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

Secure and Compatible Integration of Cloud-Based ERP Solution: A Review

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

Submitted: 28/04/2023 **Revised**: 27/06/2023 **Accepted**: 05/07/2023

Abstract: This review focuses on integration security in Enterprise Resource Planning (ERP) systems with third-party systems to propose a better and efficient solution. This research work discusses the challenges that are present in ERP solutions. However, there are several types of research in this field. A lot of techniques are used in organizations that help to maintain secure systems. But it is observed that these traditional security approaches have their limitations. It is glad to say, the deployment of security systems in real-time ERP solutions has become possible only because of the signs of progress which take place in the technology of Enterprise Resource Planning solutions in the last few years. The security under ERP solutions integration helps to provide an extensible framework for defining access to the portal and data. The customizable framework for integration security would be made by integrating technical and functional features of ERP systems to avoid interceptions. This study looks at the assessment of ERP integration with the third-party system as well as the secure extensible framework. The need for a security framework for integration has been discussed, including the algorithms which already exist and the progress made in technology for ERP integration. The work would be preferred as a brief review of the ERP security system.

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

1. Introduction

The demand for Enterprise Resource Planning solutions is increasing rapidly, but the issues regarding security still persist. Moreover, there is a need to analyze the indicators for key performance of ERP integration. ERP integration security is the need of the hour for all organizations because leakage of the company's sensitive information can lead to various dangerous repercussions. It plays an important role when it is used to protect a company's finances and reputation. ERP can be considered as a backbone for the organization and also a virtual treasure trove of data. Therefore, integration of ERP solutions with third-party systems is a vital need to automate day-to-day business processes. From the previous records, it comes into the limelight that integration security is the biggest challenge for enterprise resource planning solutions. The basic reason behind this is the lack of integration between technical and functional aspects of customizations. Due to this, the integration security of the portal is highly compromised. In most organizations, integration security, extensible and customizable framework is not properly implemented. This is considered one of the main reasons due to which the interception rate of integration security is the highest. Because of this, various organizations face issues related to data security, access control, data migrations, customizations, etc.

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]

PAPER ORGANIZATION

Section 1 is focussing on the introduction of cloud computing and cloud-based ERP system.

Section 2 is highlighting the research work already present in the area of ERP where different security models are displayed.

Section 3 is focussing on the requirement for an extensible security framework and the associated general and technical challenges.

Section 4 is focussing on analyzing cyber security laws which would apply to cloud-based ERP systems.

Section 5 is presenting the significance of security in ERP systems.

Section 6 is relating to the different challenges and issues faced during the integration of ERP systems with third-party systems.

Section 7 is related to the evaluation of the previous research and issues resolved using their work. Also, their limitations are also considered which opens up the scope for future research.

Section 8 is the conclusion part that is justifying the need for an extensible security framework for the integration of ERP systems with third-party system

1.1 CLOUD COMPUTING

Nowadays the term “Cloud” has become so huge and significant with the progression of expertise and

technology, directing itself towards being “unlimited”. It can be described as a virtual storage space where individuals, as well as organizations, store their information, in simple terms, a large-scale distributed paradigm. Almost every business that uses computers is itself a consumer of cloud-based solutions. Cloud virtual storage space has become so large that it contains a gigantic amount of information sources about all topics. Also, this virtual cloud storage space can be considered an element of cloud computing which provides computing assistance by using various resources like databases, servers, software, network, analytics, and artificial intelligence along with storage space to propose modernization, flexibility in resources, and profit in terms of finances. It is not only beneficial to store the data on a cloud platform for the people who upload the data and information details but also for the people who provide and tender cloud services to gain profit from that data and information on cloud platforms like Google Drive, One drive, and many more.

1.2 ENTERPRISE RESOURCE PLANNING

In today's instant era of modernization, ERP i.e., Enterprise Resource Planning is upcoming as most widely used technology. ERP is gaining importance, attracting an audience, and taking an important place in everyday existence. ERP-based solutions have helped to a great extent to make our work more efficient, organized, automated, and less time-consuming. There are several areas in which ERP-based solutions are used like aerospace, defense, medical, education, and technology.

AX can be considered as an ERP solution i.e., enterprise resource planning resolution for intermediate-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 defined as a customizable, multiple-lingual, and multiple-currency Enterprise Resource Planning (ERP) solution. AX has been very beneficial in various fields like manufacturing, wholesale, e-business, and service industries. AX has proven to be a unique and powerful solution that contains functional and technical features.

1.3 ERP INTEGRATION

ERP integration security is the need of the hour for all organizations because leakage of the company's sensitive information can lead to various dangerous repercussions. It plays an important role when it is used to protect a company's finances and reputation. ERP can be considered as a backbone for the organization and also a virtual treasure trove of data. From the previous records, it comes into the limelight that security is the biggest challenge for enterprise resource planning solutions. The basic reason behind this is the lack of integration between technical and functional aspects of customizations. Due to this, the security of the portal is highly compromised. In most organizations, integration of security, extensible and customizable frameworks is not properly implemented. This is considered one of the main reasons due to which the interception rate of security is the highest. Because of this, various organizations face issues related to data security, access control, data migrations, customizations, etc.

It is possible to integrate the functional and technical aspects to formulate an extensible integration security framework. This can help to define and regulate access to the system and data. This will help to enhance the security in organizations and help to eliminate the susceptibility of data leakage and misuse of ERP solutions.

It is possible to integrate the functional and technical aspects to formulate an extensible integration security framework. This can help to define and regulate access to the system and data. This will help to enhance the security in organizations and help to eliminate the susceptibility of data leakage and misuse of ERP solutions.

2. Integration Security Framework for Enterprise Resource Planning Solutions

In the last few years, in the field of security framework for cloud-based solutions, different new technologies are put in place for the first time. Out of these technologies, ERP integration security is the most important. It plays an important role when it is used for automating and streamlining business processes in organizations.

2.1 ERP INTEGRATION WITH AIS

ERP integration can be done with Accounting Information Systems using blockchain technology. [1] AIS i.e. Accounting Information Systems are the core part of any ERP solution and can be considered as the central system for ERP. With the growth of distributed ledger technology i.e. Blockchain, there has been significant improvement specifically in the sector of privacy and security. Various benefits of applying blockchain technology have been observed around system integration security. With the help of blockchain technology, integration can be achieved effectively at various levels and be helpful in various sectors like auditing compliance. The case study research methodology has been used to examine the e-procurement module and its functionality. Based on the outcomes, it has been concluded that Distributed Ledger Technology, Financial Technology, which can be

abbreviated as (FinTech), and Decentralized Finance, which can be abbreviated as (DeFI), can help the successful integration with Accounting Information Systems and ERP solutions with several advantages such as proficiency, better yield, and security. The transactions are grouped here into blocks and therefore, form a decentralized system.

Fig 1. Distributed vs Centralized vs Decentralized systems

Accounting Information Systems are used for the e-procurement module. The main components of AIS are trial balance which maintains the net debit/ credit amounts corresponding to the ledger accounts in a financial year, bookkeeping which records the ledger account details, financial statements which helps to do the reconciliation of income statements and balance sheet and the financial statements analysis.

Fig 2. Accounting Information Systems

Smart contracts are the most important part of e-procurement used in blockchain. They help to maintain a secure and compatible automated system for the contracts which are signed between individuals or companies. These are stored as logic blocks on the blockchain which get executed when certain conditions are met. These smart contracts do require the digital signatures of the concerned authority who are involved in binding the contract.

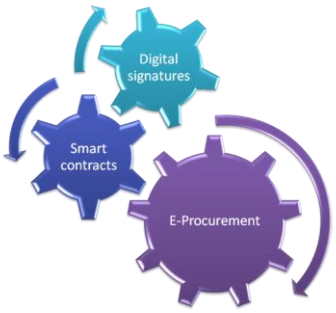

Fig 3. e-Procurement

2.2 ERP INTEGRATION WITH PROCUREMENT SYSTEM

The integration of ERP solutions with procurement systems can also be done using blockchain technology.[7] This integration has been made smart with the use of IoT i.e. Internet of Things and secure with the integration of RFID (Radio Frequency Identification). The supply chain management module has been made easier with the help of blockchain technology as it supports self-billing techniques which finish the need of standing in long queues. As it may seem that stealing things could be easier in this self-operating system, but this is not the case because of RFID. An item tracker based on RFID is used which helps to detect the items which the person may be trying to get out of the shop for which billing has not been done.

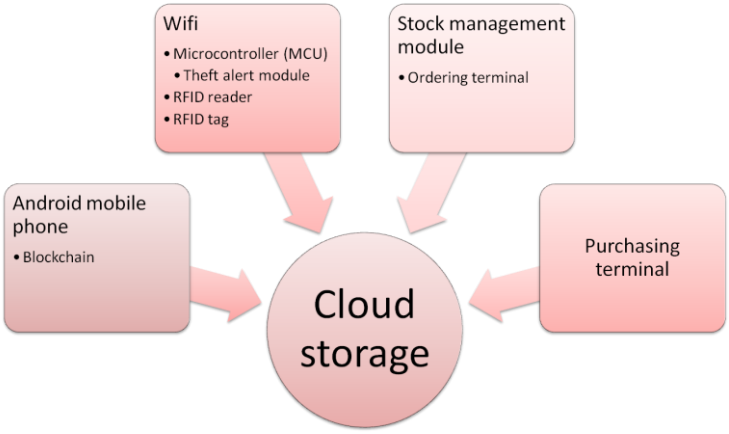

Fig 4. System Architecture for ERP Integration with Procurement System

In this system architecture, a mobile phone is used initially to initiate a connection request with the server. The server on receiving the request, updates the purchasing details of customers. This includes the linking with stock management module which is used to update the inventory count for the items and automatically place new orders in case of a shortage of items. Also, all the items' details can be fetched to maintain transparency. The server keeps track of all customers and their purchasing activities. The payment can be done in the preferable mode. When the payment corresponding to an item is received, its RFID tag gets disabled and the customer can walk out of the store. But, in case the payment has not been done corresponding to some item, its RFID tag will stay enabled and will give an alert whenever the person would try to walk out of the store. This would help to avoid stealing items from the market.

A mobile phone is used to request a connection.
The server maintains the purchasing details on the establishment of the connection.
Stock management updated the item inventory count and place new purchase orders whenever required.
When the payment is received, the RFID tag gets disabled and the person can walk out.
If the payment is not received, the RFID tag remains enabled and if the person tries to steal the item and move out of the store, an alarm is triggered.

Table 1. Algorithm for ERP integration with the Procurement system

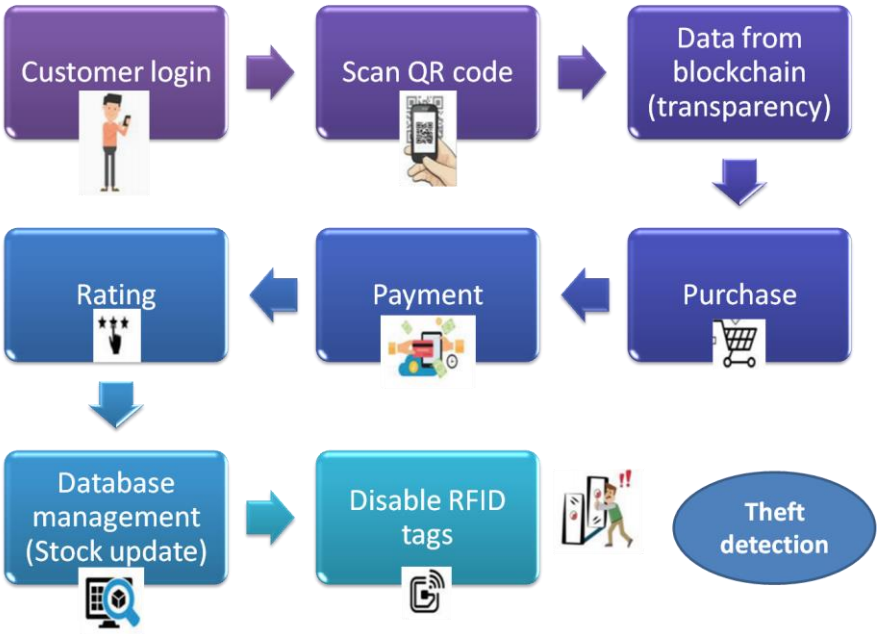

Fig 5. System design for ERP integration with the Procurement system

3. Challenges to Erp Systems: Need for a Secure Framework

Although the success rate of ERP has been great along with the same, there have been various failures too. [3] It can be enlightened that there are various challenges faced by different organizations concerning enterprise resource planning. There are about 31 major challenges to ERP solutions and the basis of this statement was past studies in the relevant area. The major issues which have been discussed are system integration, project team formation, data migration, team empowerment, change management, and project management. The issues related to security, SLAs, and functionality limitations have also been discussed which are more prominent in cloud-based ERP solutions.

To increase the productivity and efficiency of various business operations, organizations tend to shift/ migrate their on-premises ERP solution to cloud-based ERP solution.[4] This involved use of innovation resistance frameworks, diffusion of innovation, and technology-organization-environment. The various other responsible factors for the adoption of cloud-based ERP were comparative advantages, trialability, regulatory environment, organization culture, vendor lock-in, etc. It has also been observed that security, customizability, and technology skills had no impact on the purpose of migrating to a cloud-based ERP solution. This has been of good assistance to organizations who want to adopt cloud-based ERP systems, vendors who want to sell cloud-based ERP solutions, and for government sector trying to encourage organization digitalization.

Organizations these days tend to migrate to cloud-based ERP solutions.[5] There have been various benefits of migrating to cloud-based ERP, one of the most important being the cost-effectiveness as cloud service providers i.e. CSPs offer a pay-as-you-go concept. There have been various hurdles too for example integration of traditional ERP solution with the cloud-based ERP solution. There are various suggestions for reducing the integration complexity before migrating to the cloud-based solution which would result in better consistency and efficiency.

Enterprise resource planning solutions are used to incorporate all business activities.[6] It can also be highlighted that there is a need for data security within ERP solutions. Various h/w and s/w solutions have been adopted for data security. To make ERP solutions more integrated, intelligent, and cloud-based, the technologies used are cloud computing, IoT, and blockchain. As there has been an increase in e-business, therefore, ERP demand has also increased. This paper lays stress on data security in ERP solutions and the solutions for the same.

The cloud-based ERP solutions running on the vendor's cloud environment and not on-premises allow the organizations to connect via the internet.[7] The study includes the various factors and their prioritization that impact the decision for adopting cloud-based ERP solutions and also various challenges which come along. The main challenges to cloud-based ERP solutions are usability, security, and vendors which influence the adoption of the same. It is possible to identify and analyze 16 critical success factors (CSFs). This can be beneficial for the development of new policies or the modification of the existing ones to incorporate enterprise resource planning solutions with cloud computing infrastructure. Also, it aims to be beneficial for vendors that supply cloud-based ERP solutions to meet the organizations' expectations and imply appropriate and adequate procedures. A better analysis of

CSFs will help to increase the productivity and efficiency of cloud-based ERP solutions.

Various best practices should be followed to implement enterprise resource planning solutions.[8] The major challenge to the same is the security issue in ERP. The best practices for ERP implementation include proper planning with clearly defined goals and objectives, getting inside assistance and commitment, choosing the adequate s/w, distributing and training various resources, and change management. There are various challenges faced in all of these steps and security is being compromised. It can be concluded that although cloud-based ERP solutions are beneficial for organizations, it poses various security-related challenges, and therefore appropriate actions must be taken to overcome these.

There are various issues and challenges related to security in cloud computing.[9] The highlighted points of consideration can be cloud deployment models and their types also cloud service delivery models. Additionally, the basic challenges associated with cloud computing are:

i) Security

ii) Costing Model

iii) Charging Model

iv) Service Level Agreement

v) Cloud Interoperability Issue

There are various advantages that cloud computing has given not only to large companies but also to SMEs.[10] Alon with this, there have been increased problems of cyber threats which are inseparable. Any person can build their cloud service and providing information security is the responsibility of the service provider the resolution for this problem can be initiated by the use of various cyber threat recognition methods, IDS / IPS systems and cyber incident response modules, etc.

The impact of the corona virus (COVID-19) has led to high usage of the cloud due to which cyber security is at a huge leap.[11] Now cloud helps in education, e-commerce, and healthcare. The author of this paper has discovered challenges related to security while using cloud services without adequate precautions.

One of the most important concerns of cloud computing i.e. privacy has been highlighted in the chapter on privacy.[12] Various noteworthy challenges in the field of cloud computing for companies that need to adhere to worldwide privacy norms and adopt a methodical approach to address cloud privacy have also been mentioned in this book. Also, the problems in dealing with the trans-border data flows have been mentioned. Numerous intercontinental legislative jurisdictions, complexities enlarged due to incompatible norms, and authoritarian insinuations have also been mentioned.

The author is able to identify legal complexities and challenges of privacy in cloud computing but is not able to provide legal solutions relate to privacy and jurisdiction conflicting issues. However, the solutions suggested by the author were hypothetically possible but not in real life.

Various major problems linked to security and confidentiality in the field of "cloud computing" has been addressed in the chapter "Privacy, Security & Trust in Cloud Computing".[13] Also, the basis for some approaches which inscribe the situation has been considered. Also, the cloud service models which are related to Big Data dispensation and comprehensive data mining which is based on the enlarged value of individual data have been considered. It has also considered the challenge related to the discretion of data under cloud services as the data is present in the unencrypted form on an appliance owned and A challenge faced by cloud services inherently related to data confidentiality because of data being present in unencrypted form on a machine owned, handled and managed by an organization different from the data possessor. The stress has been laid on the security and privacy of private data for the betterment of companies and individuals.

The author fails to provide legal solutions to control or overcome privacy and security issues. Fails to address security compliance to be followed by service providers; Indian or International regulations/policies/ laws are missing. The latest International standards like ISO and CSA to be followed by providers or organizations are also missing.

4. Cyber Security Laws

There are various cyber security laws formulated by the government for cloud computing. These laws apply to cloud-based ERP systems as well. Therefore, any implementation model which can be proposed needs to comply with the various laws and legislations. So, a thorough analysis of such laws needs to be done and analyzed to propose a generic solution that can be accepted everywhere.

In the paper, “Regulatory Issues in Cloud Computing – An Indian Perspective” **(**Menon, G, 2013**),** it has been discussed that cloud computing models depend upon resources and data sharing which allow organizations to get their applications up and operate faster, with easier operating and less maintenance, and helps IT to fiddle with more quickly.[14]] Due to the huge deliberation of data at one center, it has become more vulnerable to cyber-attacks. To resolve such an issue, this paper helps to understand the cloud computing aptness in India,

knowing that India does not have any organized framework for the support of the same. Being deficient in privacy norms and data protection norms, insufficient information safety, inapt data erasing system, a broken system for data handling, permission, and legal issues, etc. can be attributed as the rational motive for careful acceptance of cloud-based systems in India.

This paper lacks about NIST Framework which gives all technical standards and use-case needs to follow by every service provider. Also failed to mention THE PERSONAL DATA (PROTECTION) BILL, 2013 under which the government gives protection to all customers and guidelines to all enterprises to protect their data whether it is stored physically or electronically i.e. cloud server. However, the author has tried to relate with Information Technology Act, 2000 but not in detail like what section relates to which offense. For Example, Section 43A of the Act deals with compensation for failure to protect the data by any body corporate. Not properly discussed government agencies dealing with such security and what should policy be made available to overcome such issues.

In the paper, "Understanding the Security, Privacy and Trust Challenges of Cloud Computing" **(**Nayak, D., & Huawei, B, 2012**), t**he notion of security, privacy, and conviction challenges under cloud computing have been considered.[15] The proposition related to strategy and interference has been given which helps to ensure protection for Indian users and to fortify India's cloud network. Cloud computing is becoming essential for policy authorizations and regulatory establishments. The Indian supervisory body has to expand a "pan-Indian cloud strategy" which may provide a sustained enlargement, of jobs and construct a novelty lead for India. It is a matter of concern that the risks related to security, privacy, and trust pose multiple challenges which are difficult to deal with. Also, these may destabilize the achievement of these policy aims.

The analysis of the technical, equipped, and legal niceties have been commenced under the approach for cloud computing. This also has taken into account the Indian facet, the welfare and aims of all collaborators (populace, personage users, cloud service purveyors, organizations, authoritarian entities, and pertinent communal establishments). This manuscript helps in metamorphic succession towards perceiving the imputations for security, confidentiality, and reliance by cloud computing. The challenges in the field of cloud have been defined and considered in the thesis. Also, the genuine case study executions help to analyze and consider related policies for cloud computing. This study provides great help for legislators because it provides supplementary value beyond an inclusive perception of the existing hypothetical or empirical consequential substantiation base, which will recognize the cloud-based systems and the linked general questionnaire adjoining security, privacy, and trust issues.

This paper lacks about Indian Regulatory Framework policies in detail and also failed to mention the discussion of the NIST Framework which gives all technical standards and use-case needs to follow by every service provider, THE PERSONAL DATA (PROTECTION) BILL, 2013 under which the government gives the protection to all the customers and guidelines to all the enterprise to protect their data whether it is stored physically or electronically i.e. cloud server. However, the author has tried to mention issues in regulating the cloud but not in detail like specific state privacy laws, also able to identify which law applies to the cloud and what challenges should be taken care of by regulators in cloud security. Not able to mention or discussed laws or policies in detail and their challenges also methods to overcome.

In the paper, "MeghRaj Policy- A Cloud Environment for E-Governance in India" **(**Srivastava, N, 2018**),** the author discussed how e-governance has been adopted by the Government of India and various services and projects are made obtainable online for providing facilities in an uncomplicated manner to the general citizen.[16] He also discussed that cloud computing is more economical, scalable & more secure and how the government is incorporating the cloud in e-governance. This paper mentioned all the programs launched by the government related to the cloud and the development of the MeghRaj Policy which is also known as GI Cloud and the objectives behind the initiative of GI Cloud.

Research Gap: The author fails to discuss the previous law or policies related to the cloud and what are the challenges or issues in GI Cloud, how this policy will be helpful, and whether is it secure. The security guidelines discussed under MeghRaj Policy are sufficient, whether they should be compared with Data Protection Act or Information Technology Act, or ISO 27001.

According to the paper, “The Purpose and Impact of the CLOUD Act” **(**U.S. Department of Justice-White Paper, 2019), Cloud Act was established by US government which helps in the rapid admittance of electronic information detained by the U.S. based worldwide to speed admittance to electronic data held by U.S.-based global contributors is significant for distant partners' investigations of a solemn felony, intimidation, aggressive crime, sexual mistreatment of children and cyber-crime, etc.[17] The incompatible lawful obligations have also been discussed which could have come to pass when a CSP obtains a command from one government needing the disclosure of data, however, the data access to the same has been restricted by another

government. This paper has analyzed the Cloud Act perilously and stated that it has two distinct parts. First is that the Act provides the U.S. the authorization to come into managerial accordance with other countries which meet the definite criterion. Second is that the clarification has been made in the U.S. law by the CLOUD Act which states that an organization under the country's authorization can be needed to reveal the information which the organization reins, despite the fact where the data is stored at any given particular instance. The reasons for the founding of the Cloud Act and the advantages of such norms have been discussed in this study. A new paradigm has been represented: "an efficient, privacy and civil liberties-protective approach to certain the effective access to electronic data which lies beyond a requesting country's reach due to the revolution in electronic communications".

Research Gap: The author fails to discuss cloud security standards or guidelines to overcome the issues and the legal implication of such standards. It is also not able to recognize different Acts for different fields of Organization to control and secure the data like HIPPA for Health Organizations.

The research paper “GI CLOUD-MEGHRAJ’-KEY PILLAR OF e-GOVERNANCE SYSTEM IN INDIA” **(**Srivastava, N, 2018**)** discusses the various techniques and policies which are established and made in used by Indian Government.[18] Various questioning factors, risks, advantages, and key drivers related to the GI cloud have also been discussed. It has given a brief idea about how cloud computing services can be beneficial for Indian e-Governance.

Research Gap: The author fails to mention other policies/ bills passed by the government related to the cloud, to lay down the standards to protect the cloud which need to be followed by providers as well as users.

"National e-Governance Plan (NeGP)" for the implementation of "e-governance projects" for the country in cooperation with state and central level has been discussed in the chapter “Eucalypts Cloud to Remotely Provision e-Governance Applications” **(**PRABHU, C, 2013**)**. [19] It has been explained how Network Informatics Centre works and helps in establishing a network spine and holds up to "Central Government, State Government, UT Administration, District & other Government bodies". It also includes the discussion related to the accomplishment of structural design for distinctive "e-governance service". It also discussed how Application Framework Layer, Content Management Layer, Channel Layer, Service Mediation Layer, etc. helps to provide services over the cloud to government and can be a part of e-governance policy. It also explains how summarization can be done for authorizing the technologies and how the "e-governance applications" can be implemented as web-based services to endow with integration, standardization, etc.

Research Gap: The author has been only able to discuss the technical aspect of cloud services and its layers, but fails to mention challenges/ issues involved in the cloud and by service provider. And also fails to mention other legislations laid down Government of India related to the cloud.

The abrasion amid the EU data fortification advancement and information seclusion model of the US in the department of cloud computing has been discussed by the author in the chapter “Competing Jurisdictions: Data Privacy across the Borders” **(**Edoardo Celeste and Federico Fabbrini, 2019**)**.[20] It has discussed the emergence of EU data fortification law and the US model concurrently in the 1970s. It has also been discussed that the EU served the cherishing of personal rights for the respect of confidentiality and family life, by the European principle on Human Rights enclosing the personal right of respect for confidentiality and family, communication, and home. The US, on the other hand, gives the centralized law which helps to identify the significance of confidentiality and draft Bill of Rights. Also, a development which has been made in regulating borderless cloud computing has been discussed; EU & US laws have also been discussed to save from harm by such issues, for example, enactment of the Cloud Act.

Research Gap: Authors fails to identify present issue or loopholes in laws or acts of the US or EU related to cloud computing and jurisdictional issues faced by the government of different agencies.

5. Significance of Security in Erp Integration

However, there have been several researches in the field of ERP integration security but these researches have done limited work. There is a need to propose a mechanism that would be faster, more flexible, and customizable than traditional approaches. There is a need to integrate the functional and technical features of enterprise resource planning solutions to implement security. This concept could provide a better approach to achieving this objective.

It is observed that the existing techniques or modules are not efficient. These are non-extensible and not up to the mark. In today's instant era of modernization, ERP is the upcoming most widely used technology, making ERP highly susceptible as it is an attractive target for anyone looking for stealing private information. Therefore, an extensible framework can be provided for defining access to the system integration and data by using security. ERP integration security is the need of the hour

for all organizations because leakage of the company's sensitive information can lead to various dangerous repercussions.

In the current lucrative era, companies need to provide extraordinary customer service. Enterprise resource solutions hold the most important part in delivering those over-the-top customer experiences. To ensure customer satisfaction, ERP solutions should be properly linked and provide a smooth and secure bridging with the customer-facing systems. This means that linkage and synchronization of ERP are required with third-party systems and data sources. There is a need for consolidated data view from various systems concurrently whether the data is generated from ERP systems or some other systems.

Traditionally, either slow manual procedures or some other insecure procedures are used to integrate ERP with third-party systems. The various problems related to the same can be stated below:

- Manual slow processing: This indicates that the information flows between the ERP system and other systems manually which is time-consuming. Also, the burden on the workforce increases in this case. An example of the same can be a situation where an order has been placed on the dealers' portal and that information is entered into ERP manually. This hampers the running efficiency of the organization.
- Insecure and incompatible linkage processing: This indicates that the data flow between ERP systems and other systems without appropriate security. This may lead to data leakage and data theft. This may pose a threat to the organization's sensitive information.

Therefore, there is an urgent need for organizations to opt for some modern technology to provide secure and smooth integration to provide the best customer experience.

6. Issues During Integration of Cloud-Based Erp Systems

There are various challenges and issues found while the integration of cloud-based ERP systems with third-party systems. Based on the statistics, it has been found that security is the most prominent interception found among all of them. Some of the common interceptions found while the integration of two systems have been cloud immaturity which signifies immature technologies, IT governance issues which signify that the framework should be law compliance, reliability concerns which signify service availability, regulatory issues which signify compliance issues and security, etc.

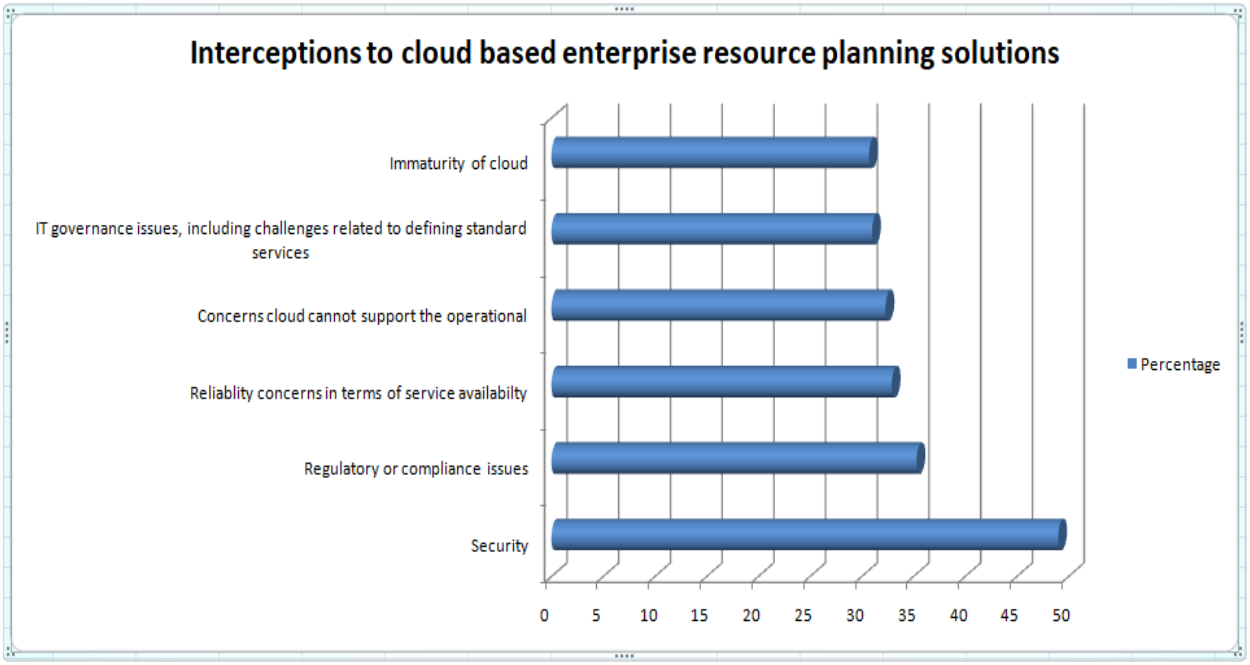

Fig 5. Bar chart depicting the percentage of threat provided by various factors in the field of integration of ERP solutions

7. Comparative Analysis

This literature study work has been used to organize the techniques used for integration security based on the deep study of accessible literature. Security algorithms, strategies, and surveys used by various researchers were examined in this review. Table 2 displays the outcome of critical analysis and evaluation of each work related to the problem which they address, merits and limitations of the work done. The major aim of this study has been to present the scope for a framework for implementing a future approach to ensure the integration security of

cloud-based ERP systems

S.no.	Authors	Research paper	Proposed work	Research gap
1.	Ahn, Byungchan, and Hyunchul Ahn, (2020)	"Factors Affecting Intention to Adopt Cloud-Based ERPfrom a Comprehensive Approach"	Data security-related issuesare more prominent in cloud-based ERP systems	No appropriate implementation technique
2.	Mahmood F., Khan, A.Z. and Bokhari, R.H., (2020)	"ERP issues and challenges: a research synthesis"	Data security issues, Data migration issues, System integration issues	No appropriate implementation solution
3.	Faccia, Alessio, andPythagoras Petratos. (2021)	"Blockchain, Enterprise Resource Planning (ERP) and Accounting Information Systems (AIS): Research on e-Procurement and System Integration"	Blockchain can facilitate integrating AISs and ERP systems	No automation technique was mentioned related to e-invoicing, and no security implementation technique was mentioned for the web services orAPIs
4.	Mandal, S., & Khan, D. A. (2020)	"A Study of Security Threats in Cloud: PassiveImpact of COVID-19 Pandemic"	The impact of the corona virus (COVID-19) has ledto high usage of cloud due to which cyber security is at a huge leap.	No appropriate implementation solution
5.	J. Shree, N. R. Kanimozhi, G. A. Dhanush (2020)	"To Design Smartand Secure Purchasing System integrated with ERP using Block chain Technology"	This research paper describes the integration ofERP solution with procurement system using IoT, RFID, and blockchain.	No generic secure integration implementation technique has been proposed for integrating ERP with

				any third-party system.
6.	Baraa K. Muslmani, Saif Kazakzeh, Eyad Ayoubi,and Shadi Aljawarneh (2018)	"Reducing integration complexity of cloud-based ERPsystems"	It involves various hurdles for integration of traditionalERP with the cloud-based ERP and provides suggestions to reduce complexity.	

Table 2. Comparative analysis of the existing research works

8. Conclusion

In this era of technology and the internet, cloud computing is the fastest-growing technology in every field. However, more advancement in the cloud means more threats to its data. Cloud-based - Enterprise Resource Planning is a concept that is gaining importance and popularity day by day. ERP is considered the backbone of any organization. Along with this, security-related issues have also posed dangerous repercussions in this field. The users' access needs to be controlled to the system integration and proper authentication should be required. Users should be able to access the data relevant and appropriate to them. Therefore, there is an urgent need to propose an integration security mechanism that is faster, more flexible, and customizable than traditional approaches.

To proceed towards meeting this criticaland urgent need, an extensible security framework will be needed to ensure the integration security in ERP with respect to the access control of the system integration as well as data appropriately. To overcome these issues, various studies have been perfomed in both areas i.e. academics and industrial, with a particular emphasis on some specific third-party systems not offering any generic solution. This review work analyzed many proposed approaches to ensure integration security for cloud-based ERP. The challenges, regulations, methods, and improvements to the outcomes has also been covered in this work. Reducing interception rates through improved quality of security is the major concern. Till now, there are no published research papers that are focussed only to the topic of generic integration of cloud-based ERP systems with third parties, however a few survey pieces are present related to the topic. In view of these anticipated outcomes for individuals and organizations, we need integration of the functional and technical features of the enterprise resource planning solutions to implement security. The security framework should also be capable to provide authentication to the required genuine users and use a single customized source code for integration security implementation. Authenticated users grouping need to be managed by the system administrator in the functional workspace whereas badge authentication checks need to be established by the developer in the developer workspace. The future of cloud-based ERP systems depends greatly on the success of the integrated security framework now being developed.

References

[1] 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.

[2] 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 Block chain technology IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2020, pp. 146-150

[3] 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

[4] Ahn, Byungchan, and Hyunchul Ahn. (2020). Factors Affecting Intention to Adopt CloudBased

ERP from a Comprehensive Approach Sustainability 12, no. 16: 6426.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

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

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

[15] 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.

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

[17] 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.

[18] 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

[19] PRABHU, C. (2013), Appendix 3: Eucalypts Cloud to Remotely Provision e-Governance 26Applications, pp. 254, E-GOVERNANCE: CONCEPTS AND CASE STUDIES (Second Edition), PHI Learning.

[20] 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)

[21] Lavanya, A. ., & Priya, N. S. . (2023). Enriched Model of Case Based Reasoning and Neutrosophic Intelligent System for DDoS Attack Defence in Software Defined Network based Cloud. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 141–148. https://doi.org/10.17762/ijritcc.v11i4s.6320

[22] Muhammad Rahman, Automated Machine Learning for Model Selection and Hyperparameter Optimization , Machine Learning Applications Conference Proceedings, Vol 2 2022.

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 Assistant 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 Assistant Professor in the same department. His research interest is in the integration of ERP systems.