

# ERP Systems and Data Security

**Radoslav Hrishev**

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

hrishev@tu-plovdiv.bg

**Abstract.** Enterprise Resource Planning (ERP) integrates all business processes in the organization. Therefore, data security is the main point of security in ERP systems. Most of the biggest ERP developers have already implemented specialized hardware and software security solutions. New ITC technologies – cloud computing, IoT, blockchain are opportunities to make the ERP highly integrated, more intelligent, more flexible, cloud based. The fast growing of the e-business is making ERP systems more open and new decisions are needed to be granted information security. This paper introduces ERP technology regarding the data security point of view. New security solutions for ERP systems are present.

## 1. Introduction

Enterprise Resource Planning is a business management software by planning the resources of an organization and covering most of business processes. ERP systems are implemented in different types of organizations. The Gartner Group first defined it in 1990 as the next generation of Manufacturing Business System and Manufacturing Resource Planning software [1]. Today, ERP has become from precondition to necessary requirement for successful business development. The mass production with low added value is impossible without effective ERP system.

With ERP, an enterprise can automate its core business applications, reduce the complexity and the cost of the integration. ERP system is a tool for fast 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 system. 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 study on this topic, but the fast grown 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 and IBM, where data security is implemented as standard important part (software and hardware) of the systems.

## 2. Overview of ERP technology

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 populate ERP systems at the moment 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 management and human resources planning. The next step started when companies such as Oracle, IBM, SAP, and Baan developed a set of typical modules, which are developed as applications of ERP

systems, intended to manage of main parts of business. The web service is a technology with a serious impact to ERP systems. New systems used secured web-based databases and applications. This technology provided opportunity to use Internet as environment for the data transmission and storage. Modern ERP systems are cloud-based ERP systems such as SAR S/4 HANA. They integrated a result of new technology – Cloud computing, IoT, Big data.

All ERP systems included some core functionalities, realized in similar applications - modules. The modules have a different name, but functionality is the same. These functionalities are presented in 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 have to be connected in enterprise to be granted business success of the supply chain [2].

These functionalities are inter-organizational, communication and data exchange is internally in the company.

The new e-business requires the development and implementation of an e-commerce modules of ERP (e-orders, e-shop, e-store, e-invoice, etc.), focuses 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 data security. Depending on the stage of growing, requirements for security also growing.

Historically, in an enterprise, on the first stage some systems have been developed by the enterprise IT team itself. On next step growing most of applications was 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. 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 organization. ERP have no alternative in enterprise, but must meet the special requirements [3] – 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.

Data security is a 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 architecture of systems, methods of data transfer, data access, databases. Implements a set of security policy.

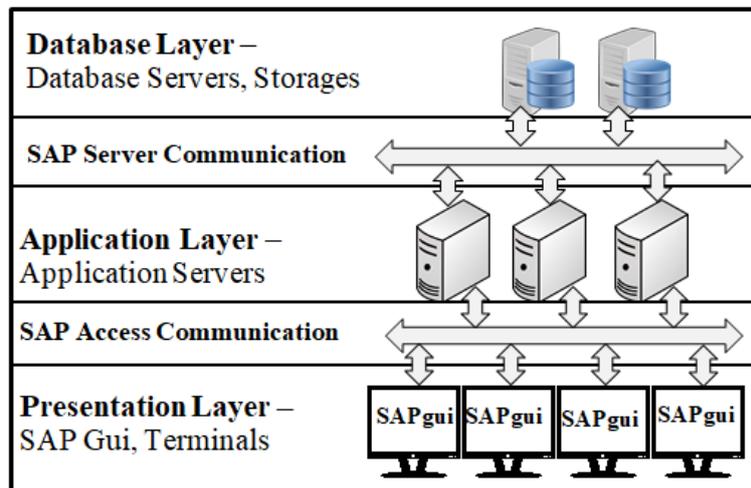
### **3. Information security in ERP**

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, defence. First step of ensuring information security begins with the development of a sustainable model beginning with architecture of the systems.

#### *3.1. Three-layer 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 data repository. The three main levels

are related each other by communication lines and platform, provided access only to services and information only for authorized people, devices and processes. For example, SAP Net Weaver is information communication server for SAP R/3 [4]. On Figure1 is presented layers' structure of the SAP [4].



**Figure 1.** Layers architecture of SAP R/3.

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, generates requests, and returns the results of data processing to the user or machine.

On Application Layer are presented application software which collect the requests from the Presentation layer and process 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. Security policy for ERP systems

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

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

These securities policies are realized using different methods of user authentication and authorization.

Most of ERP systems are using Role-Based Access Control services [6]. This service granted access to information just to be authorized users with relevant permissions, grouped by his role in

organization. Role-Based Access Control (RBAC) includes the following elements – users, roles, permissions, administration.

- Users. The user is a person, service, application, who have access to relevant of him functions in organization information.
- Roles. The role is a described job function within the organization.
- Permissions. Permission is the 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. Table of responsibility 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 of vendors. For example, the authorization process in SAP R/3 includes of the following components - authorization administration, authorization object, authorization fields, authorization profile, authorization check, user master record, which enables the users to log on to system and grant limited from permissions access to the information.

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

### *3.3. Methods for secure data transfer in ERP systems*

The first ERP systems worked in a closed networks and the most used security technology was isolation and segmentation of the network. For 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).

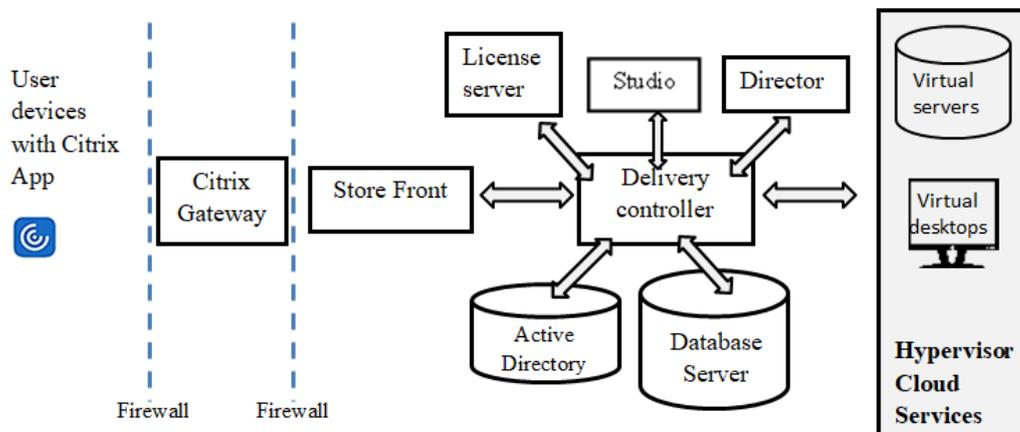
IPsec, also known as IP Security protocol, provided a security services for information exchange over IP networks. IPsec is used to provide secured data transfer in ERP systems using technology as IP tunneling. This mean that all data being exchange between two points encrypted by special protocols. Tunneling mean an establish 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 using also 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 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 commonly used solutions are the Citrix [5] applications. This company developing a full range of information security solutions. Citrix is software company that developing virtualization technology for desktops, servers and applications and cloud computing.

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

In this case users are using Citrix app for Internet browser to access ERP. They need just additional authentication by user and password. After authentication the users are working on own virtual desktop, no matter the type of access device – PC, terminal, mobile, tablet and Operation System – Windows, iOS, Android, Linux, etc. Citrix infrastructure included secured network, using 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.



**Figure2.** Typical CITRIX infrastructure for ERP.

A lot of companies are developing hardware for secure data transfer directly to ERP systems. For example, company Lantronix [10] offers a wide range of devices and services to provide secure data transfer to control systems.

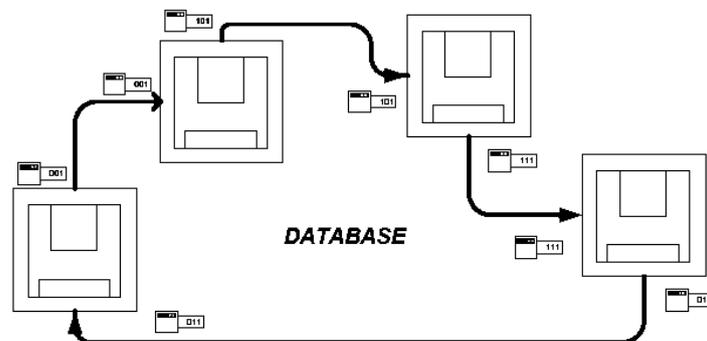
### 3.4. Database of ERP systems

All ERP systems currently are using centralized databases, located on the Database layer – figure1. 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. Mostly 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.

At the moment biggest vendors of ERP systems SAP [4] and IBM [8] 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 to each other. 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 – Figure 3. In its organization, this technology is strikingly similar to the sequential databases used in the first process management systems. By design, a blockchain is resistant to modification of the data and provides an opportunity to build a high-level security database.



**Figure3.** Illustration of new database using blockchain technology.

Blockchain is more than technology. It is a movement to help redefine most important business relationships through trust, transparency and new-found collaboration. It could be the future of the database organization of ERP systems [9]. Blockchain is transforming supply chain management (SCM), deliver confidence and transparency in the process. Blockchain technology is solving trust issues inside and between companies. For the entry of this technology into human resources (HR) management, for example, new legal regulations are needed.

#### **4. A future of ERP systems and information security**

The development and implementation of ERP systems that started more than 30 years ago began with mainframe (local PC) structure systems and reached integration with the cloud-based technologies. But the process of development of the ERP systems is not an end in itself, it is conditioned by intensive business growing and the requirement for more manageability and predictability of business performance.

Today ERP is becoming the basis for business management in various sectors and condition for the existence of many organizations. The ERP systems are requirements to benefit generation for the business. Therefore, the security of information going to be of utmost importance.

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

- Intensive developing of the modules, oriented to e-business.
- Collaboration between core ERP modules and e-commerce.
- The ERP systems will be Internet based. This mean that no 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 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 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 solution for information security will become more scarce and systems more vulnerable. The companies, generating more profits will become increasingly subject to cyberattack.

The ERP systems vendor and companies specializing in developing of new security systems have to 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, protected the data transfer in web based services.

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

### **Acknowledgements**

The author/s would like to thank the Research and Development Sector at the Technical University of Sofia for the financial support.

### **References**

- [1] Bakry A and Bakry S 2005 *Enterprise resource planning – a review and a STOPE view* (Riyadh: International Journal of Network Management 15) p 363-370
- [2] Banerjee A 2018 *Blockchain Technology: Supply Chain Insights from ERP* (Amsterdam, Elsevier: Advances in Computers, Volume 111) p 69-98
- [3] Hrishev R 2018 *Planning and implementation of the ERP system in packaging production* (Plovdiv: Seventh International Scientific Conference TECHSYS
- [4] SAP official site <https://help.sap.com/>
- [5] CITRIX official site <https://www.citrix.com/>
- [6] Wei S and Bhavani T 2007 *Security for Enterprise Resource Planning Systems* (Dallas: Information Systems Security 16) p 152–163
- [7] Thuraisingham B 2005 *Database and Applications Security* (Integrating Information Security and Data Management) p 2-19.
- [8] IBM official site <https://www.ibm.com/blockchain>
- [9] Forrester 2018 Emerging Technology Projection: *The Total Economic Impact™ Of IBM Blockchain*, Study commissioned by IBM.
- [10] Lantronix official site <https://www.lantronix.com/>