Network Intelligence Studies
Volume VI, Issue 12 (2/2018)

**Constantin BRAN,**
**Bogdan ȚIGĂNOAIA,**
**Larisa GAVRILĂ,**
**Sorin Cristian IONESCU**
*University Politehnica of Bucharest*

# INCREASING PERFORMANCE BY FLEXIBILE MANAGEMENT OF THE DATABASE

Case Study

**Keywords**
*Managerial Flexibility,*
*Productivity Management,*
*Database Security,*
*IT&C Security,*
*Technological Flexibility,*
*Strategic Management*

**JEL Classification**
*M11, M12, M15, M16, M21*

**Abstract**

*The access to data in the databases of an organization depends on different levels of specific information security. If the security level is too high, it can cause delays or blockages in the implementation of priority tasks. The study tracked the flexibility of IT security related to the access to a network and how it improves the time/cost ratio in the targeted departments. The findings suggest that there is a strong link between the level of security concerning the access to information in databases and the performance of the employees. IT changes have saved time and reduced costs, increased productivity and performance and also technological and managerial flexibility.*

## INTRODUCTION

Databases have become a working tool without which organizations can no longer compete. The issue of data storage concerns the stability and security of databases. This approach involves protecting databases against reading, modifying and destroying data, knowing that there is no 100% safe protection but only more or less effective security measures.
The security issue includes legal, social and ethical issues. Computer frauds are not necessarily linked to the database and the organization's information system is vulnerable and can always be at risk. There is a serious concern in the world about updating legislation to new needs generated by the intensive use of computers. To this end laws have been passed that protect the person or organization and take into account that some information must be private not accessible to anyone, especially if this harmed the owner of that information.

## THEORETICAL CONTEXT

Database security is a complex issue of an organization as it means a multitude of flexible policies. Access to a company database must be done by cryptographic authentication according to the specificity of the activity, with monitoring access to all data (Samarati & Sandhu, 2016).

**Intrusion Detection System** is a system in which malicious activity performed by any user or program is logged and can be viewed later by the admin (Dawle et al., 2017). The types of security depend on the technology in which the database has been prepared. One of decision support systems in the logistics industry is, for example, SIMMAG 3D (Jacyna et al., 2017), F*ig. no. 1*, developed within the project funded by the NCBR (The National Centre for Research and Development) under the Program for Applied Research (PBS3), (Jacyna et al., 2017).
Many database management systems also include a database administrator (DBA) account, with unlimited power over the database. The DBA often possesses the privilege to reset a user's password. The DBA also possesses the privilege to impersonate another user's account.
Although these permissions are very useful, if the DBA account or administrator is unavailable, these functions cannot be performed. Additionally, in some instances, a particular user may only need a subset of the functionality possessed by the DBA account but granting the full functionality of the DBA account may pose a security risk (Goel et al., 2016).

**Critical Data.** Protecting critical data involves creating a plan similar to a data recovery plan. When create a plan for protecting data there are a few things that have to be taken into consideration, as well as a few strategies that should be deployed to carry out data protection. The first step is to determine the importance of data and then divide it into categories which include very critical, critical, inactive and duplicate data. Very critical data has obviously the highest priority and duplicate data the lowest priority. Very critical data will require frequent backups and replication in the event of data loss, critical data should be backed up on a daily basis, inactive data should be retained for different compliancy reasons, and duplicate data can be deleted while the system needs to be continuously flexible (Ali & Afzal, 2017; Bran, 2015).

**Access control** is one of the fundamental services that any Data Management System should provide. It protects data from unauthorized read and write operations. Access control makes sure that all communication to the database and other system objects strictly follow the policies. Errors can be so important that they can create problems in the firm. **Access control** may also help reduce the risks that may precisely impact the security of the database in the main servers. For instance, if any table is deleted or access is modified accidently the results can be roll backed or for specific files, but by applying the access control their deletion can be restricted (Malik & Patel, 2016). Attacker can take different approaches such as bypass authentication, Default Password, privilege escalation, Password Guessing by brute force and rainbow attack when they attempt to compromise user identification and authentication (Kulkarni & Urolagin, 2012).

**Secure and protect data integrity.** A mandatory security enforcement mechanism controls write access to the secure data rows. This mechanism is activated automatically when a relational database table is known to include a specific column name. The mechanism determines which security label is recorded in the updated data rows and written in the database. This access security mechanism requires that each of those updated rows contains one of the following possible values. Once the security information is available, the security level and category of the label associated with the retrieved row are compared with the security level and category associated with the user's security label. A decision then is made whether to allow the user to access that row (Davidson & Moss, 2016; Cotner & Miller, 2016).
Facilitating employees' access to the database must be done safely. Database protection in an organization involves taking security measures at several levels:
· physical (unauthorized access);

- at individual level (granting access to certain authorized persons);
- operating system level (securing vulnerabilities through appropriate measures);
- at the SGBD level - the system itself supports data protection.

Users accessing the database can do it at different levels depending on the applications they access. All database access operations are managed by the Database Management System, according to *fig. no. 2* (Jacyna et al., 2017).

The following forms of authorization (examples) are available in a database:

- reading authorization (consultation);
- authorization to insert (add);
- authorization to delete (tuple level);
- authorization to delete relations;
- index-level authorization (create-delete indexes);
- authorization of changes at the level of relations (deletions or attributes added in the relations);
- authorization update (excluding deletions).

Some techniques to ensure data security:

- *Identification of users* (each user is given certain operating rights on different sectors of the database at different levels such as relations, registration, page, attributes, etc.)
- *Protect data by coding (encryption).* Data decoding can only be done after the user has been identified
- *Using views in applications.* It allows access to the relations level (table) or view level access. In some systems, changes are not accepted through views. Such views are read-only and are mainly used in applications where data can be read by all users (public databases), but changes are only made with approval of database administrator/ owner.
- *Administration and transmission of rights.* Strict evidence of each user's access rights is kept in portions of the database and rules are established for the transmission of the right of access from one user to another.

**Managerial Flexibility And Organizational IT Policies.** Managerial flexibility, articulated in some management policies, has positive effects on performance when they are in line with the requirements of the environment. In order to activate these practices, firms should maintain a commitment to learning capabilities and financial resources (Verdú-Jover et al., 2008).

Other research proposes a measurement scale of organizational responsiveness through four types of managerial flexibility: internal and external, structural and strategic (Verdú-Jover & Gómez-Gras, 2009). Managerial flexibility had a significant influence on employee productivity, using cyber-technologies (Bran et al., 2015), and good budgets should on average lead to zero cost overruns (Jørgensen & Wallace, 2000). Results of moderated regression analysis reveal the significant moderating role of ethical culture in HR flexibility and HR performance relationship (Kumar & Rai, 2017).

## METHODOLOGY OF RESEARCH

During March - August 2018 information (reports, analyses) on work productivity was collected for three departments of the company Mednett Market Research, some operations being outsourced in Romania. The principal activity of the company is to provide software and database for businesses offering management consultancy services.

Thus, the way to perform the monthly tasks was analyzed. Managers specifically looked at the time needed for an employee to perform their work tasks and the number of daily reports that they can draw based on the level of access to existing information in databases, which has three levels: reduced, medium, increased. In short, all employees had the same daily working norm, but different conditions to achieve it (restrictions on accessing resources). Based on the analyzed reports within the company, about 105 employees who made similar daily reports and who had partial or total access to IT resources were selected.

They were divided into 3 categories (*table no. 1*): employees with limited or restricted access (A), employees with partial or medium access (B), employees who had full or increased access (C) to databases and software (annexes - *fig.no.2*, respectively *figures 3 and 4* (personal contribution), due to seniority and level of responsibility of the job. Thus, access levels for categories A, B, and C were set with appropriate encryption algorithms so that databases could be accessed under conditions of maximum security and efficiency to increase work productivity.

The task of employees directly focused on access to databases and time available to benefit from the data stored there. Managers wanted an improvement in work productivity. For this reason, the database had to be streamlined so that managers could achieve balance between the level of access to information in the DB and the monthly productivity (work efficiency). Each category of employees from the 3 above was assigned a task in order to complete a report for certain categories of suppliers and the time of completion for the reports was monitored according to the level of access they had to the databases.

## STATISTICAL ANALYSIS AND RESULTS

The data were collected and analyzed using the single factor ANOVA test and the "t" test on the pair samples based on the following two hypotheses:

$H_0$: *Regardless of the level of access to data, the efficiency of performing work tasks remains the same.*

$H_1$: *The level of access to data directly influences the efficiency of the work tasks.*

After data collection, the 3 categories of employees with different access levels to the data were grouped into samples pairs: A and B, A and C and B and C.
Distribution verification was done using the "f" test, in Excel, according to *tables 2, 3 and 4*.
In the case of the "f" test (*tables no. 2, 3 and 4*) to check if the distribution was normal, in each of the 3 cases, we noticed that F > F Critical One -Tail, so we rejected the null hypothesis $H_0$ for all 3 pair samples ( A+B, A+C and B+C) the results showing that distributions were uneven.
Since the distribution was not normal, the "t" test for each pair was applied (A+B, A+C and B+C) and it turned out that t Stat > t Critical two-tail.
The result shows that the null hypothesis $H_0$ was rejected. It is obvious that direct observation between samples is convincing enough to say that the difference between the two types of access is significant. Since in the 3 tests above, the distribution proved to be not normal, single factor ANOVA test was eventually applied in *table no.5*.
After Single Factor Anova test (*table no*. 5 in Excel), we noted that f > F crit.
Therefore, we reject the null hypothesis that regardless of the level of access to data, the efficiency of the work tasks remains the same.
In conclusion, at least two of the three categories have a different work efficiency.

$p = 4{,}67e - 12$ that is $< 0.01$, $H_0$ is rejected with a significance threshold of 99%

## CONCLUSIONS

The management of the organization, which is the owner of the database, must take security measures that reduce the risk of losing or destroying information. By losing information it can be understood that the private nature of the information is lost, so it becomes accessible to a larger group of people than the initially forecast. The information "leak" sometimes doesn't leave traces, so it does not always materialize in detectable changes at the database level. As a result of the research we have found that in the 3 cases we reject the null hypothesis $H_0$, as t Stat > t Critical two-tail, so direct observation between samples is sufficiently convincing to say that the difference between the three types of access is significant. The conclusion of the study is that in the three groups, differences in time were reported in the monthly activity, those with increased access having a better efficiency than the ones with medium level, and those with medium level had better efficiency than those with limited access. Therefore, flexibility in the type of data access leads to an increase in the speed of task completion and ultimately to an increase in productivity by reducing time and cost. The IT security level has not been weakened by granting access to information, as security measures have been taken at the level of information security.

## LIMITATIONS

If there are more than 3 samples, applying the "t" test (Student) to the pair samples is problematic because the number of calculations would be time consuming. This model has practical value, except for the case of organizations where the family of core standards ISO 27000 have been implemented.

## REFERENCES

[1] Ali A., Afzal M.M. (2017). "Database Security: Threats and Solutions", International Journal of Engineering Inventions, e-ISSN: 2278-7461, Feb ;6(2):25-7.
[2] Bran, C. (2015). The Flexibilization of Information Systems. FAIMA Business & Management Journal, 3(4), 64.
[3] Bran, C., Militaru, G., & Ionescu, S. (2015). Cybermarketing, a key driver for the improvement of flexibility in the sales process of a company. In International Conference on Management and Industrial Engineering (No. 7, p. 91). Niculescu Publishing House.
[4] Cotner C., Miller R.L., inventors (2016). "International Business Machines Corporation, assignee. Row-level security in a relational database management system", United States patent US 9.514.328, Dec 6.
[5] Davidson L., Moss J. (2016). "Database Security and Security Patterns. In Pro SQL Server Relational Database Design and Implementation", Apress, ISBN 978-1-4842-1973-7, pp. 411-490.
[6] Dawle Y., Naik M., Vande S., Zarkar N. (2017). "Database Security Using Intrusion Detection System", International Journal of Latest Engineering Research and Applications (IJLERA), ISSN: 2455-7137, Mar 2 (03) : 01-6.
[7] Goel A., Desai A.I., Gupta R., Ghosh S., Vadodaria H. (2016). "Inventors Sybase, Inc. assignee.: Autonomous role-based security for

database management systems", United States patent US 9.298.933, Mar 29.

[8] Jacyna M., Golebiowski P., Szczepanski E., M. (2017). Wasiak, "Efficacy of Data Security in Managing the Database of SIMMAG 3D System", Procedia Engineering, ISSN: 1877-7058, Dec 31;187:526-31.

[9] Jørgensen T., Wallace S.W. (2000). "Improving project cost estimation by taking into account managerial flexibility", European Journal of Operational Research, ISSN: 0377-2217, 127(2), 239-251.

[10] Kulkarni S., Urolagin S. (2012). "Review of attacks on databases and database security techniques", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, 2.11: 253-263.

[11] Kumar V.A., Rai S. (2017). "Role of human resource flexibility in organisational performance: a study of Indian IT firms", International Journal of Indian Culture and Business Management, ISSN: 1753-0814, 14(3):306-25.

[12] Malik M., Patel, T. (2016). "Database security-attacks and control methods". International Journal of Information Sciences and Techniques (IJIST) Mar;6(1/2).

[13] Samarati P., Sandhu R. (2016). "Database Security X: Status and prospects", ISBN: 0387351671, Springer; Jan 9.

[14] Verdú A. J., Gómez-Gras J.M. (2009). "Measuring the organizational responsiveness through managerial flexibility", Journal of Organizational Change Management, ISSN: 0953-4814, 22(6), 668-690.

[15] Verdú-Jover, A. J., Gomez-Gras, J. M., & Lloréns-Montes, F. J. (2008). "Exploring managerial flexibility: determinants and performance implications", Industrial Management & Data Systems, ISSN: 0263-5577, 108(1), 70-86.

**ANNEXES**

**Table No. 1.** Access level (reduced, medium, increased) to databases, calculated in number of days

| Crt. No. | A. Low Access Level (no. of days) | B. Medium Access Level (no. of days) | C. Increased Access Level (no. of days) |
|---|---|---|---|
| 1 | 5.00 | 4.50 | 2.50 |
| 2 | 7.00 | 6.00 | 5.00 |
| 3 | 4.50 | 4.50 | 3.50 |
| 4 | 4.50 | 4.00 | 3.50 |
| 5 | 6.00 | 5.00 | 4.00 |
| 6 | 3.50 | 4.00 | 3.50 |
| 7 | 5.50 | 4.50 | 4.00 |
| 8 | 7.00 | 5.50 | 2.00 |
| 9 | 4.00 | 3.50 | 3.50 |
| 10 | 5.00 | 4.50 | 3.00 |
| 11 | 6.00 | 6.00 | 4.50 |
| 12 | 5.00 | 4.00 | 2.50 |
| 13 | 5.50 | 5.00 | 4.00 |
| 14 | 6.50 | 5.50 | 5.50 |
| 15 | 8.00 | 4.50 | 3.50 |
| 16 | 7.50 | 6.00 | 5.00 |
| 17 | 4.00 | 4.50 | 2.00 |
| 18 | 6.00 | 5.00 | 4.00 |
| 19 | 5.00 | 3.50 | 2.50 |
| 20 | 7.00 | 4.00 | 3.00 |
| 21 | 7.50 | 6.00 | 4.50 |
| 22 | 8.50 | 6.50 | 5.50 |
| 23 | 7.00 | 5.50 | 4.00 |
| 24 | 5.50 | 4.00 | 2.00 |
| 25 | 4.50 | 5.00 | 5.00 |
| 26 | 5.00 | 4.50 | 3.50 |
| 27 | 7.50 | 5.50 | 5.00 |
| 28 | 4.00 | 3.00 | 3.50 |
| 29 | 6.00 | 4.00 | 3.00 |
| 30 | 6.00 | 3.50 | 3.50 |
| 31 | 3.50 | 4.00 | |
| 32 | 7.00 | 5.00 | |
| 33 | 4.50 | | |
| 34 | 7.50 | | |
| 35 | 5.00 | | |
| 36 | 8.00 | | |
| 37 | 6.50 | | |
| 38 | 5.00 | | |
| 39 | 7.50 | | |
| 40 | 4.50 | | |
| 41 | 8.50 | | |
| 42 | 6.00 | | |
| 43 | 7.00 | | |

**Table No. 2.** Test no. 1 for A and B – "F-test" and "T-test" (in excel)

**f-Test Two-Sample for variances**

| | *Variable 1* | *Variable 2* |
|---|---|---|
| Mean | 5.91860465 | 3.6833333 |
| | 1 | 3 |
| Variance | 1.93964562 | 1.0255747 |
| | 6 | 1 |
| Observations | 43 | 30 |
| df | 42 | 29 |
| F | 1.89127676 | |
| | 6 | |
| P(F<=f) one-tail | 0.03727719 | |
| | 4 | |
| F Critical one-tail | 1.79832109 | |
| | 2 | |

**t-Test: Two-Sample Assuming Unequal variances**

| | *Variable 1* | *Variable 2* |
|---|---|---|
| Mean | 5.918604651 | 3.683333333 |
| Variance | 1.939645626 | 1.025574713 |
| Observations | 43 | 30 |
| Hypothesized Mean Difference | 0 | |
| df | 71 | |
| t Stat | 7.937988426 | |
| P(T<=t) one-tail | 1.08956E-11 | |
| t Critical one-tail | 1.666599659 | |
| P(T<=t) two-tail | 2.17913E-11 | |
| t Critical two-tail | 1.993943341 | |

**Table No. 3.** Test no. 2 for A and C – "F-test" and "T-test" (in excel)

**f-Test Two-Sample for Variances**

| | *Variable 1* | *Variable 2* |
|---|---|---|
| Mean | 5.91860465 | |
| | 1 | 4.703125 |
| Variance | 1.93964562 | 0.77192540 |
| | 6 | 3 |
| Observations | 43 | 32 |
| df | 42 | 31 |
| F | 2.51273713 | |
| | 4 | |
| P(F<=f) one-tail | 0.00448979 | |
| | 2 | |
| F Critical one-tail | 1.77166221 | |
| | 7 | |

**t-Test: Two-Sample Assuming Unequal variances**

| | *Variable 1* | *Variable 2* |
|---|---|---|
| Mean | 5.918604651 | 4.703125 |
| Variance | 1.939645626 | 0.771925403 |
| Observations | 43 | 32 |
| Hypothesized Mean Difference | 0 | |
| df | 71 | |
| t Stat | 4.619535514 | |
| P(T<=t) one-tail | 8.3597E-06 | |
| t Critical one-tail | 1.666599659 | |
| P(T<=t) two-tail | 1.67194E-05 | |
| t Critical two-tail | 1.993943341 | |

**Table No. 4.** Test no. 3 for B and C – "F-test" and "T-test" (in excel)

**f-Test Two-Sample for variances**

| | *Variable 1* | *Variable 2* |
|---|---|---|
| Mean | 4.703125 | 3.683333333 |
| Variance | 0.771925403 | 1.025574713 |
| Observations | 32 | 30 |
| df | 31 | 29 |
| F | 0.752675933 | |
| P(F<=f) one-tail | 0.21910616 | |
| F Critical one-tail | 0.544977819 | |

**t-Test: Two-Sample Assuming Unequal variances**

| | *Variable 1* | *Variable 2* |
|---|---|---|
| Mean | 4.703125 | 3.6833333 33 |
| Variance | 0.771925403 | 1.0255747 13 |
| Observations | 32 | 30 |
| Hypothesized Mean Difference | 0 | |
| df | 58 | |
| t Stat | 4.223237951 | |
| P(T<=t) one-tail | 4.30167E-05 | |
| t Critical one-tail | 1.671552763 | |
| P(T<=t) two-tail | 8.60334E-05 | |
| t Critical two-tail | 2.001717468 | |

**Table No. 5.** Testing ANOVA: single factor (in excel)

| **SUMMARY** | | | | |
|---|---|---|---|---|
| ***Groups*** | ***Count*** | ***Sum*** | ***Average*** | ***Variance*** |
| Column 1 | 43 | 254.5 | 5.918605 | 1.939646 |
| Column 2 | 32 | 150.5 | 4.703125 | 0.771925 |
| Column 3 | 30 | 110.5 | 3.683333 | 1.025575 |

| **ANOVA** | | | | | | |
|---|---|---|---|---|---|---|
| ***Source of Variation*** | ***SS*** | ***df*** | ***MS*** | ***F*** | ***P-value*** | ***F crit*** |
| Between Groups | 90.25401 | 2 | 45.127 | 34.06153 | 4.67E-12 | 3.085465 |
| Within Groups | 135.1365 | 102 | 1.324867 | | | |
| Total | 225.3905 | 104 | | | | |

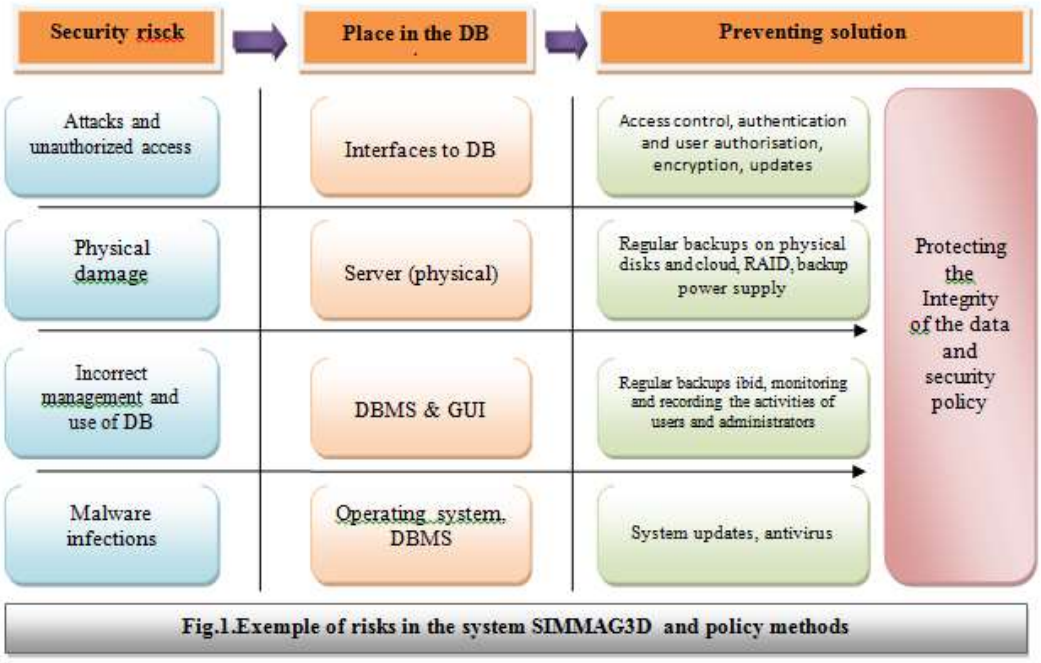


**Fig.1.Exemple of risks in the system SIMMAG3D and policy methods**

***Source****: Efficacy of Data Security in Managing the Database of SIMMAG 3D* (Jacyna et al., 2017).

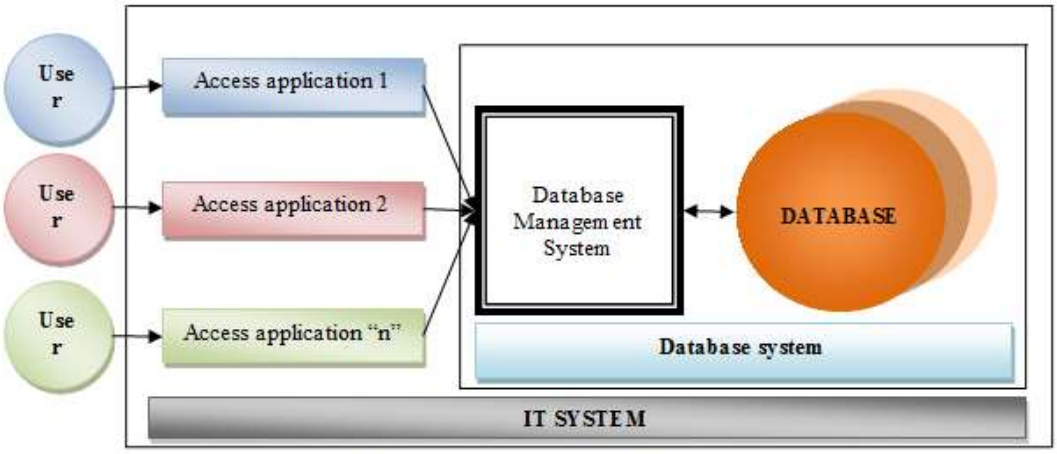


**Fig.2.Scheme of a typical IT system**

***Source**: Efficacy of Data Security in Managing the Database of SIMMAG 3D* (Jacyna et al., 2017).

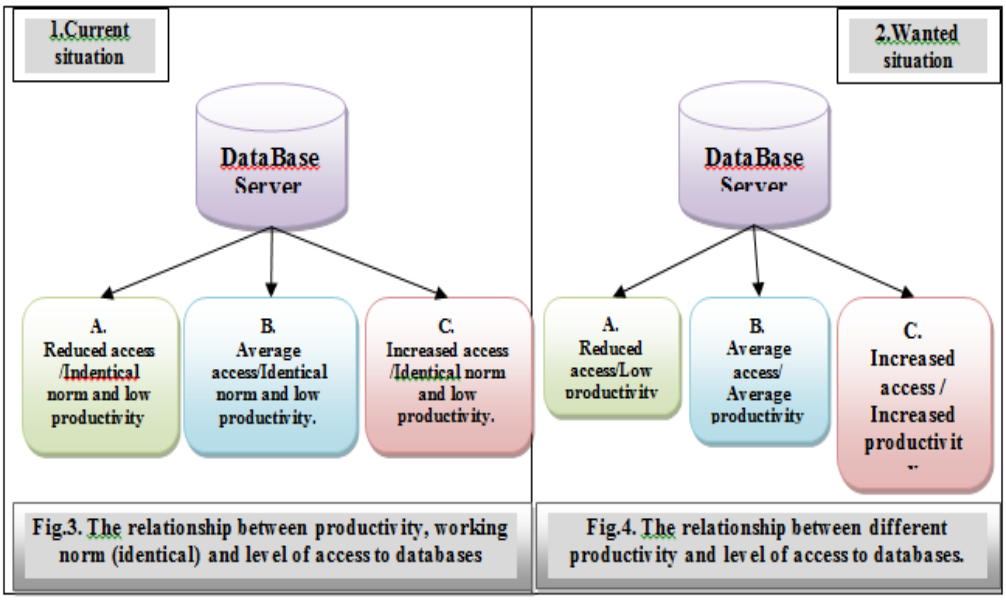


**Fig.3. The relationship between productivity, working norm (identical) and level of access to databases**

**Fig.4. The relationship between different productivity and level of access to databases.**

***Source**: Personal contribution*