NATURALISTA CAMPANO
ISSN: 1827-7160
Volume 28 Issue 1, 2024

Study of Security in Privacy Techniques in Cloud ERP System.

Vivek Malvi[1], Anita Soni[2]

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

Email: [1]vivekmalvi18@gmail.com

Abstract: The aims to build an effective approach to the cloud ERP security management model in terms of data storage, data virtualization, data isolation, and access security in cloud ERP. The following proposed techniques are used to improve the security for multi-tenant SaaS: database virtualization, implementation of data encryption and search functionality on databases and developed systems, distribution of data between tenant and ERP providers, secure application deployment in multi-tenant environments, implementation of the authentication and developed systems together as a two-factor authentication, and improved user access control for multi-tenant ERP clouds.

Keywords: ERP Security, ERP Security Solutions, Cloud Computing.

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.

ERP is a software architecture that facilitates the flow of information between the different functions within an enterprise. 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 [1].

The cloud ERP software serves multiple customers as a platform with a new solution. This concept of cloud ERP could be confused with ERP hosting, which acts as a third party to support software infrastructure and application services delivered by the cloud environment. Others defined cloud ERP as cloud computing platforms used to provide services for businesses to be flexible in conducting their processes [2]. Supports cloud computing services for business embedded with capabilities of communications, for example, ERP systems [3]. The companies of cloud-based software can develop their functionalities speedily because cloud computing can improve the perspective of ERP deployment in innovative ways. The cloud users can use the provided services directly with speed of implementation. The moving from traditional ERP to the ERP cloud environment has critical issues with greater responsibilities, such as the possibility of attacks from the internet environment or from the internal and external security consultants of the cloud provider [4].

Security control problems can be reduced by using cloud ERP, which helps users to avoid conventional ERP systems, owing to the advanced security concerns that cloud providers can perform. One of the main challenges of data security is to ensure security controls in software and hardware using IT security experts, which can be offered by cloud providers with high levels of security, processing power, and storage units. A further essential challenge for cloud ERP is to establish suitable mechanisms of authentication and authorization owing to the service sharing with several tenants by the cloud provider. The cloud ERP provider, third party, and user should have their access roles to access the cloud ERP application interface using their authentication credentials. In

cloud ERP, there are many access control methods that can be used to ensure secure access of different tenants that share resources and services in the cloud environment [5].

2. Literature Review

Security tends to be more complex in cloud computing, and this tendency is becoming more pronounced. Although there are some studies regarding the techniques used in cloud computing, few researches enter the cloud ERP field.

In [6], the authors stated that cloud computing can be highly efficient and effective; however, along with these benefits, security vulnerability and risk have been increasing, especially regarding privacy and data loss. They provided a security threat evaluation model for use in measuring threats and negotiating security service level agreements (SLAs) that cover emerging security issues, as well as traditional aspects of security, such as integrity and confidentiality.

In [19], the authors proposed an algorithm through which the cloud service provider can give control to the user itself, using two different techniques, namely compression and encryption. The encryption technique uses two different keys for better security and is performed on the user side, and for compression they used an existing method of arithmetic coding. This hybrid model reduces the size of data saved to the storage space of the cloud server and increases the throughput of cloud computing.

In [7], the authors proposed a secure model for cloud computing based on the concept of two cloud service providers, where the storage service is provided to one cloud service provider (CSP) and the authentication, encryption/decryption, and auditing services to another CSP. In this model, data can be protected only from service provider, and not from external hackers. Thus, it is not highly effective for the user and service provider.

In [8], the authors proposed a double encryption strategy; one on the client side during file upload, and the other during file distribution. Moreover, they provide back up for the data stored in the cloud. They used the hashed message authentication code (HMAC) scheme for encryption of the data. However, the use two encryptions results in double the duration, which increases the time complexity.

In [9], the authors designed a new trust model for the security of cloud storage, which examines all outgoing cloud requests in real time to identify sensitive data, and uses the trusted platform module (TPM) to encrypt these data. They used Kerberos authentication service for user authentication. Kerberos is a secure method of authenticating requests for any service, and is used to authenticate end users of the trusted gateway.

In [10], the authors presented a cloud computing architecture focused on SaaS called multitenant, secure, and load disseminated SaaS architecture (MSLD). This architecture is divided into five services, one of which is the security service, which controls the authentication and authorization process. It validates that whether the incoming request is from a legitimate user. In addition, it confirms whether the requester possesses the rights to use the service.

Proposed Work

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:

The proposed encryption algorithm can assist in achieving secure multi-tenancy in the cloud encryption of data in the cloud ERP environment.

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.

A query is responded to over a consistent duration that does not rely on the request size. The public key cloud server is unable to read encrypted data or queries, because data can be decrypted only with the key provided by the data owner. Even with all the advantages of public cloud infrastructure, it is widely accepted that cloud storage suffers from major obstacles. These obstacles, such as data integrity, confidentiality, responsibility, and accessibility, from only authorized users are the major concerns in the public clouds. The customer is assured of data safety in the cloud from internal and external threats, because the data security guarantees that only cloud providers can provide data access.

It is a challenge to using public cloud servers to store clients' data. Data access policies should be enforced to protect confidentiality of the data stored on the public server. This problem is addressed in this work, which proposes a cryptographic technique. The data owner keeps the secret keys used to encrypt data before storing

them on a server; the only way to access the data is to supply the corresponding decryption key to the client. The robust systems should be able to defend against internal and external attacks of the organization.
To normalize data access and to improve the performance regarding access the data for two datasets, we propose the data on memory technique, which means we load the tenant databases on the memory at the beginning of the business day and then return it to the database at the end of the business day.

3. Conclusion

Security in privacy of ERP setup and implementation and maintenance requirements, training requirements affecting the efficiency of ERP, and the consumed time and cost for ERP customization. One practical solution that has been proposed is to use dynamic credentials to change values according to the user's location or data packets. Another proposed solution is to use digital signature for data security using recognizable RSA algorithms of data transferred over the Internet in cloud environment. This study purposes to build an effective approach of cloud ERP security management model in terms of data storage, data virtualization, data isolation, and access security in cloud ERP.

4. References

1. Patel & M. Kumar, (2013) "A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 4.
2. X. Xun, (2012), "From cloud computing to cloud manufacturing", Robotics and Computer-Integrated Manufacturing Vol. 28, pp75–86. New Zealand.
3. L. Bangfan, Z. Huihui, & W. Meng, (2014), "How to Design the Cloud Computing Used in Egovernment's Information Security?", Applied Mechanics and Materials, Vol. 536-537, pp616-619.
4. S. Na, K. Kim, & E. Huh, (2013), "A Methodology for Evaluating Cloud Computing Security Service-Level Agreements", International Journal of Advancements in Computing Technology (IJACT), Vol. 5, No. 13.
5. R. Muhleman, P. Kim, V. J. Homan, & J. Breese-Vitelli, (2012), "Cloud Computing: Should I Stay or Should I Cloud?", presented at the Conference on Information Systems Applied Research, New Orleans Louisiana, USA.
6. G. Reddy & N. Subashini, (2014), "Secure Storage Services and Erasure Code Implementation in Cloud Servers", International Journal of Engineering Research & Technology (IJERT), Vol. 3, No. 1, pp1810-1814.
7. P. Hofmann, (2010), "Cloud Computing: The Limits of Public Clouds for Business Applications",
8. IEEE Internet Computing, Vol.. 14, No. 6, pp90–93.
9. A. Satapathy, & J. Badajena, (2013), "A Secure Model and Algorithms for Cloud Computing based on Multi cloud Service Providers", International Journal Computational Intelligence and Informatics, Vol. 3, No. 1.
10. N. Sahin, (2013), "Cloud ERP Security: Guidelines for Evaluation", Department of Computer and Systems Sciences.