JOURNAL OF INFORMATION SYSTEMS ENGINEERING & MANAGEMENT

Journal of Information Systems Engineering & Management, 2017, 2(4), 21
ISSN: 2468-4376

lectito

Moving ERP Systems to the Cloud - Data Security Issues

Pablo Saa[1]*, Andrés Cueva Costales[2], Oswaldo Moscoso-Zea[1], Sergio Lujan-Mora[3]

[1] *Faculty of Engineering Sciences, Universidad Tecnológica Equinoccial*, Quito, ECUADOR
[2] *DGPCTI Public Company Yachay*, Quito, ECUADOR
[3] *Dept. of Software and Computing Systems, University of Alicante*, Alicante, SPAIN

*__Corresponding Author:__ psaa@ute.edu.ec

Citation: Saa, P., Costales, A.C., Moscoso-Zea, O. and Lujan-Mora, S. (2017). Moving ERP Systems to the Cloud - Data Security Issues. *Journal of Information Systems Engineering & Management*, 2(4), 21. https://doi.org/10.20897/jisem.201721

Published: August 30, 2017

ABSTRACT

This paper brings to light data security issues and concerns for organizations by moving their Enterprise Resource Planning (ERP) systems to the cloud. Cloud computing has become the new trend of how organizations conduct business and has enabled them to innovate and compete in a dynamic environment through new and innovative business models. The growing popularity and success of the cloud has led to the emergence of cloud-based Software-as-a-Service (SaaS) ERP systems, a new alternative approach to traditional on-premise ERP systems. Cloud-based ERP has a myriad of benefits for organizations. However, infrastructure engineers need to address data security issues before moving their enterprise applications to the cloud. Cloud-based ERP raises specific concerns about the confidentiality and integrity of the data stored in the cloud. Such concerns that affect the adoption of cloud-based ERP are based on the size of the organization. Small to medium enterprises (SMEs) gain the maximum benefits from cloud-based ERP as many of the concerns around data security are not relevant to them. On the contrary, larger organizations are more cautious in moving their mission critical enterprise applications to the cloud. A hybrid solution where organizations can choose to keep their sensitive applications on-premise while leveraging the benefits of the cloud is proposed in this paper as an effective solution that is gaining momentum and popularity for large organizations.

Keywords: ERP, cloud computing, cloud ERP, data security, confidentiality, integrity

INTRODUCTION

Nowadays, "the cloud" has been a buzzword in the last few years and has caused a revolution in the Information and Communication Technologies (ICT) industry. As IBM states "Cloud computing, often referred to as simply 'the cloud,' is the delivery of on-demand computing resources, everything from applications to data centers over the Internet on a pay-for-use basis" (IBM, 2015). This new trend changes the way organizations deploy services, platforms and infrastructure of Information Technologies (IT). The variety of applications and services offered by this new concept affect on one hand organizations and individuals who notice the benefits of cloud services in terms of efficiency, flexibility and reduced investment effort while on the other hand, technology companies and traditional operators see an opportunity to expand their businesses (Lin and Chen, 2012).

According to Gartner, cloud-based services can be defined as "massively scalable system capabilities delivered as a service to external users using Internet technologies" (Gartner, 2015). A study about cloud computing models describes that based on the completeness and abstraction levels of services delivered to the end user, there are

three types of services offered through the cloud, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) (Gorelik, 2013).

Cloud computing has marked a substantial change in how services of IT are developed, implemented, updated, maintained and paid for. The evolution from traditional service organizations to the emergence of full Internet based service providers, namely through the cloud, enables the provision of flexible, scalable and economical services (O'Loughlin, 2014).

In an environment of global competition, there is a growing recognition of the central role of IT in determining the overall success of organizations. The alignment of business objectives, strategic vision and information technology, combined with strategic planning, could be seen as a key objective to seek efficiency in their operations. Enterprise Resource Planning (ERP) systems have played an important role in the integration of business functions within organizations to support the generation of products and services (Shehab et al., 2004). In any modern organization, the term ERP refers to the software used to plan and manage the organization's resources across all functional areas by integrating the information through those functions and beyond the boundaries of the organization (Johansson et al., 2014).

In today's highly competitive business landscape, the trend for organizations is to focus their resources and efforts on what they do best and leave the supportive services in the hands of more specialized third parties. The world's economic model in IT today is moving from "buy and own" (on-premise) to a subscription based, pay-per-use (cloud-based) model. The migration from traditional (on-premise) ERP to cloud-based ERP could help organizations to manage their costs efficiently and improve their operations. Thereby, deploying ERP software in a hosted or on-demand environment could support organizations to improve their business processes and remain competitive.

Cloud-based ERP provide organizations with the possibility to choose the provider that best suits their needs, eliminating inflexible traditional on-premise ERP solutions. Lenart (2011) argued that while there are many advantages to the use of ERP implemented in a SaaS model, there also are drawbacks, especially those related to security and integrity of the data stored in the cloud.

Hence, the research question explored in this paper is:

"**What are the data security issues in cloud-based SaaS ERPs**?"

The structure of this paper is the following. Section II presents the methodology used in this study. Following that, Section III describes a literature review done on cloud-based ERP and compares the advantages of ERP when adopted as a pay-per-use model versus the traditional on-premise solutions. Section IV presents several findings based on cloud ERP and illustrates the adoption factors and the benefits for small, medium and large organizations. Finally, in sections V and VI, the paper concludes with recommendations for organizations to ensure the security of sensitive corporate information when adopting cloud-based ERP.

METHOD

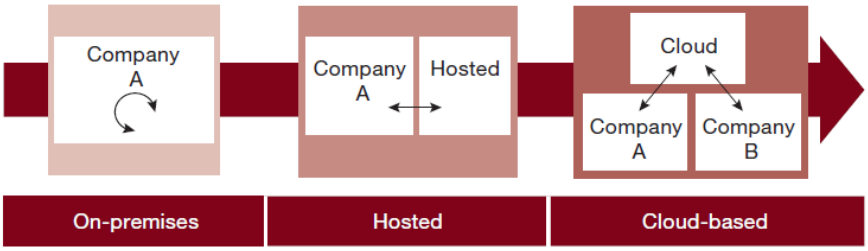
The research approach was based on an exploratory search to review the existing literature on SaaS cloud-based ERPs and its benefits. Additionally, several papers were studied to identify issues on data security, particularly confidentiality and integrity problems that organizations should be aware of before adopting cloud-based ERP solutions. More than 50 articles from 2008 to 2015 were found from several A and A* journals (CORE, 2017) like Journal of Information Systems, MIS quarterly, Journal of Innovation, Management and Technology, Journal of Systems and Information Technology, International Journal of Computer Applications, Journal of Network and Computer Applications among others. Searches were made using remarked academic databases and search engines for Computer Science and Information System fields: IEEE Xplore, Emerald, ACM Digital Library, Gartner Core Research, Science Direct, and Google Scholar. Furthermore, specific search terms included "cloud ERP", "hybrid ERP", "implementation of ERP", "SaaS ERP", "cloud computing", "data security issues".

After reviewing all the articles and papers, key insights and findings were gathered and classified according to the size of organizations. Based on the findings, several recommendations and possible solutions are outlined in this paper.

LITERATURE REVIEW

Cloud ERP

The success of cloud computing combined with the increasing pressure on organizations to respond to unique customer needs in the increasingly competitive business environments of today, has given rise to the new subscription based delivery model for ERP, also referred to as cloud-based ERP or SaaS ERP. This new model of ERP systems functions in the same way as a traditional on-premise ERP solution. The main difference is that the



	On-premises	Hosted	Cloud-based
Implementation size	Large	Medium	Small to medium
Solution complexity	High	Medium	Low
Capital costs	High	Medium	Low
Operating costs	Low to medium	Medium	Medium
Implementation time	12–36 months	9–18 months	4–8 months

Figure 1. ERP systems deployment models (Utzig et al., 2013)

infrastructure (software as well as hardware and network connection) adopts a pay-per-use model or in other words, ERP is delivered as a service (Johansson, et al., 2014). The ERP in a SaaS model is accessed over the Internet while the application and data is controlled by the cloud service provider and offered as a "ready-to-use" product to the end client for a monthly subscription fee (Johansson and Ruivo, 2013).

Traditional ERP vs Cloud ERP

A cloud-based ERP system uses the advantages of cloud computing to offer a new and more flexible approach to host and use ERP systems. A widespread shift from traditional ERP system architecture towards cloud-based SaaS ERP systems is ongoing (Lenart, 2011). The advantages of cloud computing are for example easy usage and accessibility, virtualized resources, scalability, affordability and availability, guaranteed through service level agreements (SLA) (Vaquero et al., 2008). Cloud computing, and in particular the SaaS technology, enables ERP systems to invert some of their typical weaknesses which are inflexibility, no scalability and consummation of massive local resources (hardware, man power as well as financial expenditures) into advantages. Although, significant concerns remain: limited functionality, the potential loss of internal control, performance reliability, and security among them, cloud-based models continue to gain traction (Utzig et al., 2013).

Figure 1 shows a clear understanding about the differences on operating costs, solution complexity, and implementation time of a traditional on-premise ERP system in comparison to cloud-based ERP systems.

The advantages of cloud-based ERPs in comparison to traditional ERPs (Johansson and Ruivo, 2013) are:

- Enables smaller clients who are not able to setup a complete, complex ERP system on-premise to use ERP.
- Saves infrastructure expenditures (no large upfront capital investment necessary), software, maintenance and updating costs (Elragal and Kommos, 2012).
- Reduces the staff needed for support and maintenance.
- Enables faster implementation of a cloud-based ERP with less effort needed due to their agile design (Elragal and Kommos, 2012).
- Offers better scalability (hardware/performance/user accounts can be increased quickly when needed but can also be easily reduced as well when resources are not needed anymore).
- Enables mobility (It does not matter where the employees work, the server in the cloud is always accessible).

In the other hand, there are possible disadvantages as:

- Organizational data is stored in the cloud and not on-premise.
- Possible integrity and security issues due to loss of control over data storage and system.
- Dependency on the cloud provider.

Data Security Issues in Cloud ERP

As discussed in the previous sections, there is a clear tendency to move enterprise services and systems to the cloud. However, it is important for organizations that want to implement or use an ERP in the cloud (SaaS, PaaS or IaaS) that they address the possible issues and risks of migration. Some of the main drawbacks in any cloud-based ERP are related to data security, performance and availability (Dillon et al., 2010). Dillon et al. (2010) have

categorized security of data as the primary concern for organizations. Accordingly, this paper is focused on data security issues for cloud (SaaS) ERP.

Bishop (2005) states that computer security relies on the confidentiality, integrity and availability of data. From that context, cloud computing and ERP systems directly influence the required level of security. For example, as mentioned in the previous sections, ERP systems manage organizational data for essential business operations. Therefore, it is crucial for organizations to ensure data confidentiality and integrity in a cloud environment.

Confidentiality

Weng and Hung (2014) explain that when organizations adopt cloud-based ERP systems, they should be prepared to mitigate the risks around cloud technologies and prevent unauthorized usage of data. In addition, Johansson (2015) discover that organizations might feel insecure storing their data at external providers without having a direct control over the data. Another problem that might affect the confidentially of data is the lack of control over the staff from the cloud provider, who could access and retrieve data for dishonest or even criminal activities. For instance, Hashizume et al. (2013) argues that providers might not perform detailed background checks on their staff which has unlimited access to the cloud data. Consequently, the key challenges to adopting cloud-based ERP are:

1) Uncertainty around data storage arrangements

In the SaaS model the client does not have any control over the IT infrastructure (Kumar et al., 2012). Moreover, Puthal et al. (2015) mention that the same provider often hosts data from several clients in the same data center. This type of hosting increases the risk of data leakage or corporate espionage. On the contrary, with on-premise ERP systems, organizations have absolute control over their data and infrastructure. Consequently, the way in which providers ensure the security and confidentiality of the client's data is one of the key challenges in the implementation of cloud-based ERP. Furthermore, in cases where the provider also offers public access to specific cloud services, the security challenges are even higher.

2) Lack of control over the security protocols and standards

Even though the number of security reported incidents from the industry in cloud-based ERPs is still small, its fast adoption increasingly raises security concerns for organizations, much more than traditional on-premise ERPs did (Castellina, 2011). Furthermore, the clients do not have full control or monitoring capabilities about who accesses their data from the provider side (Hashizume et al., 2013). The same applies to the protocols and standards used by providers to hire personnel, to implement or to monitor their security infrastructure. Consequently, as these factors are dependent from the provider itself, a high level of uncertainty must be considered when implementing ERP on the cloud.

Integrity

The second main concern of securing enterprise data in the cloud is the need to ensure uniformity of the stored data. As mentioned by Puthal et al. (2015), the integrity of data can easily be lost or affected because of cloud providers' errors and failures. The same authors also argue that the traditional enterprise methods to validate the correctness of data are outside the enterprises' control, they are the responsibility of the cloud provider. As a consequence, a common method used to ensure data integrity in cloud environments is public auditing. This method uses a third-party verifier that provides expert integrity checking services (Puthal et al., 2015). Even though the method we mention is commonly used by cloud providers, it raises additional issues like the risk of sensitive information leakage from organizations using cloud providers. From a similar perspective, Akande et al. claim that the methods of authentication and the levels of authorization to manipulate data are crucial concerns for the overall data integrity (Akande et al. 2013). Finally, the process of selecting and adopting a cloud provider should also take into consideration the following challenges:

1) Relationship of trust between the cloud provider and client

Assuring the integrity of data is mainly the responsibility of the provider. Therefore, clients must trust the providers to comply with the agreed-on security measures and protocols to achieve integrity of data. As mentioned by several authors (Peng and Gala, 2014; Subashini and Kavitha, 2011), the relationship of trust is based not only on the provider's reputation but also on the specifications of the SLAs between them.

2) Provider's transaction management standards

Subashini and Kavitha (2011) argue that in complex settings like cloud computing, there is a high degree of difficulty to assure data integrity. They discuss that the HTTP transaction protocol does not provide guaranteed delivery of data. Additionally, the study shows that SaaS applications should be based on standardized application program interfaces (APIs) as a technological basis for inter organizational systems communication. Standardized APIs ensure that only intended data read and write access is allowed. However, this best practice to manage data integrity is often not considered by cloud services provider.

Table 1. Data security issues

Issue	Description
Confidentiality	Lack of data control Lack of staff control from cloud provider Uncertainty on data storage arrangements Lack of control over security protocols and standards
Integrity	Lack of uniformity on stored data Information leakage by third-parties over organizations using cloud providers Lack of trust between the cloud provider and client Beware of provider's transaction management standards
Availability	Depends on cloud provider

Based on the literature review, **Table 1** resumes major data security concerns that IT leaders should consider in order to move their ERP systems into the cloud.

FINDINGS

Cloud technologies provide a disruptive alternative to traditional on-premise ERP solutions and are offering innovative ways to generate business value and maintain competitive advantage (Weng and Hung, 2014). In addition to the myriad of benefits that cloud-based ERP offers like flexibility, scalability, ease of implementation and cost savings (Utzig et al., 2013), one of the biggest impediments to adopt cloud-based ERP is the risk around data security, namely integrity and confidentiality of the organizations data. In a recent survey conducted by the IDC group, of the 1,100 organizations surveyed on the top inhibitors for cloud-based ERP solutions, 50% of the organizations responded saying security and confidentiality of the data is their primary concern when thinking about moving their enterprise systems to the cloud (Fauscette, 2013) as is stated on **Figure 2**.

SaaS is gaining popularity and is changing the way organizations deploy and use ERP systems. However, the concerns around data integrity and confidentiality need to be addressed before organizations can successfully implement SaaS based ERP solutions. Additionally, existing literature also shows that adoption rates for cloud-based ERP are highly dependent on the industry type and functions (Clarke et al., 2014). Given the important role that ERP systems play in the functioning of an organization, having to move mission critical applications to a third-party cloud vendor and the security issues associated could negatively impact the SaaS based ERP adoption rates (Johansson et al., 2013).

It can be gathered from literature that due to the low capital expenditure and accelerated time to market, Small to Medium Enterprises (SMEs) benefit from cloud-based ERPs more easily since many of the issues and challenges spin prevalently around data security, confidentiality and concerns regarding relocating mission critical applications to the cloud, which are often no primary concerns to SMEs (Johansson et al., 2014; Wailgum, 2008). The risks

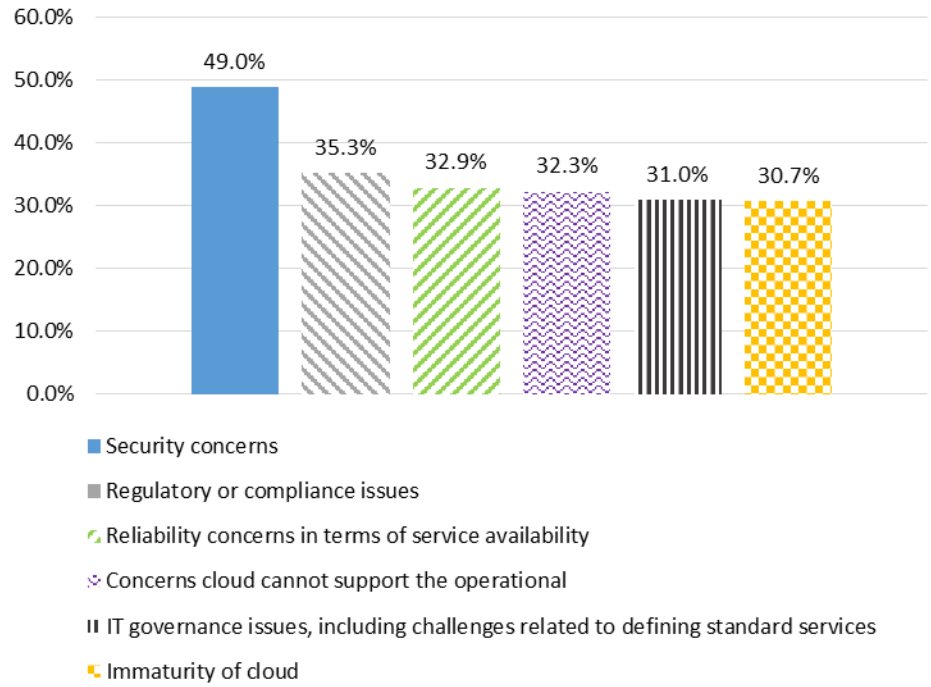


Figure 2. Top inhibitors for cloud ERP (Fauscette, 2013)

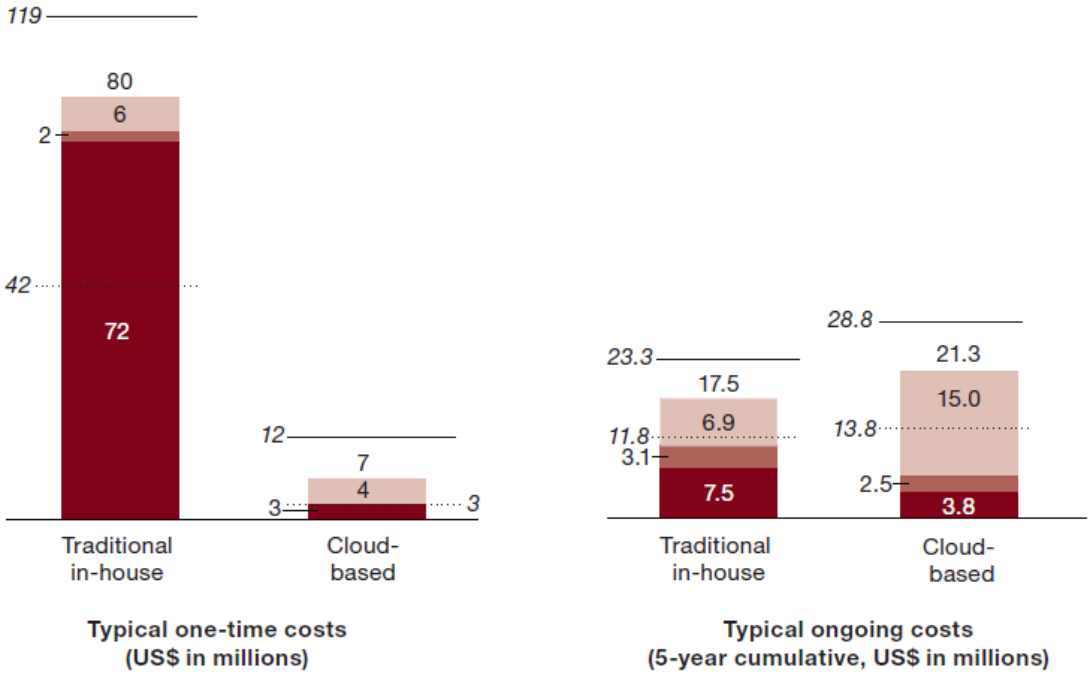


Figure 3. Cost comparison of on-premise and cloud-based solutions (Utzig et al., 2013)

associated with storing an organization's sensitive data on the cloud and its associated data confidentiality and integrity issues are less of an inhibitor for SMEs while adopting cloud-based ERP, as they do not possess the financial resources to build and implement an on-premise ERP solution in the first place (Johansson et al., 2014). SMEs also believe that due to their lack of IT expertise, the security measures that the cloud-based ERP vendors provide are more sophisticated than those that they could implement on-premise. In the long run, the operational expenditure of a cloud-based ERP solution is far less for SMEs, thereby, enabling them to reduce their overall IT expenditure but at the same time allowing them to gain access to state of the art IT infrastructure and expertise through a pay-per-use model (Johansson et al., 2014). A SaaS ERP solution also gives SMEs the opportunity to effectively channelize their resources to focus on the important aspects of their business, enabling them to maintain their competitive advantage (Johansson et al., 2014).

On the other hand, for larger organizations cloud-based ERP implementations raise a lot of security concerns, as they feel insecure to store their confidential and sensitive information on the cloud, as they have to handover the control to the provider to process the information. Larger organizations are heavily concerned about the probability and impact from a potential security breach that could for example damage their reputation, result in financial losses and in some cases, even stand for industrial espionage (Johansson et al., 2014). As a result of these concerns, larger organizations are not motivated to move their mission critical applications to the cloud and since they have normally highly skilled internal IT teams, they prefer to implement on-premise ERP systems with high security standards. Another factor that influences larger organizations to continue with their on-premise ERP solutions is the subscription model associated with SaaS based solutions. Due to the large user base and the number of ERP modules of these organizations, in the long run the subscription fees for cloud-based ERPs are higher than the cost of implementing and maintaining an on-premise solution (Johansson et al., 2014). Thus, Utzig et al. (2013) states that "the total cost of ownership for a cloud-based solution can be 50% to 60% less than for traditional solutions over a 10-year period". In other words, moving their on-premise ERP systems for large organizations cannot be engaged or related with cost savings. A previous study from Utzig et al. (2013) shows on **Figure 3** the cost comparison between on-premise and cloud-based solutions.

RECOMMENDATIONS AND POSSIBLE SOLUTIONS

Given the existing concerns about data security in cloud-based ERPs, organizations should take proactive measures to ensure that sufficient data security policies and procedures are in place and negotiated with the cloud vendor in order to secure the confidentiality and integrity of the sensitive corporate data (Clarke et al., 2014). Following are some recommendations that organizations, specifically large enterprises should follow before moving their ERP applications to the cloud (Weng and Hung, 2014):

- Organizations should negotiate stringent policies and SLAs with cloud vendors to ensure protection of sensitive information stored in the cloud. The policies should clearly outline and define what types of information are classified in which way.
- The internal IT teams and security experts of the organizations should always be involved when evaluating cloud vendors and their security standards.
- Organizations should always perform an extensive analysis and implement control mechanisms before sharing confidential and sensitive information to cloud vendors.
- Organizations should evaluate which applications are critical to their business to maintain their competitive advantage and thereby, define strict policies for the information and applications that could be moved to the cloud.
- Cloud vendors should be transparent about their network security infrastructure and should provide this information to the client.
- Organizations should educate their employees, by conducting employee education training programs and campaigns about data security risks that are possible in cloud-based ERPs and the necessary actions to mitigate those risks to ensure sensitive corporate information is not compromised (Clarke et al., 2014).

In addition to the above recommendations, organizations should also ensure that a comprehensive security strategy is defined before migrating their enterprise applications to the cloud. Specific security standards need to be enforced at all levels by incorporating a framework that addresses security at the physical, network, data and application level (Binu and Meenakumari, 2012). A security framework should include components relating to the physical security, data storage security, access security, application security and transmission security. Physical security policies should include rules of conduct for employees and mechanisms to ensure those rules are being followed.

Strict access security policies to prevent unauthorized access from internal and external sources should be enforced as well. Application security should include authentication mechanisms to verify the identity of the end users. Data security should always include strong encryption techniques to prevent any possible data leakage (Kumbhar et al., 2012). Furthermore, the authentication module should exactly define what level of access each user has.

Additionally, mechanisms to ensure integrity of data and to safeguard its uniformity across multiple locations should be put in place. In order to assure confidentiality and integrity of data, its transmission to the provider should be secured by the application of encryption mechanisms. The recommended measurement should be applied in both the provider and the client sides (Binu and Meenakumari, 2012). This should include a contingency plan that allow the organization to have the capability and resources to move to a new cloud provider in case of an emergency in the shortest possible time with less impact.

SMEs are more open to move the entirety of their applications to the cloud whereas larger organizations are still more conservative in their approach due to the risks associated with potential security breaches and their ability to implement high security standards for their on-premise solutions themselves (Johansson et al., 2014). Thus, SMEs adopt cloud-based ERP solutions at a faster rate than larger organizations. However, a recent development that is gaining popularity and momentum among larger organizations is that of a two-tier ERP strategy also known as hybrid cloud-based ERP. Accordingly, Ruivo et al. (2015) argue that more than 77% of IT firms will implement hybrid ERP solutions, however only over 20% currently have structured plans to implement this technology. In addition, Peng and Gala (2014) also consider a hybrid ERP as an effective solution for organizations to keep on-premise ERP core functions combined with business cloud services, before moving to full cloud-based ERP solution.

Hybrid cloud-based ERP provides organizations with the best of both worlds. Organizations can choose to keep their mission critical applications on-premise while migrating the other modules of the ERP into the cloud. A report from PwC (Clarke et al., 2014) suggests that one of the key aspects of hybrid ERP is allowing organizations to take out functions from on-premise ERP to the cloud. Therefore, providing organizations with a higher degree of flexibility to support business operations with the use of cloud technology. For instance, the same report shows that the core operations related to inventory, financials or employee master management, could remain as part of the on-premise ERP. This agile and highly flexible approach allows them to implement more sophisticated, customer driven business models (Columbus, 2015). It enables organizations to take advantage of the cloud-based ERP benefits while minimizing the risks for storing sensitive corporate data on the cloud (Peng and Gala, 2014).

CONCLUSION

Several benefit drives of cloud computing encourage organizations to evaluate and implement an ERP system in the cloud, based on the distribution model SaaS. This new approach to ERPs turns some of the weaknesses of

traditional ERPs into benefits. The main benefits of cloud-based ERPs are its scalability and lower investment costs, creating opportunities for SMEs.

However, the main weaknesses and threats to this new approach are the security and integrity risks to the data stored in the system, which have been discussed in this paper. Especially large organizations adopt cloud-based ERP systems only very slowly due to concerns in regards to storing sensitive information on third-party servers. The risk of breaches in security and integrity as well as possible misuse of confidential information by the service providers are further drawbacks.

Nevertheless, a new type of solution has begun to take hold in large organizations in order of combining the best of both worlds (cloud and traditional ERPs): Hybrid cloud-based ERPs or two tiered ERPs. Hybrid cloud-based ERPs allow organizations to store their most sensitive data on-premise solutions while migrating the other modules into a cloud solution. This enables them to benefit from the agility and scalability of cloud-based ERP solutions while still keeping the security advantages from on-premise solutions for their mission critical data. Another benefit inhered from cloud-based solutions is the ability to deploy services on-demand, reducing the risk associated with the implementation of an entire module for a core on-premise ERP. Moreover, the ability to enhance mobility, system performance and customization are some of the remarked benefits why organizations are moving to hybrid ERP solutions (Peng and Gala, 2014). Therefore, hybrid cloud-based ERPs they are especially suitable for larger optimizations which have been hesitating to move into the cloud with their ERPs so far.

ACKNOWLEDGMENTS

An initial version of this paper was published as "Data Security Issues in Cloud-Based Software-as-a-Service ERP" (Saa et al., 2017), in the 12th Iberian Conference on Information Systems and Technologies (CISTI'2017).

REFERENCES

Akande, A.O., April, N.A. and Van Belle, J.-P. (2013). Management Issues with Cloud Computing. *Proceedings of the Second International Conference on Innovative Computing and Cloud Computing (ICCC)*, Wuhan, China, pp. 119-124. https://doi.org/10.1145/2556871.2556899

Binu, M.S. and Meenakumari, J. (2012). A security framework for an enterprise system on cloud. *Indian Journal of Computer Science and Engineering (IJCSE)*, 3(4), pp. 548-552.

Bishop, M. (2005). *Introduction to computer security*. Boston, MA: Addison-Wesley.

Castellina, N. (2011). *SaaS and Cloud ERP Trends, Observations, and Performance 2011*. Analyst Inside.

Clarke, N., Dawson, D., Heard, K. and Manohar, M. (2014). *Beyond ERP: new technology, new options, strategy and pwc*. [online] Available at: http://www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/beyond-erp [Accessed 23 Jan. 2017].

Columbus, L. (2015). *Five Catalysts Accelerating Cloud ERP Growth In 2015. Forbes*. [online]. Available at: http://www.forbes.com/sites/louiscolumbus/2015/01/27/five-catalysts-accelerating-cloud-erp-growth-in-2015 [Accessed 23 Jan. 2017].

CORE, CORE Rankings Portal (2017). [online] Available at: http://portal.core.edu.au/jnl-ranks [Accessed 23 Jan. 2017].

Dillon, T., Wu, C. and Chang, E. (2010). Cloud computing: issues and challenges. *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, Perth, WA, pp. 27-33. https://doi.org/10.1109/AINA.2010.187

Elragal, A. and Kommos, M.E. (2012). In-house versus in-cloud ERP systems: a comparative study. *Journal of Enterprise Resource Planning Studies*, 2012, p. 659957. https://doi.org/10.5171/2012.659957

Fauscette, M. (2013). *ERP in the Cloud and the Modern Business*. [online] Available at: https://go.oracle.com/LP=1093?elqCampaignId=2026 [Accessed 23 Jan. 2017].

Gartner (2015). *Cloud Computing*. [online] Available at: http://www.gartner.com/it-glossary/cloud-computing [Accessed 27 Sep. 2015].

Gorelik, E. (2013). *Cloud Computing Models*. Massachusetts Institute of Technology.

Hashizume, K., Rosado, D., Fernández-Medina, E. and Fernandez, E. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), pp. 1-13. https://doi.org/10.1186/1869-0238-4-5

IBM. (2015). *Computing as a service over the internet*. [online] Available at: http://www.ibm.com/cloud-computing/learn-more/what-is-cloud-computing [Accessed 1 Feb. 2017].

Johansson, B., Alajbegovic, A., Alexopoulos, V. and Desalermos, A. (2014). *Cloud ERP Adoption Opportunities and Concerns: A Comparison between SMEs and Large Companies*. IT Operations Management (ITOM2014).

Johansson, B., Alajbegovic, A., Alexopoulo, V. and Desalermos, A. (2015). Cloud ERP Adoption Opportunities and Concerns: The Role of Organizational Size. In *48th Hawaii International Conference on System Sciences (HICSS)*, Johansson, Kauai, HI, pp. 4211-4219.

Johansson, B. and Ruivo, P. (2013). Exploring factors for adopting ERP as SaaS. *Procedia Technology*, 9, pp. 94-99. https://doi.org/10.1016/j.protcy.2013.12.010

Kumar, V., Garg, K.K. and Quan, C.-L. (2012). Migration of services to the cloud environment: Challenges and best practices. *International Journal of Computer Applications*, 55(1), pp. 1-16. https://doi.org/10.5120/8716-7105

Kumbhar, N.N., Chaudhari, V.V. and Badhe, M.A. (2012). The Comprehensive Approach for Data Security in Cloud Computing: A Survey. *International Journal of Computer Applications*, 39(18), pp. 23-29. https://dx.doi.org/10.5120/5080-7433

Lenart A. (2011). ERP in the Cloud–Benefits and Challenges. In *Research in systems analysis and design: Models and methods*. Heidelberg, Germany: Springer Berlin, pp. 33-50. https://doi.org/10.1007/978-3-642-25676-9_4

Lin, A. and Chen, N.C. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32(6), pp. 533-540. https://doi.org/10.1016/j.ijinfomgt.2012.04.001

O'Loughlin, M. (2014). IT Service Management and Cloud Computing. [online] Available at: https://www.axelos.com/case-studies-and-white-papers/it-service-management-and-cloud-computing [Accessed 23 Jan. 2017].

Shehab, E., Sharp, M., Supramanian, L. and Spedding T. (2004). Enterprise resource planning: An integrative review. *Business Process Management Journal*, 10(4), pp. 359-386. https://doi.org/10.1108/14637150410548056

Peng, G.C. and Gala, C.J. (2014). Cloud ERP: a new dilemma to modern organizations? *Journal of Computer Information Systems*, 54(4), pp. 22-30. https://doi.org/10.1080/08874417.2014.11645719

Puthal, D., Sahoo, B., Mishra, S. and Swain, S. (2015). Cloud Computing Features, Issues, and Challenges: A Big Picture. *International Conference on Computational Intelligence and Networks (CINE)*, Bhubaneshwar, pp. 116-123. https://doi.org/10.1109/CINE.2015.31

Ruivo, P., Rodrigues, J. and Oliveira, T. (2015). The ERP Surge of Hybrid Models-An Exploratory Research into Five and Ten Years Forecast. *Procedia Computer Science*, 64, pp. 594-600. https://doi.org/10.1016/j.procs.2015.08.572

Saa, P., Cueva, A., Moscoso-Zea, O., Lujan-Mora, S. (2017). Data Security Issues in Cloud-Based Software-as-a-Service ERP. In *12th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1828-1834. https://doi.org/10.23919/CISTI.2017.7975779

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1), pp. 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

Utzig, C., Holland, D., Horvath, M. and Manohar, M. (2013). *ERP in the cloud.* [online] Available at: http://www.strategyand.pwc.com/media/file/Strategyand_ERP-in-the-Cloud.pdf [Accessed 1 Feb. 2017].

Vaquero, L.M., Rodero-Merino, L., Caceres, J. and Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, 39(1), pp. 50-55. https://doi.org/10.1145/1496091.1496100

Wailgum, T. (2008). *Impact of SaaS on the enterprise ERP market. InfoWorld.* [online] Available at: http://www.infoworld.com/article/2652900/applications/impact-of-saas-on-the-enterprise-erp-market.html [Accessed 23 Jan. 2017].

Weng, F. and Hung, M.-C. (2014). Competition and Challenge on Adopting Cloud ERP. *International Journal of Innovation, Management and Technology*, 5(4), pp. 309-313. https://doi.org/10.7763/IJIMT.2014.V5.531

