International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Security in Enterprise Resource Planning solution

Udita Malhotra[1], Dr. Ritu[2], Dr. Amandeep[3]

Submitted: 14/09/2023 **Revised**: 20/10/2023 **Accepted**: 07/11/2023

Abstract: There is a need to propose an extensible framework to define and restrict access to the data and system by using security. As all the company's sensitive data is stored in an Enterprise Resource Planning (ERP) solution, therefore, ERP security is a pressing concern and needs to be paid attention to. There can be various dangerous repercussions if the company's data treasure is compromised with security. ERP security is very important to protect an organization's financial details and reputation. The backbone of any organization can be considered as ERP. Indeed, ERP systems are highly susceptible to security threats, given their central role as a prime target for those seeking to commit crimes involving sensitive data. 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, limited access to the system has been considered by allowing users to access specific modules. In the second phase, the limited access to data has been considered by allowing users to access user-specific data.

Keywords: *ERP, Security, Role, Duty, Privilege*

1. Introduction

In the current growing technology era, ERP is the upcoming most widely used technology. ERP is becoming popular and taking an important place in our daily routine life. ERP-based solutions are making our lives easy and comfortable. There are several fields in which ERP-based solutions are used like education, healthcare, aerospace, defense, methodology, and techniques.

AX can be considered as an ERP resolution for medium-sized and big organizations which facilitates users to operate effectively, supervise modifications, and compete worldwide. AX can be considered as a solution that computerizes and rationalizes economic, "business intelligence", and "supply chain" processes in a manner that can assist in the business. AX can also be stated as a customizable, multi-language, and multi-currency ERP solution. There are various areas in which AX has been deployed like wholesale, manufacturing, services, industries, and business. AX can be considered a unique and powerful solution that contains functional and technical features.

The security role can be related to the job role which the end-user has within the organization. The duties, privileges, and permissions need to be established for the security implementation. Role and duties need to be managed by the system administrator in the rich client whereas privileges and permissions need to be established by the developer in the developer workspace. The role needs to be assigned to the end user. The role helps to identify the behavior pattern that the user can play in an organization. For example, the project manager can be considered. The duties need to be assigned to the user role. The duties resemble the responsibilities which the user possesses in the organization. For example, the project manager's duties will be to maintain the project master. Privileges specify the access which is required to perform the responsibilities in the organization. For example, the project manager will need to have access to the project contracts and funding sources. Permissions specify the level of access the user has to the securable objects required to perform a specific function. As an illustration, the project manager needs access to or complete control over the project forms accessible via the display menu item entry point. Additionally, they require full control to generate new project quotations accessed through the action menu item entry point.

2. Problem Formulation

However, there has been research work done related to ERP security but there are several limitations present. Hence, there is a need to implement a mechanism that offers greater speed, flexibility, and customization compared to conventional methods. Integrating both the functional and technical aspects of enterprise resource planning solutions is essential for implementing security effectively. This concept represents a more comprehensive and efficient approach to achieving this objective.

3. Literature Review

There are several types of research related to security implementations for cloud-based systems. A review of existing research has been stated here.

Department of Computer Science and Engineering,
Guru Jambheshwar University of Science & Technology, Hisar-Haryana
Email ID: drmalhotraudita@gmail.com[1], ritunagpal1973@gmail.com[2], amnoliya@gmail.com[3]

The paper “Regulatory Issues in Cloud Computing – An Indian Perspective” provides an overview of cloud computing models that rely on resources and enable data sharing within organizations to facilitate quicker application deployment, streamlined operations, and reduced maintenance requirements. However, the concentration of data in a single location makes it more susceptible to cyberattacks. To address this issue, the paper seeks to explore the suitability of cloud computing in India, considering the absence of a structured framework or model to support it. Challenges such as the absence of robust privacy and data protection regulations, inadequate data security measures, insufficient data deletion mechanisms, inadequate data oversight, licensing concerns, and jurisdictional issues contribute to the cautious adoption of cloud computing in India.

The limitation of this research work is that there is no consideration of the NIST framework under which there are various norms related to use cases and standardization techniques defined which are supposed to be followed by all service providers. This paper also lacks the details related to “THE PERSONAL DATA (PROTECTION) BILL, 2013". This includes the government norms which help to provide security to all the users and also provide various instructions to organizations to secure their physically as well as electronically stored data on the cloud server. Although this research work has mentioned about Technology Act, 2000 its details are not mentioned like which offense comes under which section. For example, the crime of any corporate body's failure to protect the data comes under Section 43A of the act. The details related to government agencies that deal with security-related issues have not been mentioned. Also, it does not include the policy details that should be proposed to resolve and improve the current situation.

The paper "Understanding the Security, Privacy, and Trust Challenges of Cloud Computing" includes the strategies and techniques that can help protect the cloud network of India and its users. The area of cloud computing has become important for regulatory and authoritative bodies. The Indian authorization has to amplify the "pan-Indian cloud strategy" which leads to sustainability in growth, expansion, employment, and building a unique and unconventional lead for India. The threats related to security and privacy pose a major problem that requires attention and an adequate methodology to overcome them same. These challenges may provide a hindrance in achieving the policy objectives.

The study and research work for legal, technical, and equipped methodologies has been initiated under the sector of cloud computing. The study has also considered the Indian aspect, well-being, and aims of all collaborators. The study also helps in the sequential evolution toward recognizing the accusation of security, privacy, and trust in cloud computing. The threats and problems related to the area of cloud computing have been contemplated and explained in this research work. The authentic and realistic case studies help to examine the policies and regulations for cloud computing. This study has been helpful for legislators and lawmakers as this research work provides additional utility further on than all-inclusive insight into a present hypothetical solution that acknowledges cloud computing and the related concerns of security, privacy, and trust challenges.

This paper exhibits a deficiency in its coverage of the intricacies of the Indian Regulatory Framework policies. It also falls short in addressing the “NIST Framework”, which encompasses all technical standards and use-case requirements that must be adhered to by service providers. Furthermore, the paper overlooks the “Personal Data (Protection) Bill, 2013”, which is a government initiative aimed at safeguarding customer data and providing guidelines to enterprises, whether data is stored physically or electronically, such as on cloud servers. While the author touches upon issues related to regulating cloud services, a deeper dive into specific state privacy laws is lacking. The paper also does not sufficiently clarify which laws apply to cloud services and neglects to discuss the challenges that regulators should address in terms of cloud security. Moreover, it does not offer an in-depth examination of these laws or policies, their associated challenges, or potential methods to overcome them.

In “MeghRaj Policy- A Cloud Environment for E-Governance in India”, the author delves into the integration of cloud computing into India's e-governance initiatives, highlighting its cost-effectiveness, scalability, and enhanced security. They explore various government programs aimed at leveraging the cloud, such as the MeghRaj Policy (GI Cloud), elucidating its objectives and the drive behind this cloud-centric initiative. This paper underscores the shift towards online accessibility of government services for the convenience of the general public.

The author does not address prior laws or regulations concerning cloud computing and does not explore the challenges or problems associated with the GI Cloud. There is a need to evaluate the potential effectiveness and security of this policy. Additionally, it is important to assess whether the security guidelines outlined in the MeghRaj Policy are adequate, and if they should be compared to the “Data Protection Act”, the “Information Technology Act, or ISO 27001”.

In the research paper "The Purpose and Impact of the CLOUD Act”, the author explores the implications of the CLOUD Act, a legislative initiative introduced by the U.S. government. The primary objective of this act is to facilitate swift access to electronic data held by U.S.-based global entities, thereby aiding in remote partners' investigations related to serious crimes such as felony, terrorism, violent offenses, child exploitation, and cybercrime, among others. The paper also delves into the complexities of legal obligations that may arise when a Cloud Service Provider (CSP) receives a request from one government for data disclosure, while another government restricts such access.

The study critically analyzes the CLOUD Act, highlighting its two key components. First, it empowers the United States to establish operational agreements with other nations meeting specific criteria. Second, the act clarifies U.S. law by asserting that an organization subject to U.S. jurisdiction can be compelled to disclose data it controls, regardless of the data's physical location at any given time.

This research also elucidates the motivations behind the inception of the CLOUD Act and underscores the advantages of implementing such regulatory norms. It proposes a novel approach characterized by "an efficient, privacy-conscious, and civil liberties-protective strategy for ensuring effective access to electronic data that may lie beyond the reach of the requesting country, owing to the evolution of electronic communications."

The author's omission of a discussion on cloud security standards and guidelines to address these issues, as well as the legal implications surrounding such standards, is a notable gap in the analysis. Furthermore, the paper does not acknowledge the various acts that pertain to different organizational fields, such as HIPAA for healthcare organizations, which are instrumental in data control and security.

The paper “Cloud Computing Security Issues and Challenges” explores security concerns and difficulties in cloud computing. It delves into cloud deployment models, service delivery models, and fundamental challenges in cloud computing, which encompass security, cost modeling, pricing structure, service level agreements, and cloud interoperability issues.

The author of the paper has addressed key security considerations and challenges in the field of Cloud computing with technology advancements, but they have not provided any solutions to address these issues.

In the paper "GI CLOUD-MEGHRAJ’-KEY PILLAR OF e-GOVERNANCE SYSTEM IN INDIA”, the author explores the Government of India's vision and strategy for the development and deployment of the GI Cloud, highlighting its significance as a fundamental component of the e-Governance system in India. The paper also examines the possible drawbacks and obstacles associated with GI Cloud, as well as the main factors driving its adoption and the advantages it offers. Additionally, it discusses how this emerging model of Cloud Computing Services can contribute to the enhancement of e-governance in India.

The author overlooks the omission of reference to additional government policies and bills about cloud computing that establish standards for safeguarding the cloud, standards to which both providers and users are obligated to adhere.

In the document “Secure Cloud Computing Information System for Critical Applications”, the author explores the benefits of cloud computing for both large enterprises and SMEs. Additionally, the author highlights the growing concern of cyber threats, emphasizing that anyone can create their cloud service. Ensuring information security falls on the shoulders of the service provider, and addressing this issue involves implementing various methods such as cyber threat detection, IDS/IPS systems, and cyber incident response modules.

While the author extensively explores the theoretical aspects of cyber threats in cloud services and their architecture, they do not offer practical solutions to address these issues or identify relevant laws.

The paper "A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic" highlights the surge in cloud usage driven by the COVID-19 pandemic, impacting sectors like education, e-commerce, and healthcare. However, it falls short of providing concrete solutions to the security challenges associated with cloud services when adequate precautions are lacking.

Privacy, a paramount concern within the realm of cloud computing, is extensively discussed in the chapter dedicated to this topic. The chapter elucidates several significant challenges faced by companies operating in the sphere of cloud computing as they endeavor to comply with global privacy standards and implement a systematic strategy for addressing cloud privacy concerns. Furthermore, the book delves into the complexities associated with managing cross-border data transfers, which are compounded by the existence of various international legal jurisdictions and the complications arising from conflicting regulations and regulatory implications.

While the author adeptly recognizes the legal intricacies and privacy challenges within cloud computing, they fall short in offering practical legal resolutions for addressing issues related to privacy and conflicting jurisdiction.

Although the author does propose potential solutions, they remain theoretical rather than grounded in real-world feasibility.

The chapter “Privacy, Security & Trust in Cloud Computing” addresses various significant issues concerning security and privacy within the realm of cloud computing. It also explores the foundations of certain approaches that tackle these issues. Additionally, it delves into cloud service models relevant to Big Data processing and extensive data mining, which revolve around the increased value of personal data.

A significant challenge associated with cloud services is the inherent risk to data confidentiality, given that data may exist in an unencrypted form on a machine owned, operated, and managed by an entity separate from the data owner. Emphasizing security and privacy measures for sensitive data is crucial for the well-being of both companies and individuals.

The author does not offer legal remedies to manage or address privacy and security concerns. Moreover, the author does not cover security compliance requirements for service providers, including both Indian and international regulations, policies, and laws. Additionally, the absence of guidance on adhering to the latest international standards such as ISO and CSA by providers and organizations is notable.

The chapter “Eucalypts Cloud to Remotely Provision e-Governance Applications” discusses the "Eucalypts Cloud for Remote Provisioning of e-Governance Applications" within the context of the National e-Governance Plan (NeGP). It elaborates on the role of the Network Informatics Centre in establishing a network infrastructure that supports the Central Government, State Government, UT Administration, District, and other Government bodies. The chapter also delves into the architecture required for typical e-governance services, including the Application Framework Layer, Content Management Layer, Channel Layer, and Service Mediation Layer, highlighting their contribution to delivering government services via the cloud and their relevance to e-governance policy. Additionally, it explores the concept of summarization for authorizing technologies and the implementation of e-governance applications as web services to facilitate integration and standardization.

The author's focus is primarily on the technical aspects of cloud services, including its layers, while neglecting to address the challenges and issues associated with cloud computing, particularly from the perspective of service providers. Additionally, the author does not explore the various regulations set forth by the Government of India concerning cloud technology.

In the chapter “Competing Jurisdictions: Data Privacy across the Borders”, the author delves into the friction between the EU's data protection approach and the US data privacy model within the realm of cloud computing. The chapter explores the simultaneous emergence of EU data protection laws and the US model back in the 1970s. It also delves into how the EU prioritizes the safeguarding of personal rights, such as respect for private and family life, communication, and home, as enshrined in the European Human Rights principle. In contrast, the US employs a centralized legal framework to emphasize the importance of confidentiality and the drafting of a Bill of Rights. Furthermore, the chapter discusses the progress made in regulating borderless cloud computing and examines how EU and US laws aim to address such issues, including the enactment of the Cloud Act for protection.

The authors do not adequately pinpoint the current issues or deficiencies in US or EU laws and regulations concerning cloud computing and the jurisdictional challenges experienced by various government agencies.

4. Methodology

Research Methodology can be defined as a pattern or method that has been followed in research by the researchers. In simple terms, it can also be stated as a process that is contemplated to research a precise topic. The various types of research methodologies should be recognized by a researcher before she specifies 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 education such as academies 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 designed to be a superset of Java with strong data access 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. Process Flow

- Security based on access to the system: Allowing the user to access user-specific modules

- ➢ A user ID will be created in the portal.
- ➢ Entry points will be made for the forms which need to be visible under the required modules.
- ➢ Privileges will be made for the required menu items.
- ➢ Duties will be made by having the required privileges.
- ➢ Roles will be made accurately as per the requirements containing appropriate duties and privileges.
- ➢ Roles will be assigned to the corresponding user.

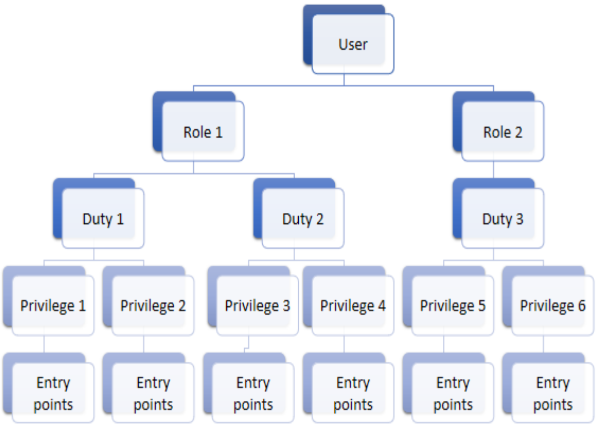


Fig. 1 Restricting access to entry points

- Security based on the access to the data: Allowing the user to access user-specific data
- ➢ A user ID will be created in the portal.
- ➢ The user will be assigned access to the module with the help of the previous algorithm.
- ➢ A query will be written using X++ with embedded SQL which will help to filter the data according to requirements.
- ➢ The query will be used on the list page.
- ➢ An entry point will be made for that list page.
- ➢ Appropriate duties and privileges will be created with required entry points.
- ➢ The role will contain accurate duties and privileges.
- ➢ The role will be assigned to the respective user.

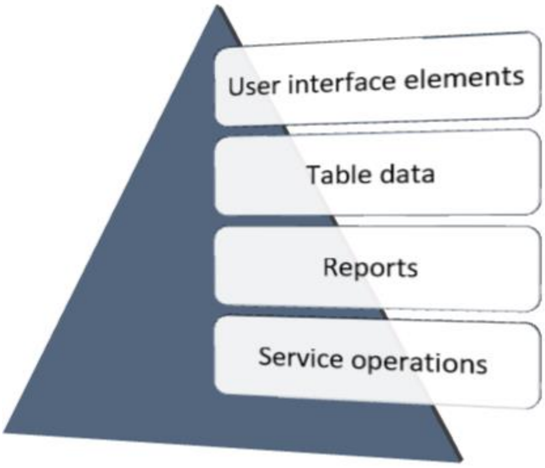


Fig. 2 Securable objects

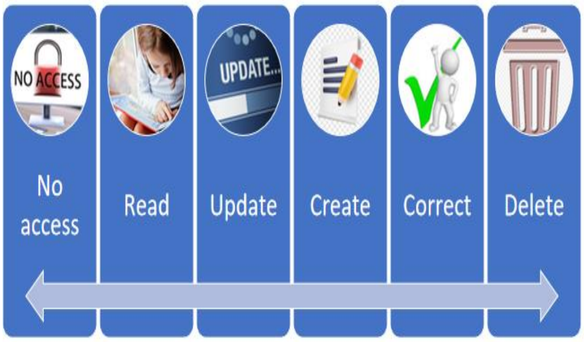
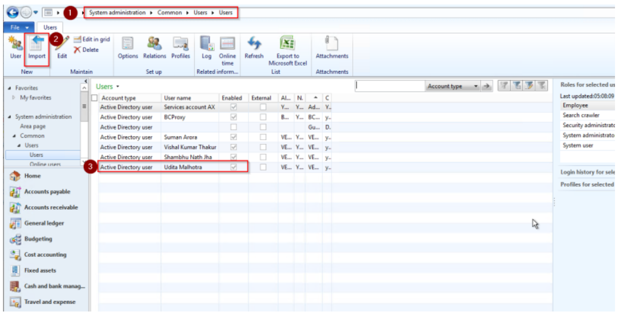


Fig. 3 Access levels

7. Results of Implementation

➢ Security based on access to the system: Allowing the user to access user-specific modules

First of all, the user needs to be imported to the portal.



Account type	User name	Enabled	External	Al...	N.		C
Active Directory user	Services account AX	☑	□	Y...	Y...	Ad...	Y..
Active Directory user	BCProxy	☑	□	B...	Y...	BC...	y..
Active Directory user		□	□			Gu...	D.
Active Directory user	Suman Arora	☑	□	VE...	Y...	VE...	y..
Active Directory user	Vishal Kumar Thakur	☑	□	VE...	Y...	VE...	y..
Active Directory user	Shambhu Nath Jha	☑	□	VE...	Y...	VE...	y..
Active Directory user	Udita Malhotra	☑	□	VE...	Y...	VE...	y..

Fig. 4 Importing a user into the ERP system

An appropriate role needs to be assigned to the user according to the requirements.

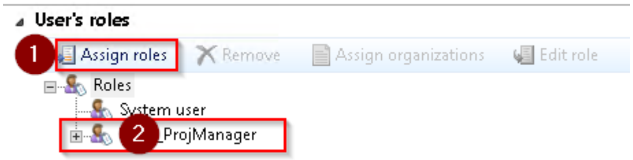


Fig. 5 Assignment of roles to the user as per the requirements

All the modules will not be visible to the user according to the privileges assigned to the user. Only a specific module i.e. the project management module will be visible as shown in the below screenshot. The Home module is the standard system module visible to all users of the ERP portal.

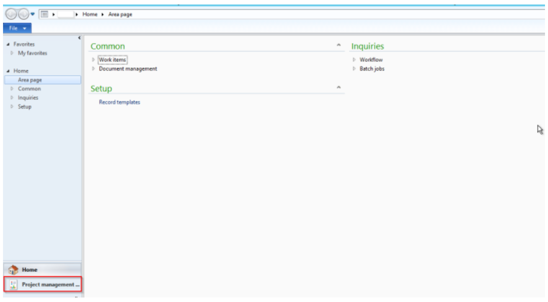


Fig. 6 Restricted access to the user based on modules

The admin account will have access to all the modules as shown in the below screenshot.

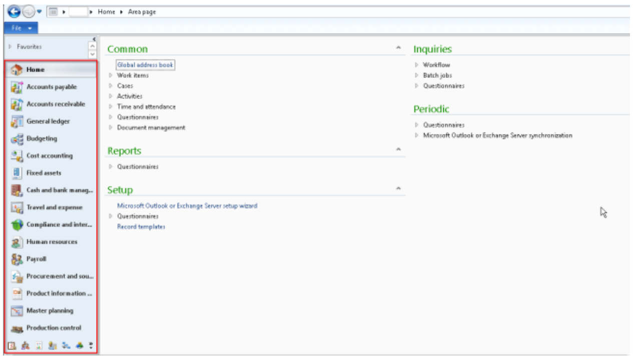
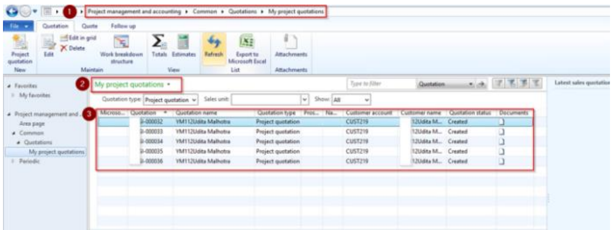


Fig. 7 Complete access of all modules to the system administrator

➢ Security based on the access to the data: Allowing the user to access user-specific data

The user will have access to the project quotations created by her. The project quotations created by other users will not be visible to her. As shown in the below screenshot, the user has access to personal quotations only.



Quotation type: Project quotation

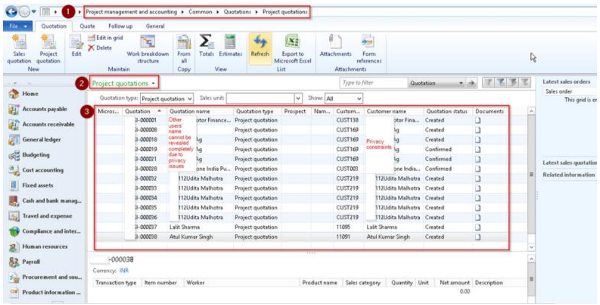
Sales unit:

Show: All

Microso...	Quotation	Quotation name	Quotation type	Proj...	Na...	Customer account	Customer name	Quotation status	Documents
	-000032	YM112Udita Malhotra	Project quotation			CUST219	12Udita M...	Created	
	-000033	YM112Udita Malhotra	Project quotation			CUST219	12Udita M...	Created	
	-000034	YM112Udita Malhotra	Project quotation			CUST219	12Udita M...	Created	
	-000035	YM112Udita Malhotra	Project quotation			CUST219	12Udita M...	Created	
	-000036	YM112Udita Malhotra	Project quotation			CUST219	12Udita M...	Created	

Fig. 8 Restricted access to the user based on data

The admin account has access to all users' data. Therefore, all the quotations created on the ERP portal will be visible to him as shown in the below screenshot.



Quotation type: Project quotation

Sales unit:

Show: All

Micros...	Quotation	Quotation name	Quotation type	Prospect	Nam...	Custom...	Customer name	Quotation status	Documents
	3-000001	otor Finance...	Project quotation			CUST138	otor Fina...	Created	
	3-000008		Project quotation			CUST169	Ag	Created	
	3-000018	Ag	Project quotation			CUST169	Ag	Created	
	3-000019	Ag	Project quotation			CUST169	Ag	Confirmed	
	3-000021	Ag	Project quotation			CUST169	Ag	Confirmed	
	3-000028	one India Pv...	Project quotation			CUST003	one India...	Confirmed	
	3-000032	112Udita Malhotra	Project quotation			CUST219	112Udita Malhotra	Created	
	3-000033	112Udita Malhotra	Project quotation			CUST219	112Udita Malhotra	Created	
	3-000034	112Udita Malhotra	Project quotation			CUST219	112Udita Malhotra	Created	
	3-000035	112Udita Malhotra	Project quotation			CUST219	112Udita Malhotra	Created	
	3-000036	112Udita Malhotra	Project quotation			CUST219	112Udita Malhotra	Created	
	3-000037	Lalit Sharma	Project quotation			11095	Lalit Sharma	Created	
	3-000038	Atul Kumar Singh	Project quotation			11091	Atul Kumar Singh	Created	

-000038

Currency: INR

Transaction type	Item number	Worker	Product name	Sales category	Quantity	Unit	Net amount	Description
							0.00	

Fig. 9 Complete access of data to the system administrator

8. Conclusion

Enterprise Resource Planning (ERP) is a concept that is continuously growing in significance and popularity. In tandem with this, security concerns in this field have also become increasingly critical. The proposed mechanism has proven to be effective in safeguarding ERP systems by regulating access and securing data appropriately. This research has considered the limitations of traditional research works. This proposed framework is also capable of grouping the users with the same job role and using 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. Role and duties need to be managed by the system administrator in the functional workspace whereas privileges and permissions need to be established by the developer in the developer workspace.

9. Future Scope

This proposed review on extensible security framework for Enterprise Resource Planning solutions would be beneficial to propose a better and more efficient solution to resolve the existing issues in the field of security under cloud-based enterprise resource planning solutions. This research work discusses the 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 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.

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] Udita Malhotra, Ritu, & Amandeep. (2023). *Secure and Compatible Integration of Cloud-Based ERP Solution*. Journal of Army Engineering University of PLA, Vol. 23 Issue 1, 183-189.

[3] Udita Malhotra & Ritu. (2023). *Incorporating E-invoicing in Cloud-based*

[4] *ERP Solution*. 8th International Conference on Research Developments in Applied Science, Engineering and Management (AEM-2023), 334-341.

[5] 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.

[6] 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

[7] 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

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

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] Yee, G., Pearson, S. (2013), Chapter 1: *Privacy, Security & Trust in Cloud Computing*, pp. 3, Privacy and Security for Cloud Computing, Springer London.

[18] Menon, G. (2013), *Regulatory issues in cloud computing—an Indian perspective*, J EngComput Applied Sciences, 2(7), 18-22.

[19] 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.

[20] Srivastava, N. (2018), *MeghRaj A Cloud Environment for e-governance in India*, International Journal of Computer Sciences and Engineering, 6, 759-763.

[21] 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.

[22] 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

[23] 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.

[24] 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)

[25] Mr. Dharmesh Dhabliya, Ms. Ritika Dhabalia. (2014). Object Detection and Sorting using IoT. International Journal of New Practices in Management and Engineering, 3(04), 01 - 04. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/31

[26] Pise, D. P. . (2021). Bot Net Detection for Social Media Using Segmentation with Classification Using Deep Learning Architecture. Research Journal of Computer Systems and Engineering, 2(1), 11:15. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/13

Authors

Udita Malhotra is pursuing Ph.D. from Guru Jambheshwar University, Hisar, India. She received a master's degree (M.tech) from OM Sterling Global University, Hisar, Haryana, India. Her area of research is security in cloud-based ERP systems.

Ritu Nagpal is working as an Associate Professor at Guru Jambheshwar University, Hisar, Haryana, India. Her area of research interest is network security.

Amandeep received his B.Tech, M.Tech, and Ph.D. Degree in Computer Science and Engineering from the Guru Jambheshwar University of Science and Technology Hisar (Haryana), India. He is currently working as an Assistant Professor in the same department. His research interest is in the integration of ERP systems.