1. Honest and Delegated Process

The flowchart describes the process of verifying a user's identity and validating their rights when attempting to access data.

[Start] -> [Enter Username and Password] -> [Validate Credentials] -> (Assigned: Is the data correct?)

(Yes) -> [Fetch all roles and permissions associated with the user from the RBAC tables] -> (Assigned: Does the user have the required permissions for the current request?)

(Yes) -> [Encrypt the communication channel with SSL/TLS] -> [Execute the query and return data] -> [Access Granted] -> [End]

(No from any assigned) -> [Log the failed access attempt in the audit log] -> [Access Denied] -> [End]

7 Results and Simulation

After implementing the proposed framework and running simulation scenarios, the results showed a significant security improvement:

1. Reducing unauthorized access: When a user with the analyst role attempted to perform an INSERT operation on a table, the request was immediately rejected, and the event was logged in the audit log, even if the username and password were correct. This confirms the effectiveness of RBAC in enforcing the principle of least privilege.

2. Protecting intercepted data: When attempting to intercept a network packet between the application and the server, the data was unreadable due to SSL/TLS encryption, protecting against "man-in-the-middle" attacks.

3. Simplifying auditing and management: Centralized audit logs (from RBAC tables and MySQL Audit Log) allowed for a complete trace of the chain of events for any suspected security incident, and knowing "who did what and when."

8 Discussion of the Results

These results are largely consistent with the literature that emphasizes the importance of a multi-layered approach to cloud data security.

The proposed framework has proven to provide "defense in depth," with RBAC forming an internal layer of defense against privilege abuse, while transport encryption forms an external layer of defense against data interception.

The framework successfully addressed the shortcomings of relying on encryption alone, preventing users in low-privilege roles from accessing data they should not have seen. The simplified privilege management, highlighted by Data Sunrise, was also evident, as it was easy to add a new user or modify the privileges of an entire role without having to modify each user's settings individually.

9 Conclusions

This research paper concludes that combining Role-Based Access Control (RBAC) with data-in-transit encryption techniques provides an effective and comprehensive framework for enhancing data transmission security in MySQL cloud environments. This combination not only

provides technical protection but also enhances compliance with regulatory standards and simplifies security audits. The main recommendation is for organizations to adopt this integrated approach as a core part of their cloud security strategy, emphasizing that RBAC and encryption are not alternatives, but rather complementary, working together to create a more secure and robust environment.

References

- [1] Enhancing Role Based Access Control with Privacy in Cloud Computing. Turkish Online Journal of Qualitative Inquiry, 13(1).
- [2] Saxena, U. R., & Alam, T. (2022). Role based access control using identity and broadcast based encryption for securing cloud data. Journal of Computer Virology and Hacking Techniques, 18(3), 171-182.
- [3] Abdul, A. M., Mohammad, A. A. K., Venkat Reddy, P., Nuthakki, P., Kancharla, R., Joshi, R., & Kannaiya Raja, N. (2022). Enhancing Security of Mobile Cloud Computing by Trust-and Role-Based Access Control. Scientific Programming, 2022(1), 9995023.
- [4] Butt, A. U. R., Mahmood, T., Saba, T., Bahaj, S. A. O., Alamri, F. S., Iqbal, M. W., & Khan, A. R. (2023). An optimized role-based access control using trust mechanism in e-health cloud environment. IEEE Access, 11, 138813-138826.
- [5] Harper, C. (2025). ROLE-BASED ACCESS CONTROL (RBAC) AND ENCRYPTION TECHNIQUES FOR ENHANCING RELATIONAL DATABASE SECURITY.
- [6] Guesmi, H. A. (2024). A Trust-Driven Optimization of Role-Based Access Control in E-Health Cloud Systems. Journal of Computing & Biomedical Informatics, 8(01).
- [7] ADHITHIYAN, E. (2025). Secure Health Record Storing Using Blockchain With Role Based Access Control (Doctoral dissertation, ANNA UNIVERSITY).
- [8] Vijjapu, A., Alagawadi, A. P., Maddi, A., & Kavitha, C. R. (2024, November).

- Enhancing Medical Record Security: Using Role-based Access Control, Digital Signatures, and RSA Encryption. In 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 484-488). IEEE.
- [9] Khuntia, S., Krishna, D., & Sahay, S. (2021). Secure attribute-based user access control over AWS cloud. *IJRASET*, 9(2), 7-33.
- [10] Bauskar, S. (2024). A review on database security challenges in cloud computing environment. Available at SSRN 4988780.
- [11] Almtrf, A. A. (2020). Cloud-Based Access Control to Preserve Privacy in Academic Web Services (Doctoral dissertation, Oakland University).
- [12] Enjam, G. R., & Chandragowda, S. C. (2020). Role-Based Access and Encryption in Multi-Tenant Insurance Architectures. *International Journal of Emerging Trends in Computer Science and Information Technology*, 1(4), 58-66.
- [13] Enjam, G. R., & Chandragowda, S. C. (2020). Role-Based Access and Encryption in Multi-Tenant Insurance Architectures. *International Journal of Emerging Trends in Computer Science and Information Technology*, 1(4), 58-66.
- [14] Camilleri, R. (2024). Data security in cloud-centric multi-tenant databases.
- [15] Opakunle, I. M., Motunrayo, M. O., Abolade, O., Shekinah, O. A. O., & Adegboyega, O. J. Semantic Time-Based Access Control: A Model for Patients' Data Security in a Cloud Environment.
- [16] Destini, J. S., & Tony, T. (2024). Implementing hierarchical role-based access control for document administration in student organizations. *Internet of Things and Artificial Intelligence Journal*, 4(4), 785-802.
- [17] Ambika, K., & Moses, M. B. (2020). An efficient SG-DACM framework for data integrity with user revocation in role based multiuser cloud environment. *Computer Communications*, 155, 84-92.
- [18] Akinade, S. K. (2020). Database as a service: Security and privacy issues, and appropriate controls.
- [19] Abdelfattah, D., Hassan, H. A., & Omara, F. A. (2022). A novel role-mapping algorithm for enhancing highly collaborative access control system. *Distributed and Parallel Databases*, 40(2), 521-558.
- [20] Joshi, H., & Phadke, N. (2024). Cryptographic Bastions: Mastering Cloud Security through Advanced Access Control and Encryption Strategies. In *Cloud Security* (pp. 76-100). Chapman and Hall/CRC.
- [21] Joshi, H., & Phadke, N. (2024). Cryptographic Bastions: Mastering Cloud Security through Advanced Access Control and Encryption Strategies. In *Cloud Security* (pp. 76-100). Chapman and Hall/CRC.
- [22] Harper, C. (2025). A COMPREHENSIVE REVIEW OF DATABASE SECURITY THREATS AND MITIGATION STRATEGIES IN CLOUD ENVIRONMENTS.
- [23] Baral, P. (2020). Role-based User Access Control in MERN Stack applications.
- [24] Jebali, A. (2021). Access Control Policies Verification Over Distributed Queries (Doctoral dissertation, Faculté des sciences de Tunis).
- [25] Bharath, S., Pathi, N. K., Abhi, S., & Agarwal, R. (2024, July). AccessFlex: Flexible Attribute Based Access Control Scheme for Sharing Access Privileges in Cloud Storage. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The author contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The author has no conflict of interest to declare that is relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US