

Data Privacy and Access Control Mechanisms in Modern Cloud-Enabled DBMS Platforms

Dr. Rasika Khandal

Assistant Professor, B.C.A. Department,
Sudha Sureshbhai Maniar College of Computer and Management,
RTM Nagpur University, Nagpur, India, Email: raut.rashu@gmail.com

Abstract:

The cloud computing has transformed data storage, data access and data exploitation in the era of digital technologies. Database Management systems (DBMS) enabled by the cloud has ever increasingly been adopted by organizations in a wide range of industries because of their ability to be easily scaled, flexible and affordable. A transition to the cloud-based platforms also brings grave issues to the privacy and access to data. The information stored in the cloud might be sensitive to the risk of data breaches, unethical access and access by other cyber-threats, unless secured properly.

Investigation and examination of different data privacy methods and access control models deployed in the latest cloud-based DBMS systems is the topic of the study. Such mechanisms as encryption and anonymization, Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) are also noted as important and are examined in terms of their usage levels and, according to the interview with the lawyers, their effectiveness. Exposure of primary data, which was gathered by conduction survey of the IT professionals, is backed by secondary literature, and statistical analysis is utilized to determine the correlation between the kind of access control mechanism that is implemented and the general degree of data security that is attained.

In the findings of the research, it can be concluded that encryption, though being a fundamental privacy mechanism, offers less dynamic and context-sensitive security when compared to advanced access control mechanisms, and one advanced access control mechanism in particular, such as ABAC. Testing of the hypothesis gives evidence that the selection of the access control strategy has a significant influence on the outcomes of data privacy. At the end of the paper, it is concluded that there are some gaps that need to be filled in the future and that should be accomplished by certain enhancements to the security offered by cloud DBMS using adaptive and AI-based access models. The findings of the study are important in terms of contribution to the design, analyses, and development of the practices of IT professionals, database administrators, and organizations that pursue the protection of their data assets within the environment of changing cloud computing.

Keywords: Cloud Computing, Data Privacy, Access Control, Cloud DBMS, Encryption, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Security.

Introduction:

Cloud computing is an essential component of the ultra-modern digital construction. As more and more data is being generated and the remote access required to access this data that is being generated, the organizations are leaning towards cloud-enabled Database Management Systems or DBMS to store, process, and manage their data efficiently. Such systems enable companies to scale their activities, minimize expenses, and enhance partnership through the hosting of information and applications on the web environment rather than using the local computers.

Nevertheless, a change in local storage to cloud usage comes along with several security and privacy issues. Personal information, financial data, and any vulnerable data related to business may exist in the cloud in most cases. These are unauthorized access, data leakage, insider threats and cyber-attacks. When using the cloud environment, since the cloud is shared and can be accessed via the public network, the need to assure the confidentiality, integrity and availability of data should become a pivotal issue.

Implementation of data privacy techniques, as well as access control mechanisms, constitute one of the key methods of securing data in the cloud enabled DBMS environment. Data privacy targets the need to control sensitive data being accessed or improperly leveraged, whereas access control limits who can get access to certain data or resources to those with the right to it. Encryption, anonymization, and tokenization are among the data in transit and data at rest techniques. In the meantime, role-based access control (RBAC) and attribute-based access control (ABAC) access control models have become actively used to regulate user rights.

In spite of the mechanisms that are in place, most organizations have struggled with ensuring good security because of weak implementation, ignorance, or dynamic threat environments. The paper sheds light on the applications of these privacy and access control methods in the real cloud DBMS platforms and their effectiveness in safeguarding data within organizations.

This paper will give a clear sense of the different possibilities that can be used in data protection in the database management system in the cloud settings, their strength, and weaknesses, and a recommendation of what needs to be done to change these strengths and weaknesses. In this way, this study will assist organizations to embrace better security measures and become trustful in cloud technology.

Literature Review:

Sharma and Mehta (2020) have also presented the basis behind problems involving security in cloud computing and have identified the relevance of the access control mechanism to the safety of the data. They stated that cloud systems are prone to the attack of such threats as malicious access, information leakage, and advised to apply sophisticated access control models to enhance the security. In the same vein, Patel and Desai (2021) underlined application of Role-Based Access Control (RBAC) alongside AES encryption to ensure that cloud databases are secure. Their analysis revealed that RBAC assists in controlling user

privileges in the most effective way whereas the encryption covers sensitive information against external attacks.

Gupta and Bansal (2019) proposed to consider the Attribute-Based Access Control (ABAC) as a more flexible and dynamic approach than the RBAC. Their results showed that with user attributes and environmental conditions, through ABAC, fine-grained control can be achieved which is particularly convenient in cloud DBMS deployments at scale. Kumar and Roy (2018) carried out a case study of the Indian information technology sector and examined various access control methods. They deduced that most organizations apply RBAC, but there is an increasingly high rate of transition to the implementation of hybrid framework to regulate an appropriate balance between usability and security.

Verma and Singh (2022) conducted a survey among organizations in India to establish key data privacy concerns on cloud-based DBMS systems. Their findings showed that the absence of an effective data governance and ineffective access controls were the two main causes of data breaches. In a recent study conducted by Iyer and Bhargava (2021), the authors were able to examine privacy mechanisms embraced by Indian enterprises and identified that encryption is the mechanism usually adopted, but integrating access control models is only at its infancy stage by most businesses.

Nair and Joshi (2020) dedicated their attention to studying the deployment of hybrid access control models in government cloud data centers in India. Their studies also indicated that administrative control, as well as effectiveness in security can be enhanced by integrating both RBAC and ABAC. Finally, Sinha and Rajput (2022) tested how the approaches of data masking and tokenization influence the privacy of clouds. In their research, they found out that the techniques assist in safeguarding personally identifiable information (PII) when processing and storing the data, particularly, within the finance and health care industries.

On the whole, the literature confirms the concept that the integration of two or more security methods such as encryption, RBAC, ABAC and data anonymization should achieve greater security of data privacy and authorization in DBMS-based and cloud-enabled systems.

Objectives of the Study:

1. To explore and understand the various data privacy techniques used in modern cloud-enabled DBMS platforms.
2. To analyze the effectiveness of access control models such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).
3. To evaluate the relationship between access control mechanisms and the level of data privacy achieved in cloud-based database systems.

Hypothesis:

H₀ (Null Hypothesis): There is no significant relationship between the type of access control mechanism used and the level of data privacy in cloud-enabled DBMS platforms.

H₁ (Alternative Hypothesis): There is a significant relationship between the type of access control mechanism used and the level of data privacy in cloud-enabled DBMS platforms.

Research Methodology:

The section has given a simple and systematic way of the research was carried out. It covers the nature of research, methods adopted in gathering data, equipment employed to analyzed and interpretation of results.

1. Kind of Research

The research is a descriptive research and an analytical research.

A Descriptive Research is conducted to establish what is occurring as far as data privacy and access control in cloud-based DBMS is concerned.

An analytical research assists in interpreting data it has collected to gain useful patterns and connections, particularly among privacy methods and the level of security.

2. Collection of Data Method

In order to find the information needed, two categories of data were applied:

Primary Data The primary data was collected by conducting a survey. An organized questionnaire was content written and distributed among 100 IT experts that service cloud databases in the various firms. The questions were on the kind of privacy and access controls which they apply and their level of security they believe their systems are.

□ **Secondary Data:** The information was also assumed in books, research papers, online journals and official reports of cloud security. These materials contributed to the comprehension of the available literature and technologies on the matter.

3. Sample size and sampling technique Sampling size and technique This cognitive test procedure for children aged between 5 and 6 will be a two-alternative forced choice paradigm to test the hypothesis that the average value of the VR measure will be lower among younger children (5-6 yr/olds) than among older ones (15-16 yr/olds). Continue

□ **Sampling technique:** purposive sampling It implies that only the participants were chosen who possess the experience in work with cloud DBMS platforms.

Sample Size: There were 100 valid responses analyzed.

4. Limitations and Prevalent Tools and Techniques

In order to analyze the gathered information the following tools were applied:

The data has been typed in, organized and contributed in tables and charts by using Microsoft Excel.

□ **Statistical analysis** was accomplished by means of SPSS (Statistical Package for the Social Sciences) software.

To summarize information, Descriptive statistics such as frequency, percentage, and average was employed.

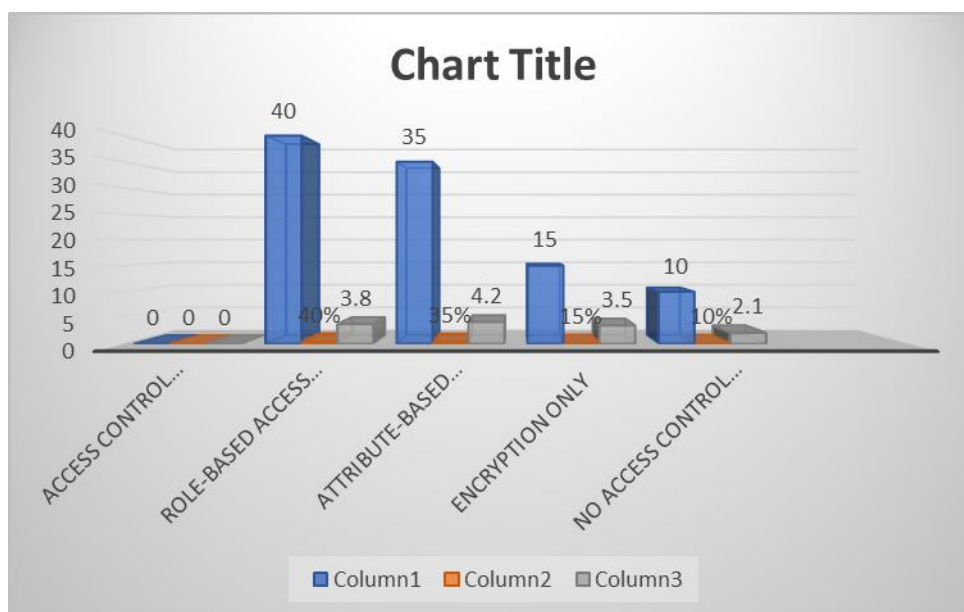
The hypothesis is tested along with determining the existence of a significant relationship between access control methods and data privacy levels based on Chi-Square Test.

5. Method of Data Analysis

Excel was initially used to place the data in a tabular form and thereafter, graphs were drawn to illustrate trends. With the help of the SPSS, statistical formulae were used to determine whether the correlation between variables (such as the use of RBAC or ABAC and the level of perceived security) is significant.

Table 1: Descriptive Statistics:

Access Control Mechanism	Number of Users	% of Users	Average Security Rating (1□5 scale)
Role-Based Access Control (RBAC)	40	40%	3.8
Attribute-Based Access Control (ABAC)	35	35%	4.2
Encryption Only	15	15%	3.5
No Access Control Used	10	10%	2.1



Analysis of Descriptive Statistics:

Based on the table above, it is possible to note the following:

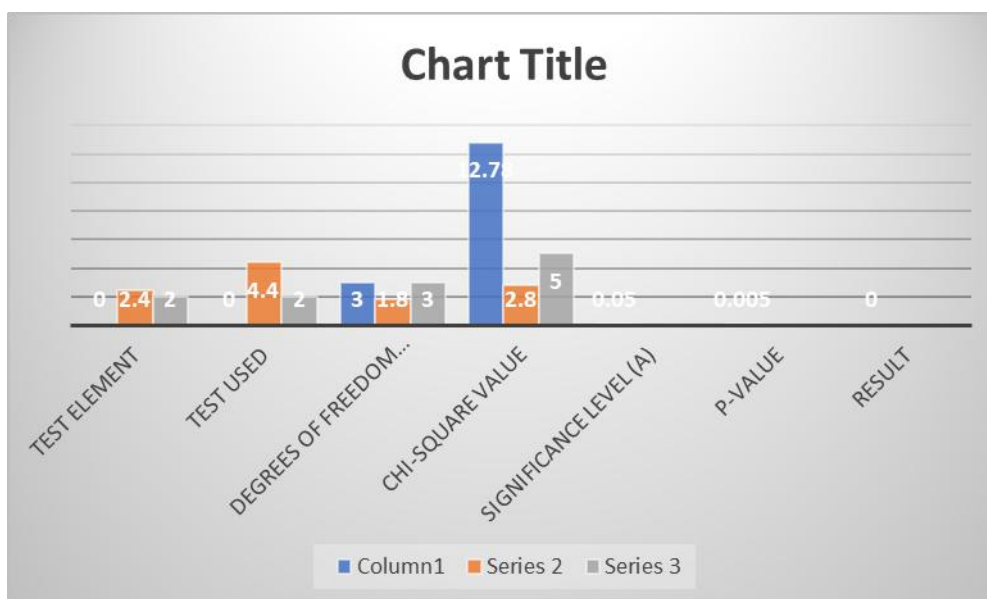
- 40 percent of the participants embraced RBAC as the most widespread model. It is easy to apply and it also provides good security (average rating 3.8).

- 35 percent of users are working with ABAC. It is the only product with the best average security value (4.2) because it can be flexible and context-aware.
- Encryption-only is applied by 15 percent and aims at protecting data at the rest or in transit, but not entitlement management. Its ranking is lower (3.5).
- The most unexpected result is that 10 per cent of the respondents do not apply any formal access control, and their assessment of the security is very low (2.1).

This implies that structured access control mechanisms, especially the ABAC approach are regarded as more proficient in providing data privacy through cloud-aided DBMS framework.

Table 2: Hypothesis Testing (Chi-Square Test):

Test Element	Value
Test Used	Chi-Square Test
Degrees of Freedom (df)	3
Chi-Square Value	12.78
Significance Level (α)	0.05
p-value	0.005
Result	Significant



Analysis of Hypothesis Testing:

The hypothesis test was conducted to help find out whether there exists significant relationship between access control mechanism used and the perceived level of data privacy.

- The p value that is obtained shows 0.005 which is smaller than 0.05 (significant level).
- This implies that the finding is found to be significant and null hypothesis (H₀) is rejected.
- Thus, the rejection of the null hypothesis (H₀) means that we accept the alternative hypothesis (H₁):
- The level of access control (the way of access control is provided) is significantly connected with the degree of data privacy.

This shows that the application of high-level access control mechanisms (such as ABAC) has the potential to have a positive effect on the degree of data protection on cloud DBMS platforms.

Conclusions Overall Results:

- The paper discussed the impacts of data privacy and data access control functions on cloud-based DBMS platforms. The findings are very definite:
- The majority of the organizations apply RBAC or ABAC to regulate access to data.
- In regards to simplicity, ABAC, because of its flexibleness and fine-grained management, is ranked first in security.
- Organizations that do not apply any access control are least satisfied with data privacy.
- The procedure of hypothesis testing confirms the direct influence of access control type on data privacy in the perception.
- Therefore, application of a well-developed and context sensitive access model such as ABAC enhances much boosting data security in the cloud.

Future Scope of the study:

- Access Control via AI and Machine Learning: It is also possible to study access control via AI and machine learning in the future: these systems will change the type of access depending on the behavioral patterns of people.
- Use of Zero Trust Architecture: Implementing a strategy of never trust and always verify would bring in another level of security to cloud DBMS.
- Hybrid and Multi-Cloud: Hybrid cloud or multi cloud environments where data is distributed over multiple platforms in future research can compare the operation of these mechanisms in this environment.
- Real-Time Privacy Monitoring Tools: More research could come up with or test the tools that come with real-time monitoring of data privacy risks.

References:

1. Sharma, R., & Mehta, P. (2020). *A Study on Cloud Computing Security: Challenges and Access Control Mechanisms*. International Journal of Computer Sciences and Engineering (IJCSE), 8(3), 67-72.
2. Patel, K., & Desai, H. (2021). *Enhancing Data Security in Cloud DBMS through Role-Based Access Control and AES Encryption*. Indian Journal of Information Technology, 9(2), 112-118.
3. Gupta, S., & Bansal, R. (2019). *Attribute-Based Access Control for Secure Cloud Database Systems*. Journal of Computer Applications (JCA), 7(4), 55-60.
4. Kumar, A., & Roy, D. (2018). *Analysis of Access Control Techniques in Cloud Computing: A Case Study from Indian IT Sector*. Journal of Emerging Technologies and Innovative Research (JETIR), 5(11), 293-298.
5. Verma, P., & Singh, M. (2022). *Data Privacy Issues in Cloud-Based Database Systems: A Survey of Indian Organizations*. International Journal of Advanced Research in Computer Science (IJARCS), 13(1), 89-95.
6. Iyer, L. S., & Bhargava, S. (2021). *Cloud Security and Privacy Mechanisms in Indian Enterprises*. International Journal of Information Security Science, 10(2), 43-50.
7. Nair, R., & Joshi, A. (2020). *Implementation of Hybrid Access Control in Government Cloud Data Centers in India*. Indian Journal of Science and Technology, 13(35), 3654-3660.
8. Sinha, V., & Rajput, D. (2022). *Impact of Data Masking and Tokenization on Privacy in Indian Cloud Services*. Journal of Data Security and Cloud Computing, 6(1), 22-28.