Study of Privacy and Security in Multitenant Cloud ERP System

Vivek Malvi, Anita Soni

[1,2]Department of Computer Science, IES University, Bhopal

Email: vivekmalvi18@gmail.com

Abstract: Cloud ERP security issues and available solutions. First, a series of details regarding ERP systems, cloud computing, and multi-tenant are presented, as well as their security and privacy challenges and issues. Security procedures are then defined and discussed, and existing solutions to these problems are signed off on. This article is designed to create a cloud ERP security management model from elements such as cloud ERP data storage, data virtualization, data isolation and access security. The following techniques are recommended to increase the security of multi-tenant SaaS: database virtualization, use of data encryption and data and development mining capability, data distribution between tenants and ERP providers, security across multiple locations in application deployment, authentication and development systems as two-factor authentication brings together and improves user access control in multi-tenant ERP cloud.

Keywords: Challenges, Cloud Computing, Security, Techniques.

1. Introduction

In this study, we aim to investigate and discuss the potential security issues and challenges arising from cloud ERP and list some existing solutions. In addition, the contributions of this paper are:
1) providing an overview of cloud computing services models, approaches, and requirements; 2) understanding the relationship between cloud computing security risks and cloud computing models; 3) understanding the risks, success factors, benefits, and main drivers of ERP clouding; 4) analyzing the existing security controls, threats, and legal issues of clouds; 5) discussing major issues of infrastructure security in cloud ERP; 6) improving data storage and access security in cloud ERP; 7) improving application security in cloud ERP; 8) proposing trusted platform models of the computing environment for cloud computing without vulnerabilities; and 9) proposing flexible data storage for cloud computing.

The research methodology is based on a literature review of cloud ERP systems to define the security challenges and issues arising from the cloud ERP from the perspective of both the user and service provider. We use the best ideas and suggestions collected in the literature review to propose a model to improve the security and privacy in the cloud ERP. Additionally, we analyse ERP cloud architecture to determine the security improvement points. Moreover, the potential security attributes are defined to show how our model can satisfy these requirements taking into consideration the challenges discussed. Finally, we design a model to improving the security and privacy of the data based on authentication, authorization, and encryption.[1]

In this section, we present the historical background of ERP and cloud computing, the two subjects of this article. We provide detailed description of ERP life cycle, ERP platform, cloud computing service model, cloud computing model, cloud ERP and many other models. With the emergence of e-commerce and the need to leverage various information sources in the business, ERP (Enterprise Resource Planning) software has become a major source of interest for many businesses. ERP systems are now focused on all types of organizations as they offer integrated solutions to meet their information needs. ERP has become a simple business information system that meets the needs of large businesses. Today, ERP systems are considered to be an essential information systems infrastructure ERP is a software architecture that facilitates the flow of information between the different functions within an enterprise.[2]

Likewise, ERP assists information sharing across organizational units and geographical locations. ERP consists of management, documentation, planning, and control of all business processes and resources of an enterprise. ERP is used to manage and integrate all the business functions within an organization, which usually include a set of mature business applications and tools for financial and cost accounting, materials management, sales and distribution, production planning, human resources, and computer integrated manufacturing, supply chain, and customer information [3].

Successful implementation of ERP systems needs to involve excellent project management of an organization to implement it successfully. ERP implementation project consists of defining objectives clearly, developing resource and work plans, and tracking the progress of the project carefully. Therefore, the project plan should consist of aggressive and achievable tasks organized into schedules that enhance the perception of urgent and dependent tasks [4].

ERP Life Cycle
In 1999, Estaves and Pastor proposed a framework of ERP lifecycle that included structured phases, and consisted of multiple stages that hosting organizations should follow throughout the ERP life cycle [5]. This section focuses on the structured stages of ERP systems, as follows:
- Adoption decision stage: This stage allows managers to identify their requirements for ERP implementation by addressing their critical challenges, selecting the best approach for general information systems, and improving the organization's strategy.
- Acquisition stage: In this stage, managers should select the best-fit product compatible with the specified and minimized customization requirements.
- Implementation stage: This stage is also called customization of ERP software package to fit with the organization's needs, including ERP parametrization and adaption.
- Using and maintenance stage: The ERP packages are applied in this stage to return the expected benefits with minimized interruption.
- Evolution stage: Additional ERP systems benefits can be obtained through the integration of additional capabilities to existing implemented functionalities.
- Retirement stage: ERP systems are not stable; however, they are modified continuously according to organization's needs and the evolution of new technologies [6].

Cloud Computing:
Cloud computing is changing the way business and business create new opportunities by virtualizing the Internet and providing dynamically scalable programs to perform their processes [7]. Cloud computing refers to applications offered as services over the Internet. Hardware and system software of the Internet and the data centres that serve it. Cloud computing provides a significant opportunity for the delivery of so-called "X as a service." This type of electricity payment is considered one of the main benefits of using air [8]. There is no need for an up-front investment such as a software license investment, that is, there is no risk of not using the software license and paying the price; including investment in hardware infrastructure and maintenance and personnel. Users of cloud services use only the IT resources needed and pay only for the IT resources used. They take advantage of the scalability and flexibility of the cloud. Cloud computing can easily and quickly expand computing resources as needed [9] ERP software delivered in the cloud environment becomes "cloud ERP software". Most, if not all, cloud environments are built using virtualization and load balancing technologies, allowing applications to be distributed across multiple server and database resources. Cloud ERP is positioned as a revolutionary approach to the deployment of ERP solutions. It provides scalable, flexible, cost-effective, adaptable and efficient solutions. As a business management software, cloud ERP provides important and successful business information [10].
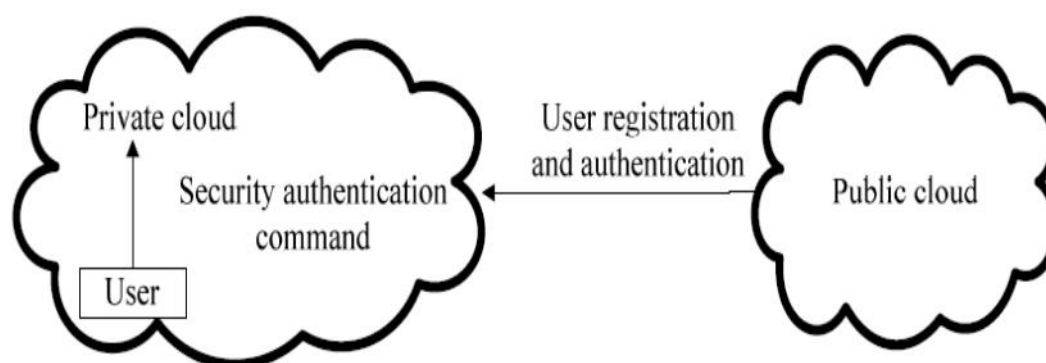

Figure 1: Structure of cloud computing security

Figure 1 illustrates the structure of cloud computing security, showing the frame structure of safety certification. This structure allows users to register and have authentication measures to access the cloud computing private

cloud. The authentication verifies the users using the data security model, which allows users to pass their information to the clouds to be stored in protected databases, and the clouds should be safety certified to guarantee continuous security updates [11].

Cloud Computing Platform

The earliest key business technology trends, such as cloud, internet of things, and collaboration, have been identified as major factors in reforming international enterprises. One such smart technology is cloud computing, which is the major contributor to the transformation of the manufacturing industry to be enabled with smart technologies and IT. In distributed environments, the primary function of cloud computing is to provide on-demand cloud computing services and to introduce high availability, reliability, and scalability cloud services [12].

Cloud Computing Deployment Models

Cloud deployment models include: private cloud, public cloud, community cloud, and cross-cloud, which provide one-way access to cloud services suitable for different situations, differences, and patterns. A cloud computing model can be implemented in many cloud environments by sharing third-party services and infrastructure with service providers. [13]. In contrast, the private model of cloud computing can be implemented in the tenant environment by sharing the provider's processes and the organization's services. While private clouds are designed to store a business's mission-critical and business-critical applications, community clouds are under protected because they are supported by a unique community with the most common concerns and interests and may be shared by many businesses. [14] The fourth cloud model is the hybrid cloud, which includes many private clouds and public clouds, making cloud services even more challenging due to the additional complexity determined by the distribution of applications across and outside the cloud.

Cloud ERP

Cloud ERP software helps many customers as a platform that offers innovative solutions. The concept of cloud ERP can be confused with ERP hosting, which acts as a third party to support the software infrastructure and application services provided by the cloud environment. Others define cloud ERP as a cloud computing platform used to provide businesses with services for process completion [15]. SaaS supports business cloud services with business communication systems such as ERP systems. Cloud-based software companies can quickly expand their capabilities because cloud computing can improve the reliability of ERP deployment in new ways. Cloud users can directly access the service and use it quickly. The migration from a traditional ERP to an ERP cloud environment is responsible for more serious problems, such as the possibility of attacks from the network environment or secure technical consultants inside and outside the cloud [16]. Cloud-based ERP is the development of an integrated business suite that supports ERP, CRM and business operations, with application modules accessible using the Software as a Service (SaaS) delivery model and easily modified by the user application. and subscribing to a set of application modules based on multi-family user architecture [17].

Proposed Model

In our proposed security model for multi-tenancy architecture, we provide storage and communication overhead for verification of authorized cloud users and to access the cloud. The design of our model can block level data operations by designing efficient block-level encrypted data operations. Additionally, we propose a confidential and integrity design for data encryption prior to outsourcing to the cloud server, while the decryption algorithm can be used on the user side. The data owner can encrypt the intended file data before sending it to the cloud. Our proposed encryption algorithm has several factors; the information is at the highest factor by applying a set of rotations for each block character. The benefits of our proposed encryption in the cloud ERP environment are:

- Encryption algorithm can ensure organizational data privacy according to the three states of encrypted data; in transmission, in use, and in storage location.
- The proposed encryption algorithm can assist in achieving secure multi-tenancy in the cloud encryption of data in the cloud ERP environment.
- Data owners can avoid the cloud service provider accessing the data by holding the encryption key.
- The encryption algorithm provides confidence of data backups to store them safely in the cloud ERP environment.
- Our proposed model can be expanded to be customized according to customers' requirements.

Only the data owner can control data entry. Questions are answered in a consistent amount of time that does not depend on the size of the request. Public key instances cannot read encrypted data or queries because data can

only be decrypted using the key provided by the data owner.[18] Despite all the advantages of public cloud infrastructure, cloud storage is still considered to face significant problems. Issues such as data integrity, confidentiality, liability, and access only by authorized users are important issues in the public cloud. Since data security is guaranteed only by the cloud provider, customers can ensure that their data in the cloud is safe from internal and external threats. In the cloud infrastructure, all lines used to communicate with data owners, customers and cloud service providers are protected for secure sharing of public keys. However, not all users can make calculations and studies because they do not have enough working power. Any client that is trusted to access data can only access encrypted directories of accessible data. [19]

This layer restricts access to the data by only using data object classes. Tenants and cloud providers should use data object layers to read and update the database. The data object classes also use access control to give the right access authorizations to users. Each table in the database has a corresponding class in the data object layer. The data object class has four methods:

- Get method: This allows selection from a database table
- Insert method: This allows insertion of a row or set of rows in a database table
- Update method: This allows updating of a row or set of rows in a database table
- Delete method: This allows updating of a row or set of rows in a database table Each method is designed as follows:
- Read input parameters (table attributes)
- Filter the attributes based on access control
- Build SQL script
- Execute SQL script
- Return the result based on the filtered attributes

It is difficult to use public cloud servers to store customer data. Data protection policies should be implemented to protect the confidentiality of data stored on public servers. This work solves this problem and presents encryption methods. The data owner stores the key used to encrypt the data before it is stored on the server; The only way to access the data is to provide the client with the corresponding decryption key. A strong system should be able to protect the organization from internal and external attacks. The data owner must allow the client to authorize the private key to allow access to external cloud data. After successful authentication, the user can download the data from the cloud via local decryption. Profile sharing is another way for renters to save and protect their profiles. The tenant can choose which database table they want to use in the company database and the database information will be in the given database.[20] According to the data access model and data access developed for both data sets, we prepared the data in memory, that is, we loaded the data sent to memory at the beginning of the working day and returned it later. It goes into the database at the end of the workday. By using decentralized technology, tenants will have better privacy for their data without losing their business as all data will be stored in memory.

2. Conclusions

This study examines several issues in various cloud applications: loss of security control; SaaS application security integration; SaaS application security customization; and provides for the exclusion of rental documents. One of the main goals is to secure the cloud ERP system by using the latest design to secure the cloud ERP environment. It focuses primarily on services provided by SaaS, PaaS, and IaaS, and on key issues and issues related to security and privacy. The main issues that limit the functionality of ERP systems are network requirements, large storage requirements, and required personnel training.

There are also many disadvantages such as privacy concerns, high costs due to the small size of the business, ERP installation, implementation and maintenance, training that affects ERP performance, and the time and cost of ERP customization. A suggested solution is to use dynamic credentials to change the value based on user location or package information. Another solution is to use digital signatures to ensure data security by using the verifiable RSA algorithm to ensure the security of data sent over the internet in the cloud environment. This research is designed to create a cloud ERP security management model from the elements of Cloud ERP such as data storage, data virtualization, data isolation and access security.

3. References

1. Dheresh Soni, Deepak Srivastava, Ashutosh Bhatt, Ambika Aggarwal, Sunil Kumar, Mohd Asif Shah, "An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol", Mathematical Problems in Engineering, vol. 2022, Article ID 4696649, 14 pages, 2022. Hindawi.
2. Sun, X.; Liu, P.; Singhal, A. Toward Cyberresiliency in the Context of Cloud Computing [Resilient Security]. IEEE Secur. Priv.2018, 16, 71–75.
3. Chen, D.; Zhao, H. Data security and privacy protection issues in cloud computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 1, pp. 647–651.
4. Zhan, Z.H.; Liu, X.F.; Gong, Y.J.; Zhang, J.; Chung, H.S.H.; Li, Y. Cloud computing resource scheduling and a survey of its evolutionary approaches. ACM Comput. Surv. 2015, 47, 1–33.
5. Afnan U.K. (2014) Data Confidentiality and Risk Management in Cloud Computing2 Feb, 2019.
6. Sarojini G. et.al (2016) Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016).
7. Dimitra A. G. (2017) Security Policies for Cloud Computing, 26 Jan.
8. Nabil Giweli (2019) Enhancing Cloud Computing Security and Privacy, 20, Jan.
9. M. Vermaat, S. Sebok, S. Freund, J. Campbell, and M. Frydenberg, Discovering Computers: Tools, Apps, Devices, and the Impact of Technology. 2016.
10. M. I. M. Hanifah, R. C. Omar, N. H. N. Khalid, A. Ismail, I. S. Mustapha, I. N. Z. Baharuddin, R. Roslan, and W. M. Z. Zalam, "Integrated Geo Hazard Management System in Cloud Computing Technology," IOP Conf. Ser. Mater. Sci. Eng., vol. 160, p. 12081, 2016.
11. D. Tse, "Challenges on Privacy and Reliability in Cloud Computing Security," in International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), 2014, pp. 1181–1187.
12. L. Xu and J. Li, "Building Efficient Resource Management Systems in the Cloud: Opportunities and Challenges," Int. J. Grid Distrib. Comput., vol. 9, no. 3, pp. 157–172, 2016.
13. B. Al-shargabi and O. Sabri, "A study of Adopting Cloud Computing from Enterprise Perspective using Delone and Mclean IS Success Model," Int. J. Comput. Sci. Inf. Secur., vol. 14 S1, no. February, p. 5500, 2016.
14. M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," Journal of Network and Computer Applications, vol. 84. pp. 38–54, 2017.
15. Campbell, L. H., & Milner, M. (2019). The NBN Futures Forum: Discussing the future ownership of Australia's National Broadband Network, Journal of Telecommunications and the Digital Economy, 7(3), 1-9.
16. A. Narang, D. Gupta and A. Kaur, Biometrics-based un-locker to enhance cloud security systems, International Journal of Cloud Applications and Computing (IJCAC) 10(4) (2020), 1-12.
17. K. Goel, C. Gupta, R. Rawal, P. Agrawal and V. Madaan, FaD-CODS Fake News Detection on COVID-19 Using description logics and semantic reasoning, International Journal of Information Technology and Web Engineering (IJITWE) 16(3) (2021), 1-20.
18. P. K. Verma, P. Agrawal, V. Madaan and C. Gupta, UCred: fusion of machine learning and deep learning methods for user credibility on social media, Social Network Analysis and Mining 12(1) (2022), 1-10.
19. Zhan, Z.H.; Liu, X.F.; Gong, Y.J.; Zhang, J.; Chung, H.S.H.; Li, Y. Cloud computing resource scheduling and a survey of its evolutionary approaches. ACM Comput. Surv. 2015, 47, 1–33.
20. Afnan U.K. (2014) Data Confidentiality and Risk Management in Cloud Computing 2 Feb, 2019.