

Business Role Security in Enterprise Resource Planning System

Shailesh Birthare^{1*}, Surabhi Tripathi²

^{1,2}Student, Department of Computer Science and Engineering, Maharana Pratap College of Technology, Gwalior, India

*Corresponding author: shbirthare2@gmail.com

Abstract: Enterprise Resource Planning, a collective integrated approach for all business solutions, has been broadly accepted across various industries since 1990 as the upcoming generation of Manufacturing Business System and Manufacturing Resource Planning software. ERP can be taken as to be “the cost of entry for running and growing a business” (Kumar and van Hillegersberg, 2000). An ERP is an information system, which seamlessly integrated and configured for planning, execution and managing all the resources and their maximum use in the enterprise, and streamlines and incorporates the business threads within and across the functional or technical boundaries in the enterprises. With the use of such information system, an organization can automate its elementary business requirements by reducing the complexity and cost of the related integrations for its components. Enterprise may also apply business process reengineering for optimum utilization of its ERP system, and finally output as growth in business can be recorded.

Thus, ERP Security plays major role in protecting an organization business data and their employee’s and customer information as well. Study of Access Control Model of ERP Security is very important to keep the enterprise IT environment safe and secure. This paper focuses on the Risk of Fraudulent behavior of user roles across in terms of usage of ERP system. The case study used the information and data based on questionnaire and various inputs from industry experts.

Keywords: ERP, ERP role based security, ERP security issues.

1. Introduction

ERPs are widely used information system across different domains like Banking and Finance, Retail, Telecom industries and it is the core system, which contains the complete information, and important data facts needed to run the Organization. This information is very critical and confidential as complete business runs around this data hence any leakage or vulnerability to this information may ruin the enterprise and its business.

Moreover, the software system contains information about its employees, behaviour of its business, data related to its customer, purchasing details, billing and invoices related reports, Ledger entries, Employee’s personal and benefits data and their compensation details etc.

All the Finance data, reports and related queries are very crucial in aspect of any enterprise’s nature of business. HR related data like Employee Protected health information and

their personal details are very sensitive, should not be disclosed. Sensitive Protected information (SPI) of Individual under the US law is any information about individual’s health status, provision of health care, or payment for health care that is created or collected by a covered Entity (or a Business partner of respective Entity), is highly confidential data. Any disclosure of such information could lead to penalties on the organization.

2. Research Problem

Restrict the unauthorized access to ERP system based on Segregation of Duties (SoD) is a challenge in the rapid growing digital environment across the industries.

3. Research Objective

Designing a standard process that regularly monitors how users are granted access to the system is the first defense against data unauthorized access to data. Clearly defined area of responsibilities between IT and business staff help to build up secure environment which confirms that only authorized and verified personnel is given access to the particular system and that proper authorizations are granted to each user.

As ERP system supports majority of business functions within organization, the concern of segregating conflicting duties is being transferred from enterprise to ERP level. In IT dimension, the organization has to monitor which users are assigned conflicting combinations of access roles in ERP.

Such combinations of access role and rights represent conflicts of interest and create risk of fraudulent behaviour by allowing one user to execute the majority of tasks and activities in the process and to skip any control and necessary approval steps.

So, the clear objective is defining process which can control the data functions based on various business segments inside the enterprise.

4. Research Methodology

Research Design: Aim of this study is to gain understanding of various security aspects of ERP based on defined roles and duties.

Research Approach: Respondents are the ERP users who

provided their inputs through different digital platforms.

Research Analysis on Inputs: Input analysis were made on the different inputs gathered from various platforms to conclude and provided further scope of analysis.

5. Case Study

In Existing PeopleSoft ERPs, Manual human intervention needed to maintain the security of implemented HR and Finance applications hence in turn more human efforts and cost investment needed to effectively run and manage the entire process.

In most of the Corporates, business associates have to approach designated helpdesk and follow the defined process to get the required access of applications (In case they are aligned with task for the applications to which they don't have access) then helpdesk team route associates to respective approvers if the requested access need any approvals.

Upon all the approvals, helpdesk team assigns the required business roles to associate so that they can start working with their new tasks.

Mentioned Business Process is very tedious and takes lot of human efforts and time consuming too. Most of the big enterprises facing this challenge while managing maintenance and support activities after investing a lot of human Effort and Cost.

Risk Factor of Fraudulent User: None of the associates raises request for revoking the roles during the cutover phase of job role and responsibilities. This was a major conflict for segregation of duties (SoD), associates were having the access to multiple business which ideally they should not have.

Research based Solution: A process-based solution where security based security process could be enhanced for business role users. The process transforms the current business scenarios and provides solution in a way to improve user role security for implemented ERPs.

The process will allow business associates to request the required business roles by themselves by navigating into the system and this request will follow the approval process if required for respective roles. Upon defined approval, requested business roles will be assigned to associates and they will have

access to particular applications/modules on which they are aligned with tasks.

6. Conclusion

EPR system must regularly monitor the tasks users are performing based on their user roles. Authentication controls must be implemented across applications. Segregation of duties must take into consideration.

Although, vulnerability assessments of ERP are necessary as business security functions, they are not sufficient to protect system from all security threats. External as well as Internal, both measures should be included in a more comprehensive security strategy that includes security policy and strong identification and authentication mechanisms, access control mechanisms, physical security measures and security training.

A simple approach to sensitive data protection looks the various layer of security that can be applied. This approach secures the business tasks and applications based on job role and responsibilities of users.

References

- [1] Wei She, Bhavani Thuraisingham, "Security for Enterprise Resource Planning Systems" in *Information Systems Security*, vol. 16, pp. 152-163, 2007.
- [2] A. R. Mudiraj, "Study on Critical Factors affecting on ERP implementation process," in *International Journal of Recent Trends in Engineering and Research*, vol. 3, no. 6, pp. 177-181, June 2017.
- [3] S. Goal, R. Kiran, and D. Garg, "Vulnerability Management for an ERP System," in *International Journal of Computer Application*, vol. 53, no. 4, pp. 19-22, Sept. 2012.
- [4] A. Gupta, T. S. Rathore, and V. K. Jha, "Security Issue and their Countermeasures in ERP Implementation," in *International Journal of Advances in Electronics and Computer Science*, vol. 4, no. 4, pp. 39-43, April 2017.
- [5] S. K. Panday, "Major Challenges in Auditing ERP Security," in BOS, ICAI, 2009.
- [6] C. Marnewick, and L. Labuschagne, "Security Framework for an ERP Systems, 2006.
- [7] S. Matende, and P. Ogaob, "Enterprise Resource Planning (ERP) System Implementation: A case for User participation," in *Procedia Technology*, vol. 9, pp. 518-526, 2013.
- [8] A. Elragala, and M. Haddarab, "The Impact of ERP Partnership Formation Regulations on the Failure of ERP Implementations," in *Procedia Technology*, vol. 9, pp. 527-535, 2013.