# MANAGEMENT OF DATA SECURITY AND DATA NETWORK PROTECTION IN AN ORGANIZATION WITH THE OBJECT OF ACTIVITY IN INTELLECTUAL PROPERTY PROTECTION

**Radu Costin Moisescu [1],**
**Aurel Mihail Țîțu [2,3,4]**

***Abstract:*** *The scientific paper makes an important contribution regarding the detailing and analysis of the most important activities regarding the management of data security protection that can be implemented in intellectual property organizations. The research contains a detailed presentation of the access mechanisms that can be adapted and implemented to secure users' access to data from the databases of organizations active in the field of Intellectual Property. In this context, it is appreciated that improving the security of data and data networks in these organizations can be achieved by adapting and implementing new applicable technologies in terms of access to information published online according to legal regulations by these organizations. In this sense, the study and analysis of technologies that can be adapted and applied in intellectual property organizations is a contribution that can be essential for securing access to information and also for ensuring integrity, confidentiality, and data availability.*

***Keywords:*** *information system, computer system, security, data, data networks*
***JEL Classification:*** *O30, O32, C82*

[1] State Office for Inventions and Trademarks, Bucharest, Romania, radu.moisescu@osim.ro
[2] Aurel Mihail ȚÎȚU, Lucian Blaga University of Sibiu, Romania, mihail.titu@ulbsibiu.ro
[3] Aurel Mihail ȚÎȚU, The Academy of Romanian Scientists, Bucharest, Romania
[4] Aurel Mihail ȚÎȚU, Romanian Association for Alternative Technologies Sibiu, Romania

## 1. Introduction

With the technological evolution of the last years and due to the electronic environment of transmission, storage, and management of information in the present century, a century of speed and globalization, the problem of information security is more and more often posed.

Communications and networks, becoming more and more efficient, have expanded the area of users, both in terms of numbers and dispersion in the territory, the entire terrestrial space being accessible to very large networks. With the new progress, the area of malicious users, computerized theft variants and their methods of operation have diversified. Strong integration of systems appears as a consequence of improved forms of communication and the proliferation of information networks. In this context, the analysis of risks and vulnerabilities in information systems becomes a main component in defining modern communication systems.

Network security aims to protect them and network applications from attacks. To achieve this, organizations approach network security by creating security policies and, based on them, a network security architecture. This architecture is based on principles such as: access based on the identity of people on the network and the type of access they are allowed, access to network applications, data and critical services, perimeter security, data confidentiality or secure network connectivity (Kiser, 2020).

Finally, as networks grow in size and complexity, it is necessary to use security policy management tools that can centrally manage the security elements mentioned above. As different levels of Internet connectivity become essential to maintaining the competitiveness of organizations, ensuring the security of network infrastructure becomes an essential requirement. Data that is transferred from one place to another, such as when it is transmitted over the Internet, can be called moving data. Secure methods of these types are encryption such as SSL, HTTPS and TLS and are often used to protect moving data (Gertz, 2007).

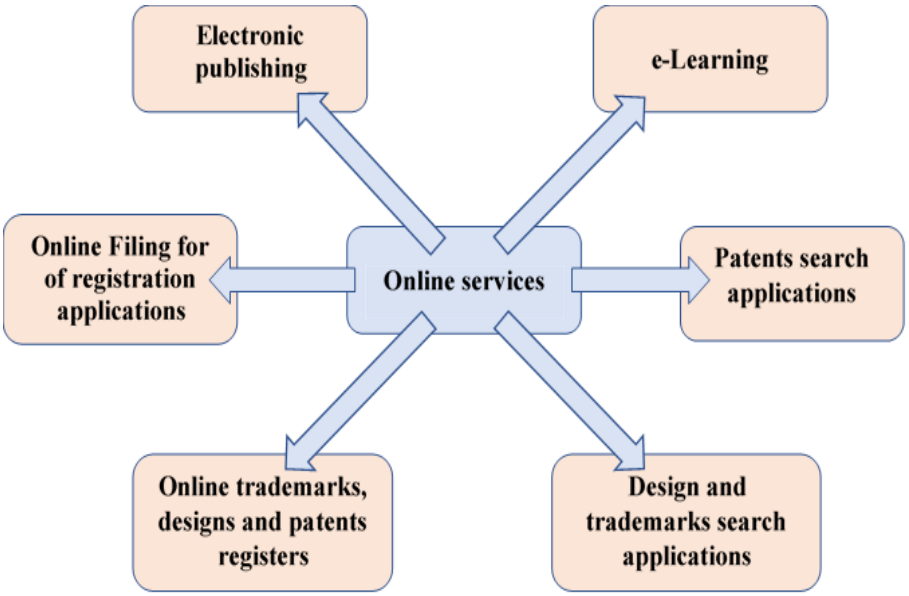


*Figure no.1. Electronic services in Intellectual Property organizations*

In organizations engaged in intellectual property, electronic services, abbreviated as e-services, represent the provision of certain categories of services by means of electronic means provided by information and communication technologies. The purpose of implementing such tools in these organizations is to facilitate the online access of applicants for protection applications to the services provided (Echeverria & Spivey, 2015). In this context, intellectual property organizations must ensure that applicants for protection claims a level of security appropriate to the electronic communications and transactions thus carried out. At the same time, the organization with the field of activity must ensure the implementation of all mechanisms, technologies and all the necessary tools to secure the databases containing the information of the applicants for protection requests.

In organizations engaged in intellectual property, the electronic services abbreviated and e-services represent the provision of certain categories of services using electronic means provided by information and communication technologies and are shown in Figure 1. It is considered

that the implementation of such of services in these organizations will facilitate the access of applicants for protection applications to a variety of applications for search, publication and information in the field of intellectual property.

**Table no. 1:** Database access applications in intellectual property organiations

| | |
|---|---|
| **Aplicațiile de căutare în bazele de date de invenții** | **Ropatent Search**<br><br>**Espacenet,**<br><br>**Patentscope - baze de date ale Oficiului European de Brevete** |
| **Aplicațiile de căutare în baza de date naționale și internaționale de mărci sau desene și modele industriale** | **DesignView, TMview - baze de date ale Oficiului Uniunii Europene pentru Proprietate Intelectuală** |
| **Registrele online de invenții, mărci sau desene și modele industriale**<br><br>**Depunerea electronică a cererilor de înregistrare: brevete de invenție, mărci, desene și modele industriale** | **Patreg**<br><br>**Servicii de on-line filing** |
| **Serviciile de publicarea electronică** | **Buletinele oficiale de proprietate industrială – BOPI** |
| **Serviciile de e-Learning** | **Instruirea on-line în domeniul proprietății intelectuale**<br><br>**WIPO eLearning Center** |

The quality criteria of online services are grouped into five evaluation areas: use, content, management, production, and benefits (Puşcoci, 2009). These online services that organizations engaged in the field of Intellectual Property can make available to the public are summarized in Table 1. The implementation of electronic services has a direct effect on the steps that need to be taken to acquire intellectual property rights by facilitating access to analysis, search, and submission tools, but especially shortening the time required for these operations (Calderon, 2017).

## 2. Database security technologies applicable to organizations in the field of intellectual property

Communications technology has penetrated and produced major transformations in economic, social, and cultural life with the transition from the industrial to the information society. With these technological transformations and developments, more and more cases of cyber-attacks targeting intellectual property, privacy data and the reputation of organizations have been reported (Vacca, 2017).

In this context, information security has become an essential tool for protecting them against potential threats and vulnerabilities and for ensuring business continuity and risk reduction (Sushil, 2013). Thus, there is a permanent problem of implementation at the level of technological organizations to ensure an adequate level of security.

In this context, in IP organizations, security policies together with the mechanisms that ensure the protection of databases from unauthorized access, loss, theft or corruption must be defined, created and implemented, in order to ensure the recovery and continuation of operations in case of disasters. The main security measures at different levels are shown in Figure 2.

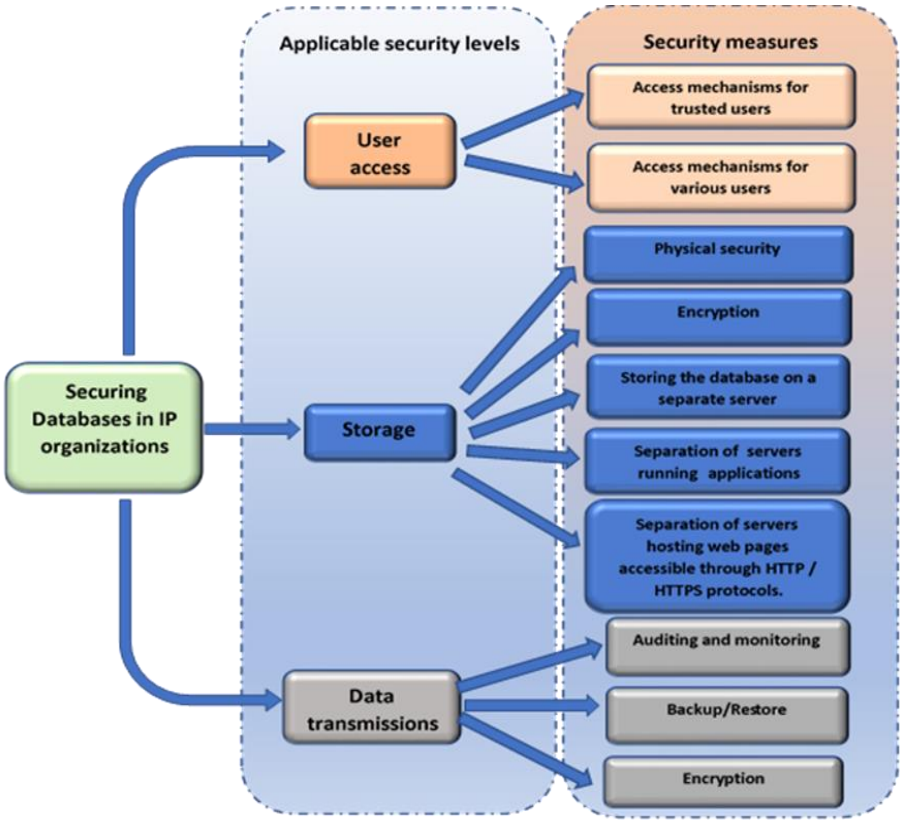


*Figure no. 2. Security levels applicable to databases in intellectual property organizations*

Thus, three main levels are differentiated to which these security measures relate:

a. the level of access of the users;

b. the level of data storage and databases;

c. the level of transmission of information through communication channels.

In this document we will address some of the main technologies for securing databases that IP organizations can implement at the user access level (Carlton, 2008). A database is in a very broad definition, a collection of interrelated information managed as a single entity, thus

there are conceptual differences between different manufacturers that provide such systems (Date, 2003). Regarding the security of databases in IP organizations at the level of user access, we will approach this access from the point of view of the existence of two categories of users (Ben-Natan, 2005). The first category refers to trusted users (database administrators and users with administration rights) and regular users about whom we do not know details about the level of trust we can give (Nag, Arunava , & Dipankar , 2017). One of the measures to secure databases is to define differentiated user access to these systems. In this context, the following access levels can be classified:

a. user access through a security architecture with a single authentication factor;

b. user access through a security architecture with several authentication factors;

c. user access through management systems with security architecture and differentiated access to databases;

d. differentiated access of users to databases through the implementation of encryption technologies;

e. differentiated user access to databases through replicated architectures.

Administrator and user authentication technologies, as well as the interactions of these two categories with databases through the database management systems (DBMS) and the server operating systems on which these databases are stored, are one of the applicable basic levels. to protect access to information systems resources (Guy, 2015). Figure 3 shows the technology for accessing a database for both categories of users through a secure management system with a security architecture with a single authentication factor (account and related password) (Flannery, 2000). The simplest default authentication method works for a local connection based on the operating system user's search. For this type of connection, a user and the corresponding password are transmitted directly to the operating system to verify that the user is legitimate (Connolly & Begg, 2014).

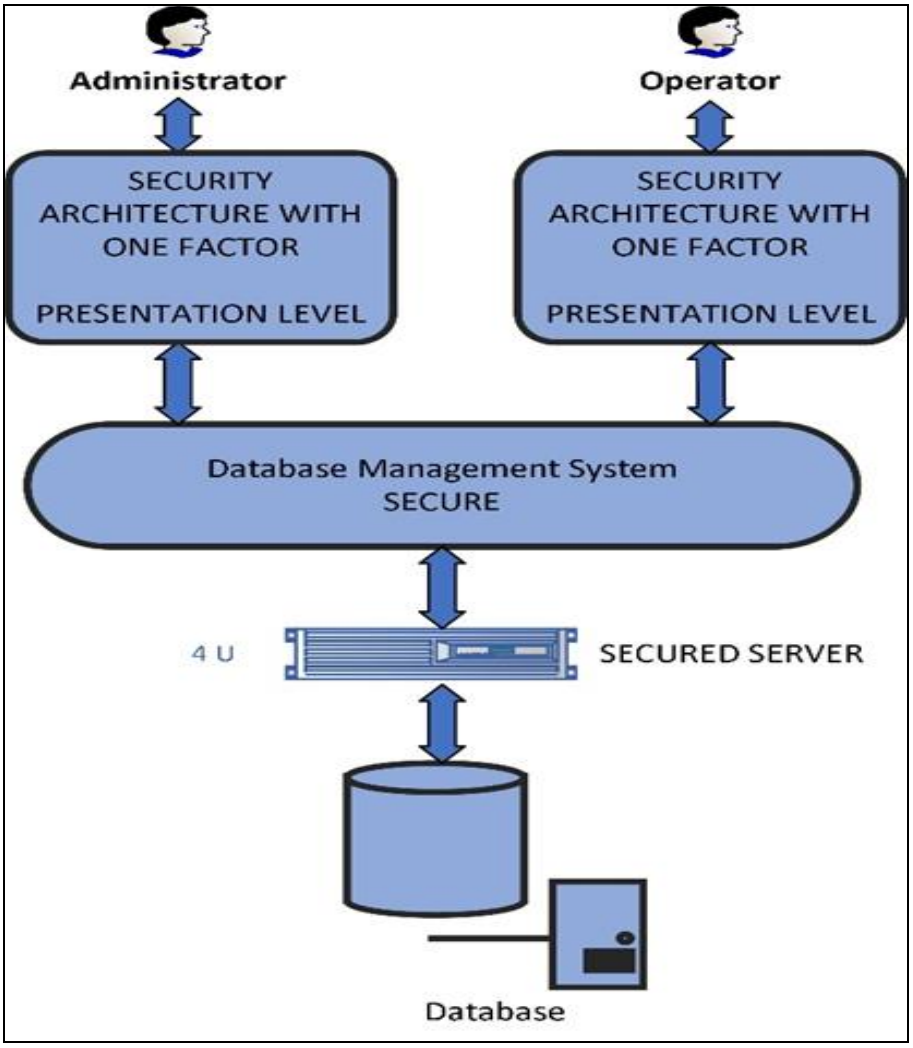


*Figure no. 3. Single-factor security architecture*

In this process, authentication takes place on the server through the security mechanism in place for that configuration (Ramakrishnan & Gehrke, 2002). The default security mechanism is that if a user and password are specified during the login attempt, they are sent to the server and compared to valid server-level combinations to determine if the user has permission to access the instance.

Figure 4 shows the database access technology for both categories of users through a secure management system with a security architecture with multiple authentication factors.

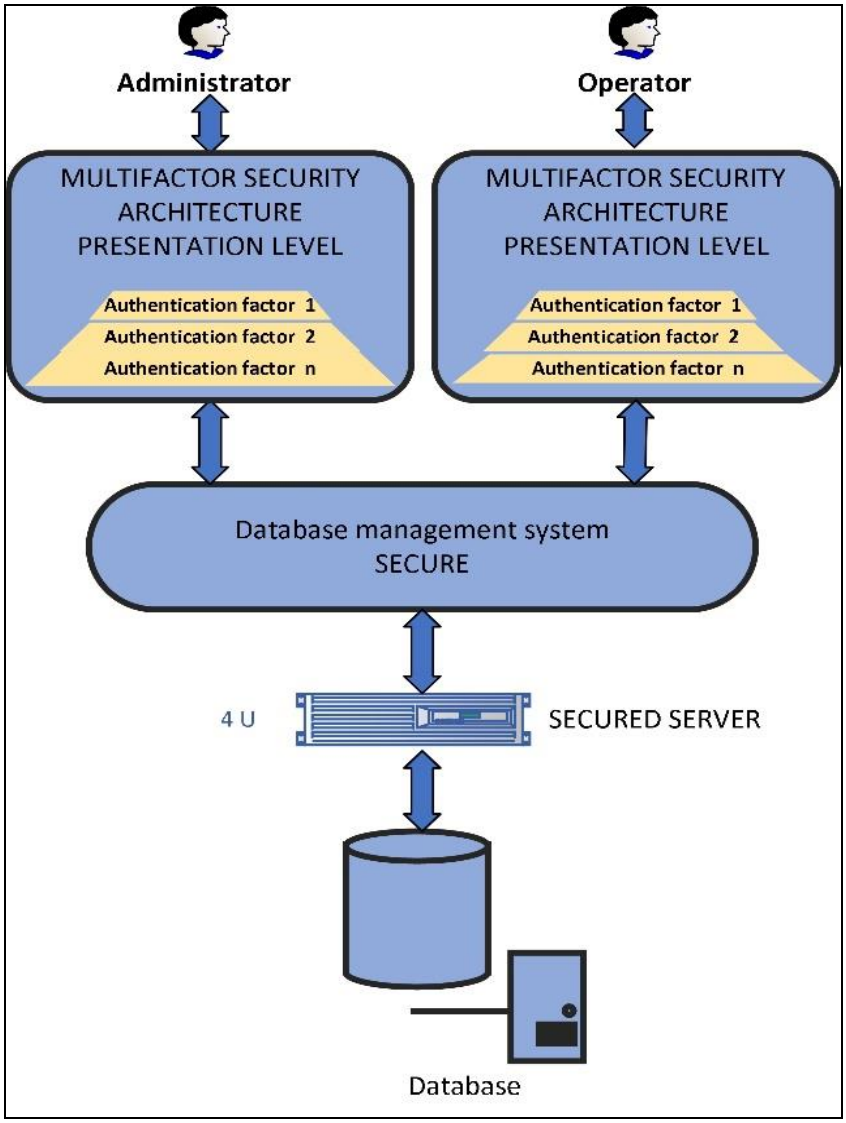


*Figure no. 4. Multi-factor security architecture*

Multi-factor authentication, also called step-by-step verification, is a security process in which the user, in order to authenticate, provides two or more different authentication factors. Thus, this process will help secure access to both user credentials and that user's resources (Jajodia, Database Security XII, 2013).

This access technology is an additional security measure with the advantage that it introduces in the authentication process also reliable elements, such as mobile devices or access to other accounts through which the user's identity is further verified (Libicki & Brian, 2011). There are multiple different services and devices for implementing MFA (Multiple Factors Authentication): from chips, to RFID cards or smartphone applications.

Figure 5 shows database access technology for both categories of use through two management systems with security architecture and differentiated access. Differentiated access is achieved depending on the role of users so there is one level of access for database administrators and another level for user access (Blokdyk, 2017).

In this process, authentication takes place on the server through the security mechanism implemented for that configuration. In this case, the security mechanism is defined as follows: if a username and password are specified during the login attempt, they are sent to the server and compared to valid server-level combinations to determine what level of access each person is entitled to. between those administrators and users (Basta & Zgola, 2012).

Organizations can use encryption to combat threats to their data in databases. Data encryption protects information from disclosure, even if that information is lost or stolen (Natan, 2005).

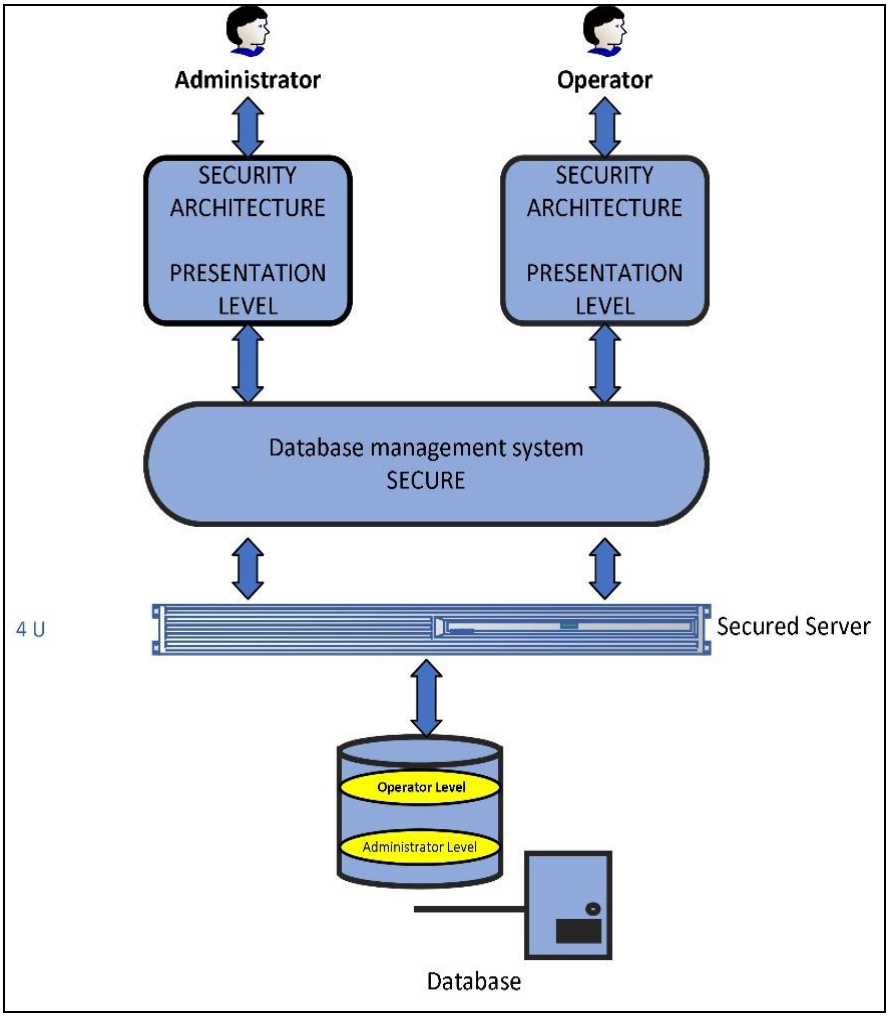


*Figure no. 5. Security architecture with differentiated access level*

Figure 6 shows the database access technology for both categories of users through a management system with insecure architecture, but which has implemented encryption technology to ensure differentiated access to data according to the different rights that each user has (Kenan, 2005). To do this, the administrator can configure the server to encrypt user / password attribute values in either a specific encryption format or a dual encryption mode. Thus, when the encryption configuration is

changed, the existing encrypted passwords remain unchanged so that they can continue to be used in the authentication process (Kemmeand. & Alonso, 1998).

Database replication aims to ensure data synchronization, in order to ensure the best possible availability of data.

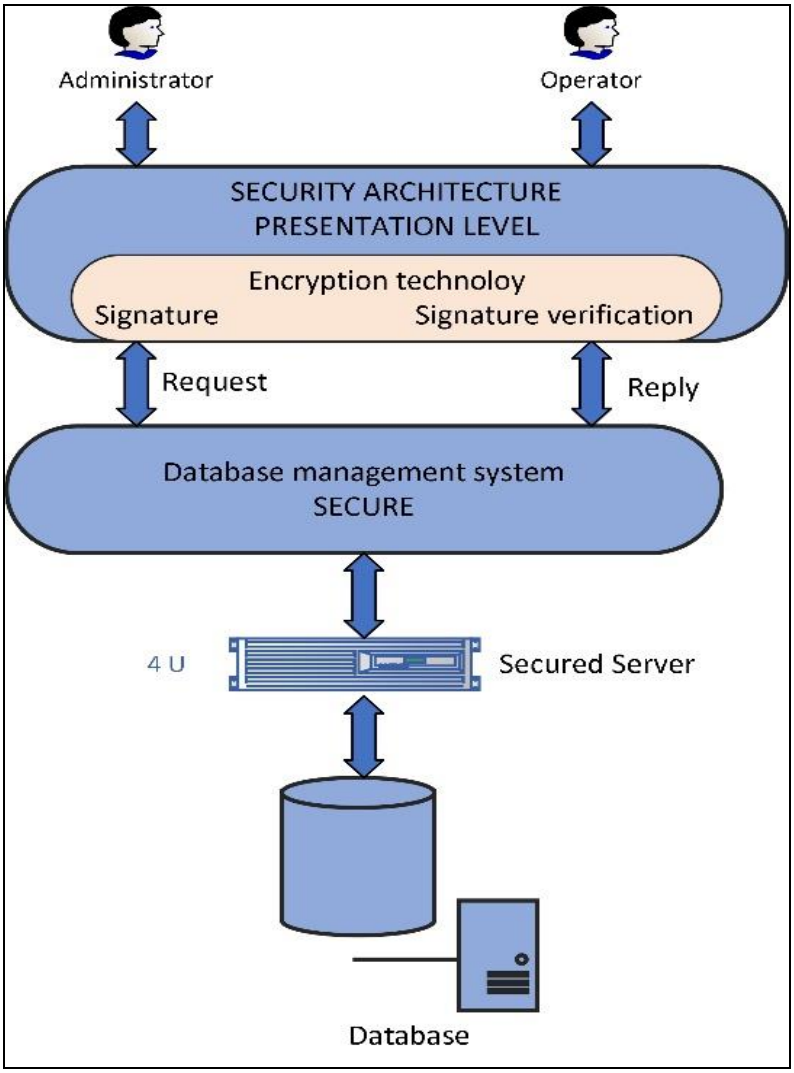


*Figure no. 6. Secure architecture with encryption and differentiated access*

The technology by which the database is accessed through a replicated architecture is presented in Figure 7 (Carter, 2016). The advantage of using such technology is that it allows the segregation of requests from users, so that the database administrator can access through this architecture and the data of operators who have certain restrictions specified in access rights (Défago, Schiper, & Sergent, 1998).

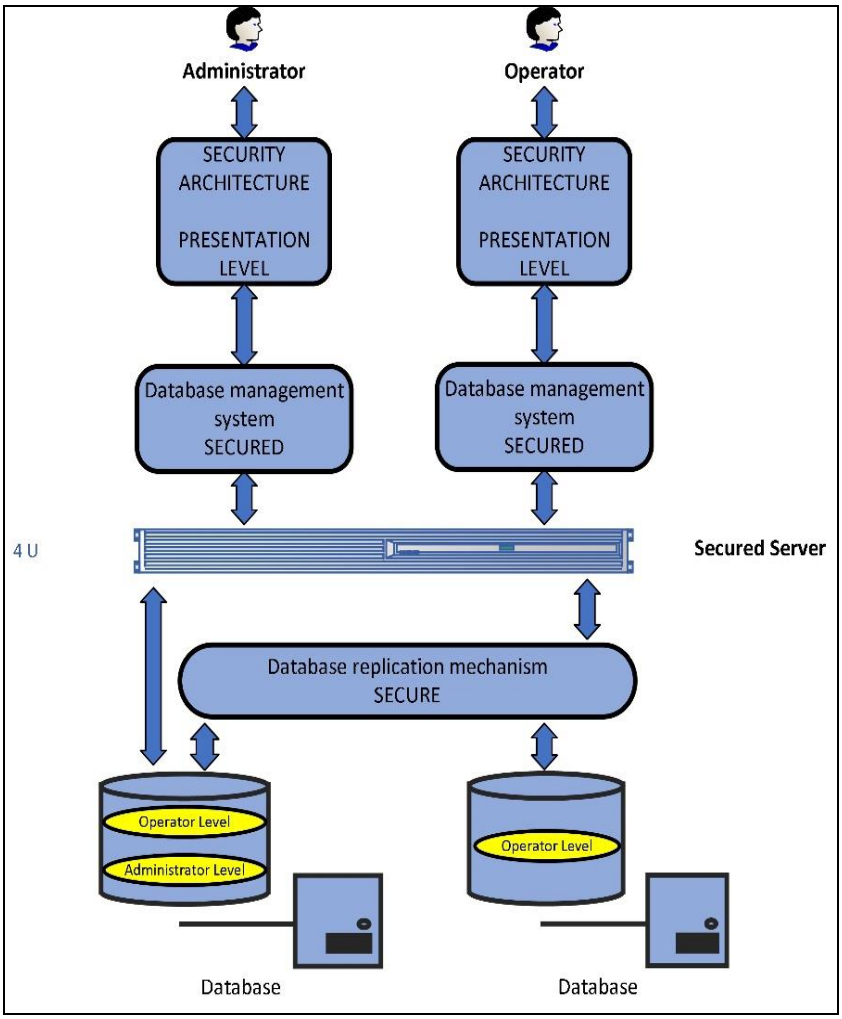


*Figure no. 7. Security architecture with replication technology and application segregation*

As organizations become more and more dependent on the proper functioning of information systems, the issue of the security of these systems and databases becomes more and more important. We can say that, in many cases, a general approach to the problem of database security can bring greater benefits, and the investments and efforts made will be smaller than if the problem is analyzed in time or, in the worst case, is acted upon only to eliminate the effects after a security incident.

## Conclusions

Data and databases are a fundamental resource of intellectual property organizations and, if they are compromised, lost, or stolen, the effects on these organizations can be devastating. Thus, it is considered that the implementation of the latest technologies and systems to ensure the protection of this data, either static or in transit, from unauthorized access becomes a fundamental mission of organizations.

In order to cope with new threats from the new IT environment, organizations need to analyze and implement a complete network security solution tailored to their needs to protect their data and IT resources. Access control strategies should be dynamically adjusted based on the assessment of user confidence. To this end, access control needs to be rebuilt based on adaptive authentication, authorization, and encryption technology. In this context, the analyzed solution must be based on principles such as: authentication and authorization, data confidentiality and perimeter security.

With the technological evolution of the last years and due to the electronic environment of transmission, storage, and management of information in the present century, a century of speed and globalization, the problem of information security is more and more often posed. In order to maintain the highest possible level of individual and social security, given that hardware and software products are constantly evolving, there are human concepts, with vulnerabilities, which can be exploited by certain people by counter methods or reverse engineering, a

growing large amount of data and information require adequate protection and an appropriate level of classification.

Communications and networks, becoming more and more efficient, have expanded the area of users, both in terms of numbers and dispersion in the territory, the entire terrestrial space being accessible to very large networks (Killmeyer, 2006). With the new advances, the area of malicious users has also increased, as well as the variants of computer theft. It can be concluded that the strong integration of systems appears as a consequence of the improvement of the forms of communication and the proliferation of computer networks. In this context, the analysis of risks and vulnerabilities in the IT systems of organizations engaged in the field of Intellectual Property is an essential contribution to increasing the security of these modern communication systems (Buglioni, 2013).

Network security aims to protect them and network applications from attacks. To achieve this, organizations approach network security by creating security policies and, based on them, a network security architecture. This architecture is based on principles such as: access based on the identity of people on the network and the type of access they are allowed, access to network applications, critical data and services, perimeter security, data confidentiality or secure network connectivity.

Finally, as networks grow in size and complexity, it is necessary to use security policy management tools that can centrally manage the security elements mentioned above (Rob, 2017). As different levels of Internet connectivity become essential for maintaining the competitiveness of organizations, ensuring the security of network infrastructure becomes an essential requirement (Abel, 2007). Organizations need to analyze and implement a complete network security solution tailored to their needs to protect their data and IT resources. The solution must be based on principles such as: authentication and authorization, data confidentiality and perimeter security.

In this regard, in recent years, European states have given high priority to cybersecurity, believing that improving cyber resilience in general, achieving a better level of cybersecurity in the EU will still remain a colossal and difficult task to implement. Thus, strengthening the security

of the Internet and other critical IT networks and systems is becoming one of the main targets to be achieved by EU countries. In order to form a community of cybersecurity expertise, the EU is considering setting up a European Industrial, Technological and Research Center for cybersecurity. This center will bring together key European stakeholders, including industry, academic and research institutions, and other relevant civil society associations, to form a community of expertise on cyber-security (Promovarea rezilienței cibernetice, 2021).

## References


Abel, J. (2007). Oracle E-Business Suite Security. Oracle Press.

Basta, A., & Zgola, M. (2012). *Database Security 1st Edition.* Cengage Learning; 1st edition.

Ben-Natan, R. (2005). *Implementing database security and auditing.* Digital Press; 1st edition.

Blokdyk, G. (2017). *Multi-factor Authentication.* CreateSpace Independent Publishing Platform.

Buglioni, E. F. (2013). *Designing Secure Architectures Using Software Patterns.* John Wiley & Sons Inc.

Calderon, P. (2017). *Nmap: Network Exploration and Security Auditing Cookbook.*

Carlton, D. (2008). *Administering Informix Dynamic Server.* MC Press.

Carter, P. (2016). *Securing SQL Server: DBAs Defending the Database.* Apress.

Connolly, T., & Begg, C. (2014). *Database Systems: A Practical Approach to Design, Implementation, and Management, Global Edition.* Pearson Education Limited.

Date, C. J. (2003). *Introduction to Database Systems.* Pearson Education Inc.

Défago, X., Schiper, A., & Sergent, N. (1998). *Semi-passive replication.* Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems (SRDS).

Echeverria, J., & Spivey, B. (2015). *Hadoop Security: Protecting Your Big Data Platform.*

Flannery, R. (2000). *The Informix Handbook*. Informix Press.

Gertz, M. (2007). *Handbook of Database Security*.

Guy, H. (2015). *Next Generation Databases*. Apress.

Jajodia, S. (1999). *Database Security XII*. Kluwer Academic Publishers.

Jajodia, S. (2013). *Database Security XII*. Springer US.

Kemmeand., B., & Alonso, G. (1998). *A suite of database replication protocols based on group communication primitives*. Amsterdam: Proceedings of the 18th Internationnal Conference on Distributed Computing Systems.

Kenan, K. (2005). *Cryptography in the Database: The Last Line of Defense*. Symantec Press.

Killmeyer, J. (2006). *Information Security Architecture*. Auerbach Publications.

Kiser, Q. (2020). *Computer Networking and Cybersecurity*. Franelty Publications.

Libicki, M., & Brian, J. (2011). *Influences on the Adoption of Multifactor Authentication*. Homeland security and defense center.

Nag, A., Arunava , R., & Dipankar , D. (2017). *Advances in User Authentication*. Springer.

Natan, R. (2005). *Implementing Database Security and Auditing*. Digital Press; 1st edition.

*Promovarea rezilienței cibernetice*. (2021, April 20). Retrieved from https://www.consilium.europa.eu/ro/policies/cybersecurity/

Puşcoci, S. (2009). *Servicii electronice de asistenţă la domiciliu*. Revista Telecomunicaţii.

Ramakrishnan, R., & Gehrke, J. (2002). *Database Management Systems*. McGraw-Hill Education – Europe.

Razvan Dinca, V. R.-V. (2018). *Proprietate intelectuală*. C.H. Beck.

Rob, A. (2017). *Cybersecurity: A Business Solution: An Executive Perspective on Managing Cyber Risk*. Threat Sketch.

Vacca, J. (2017). *Computer and Information Security Handbook*. Morgan Kaufmann.