陆军工程大学学报 JOURNAL OF ARMY ENGINEERING UNIVERSITY OF PLA ISSN 2097-0730

SECURE AND COMPATIBLE INTEGRATION OF CLOUD-BASED ERP SOLUTION

Udita Malhotra[1], Dr. Ritu[2], Dr. Amandeep[3]
Corresponding Author: Udita Malhotra
Email ID: drmalhotraudita@gmail.com[1]
Department of Computer Science and Engineering,
Guru Jambheshwar University of Science & Technology, Hisar-Haryana[1, 2,3]

Received: 10th June, 2023 Revised: 1st August, 2023 Accepted: 15th September, 2023

Abstract

An extensible framework can be provided for secure and compatible integration of cloud-based ERP solutions with third-party systems. An organization uses ERP-based solutions to store their sensitive data which they cannot afford to be leaked, therefore, security is the major concern for cloud-based ERP solutions. Security is the pressing priority to safeguard an organization's reputation and financial details. ERP can be considered the main foundation for the company and also a virtual treasure trove of data. ERP has become an attractive target for intruders who are looking for sensitive information about organizations, thus making ERP security a vulnerable and susceptible target. Although much research has been conducted in this sector, still ERP solution integration security remains an alarming issue. Many techniques and approaches have been used to safeguard ERP systems but all these traditional approaches tend to have some limitations. Because of the technological advancement in Enterprise Resource Planning solutions in the past few years, it is gladiolus to say that it has become possible to deploy various security models on real-time ERP solutions. An extensible framework can be proposed for implementing secure integration between the portal and ERP solution, thus helping to maintain smooth and secure data flow between the two. To avoid interceptions, the technical and functional features need to be integrated to formulate a customizable framework for integration security. In this research, security implementation has been considered for the AX portal. The proposed work has been implemented in two phases. In the first phase, security has been considered for outbound flow i.e. data flow from the ERP portal to a third-party system. In the second phase, security has been implemented for inbound flow i.e. data flow from a third-party system to an ERP portal.

Keywords: ERP, Third-party system, Interception, Extensible, Security, Integration, Portal

1. Introduction

In the current era of growing technology, ERP is the forthcoming widely deployed technology. ERP has become popular and has taken a vital place in our day-to-day regular life. ERP-based solutions have made our existence easygoing and comfortable. Solutions based on ERP are used in various sectors like education, technology, defense, aerospace, and medical. AX is one of the most widely used ERP solutions for medium-sized and big companies which alleviate users to monitor alterations, function effectively, and compete globally. AX can be seen as a resolution that automates and rationalizes supply-chain processes, business-intelligence processes, and economic tasks in a way that can be supportive of the business.

AX can be outlined as a multi-language, customizable, and multi-currency enterprise resource planning solution. There are various fields in which AX is very beneficial like service industries, wholesale, manufacturing, and e-business. AX has been a unique and strong solution with extensible technical and functional features.

Web API can be used to import and export

data from AX to the portal. There is an integration framework required to maintain consistent integration between AX and the portal.

2. Problem Formulation

Although there have been many techniques and research methodologies proposed in the sector of secure integration of cloud-based ERP systems there are various limitations of these researches. Therefore, a better, customizable, flexible mechanism can be proposed to overcome the limitations of traditional approaches. The technical and functional features need to be integrated to formulate a customizable framework for integration security to avoid interceptions. This research work could provide a better and more efficient solution to achieving the aim of secure and compatible integration of cloud-based ERP systems.

3. Existing Systems

There are several types of research related to the integration security implementations for cloud-based ERP solutions. The below segment provides a literature review related to the integration of a cloud-based ERP system with a third-party system using blockchain technology and an IoT-based smart retailing system. The methods used in these are blockchain technology, cloud, radio frequency identification technology, and several data-mining methods.

A. Methods based on blockchain technology for procurement

a.) Bumble Bee Foods: This is an SAP portal that is a cloud-based ERP solution. It makes use of blockchain technology so that the customers can fetch the product origin and history details by scanning a QR code that is present on the item packet via their smartphones.

b.) Starbucks: They are functional with the Microsoft team to implement a system based on blockchain technology that can be used to maintain tracking information of supply chain management which the customers can use to get transparent information related to the purchased beans and coffee.

c.) Food security observation in the Procurement module based on HACCP: This involves a supply chain system providing a transparent, secure, and reliable platform for users. The system has been developed using blockchain, IoT, and HACCP which helped to make an innovative decentralized system to ensure openness.

d) Walmart: This involves a supply chain management for food items which is based on blockchain technology and Linux Foundation's Hyperledger Fabric. This involves tracking the origin of food items from various vendors and their end-to-end supply.

B.) Smart procurement systems using IoT

a.) Merchandising Security: This has been used by several marketers to secure their worthy items like mobiles, cameras, tablets, and watches. The same has been achieved by a security stand that lies above their showcased products.

b) Management Tool based on Smart Inventory: In this technique, retailers use smart barcode scanners to analyze and monitor the inventory stock. This has helped them to avoid stealing things. They keep an eye on the stock counts and observe keenly in case any discrepancy is found.

c) Electronic Article Surveillance (EAS): Many retailers use this technology in which security tags are attached to the items and an alarm is triggered if any customer tries to steal the product and walks out of the store with the tag still on. This is achieved with the help of electronic sensors present at the outlets.

d) Cameras and Video Analytics:

Under this technique, the software is used to detect any malicious activity or suspicious movement of the customers. In case any such activity is found, an alert can be generated instantly.

4. Methodology/Technology

Research Methodology can be defined as a procedure or method which the researchers use to achieve their aim/ objective in their research work. In simple terms, it can also be stated as a process that is contemplated to make research on a precise topic. The

various types of research methodologies should be recognized by a researcher before she specified her research work. A technology that is used to perceive, select, treat, and scrutinize information related to a precise subject turns out to be research methodology. The methodology segment under a research work allows the readers to critically estimate the study's overall rationality and consistency.

5. Tools and Technology Used in Research Work

AX ERP portal is used in various sectors of learning like academics and exploration. AX provides an integrated ERP solution that can be modified however and whenever necessary. This is possible due to the customizable source code available for this platform. The development is done using X++ language which is an object-oriented language with similarities to C#. X++ was intended to be a superset of Java using well-built data admittance features. In the proposed work, the integration of functional and technical customizations using X++ would reduce the time consumption along with the high quality of the desired outcome.

6. Proposed System

There is an integration framework required to maintain consistent integration between AX and the portal. Web API is used to import and export data from AX to the dealer's portal. Sync status is used in AX to indicate the synchronization status of the data. There are three possible values:

- AX only: This indicates that data is present only in AX and has not been shared with the portal.
- AX and portal: This indicates that the data has been shared with the portal.
- AX Updated: This indicates that data was shared with the portal but afterward, some modifications have been done to the data which are not shared with the portal.

Therefore, when the API will be called to share the data from AX to the portal, only the data which comes under 'AX Only' and 'AX Updated' will be shared.

Hosting of URLs is done in the portal (e.g., dealers' portal). Initiation of requests either GET or PUT is always from AX. We can prevent the declining operative speed of the computers or servers with the help of batch jobs so that server performance is not impacted during busy working hours. The history log for batch jobs will also be maintained which will provide various informative fields like start and end date time. API integration setup will also be done in which badge details will also be configured.

I. Outbound Algorithm

1. Fetch the data from main tables which need to be shared with third-party systems.
2. Validate and extract the selected records as per the requirements.
3. Create an XML document for the extracted data where the portal sync status is 'AX only' or 'AX updated'.
4. Save the XML document created at a specified destination path.
5. Request the URL provided with the appropriate content type i.e., POST.
6. Update the portal sync status of the selected records to ‘AX and portal’.

II. Inbound Algorithm

1. Request the URL provided with the appropriate content type i.e., GET.
2. Read the response for the request triggered.
3. The data is extracted from the response file which can be in the desired format (for example XML).
4. Iterate each record present in the data file.
5. Assign the staging field values from the data file before inserting the data values directly into the main tables database.
6. Validate the data fields if the data present in the staging is accurate and can be inserted into the main tables without having any adverse effects.

7. Process the successfully validated data further.

III. Applying security features to the third-party integration

The concept of badges is used for authentication between AX and the portal. A badge may be defined as a string of 255 characters that is used to allow and authenticate the sharing of data between AX and the portal.

Badge timeout: Time between the sending of the request and the arrival of the response.

Badge expiry buffer: The time after which the badge will not be valid.

Base URL: URL of the API which is going to be hit.

Document path: Path of the location where Xml files generated will be saved.

API nature: This can be inbound or outbound. In case the data is shared from AX to the portal, outbound API will be used. On the other hand, in case the data is shared from the portal to AX, an inbound API will be used.

Data file: This is the XML file generated.

Log file: This file contains the error id and description, if any.

Records: Number of records that will be sent at a time. (Used only in case of outbound APIs)

Call API: Request goes to the portal. Although, it is preferred to run the batch job instead.

Staging details: It contains the inbound data. When data comes from the portal, it first gets stored in a separate table called the staging table. Then a separate job may be used to transfer the data to the respective location.

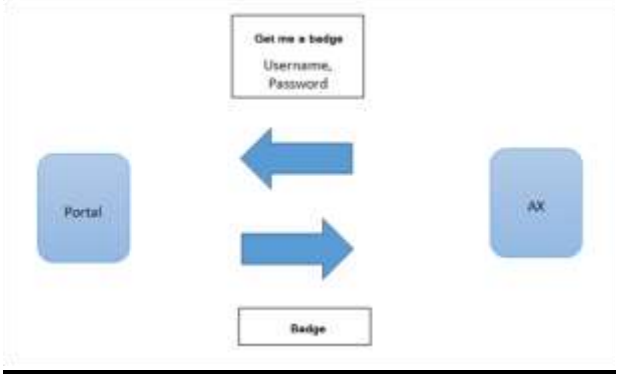

Fig.1. Applying security features to the third-party integration

Algorithm:

1. A request is initiated from the ERP side with the appropriate authentication card information to the portal side.

2. The portal then checks and authenticates the credentials from the ERP request.

3. The portal then generates and returns the access badge.

4. Assign the time for which the badge is valid.

5. The ERP then includes the access badge in the authorization header of the sent request.

6. The data can be shared between ERP and the portal until the badge is expired.

7. Results of Implementation

First of all, an item needs to be created on the cloud-based ERP portal which needs to be released. As this unit is newly created and not yet shared with the portal, its sync status would be ‘AX Only’. This makes it eligible for outbound data sharing.

Fig.2. New product released on cloud-based ERP solution

After that, the unit master API will be run through which a cloud-based ERP

solution will try to establish a connection with the dealer's portal for outbound data sharing. If the connection is authorized and an accurate badge is generated, then the data will be shared successfully and the dealer's portal will reflect the item from a cloud-based ERP solution.

Fig.3. Product created on a cloud-based ERP system successfully shared with the dealer's portal

A sales order can be created on the dealer's portal to check the inbound data flow.

Fig.4. Unit order created on the dealer's portal

Unit order API will be triggered to initiate a connection of the dealer's portal with the cloud-based ERP solution. If the authorization is successful, the generated badge will be used for the inbound data flow. The data will be inserted into the staging, validated, and then pushed to the main tables.

Fig.5. Unit order successfully shared with the cloud-based ERP solution and data present at staging

Fig.6. Unit order successfully created in cloud-based ERP solution after validation

In case, some unauthorized user tries to establish a connection, an alert message will be generated and the data won't be shared. If incorrect badge information is used for data sharing, then the connection between the cloud-based ERP solution and the dealer's portal will not be established.

Fig.7. Unauthorized interruption trial by the intruder which generates an alert

8. Conclusion

In the current era of growing technology, a cloud-based ERP solution is the most widely used system for storing and organizing the company's data systematically. Being the virtual treasure trove of data, ERP security-related issues can lead to dangerous repercussions. The proposed mechanism is found capable to ensure an efficient integration of ERP systems concerning the secure, streamlined, smooth, and compatible data flow between the two systems. This research has considered the limitation of traditional research works. This proposed framework is also capable to group the users with the same job role and use a single customized source code for security implementation. The integration of functional and technical customizations using X++ code enabled the security implementation in the ERP system. API and badge initiation need to be established by the developer in the developer workspace whereas badge timeout need to be configured by the system administrator in the functional workspace.

9. Future Scope

This proposed review of the extensible security framework for ERP solutions' integration with third-party systems would be beneficial to propose a better and more streamlined solution to resolve the existing issues in the field of security under cloud-

based enterprise resource planning solutions. This research work discusses various limitations and challenges that are faced by organizations using ERP portals. It also consists of a proposal for an extensible security framework. This security framework can be deployed in organizations to avoid malicious activities and maintain a secure environment. This integration security framework includes the functionality for defining and maintaining access control over the system and data. In addition to this, this research work provides us with a review of existing research and modules used in the field of cloud security. The work would be preferred as a brief review of the security framework based on the integration of functional and technical aspects. In this paper, there is a section in which the issues and problems of existing research are discussed which would be very helpful for a researcher who wants to propose a better solution in this field.

10. References

[1] Malhotra, U. ., Ritu, & Amandeep. (2023). *Secure and Compatible Integration of Cloud-Based ERP Solution: A Review*. International Journal of Intelligent Systems and Applications in Engineering, 11(9s), 695–707.

[2] Faccia, Alessio, and Pythagoras Petratos. (2021). *Blockchain, Enterprise Resource Planning (ERP) and Accounting Information Systems (AIS): Research on e-Procurement and System Integration* Applied Sciences 11, no. 15: 6792.

[3] J. Shree, N. R. Kanimozhi, G. A. Dhanush, A. Haridas, A. Sravani and P. Kumar, (*2020*) *To Design Smart and Secure Purchasing System integrated with ERP using Blockchain technology* IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2020, pp. 146-150

[4] Mahmood F., Khan, A.Z. and Bokhari, R.H. (2020). *ERP issues and challenges: a research synthesis*, Kybernetes, Vol. 49 No. 3, pp. 629-659

[5] Ahn, Byungchan, and Hyunchul Ahn. (2020). *Factors Affecting Intention to Adopt CloudBased ERP from a Comprehensive Approach* Sustainability 12, no. 16: 6426.

[6] Baraa K. Muslmani, Saif Kazakzeh, Eyad Ayoubi, and Shadi Aljawarneh (2018) *Reducing integration complexity of cloud-based ERP systems* Proceedings of the First International Conference on Data Science, E-learning and Information Systems (DATA '18). Association for Computing Machinery, New York, USA, Article 37, 1–6.

[7] Radoslav Hrischev (2020) *ERP systems and data security* Materials Science and Engineering, 9TH INTERNATIONAL SCIENTIFIC CONFERENCE

[8] Salih, Sayeed, Mosab Hamdan, Abdelzahir Abdelmaboud, Ahmed Abdelaziz, Samah Abdelsalam, Maha M. Althobaiti, Omar Cheikhrouhou, Habib Hamam, and Faiz Alotaibi.2021. *Prioritising Organisational Factors Impacting Cloud ERP Adoption and the Critical Issues Related to Security, Usability, and Vendors: A Systematic Literature Review* Sensors 21, no. 24: 8391.

[9] Mutuku Kaunda Morrisson,(2020). *Best Practice Models for Enterprise Resource Planning Implementation and Security Challenges*. Journal of Business and Management Sciences, vol. 8, no. 2: 55-60.

[10] Kuyoro, S. O., Ibikunle, F., &Awodele, O. (2011), *Cloud computing security issues and challenges*, International Journal of Computer Networks (IJCN), Vol. 3 Issue 5, 247-255.

[11] Gnatyuk, S., Kishchenko, V., Tolbatov, A., &Sotnichenko, Y. (2020), *SECURE CLOUD COMPUTING INFORMATION SYSTEM FOR CRITICAL APPLICATIONS*, Scientific and practical cyber security journal.

[12] Mandal, S., & Khan, D. A. (2020). *A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic*. International Conference on Smart Electronics and Communication (ICOSEC) (pp. 837-842). IEEE.

[14] Kumaraswamy, S., Latif, S., Mather, T. (2009), Chapter 7: *Privacy*, pp. 145, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (1st edition), O'Reilly Media.

[14] Yee, G., Pearson, S. (2013), Chapter 1: *Privacy, Security & Trust in Cloud*

Computing, pp. 3, Privacy and Security for Cloud Computing, Springer London.
[15] Menon, G. (2013), *Regulatory issues in cloud computing—an Indian perspective*, J EngComput Applied Sciences, 2(7), 18-22.
[16] Nayak, D., & Huawei, B. (2012), Understanding the security, privacy and trust challenges of cloud computing, Journal of Cyber Security and Mobility, 1(2), 277-288.
[17] Srivastava, N. (2018), *MeghRaj A Cloud Environment for e-governance in India*, International Journal of Computer Sciences and Engineering, 6, 759-763.
[18] U.S. Department of Justice-White Paper, (2019). *The Purpose and Impact of the CLOUD Act* Promoting Public Safety, Privacy, and the Rule of Law Around the World.
[19] S. Chouhan (2019), *GI Cloud-MEGHRAJ-key pillar of e-governance system in India*, Advance and Innovative Research, Volume 6, Issue 1, pp 348 - 352
[20] PRABHU, C. (2013), Appendix 3: *Eucalypts Cloud to Remotely Provision e-Governance* 26*Applications*, pp. 254, E-GOVERNANCE: CONCEPTS AND CASE STUDIES (Second Edition), PHI Learning.
[21] Edoardo Celeste and Federico Fabbrini, Chapter 3, *Competing Jurisdictions: Data Privacy Across the Borders*, Data Privacy and Trust in Cloud Computing, Palgrave Macmillan (ISSN 2662-1282)