Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 1 (2025)

Enhancing Data Security in Cloud-Based ERP Systems for Higher Education Institutions

Amudha T [1], N Shunmuga Karpagam [2], S Suganya [3]

[1]*M.E. Student, Computer Science and Engineering, Er.Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India,*

[2]*Professor and Head, Computer Science and Engineering, Er.Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India,*

[3]*Assistant Professor, Computer Science and Engineering, Er.Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India,*

Abstract: -

The adoption of cloud-based Enterprise Resource Planning (ERP) systems in higher education institutions (HEIs) provides significant advantages in terms although these benefits are accompanied by information security and protection concerns these benefits may be a significant burden. This paper provides a comprehensive analysis of the security challenges associated with cloud-based ERP in HEIs and proposes a robust framework to mitigate these risks. Through an extensive literature review and evaluation of current ERP modules we identify critical gaps and suggest enhancements to bolster data protection. The study aims to guide HEIs in securely leveraging cloud ERP solutions for efficiency and cost reduction.

Keywords: *Cloud ERP1, Higher Education Institution2s, Data Security3, Enterprise Resource Plannin4, Data Privacy5.*

1. Introduction

The Digital Transformation of Advanced education has driven foundations to take on cutting edge information systems to manage administrative and academic functions efficiently. Cloud ERP frameworks have arisen as a feasible arrangement offering centralized data management, real-time updates and enhanced operational efficiency. Despite these advantages concerns about data security and privacy remain paramount given the sensitive nature of academic and personal information addressed by these systems. This paper explores the security implications of cloud-based ERP systems in Higher Education Institutions and proposes strategies to mitigate potential risks.

2. Literature Review

In a number of studies Cloud ERP frameworks have been investigated in academia. Roughly 25 percent of the companies that employ ERP systems report that while ERP systems improve efficiency many existing solutions lack robust security measures and seamless integration capabilities. This segment surveys earlier work on cloud ERP reception, basic achievement factors and security concerns.

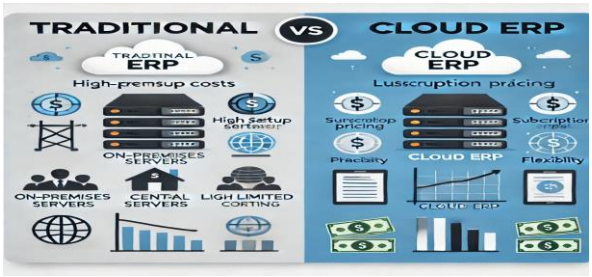

Figure 1. Comparison of Traditional vs. Cloud ERP

3. Methodology

This study employs a qualitative approach conducting an extensive literature review to identify existing security challenges in cloud-based ERP systems within HEI. We analyzed current ERP modules and security models to determine their effectiveness in addressing data protection concerns. Based on the insights gained, we propose a comprehensive framework constructed to enhance data security in cloud ERP deployments.

4. Proposed Framework for Enhancing Data Security

The proposed framework focuses on several key areas to enhance data security in cloud-based ERP systems.

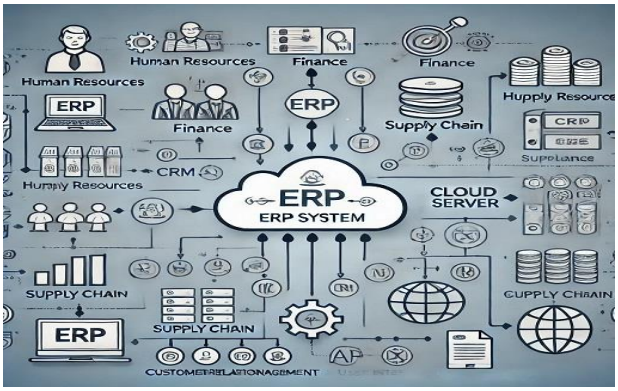

Figure 2. ERP System Architecture

4.1 Data Encryption: An executing vigorous encryption convention for information very still and in transit ensures protection against unauthorized access.

4.2 Multifaceted Verification (MFA): Consolidating MFA components add an additional layer of security, reducing the risk of unauthorized access.

4.3 Conducting regular security audits helps identify vulnerabilities and implement necessary security patches.

4.4 Client preparing and Mindfulness: Teaching clients on security best practices is critical in preventing data breaches.

4.5 Data access controls: Laying out severe access controls guarantees that just approved workforces can get to delicate information.

Figure 3. Proposed Security Framework

5. Discussion

HEIs now employing cloud-based ERP frameworks offer various advantages including improved scalability, cost savings and enhanced collaboration. However these advantages must be balanced against the imperative to safeguard delicate data. The proposed framework addresses critical security concerns by carrying out extensive measures that incorporate technological solutions policy development and user education.

Figure 4. User Role

6. Conclusion

As higher education institutions continue to adopt cloud-based ERP systems, ensuring data security remains a critical concern. This paper has distinguished key security challenges and proposed a comprehensive framework to enhance data protection in cloud ERP implementations. We will provide your comments and suggestions by adopting robust encryption techniques, authorizing multifaceted validation and directing ordinary security reviews they can actually shield delicate data while utilizing the advantages of cloud technology.

References

1. Soliman, M., & Karia, N. (2015). Enterprise Resource Planning (ERP) Systems in Higher Education: A Literature Review and Implications. International Journal of Supply Chain Management, 4(5), 147-154.
2. Abazi, B., Chaushi, A., & Ismaili, F. (2018). ERP Systems in Higher Education Institutions: Review of the Information Systems and ERP Modules. In MIPRO 2018 (pp. 811-816).
3. Eya, N. (2021). End-User Authentication Control in Cloud-based ERP Systems. In National Computing Colleges Conference (NCCC), 2021.
4. Makkar, G. D., & Bist, M. (2012). ERP as a Service: A Cloud-Based Approach to ERP Systems. International Journal of Engineering and Advanced Technology, 1(5), 147-151.
5. Leyh, C., Gebhardt, A., & Berton, P. (2017). Implementing ERP Systems in Higher Education Institutes: Critical Factors Revisited. Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), 913-917.