Chapter 8
Print ISBN: 978-93-5547-447-6, eBook ISBN: 978-93-5547-455-1

Determining the Role of Information Security in Enterprise Resources Planning Systems

Radoslav Hrischev [a*]

DOI: 10.9734/bpi/ist/v7/1953B

ABSTRACT

This article analyzes and describes the role of information security in Enterprise Resource Planning (ERP) systems. These systems integrate information flows in business organizations. Therefore, information security is an important requirement for the effective functioning of ERP systems. The author defines the methods for ensuring the protection of information in ERP systems and illustrates them with examples. Most of the largest ERP developers have already implemented specialized hardware and software solutions for guaranteed information security. The new cloud ERP systems with e-business and e-government functionalities require new solutions. Directions for developing information security in the light of new technologies are proposed.

Keywords: ERP systems; information security; security policy.

1. INTRODUCTION

Enterprise Resource Planning (ERP) is a type of business management software that plans an organization's resources and manages the majority of its business processes. ERP systems are used in various types of organizations. It was first defined by the Gartner Group in 1990 as the next generation of Manufacturing Business System and Manufacturing Resource Planning software [1].

ERP has progressed from a precondition to a requirement for successful business development. Without an effective integrated information system, mass production with low added value is impossible. An ERP system is a tool for rapid and effective business reengineering, optimization of operations, and generation of benefits.

The goal of the article is to prepare an overview of the status of the ERP technology and the security risk for information exchange in ERP systems. It will be explained the evolution of ERP, its key components – internal and external modules, evolution from a security point of view, and the perspective of development. There are many studies on this topic, but the fast growth of developers of ERP systems and new information technology requires new approaches to information security. The examples considered are from the biggest developers of ERP systems SAP, Oracle, and IBM, where data security is implemented as a standard important part (software and hardware) of the systems.

2. ENTERPRISE RESOURCES PLANNING SYSTEMS AS CORE OF THE ADVANCED BUSINESS FUNCTIONALITY

The ERP system covered all information flow in the organization. It has represented the highest level of information systems. At the base of ERP systems is a client-server technology. Most popular ERP systems now are centralized information systems.

The spread of ERP systems has grown significantly over the years. First systems were developed locally for simple separated business functions such as accounting, controlling, planning, warehouses

[a] *Technical University–Sofia, Branch Plovdiv, 25 Tzanko Djustabanov Str., 4000 Plovdiv, Bulgaria.*
**Corresponding author: E-mail: hrischev@tu-plovdiv.bg;*

management, and human resources planning [2]. The next step started when companies such as Oracle, IBM, SAP, and Baan developed a set of typical modules developed as applications of ERP systems, intended to manage the main parts of the business. The web service is a technology with a serious impact on ERP systems. New systems used secured web-based databases and applications. This technology provided an opportunity to use the Internet as environment for data transmission and storage. Modern ERP systems are cloud-based ERP systems such as SAR S/4 HANA. They integrate the results of new technologies – Cloud computing, IoT, Big data.

All ERP systems included some core functionalities, realized in similar applications - modules. The modules have a different name, but the functionality is the same. These functionalities are presented in the following modules: Financial Management /FI and CO modules in SAP/; Human Resource Management /HCM in SAP/; Manufacturing Management /MES or MAP modules/; Sales, Distribution, and Logistics Management /SD module in SAP/; Customer Relationship Management (CRM); Product Lifecycle Management /PP in SAP/; Supplier Relationship Management (MM in SAP); Business Intelligence /BI/; Supply Chain Management (SCM). The SCM includes business processes, part of CRM, SRM, MES, PP modules. Idea is that these business processes must be connected in enterprise to be granted the business success of the supply chain [3]. These functionalities are interorganizational, communication, and data exchange are internally in the company.

The new e-business requires the development and implementation of e-commerce modules of ERP (e-orders, e-shop, e-store, e-invoice, etc.), focusing on business between companies and customers. The basis of e-business is an electronic way to exchange business information (documents) Electronic Data Interchange /EDI/. Therefore, new external information exchange modules also set new requirements for information security. Depending on the stage of growing, requirements for security also growing.

Historically, in an enterprise, some systems have been developed by the local enterprise IT team itself in the first stage. In the next step growing most of the applications were developed from different external vendors using different databases, languages, and technologies may develop others. All systems have to work together. Systems differ from each other, making it difficult to effectively upgrade the organization's business, strategy, and information technology. Also, applications need ongoing support from different suppliers.

ERP systems are using common standards for communication infrastructure, application, database, data exchange, and security. Specialized standards for ensuring information security are also being developed [4]. How many and what modules will be implemented in the organization depends mainly on the goal set for the realization, the vision of the leadership, the budget, and the available resources of the organization. ERP has no alternative in enterprise but must meet the special requirements [5] – modularity, integrality, flexibility and scalability, profitability. ERP should lead to cost reductions and increased profits, as these are the basic requirements for the organization's existence and the goal of implementing the system.

Information security is the main requirement for ERP systems. Regardless of the quantity and types of modules implemented, the amount and way of information exchange, the system must ensure that information is fully protected.

To realize this requirement, the vendors are using special methods of information security, starting from the architecture of systems, methods of data transfer, databases, management of data access, and security policy.

3. INFORMATION SECURITY IN ERP SYSTEMS

ERP systems are used not only in business – production, and commerce but also in other branches, where information security is critical, such as medicine, finance, defense [6]. The first step of ensuring information security begins with the development of a sustainable model [7] beginning with the architecture of the systems.

3.1 Architecture of ERP Systems

The ERP system is based on the architecture client-server to distribute by level information processing. Most vendors distributed information processing in three logical layers – Presentation for user connect, Application for data processing, and Database for the data repository.

The three main levels have related each other by communication lines and platform, providing access only to services and information only for authorized people, devices, and processes. For example, SAP Net Weaver is an information communication server for SAP R/3 [8]. Fig. 1 is presented the layers' structure of the SAP R/3.

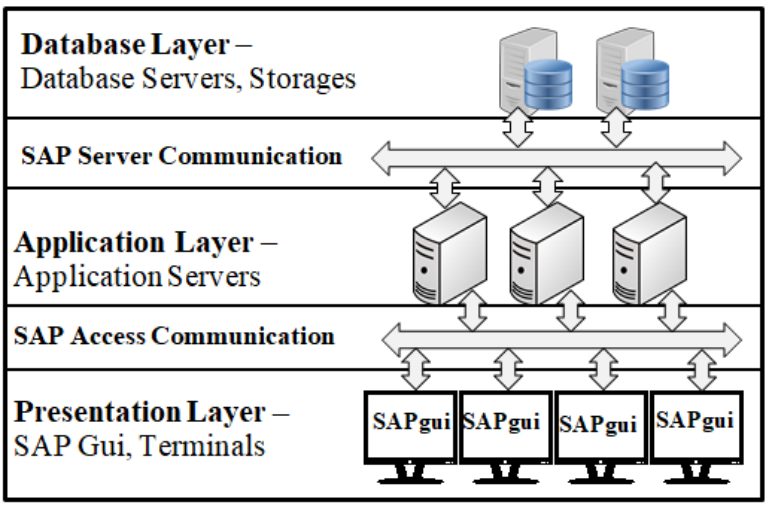

Fig. 1. Three layers architecture of SAP R/3 [6]

On Presentation Layer (Front End) are remote terminal /hardware or virtual/ with Graphical User Interface (GUI) on desktops or browser that collects input data, transfer information to next layers, generate requests, and returns the results of data processing to the user or machine.

On Application Layer are presented application software which collects the requests from the Presentation layer and processes the requests based on the business algorithms and functions.

On Database Layer is Database Management Service that manages the business and operational information. There is stored also information about user access to this information, all operations for every user and service, defined on relevant security policies. This layer included local or cloud-based servers and storage of data.

3.2 Secure Data Transfer

The first ERP systems worked in a closed network and the most used security technology was isolation and segmentation of the network. The biggest companies were used leased optical lines. But leased lines are very expensive. Also, with the development of web-based ERP systems began using modern methods for information protection such as IPsec (Internet Protocol Security).

IPsec, also known as IP Security protocol, provided security service for information exchange over IP networks. IPsec is used to provide secured data transfer in ERP systems using technology such as IP tunneling. This means that all data being exchanged between two points is encrypted by special protocols. Tunneling means establishing a Virtual Private Network (VPN) connection. The ERP systems are using often public wireless networks for data transfer and VPN technology is a perfect way for secured data transfer over wireless networks.

E-business modules are also using security protocols Secure Socket Layer (SSL) and Secure Hypertext Transfer Protocol (SHTTP) to be granted security of document exchange between customers and web-based ERP services over the public Internet.

The ERP vendors are developing and implementing more and more strict solutions to improve information security, but also specialized companies are developing software and hardware information security solutions. The most used solutions are the Citrix [9] applications. This company developing a full range of information security solutions. Citrix is a software company that develops virtualization technology for desktops, servers and applications, and cloud computing.

An ERP system collects information from terminals, GUI of users, specialized devices and cannot secure the system by limiting access. Therefore, the best way to increase security level is using of Citrix infrastructure between the users and the ERP system – Fig. 2.

In this case, users are using the Citrix app for the Internet browser to access ERP. They need just additional authentication by user and password. After authentication the users are working on their virtual desktop, no matter the type of access device – PC, terminal, mobile, tablet, and Operation System – Windows, iOS, Android, Linux, etc. Citrix infrastructure included a secured network, using a gateway, and the whole range of IT controllers, services, and servers. Citrix also supports server virtualization. At the moment more than 100 million users using Citrix services.

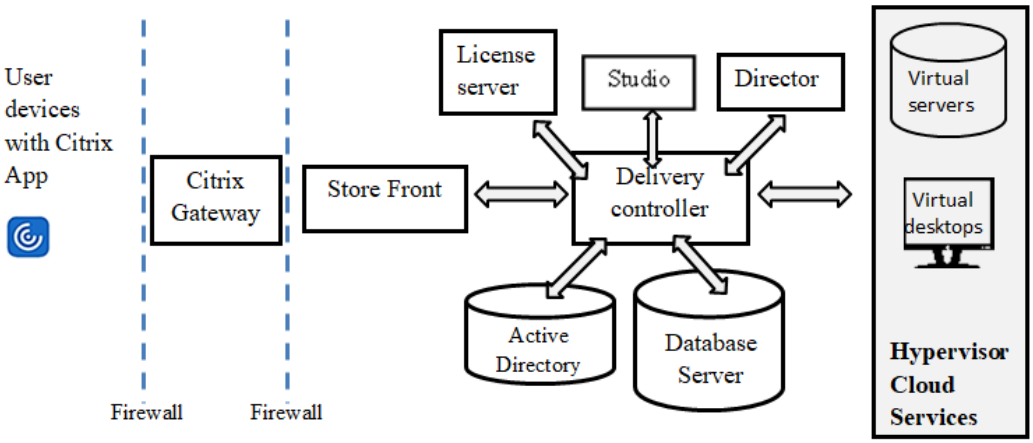

Fig. 2. Typical CITRIX infrastructure for ERP

A lot of companies are developing hardware for secure data transfer directly to ERP systems. For example, the company Lantronix [8] offers a wide range of devices and services to provide secure data transfer to control systems.

3.3 Database of ERP Systems

All ERP systems currently are using centralized databases, located on the Database layer – Fig. 1. The database is a collection of data. The organization of the data follows a particular model. According to the model, two types of databases can be described - relational and non-relational. Most of the ERP systems are using relational SQL /Structured Query Language/ databases. Most are used Microsoft SQL Server and Oracle DB.

NoSQL databases appeared in the early 21st century. They appeared to solve the need to manage large volumes of information in modern web and mobile applications. NoSQL databases are used for big-data and online working web applications. Therefore, new versions of ERP systems are using NoSQL databases, SAP HANA, for example.

Now biggest vendors of ERP systems SAP [8,10] and IBM [11] are working on the implementation of new databases based on blockchain technology. A blockchain is a series of matrices containing encrypted information in the form of records called blocks connected. The blocks form a dynamic and distributed database. The database is decentralized and secure because each block contains an encrypted address of the previous block and transaction data – Fig. 3. In its organization, this technology is strikingly like the sequential databases used in the first process management systems.

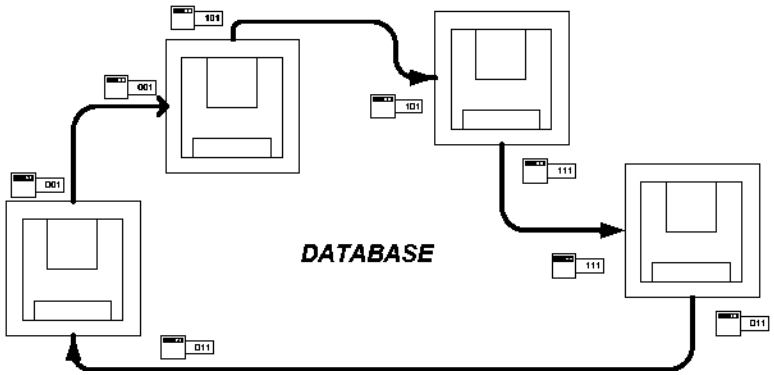

Fig. 3. Illustration of new database using blockchain technology

By design, a blockchain is resistant to modification of the data and provides an opportunity to build a high-level security database. Blockchain technology could be the future of the database organization of ERP systems [12]. Blockchain is transforming supply chain management (SCM), delivering confidence and transparency in the process [13]. Blockchain technology is solving trust issues inside and between companies [14]. For the using this technology in human resources (HR) management, new legal regulations are needed.

3.4 Security policy

The conception of confidentiality is the main point of security policy, and access control to information and data flow consists of the following separated elements:

- Every user has access just to this part of the information, which he has to know for his daily work.
- Level of sharing information has to be strictly defined depending on functionality, described in communication between modules.
- The information, shared between users, departments, organizations, must be trusted.
- An information must be modified just by authorized users, services, applications, and the result of this modification has to be visible just for authorized users.
- During transmission in communication network information should not be changed.
- If concrete implementation included e-modules, information must be encrypted and decrypted only by an authorized user.

These securities policies are realized using different methods of user authentication and authorization. Most ERP systems are using Role-Based Access Control services [8]. This service granted access to information just to be authorized users with relevant permissions, grouped by their role in the organization. Role-Based Access Control (RBAC) includes the following elements – users, roles, permissions, administration.

- Users. A user is a person, service, application, who has access to relevant of him functions in organization information.
- Roles. The role is a described job function within the organization.
- Permissions. Permission is granted access to part of information, service, or application in the system.

- Administrator. The administrator is a user, responsible for granting access of users to this information, described on the table of responsibility. A table of responsibilities is a list or matrix distributing the permissions of users by roles in the business process.

The realization of the granted permissions (rights) is possible through a process of authorization. The authorization process is an important part of security and is different for most vendors. For example, the authorization process in SAP R/3 includes the following components - authorization administration, authorization object, authorization fields, authorization profile, authorization check, user master record, which enables the users to log on to the system and grant limited permissions access to the information.

For authorization in e-business, modules are using also digital signature and security certificates. A digital signature is an e-signature authenticated using encryption and ensures the authenticity of the information. The security certificate is a unique digital ID used for verification of users or services, requesting access to information.

The considered methods for information security have proven over time and guaranteed the smooth functioning of information systems and business as result.

4. THE FUTURE OF ERP SYSTEMS AND INFORMATION SECURITY

The process of development of the ERP systems is not an end in itself, it is conditioned by intensive business growth and the requirement for more manageability and predictability of business performance.

Today ERP is becoming the basis for business management in various sectors and conditions for the existence of many organizations. Therefore, the security of information going to be of utmost importance.

The future ERP systems depend on three main factors - business growth and benefit generation, implementation of the new modern technologies, and provision of information security. With sufficient confidence we can expect an evolution in the following directions:

- Intensive development of the modules, oriented to e-business and e-government.
- Collaboration between core ERP modules and e-commerce.
- The ERP systems will be Internet-based. This means that not just databases will be cloud-based, but also applications will be placed on the Web.
- Network connectivity will go to wireless data exchange as a result of the implementation of new fast-speed Wi-Fi networks – 5G, for example.
- The ERP will be more and more intelligent. In the future, ERP will include more components for business analysis and decision-making. Elements of AI /Artificial Intelligence/ will be integrated into ERP.

5. CONCLUSION

Enterprise Resource Planning is the technology that reforming business, its condition for economy growing and impact to more and more people and organization. Information security has been a goal for system developers from the beginning, but implementation in newer, sometimes critical areas, also puts new requirements to security. We need a new approach, new security technology, new solutions, new tools to grant the security of the systems.

Existing security solutions are based on the features of the implemented currently ERP system, but e-business, the implementation of new e-modules make systems more open, and existing solutions for information security will become more scarce and systems more vulnerable. The companies, generating more profits will become increasingly subject to cyberattacks.

The ERP systems vendor and companies specializing in developing new security systems must look for:

- New design of the ERP architecture granted information security.
- New security policy and authentication and authorization methods in an open environment.
- Systems and devices protect the data transfer in web-based services.

The role of public authorities should also be more proactive in developing adequate legislation to ensure the effective protection of information.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Bakry A, Bakry S. Enterprise resource planning – a review and a STOPE view (Riyadh: International Journal of Network Management. 2005;15:363-370.
2. Goldston J. The Evolution of ERP Systems: A Literature Review (International Journal of Research Publications. 2020;50(1):122-142.
3. Banerjee A. Blockchain Technology: Supply Chain Insights from ERP (Amsterdam, Elsevier: Advances in Computers. 2018;111:69-98.
4. Fonseca-Herrera OA, Rojas AE, Florez H. A model of an information security management system based on NTC-ISO/IEC 27001 standard. (IAENG International Journal of Computer Science). 2021 Jun 1;48(2):213-22.
5. Hrischev R. Planning and implementation of the ERP system in packaging production, (Plovdiv, Journal Fundamental Sciences and Applications. 2018;24:25-28.
6. Scheel H. U.S DOD - Achieve ERP success in Federal Government (In book: The Complete Business Process Handbook, Volume 3) Publisher: Morgan Kaufmann; June 2013.
7. Behara R, Huang C, Hu Q. A System Dynamics Model of Information Security Investments. ECIS Proceedings. 2007;177.
8. SAP.
   Available:https://help.sap.com/
9. CITRIX.
   Available:https://www.citrix.com
10. Lantronix.
    Available:https://www.lantronix.com
11. Thuraisingham B. Database and Applications Security (Integrating Information Security and Data Management). 2005;2-19.
12. Wei S, Bhavani T. Security for Enterprise Resource Planning Systems (Dallas: Information Systems Security. 2007;16:152–16.
13. IBM Blockchain Services and Consulting. IBM; 2021.
    Available:https://www.ibm.com/blockchain/services
14. Forrester. Emerging Technology Projection: The Total Economic Impact Of IBM Blockchain, Study commissioned by IBM; 2018.

Biography of author(s)

Radoslav Hrischev
Technical University–Sofia, Branch Plovdiv, 25 Tzanko Djustabanov Str., 4000 Plovdiv, Bulgaria.

He is a lecturer at the Technical University - Sofia, Plovdiv branch, Bulgaria, and is also a part-time researcher at the Center for Competence Intelligent Mechatronic Systems and Technologies, Plovdiv. He received his PhD in Control Systems from the Moscow University of Civil Engineering and Architecture, Russia in 1992. He works as a developer and implementer of control systems in various fields. For more than 20 years he has worked as an IT manager for international companies and is responsible for the implementation of ERP systems, especially SAP. His research interests are information systems in industry and information security.

DISCLAIMER
This chapter is an extended version of the article published by the same author(s) in the following journal.
IOP Conference Series: Materials Science and Engineering, 878(012009), 2020.