International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 4 Issue 2, February – 2020, Pages: 37-44

Secure Cloud-Based Academic Enterprise Resource Planning (Caerp) Model For A Higher Institution

Ibrahim Adabara[1], Sanni Shamsudeen[2], Margaret Kareyo[3], Ajiboye Priscilla Oyeladun[4], Faseun Yusuf Olusola[5]

[1]Department of Electrical and Computer Engineering, Kampala International University, Uganda.
Email: connectadabara@gmail.com
[2]Department of Computer Science and Information Technology, Kampala International University, Uganda.
Email: sanniade01@gmail.com
[3]Department of Computer Science and Information Technology, Kampala International University, Uganda.
Email: magsterkami@gmail.com
[4]Department of Electrical and Computer Engineering, Kampala International University, Uganda.
Email: oyeladri@gmail.com
[5]Department of Computer Science, Kampala International University, Western Campus Uganda.
Email: faseun.yusuf@kiu.ac.ug

Abstract: *Academic Enterprise Resource Planning (ERP) systems are meant to integrate the separate activities, processes, and functions within a higher institution to help streamline the process and to provide real-time, on-demand information needs. The volume of data produced by academic institutions grows every day. Due to the increasing numbers of staff, students, departments, and programs, this continuous growth requires continuous scaling and improvement of the academic ERP system. Therefore, to adapt to this continuous growth, the system should be constructed based on a cloud computing platform. Cloud-based Enterprise Resource Planning system address many security and privacy issues in higher institutions: the increase of data/information, cost of hardware/software, data alteration, loss of data during migration from one server to another server, limited teaching materials and resources, high administrative costs, difficulties in managing large population of learners against small number of lecturers. This study designed a security and privacy model for an academic cloud-based ERP system. which recommend that higher institution should migrate to cloud computing, Infrastructure as a Service (IaaS) should be adopted since higher institution are concerned with security and privacy issues in the cloud, Data Encryption, and Tokenization should be used when storing data/information in the cloud and also comply with the ISO27002 security standard after migrating to the cloud. Hence, it is undeniable that a cloud-based ERP system provides a secure environment, reduces costs in terms of hardware, software, upgrades, up-front expenses, and promotes mobile computing, which is the ability to access resources from anyplace at any time.*

Keywords: Cloud Computing, ERP, Higher Institution, IaaS, PaaS, Privacy SaaS, and Security

Introduction

It is a known reality that Higher Institutions of learning play a significant role in the growth of societies (Alharthi et al., 2017). Like many other organizations, these institutions employ Information and Communication Technology and other internet-based services. However, Academic Institutions in developing countries still lag in incorporating advanced technologies (A Al - Shqeerat et al., 2017). This is attributed to inadequate ICT infrastructure, financial constraints, lack of space to meet the high demand in the education sector, the increase of data due to the growing population in Higher Institutions, cost of hardware/software, data alteration/theft, loss of data during migration, limited teaching materials and resources such as books, journals, and libraries, high administrative costs and difficulties in managing large population of learners against small number of lecturers and other violation to server-based ERP systems (Surendro & Olivia, 2016).

Academic Enterprise Resource Planning (ERP) systems are meant to integrate the various activities, processes, and functions within a Higher Institution in order to streamline the process and to provide real-time, on-demand information needs (Muli & Kimutai, 2015). However, as these activities, processes, and functions continue to grow, more resources are needed to manage the system. The volume of data produced grows every day due to the increase in staff members, students, department as well as academic programmes (Ibrahim Adabara, Sanni Shamsudeen, Ajiboye Adeleke Raheem, 2018). Cloud Computing is the delivery of services, servers, storage, databases, networking, software and more, over the Internet to offer faster innovation and flexible

resources (Kattimani & Mallinath, 2017). In order to adapt to these emerging trends, and Academic ERP system must be migrated to the cloud-computing platform and such platforms offer improved security and privacy, reduce hardware, software procurement, and maintenance cost. It also serves as a reliable backup for future reference in the event of disasters. Nevertheless, the numerous advantages presented by cloud computing, Higher Institutions continue to worry about the security and privacy of their data/information in the cloud (Venkatachalam & Arts, 2017). Hence, this paper proposes a security and privacy model which will help to secure data/information while implementing or migrating from server-based to cloud-based ERP system.

Generally, there are three types of cloud computing service models. These include: Cloud service models

Software as a service (SaaS): This is the highest layer and comprises a complete application layer offered as a service, on-demand, via multi-tenancy. For example, Salesforce, Facebook, LinkedIn, Intuit, Google Apps and Microsoft Office Live offer basic business services such as e-mail and messaging using the SAAS model (Sanchez-Puchol et al., 2017). In this model, the client has no role to play in the security of the system, and the service is accessed over the internet.

Platform as a Service (PaaS): Consumers using PaaS can develop and/or deploy applications by using the provider's services and tools. PaaS providers provide tools for every phase of software development and testing which can be utilized to deploy any service quickly. Examples include Google App Engine and Microsoft Azure (Sanchez-Puchol et al., 2017), allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure.

Infrastructure as a Service (IaaS): Offers a means of delivering basic storage and compute capabilities as standardized services over the network. Amazon (AWS) and Rackspace are IaaS providers, which provide servers, storage, and other computing resources. In securing the model both the service provider and the client have roles to play.

A cloud deployment model is a "configuration" of certain cloud environment parameters such as storage size, accessibility, and proprietorship. To choose the most suitable one, it is better to make a choice based on their computing, networking, storage requirements, business goals, as well as available resources.

The four main cloud deployment models are listed and explained below. However, there are also web-based organization systems that are not so widespread, such as virtual private, inter-cloud and others.

Public Cloud: In this model, a single organization generally owns the infrastructure. The infrastructure is made available for public or other organizations and is leveraged to provide different services. This is currently the most widely used model globally.

Private Cloud: In this model, the infrastructure is utilized by a single organization and hence, it is not made available to anyone outside the organization. The infrastructure can either be managed by the organization or another organization may manage it on behalf of the first organization.

Community Cloud: In the model, the infrastructure is shared among multiple organizations, which may share a set of common goals and requirements among themselves. The infrastructure of this type is managed by different members of the community using a predetermined level of agreement.

Hybrid Cloud: In this model, the cloud infrastructure is a combination of two or more other cloud models where particular application scenarios prohibit the usage of a certain cloud model.

Cloud Computing in Education Environment

The future of Information Technology in education is anticipated zeroing around accessing resources for learning, teaching, and collaboration. This point to cloud computing as the future of technology in education. The students can use cloud services to aid independent learning, which enables them to study in their way from anywhere. The collaboration can be achieved using shared applications such as Google Apps and Office 365 which allow students and teachers to work on the same documents from anywhere in the world. With cloud computing, teachers and students can be connected within and outside their campuses, and classrooms can be everywhere since educational resources will be available around the clock(Mircea & Andreescu, 2012).

The figure below shows services that could be attached to the education cloud.

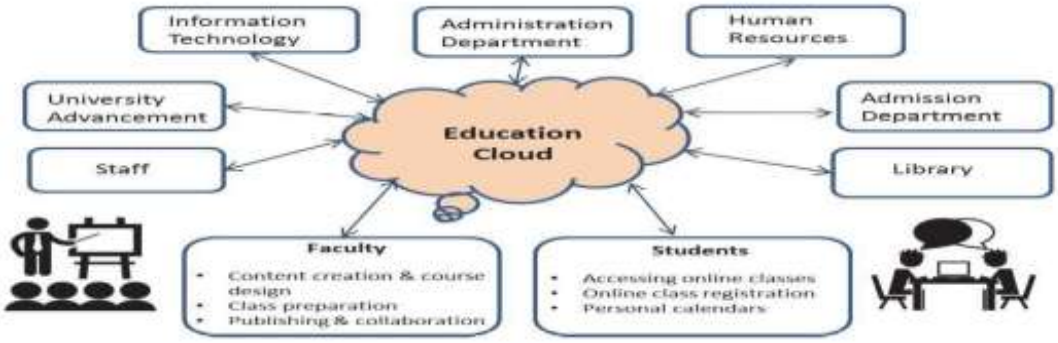

Figure 1: Cloud services for Higher Education

Consumer acceptance of Web-based cloud services for everything from e-mail to video is, of course, becoming universal, and educational institutions are following suit. Many higher educational institutions, for example, use Google Apps for email and to create documents and spreadsheets, bypassing capital investments in servers and software licenses.

Cloud vendors are a unit competitive, with innovation and new business models to match the needs of different colleges and universities. The figure below shows how different departments and university users may consume services from cloud computing architectures.

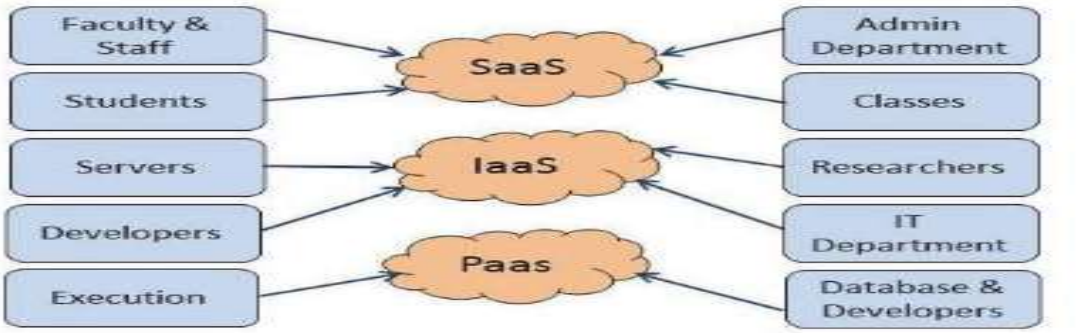

Figure 2: Users of education cloud services

Security and Privacy in the Cloud

Security is the right not to have one's activities adversely affected via meddling with one's objects. In an equally succinct way, According to (Vanbaelen & Harrison, 2011) "Privacy is the right to have information about oneself left alone.

Similarly, privacy as the selective control of access to "self." Selective control refers to the process where individuals control their interaction and information exchange with others. Individually try to control their privacy by controlling their openness to others. (*Higher Education | Pearson*, n.d.) in 2009 explains that the level of the openness between individuals is determined by their relationship and the value given to the information safeguarded.

Classic "CIA" Security Triad. A classic definition of security in terms of its essential characteristics specifies it in terms of the CIA triad; the acronym "CIA" stands for confidentiality, integrity, and availability which is the three critical requirements for any secure system (Mokia & Rolen, 2012; Zhang et al., 2010).

They are defined as follows:

Confidentiality: It is the power to cover information from those folks unauthorized to look at it. It is the premise of many security mechanisms protective not solely information, however different resources.

Integrity: It is the ability to ensure that data is an accurate and unchanged representation of the original information.

Availability: It ensures that a resource is quickly accessible to the approved user upon the user's request.

This model is applicable across the whole subject of security analysis, from access to a user's Internet history to the security of encrypted data across the Internet. (Singh et al., 2016). Security and privacy in clouds over the years, many researchers have surveyed and studied the issues of privacy and security in cloud environments. To better comprehend those problems and their connections, technology researchers and experts have taken advantage of different criteria to establish a general impression. (Jensen et al., 2009) Recommend modeling of the security ecosystem in terms of three cloud system participants: service instance, service user, and the cloud provider. Furthermore, they identify attack categories: user to service, service to the user, user to the cloud, cloud to the user, service to the cloud, and cloud to service. While cloud computing is associated with numerous security and privacy problems, it can be made active by implementing efficient solutions.

Security models

The Bell-Lapadula confidential model is a state machine model used for enforcing access control in government and military applications, which is design to address confidentiality? It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to reliable guidance from Roger R. Schell(Hansche et al., 2003), to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policies that supplement the access matrix with the above restrictions to provide access control and information flow. For instance, if a subject has read access to an object in the access matrix, it may still not be able to exercise this right if the object is at a security level higher than its clearance level. The following restrictions are imposed by the model:

Reading down: A subject has only read access to objects whose security level is below the subject's current clearance level. This prevents a subject from getting access to information available in security levels higher than its current clearance level(Sandhu, 1994).

Writing up: A subject has to append access to objects whose security level is higher than its current clearance level. This prevents a subject from passing information to levels lower than its current level.

The Biba Integrity Model developed by Kenneth J. Biba in 1975, is a formal state transition system of the computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. The Biba model has these three rules:

1. Prevent data modification by unauthorized parties.
2. Prevent unauthorized data modification by authorized parties.
3. Maintain internal and external consistency (i.e. data reflects the real world).

The Clark-Wilson model does the same thing, but it does so in a completely different way. With Clark-Wilson, instead of using integrity levels like in the Biba model, it uses a stringent set of change control principles and an intermediary. This model is that if a subject is trying to access an object, it does so without having a direct connection to it - without having direct access to the object (Bishop, 2003).

The model’s enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state.

Proposed Cloud-Based Academic Security and Privacy Model

The Cloud-Based Academic ERP security and privacy Model is a refined model from Bell-Lapadula confidential model, Biba Integrity Model, and Clark-Wilson Model which addresses the security and privacy issues in the cloud while implementing or migrating from server-based to cloud-based academic ERP, the model look at the challenges and how to prevent them from occurring while in the cloud.

International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 4 Issue 2, February – 2020, Pages: 37-44

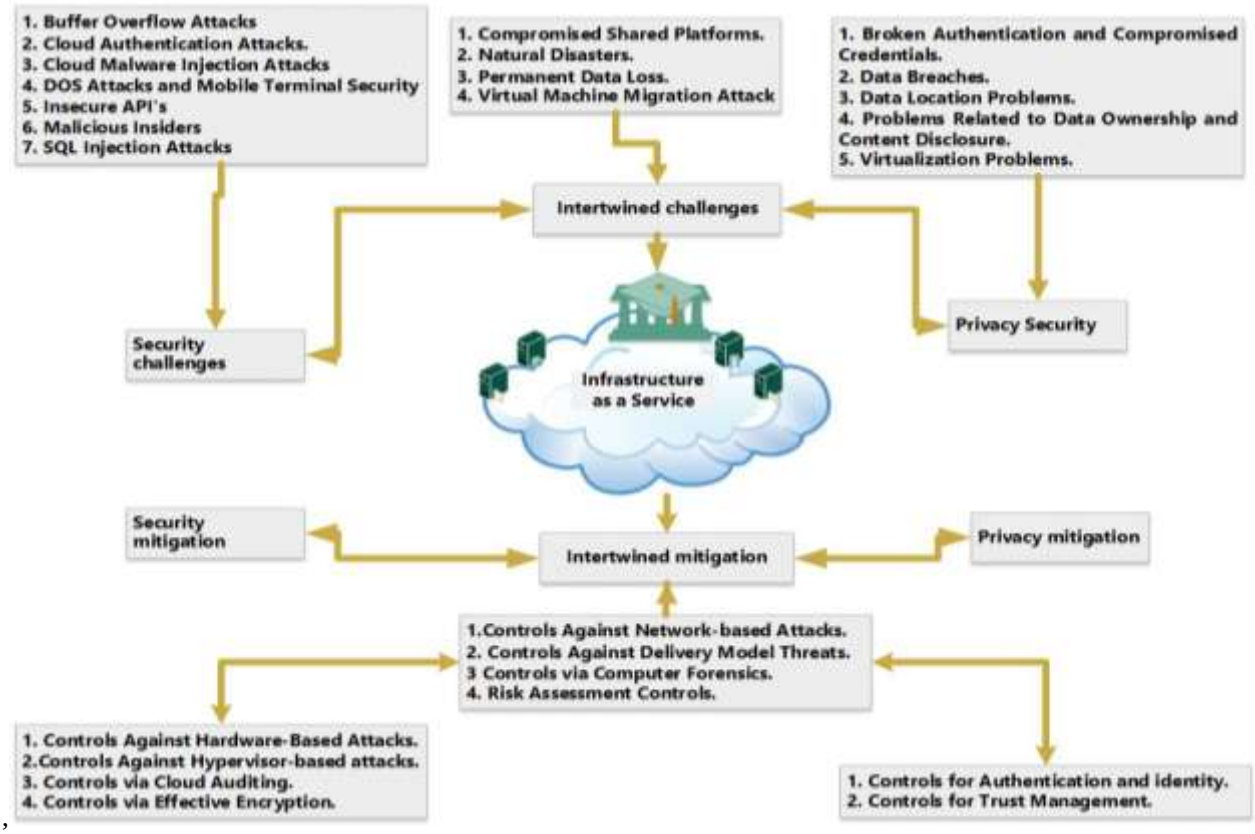

Figure 3. Proposed Cloud-Based Academic Security and Privacy Model

Model validation

The figure 4, 5 and 6 is used to validate the developed model which uses access control (role and permission) to control how users interact with the system by using CURD (Create, read, update and delete) function to implement the system which is the essential operation a user can perform on any system.

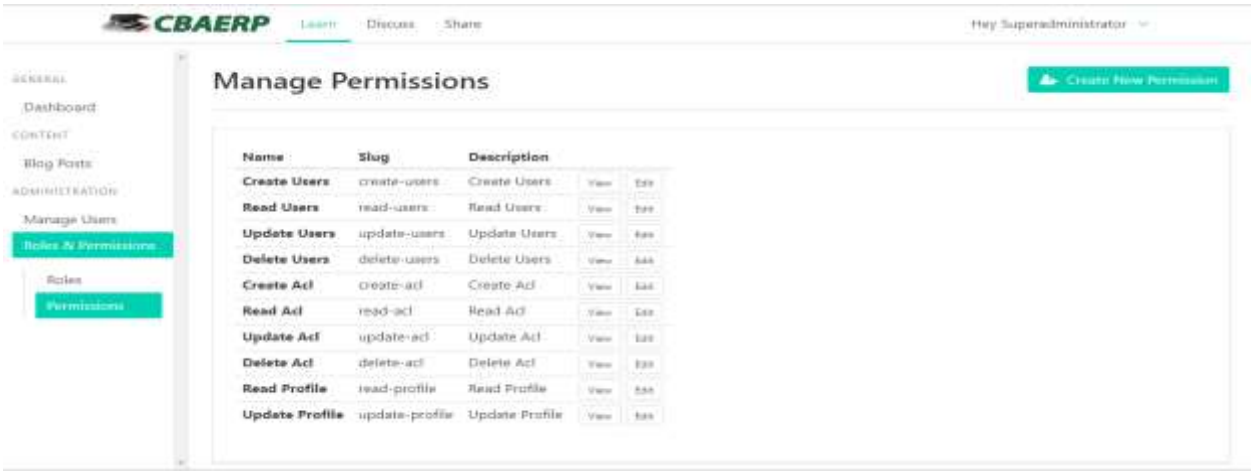

Figure 4: Permission Management

International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 4 Issue 2, February – 2020, Pages: 37-44

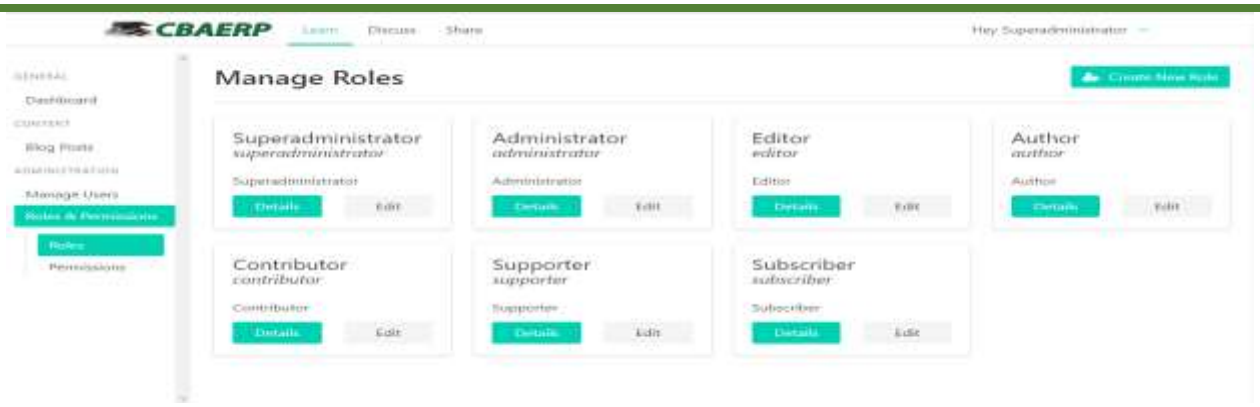

Figure 5. Role Management

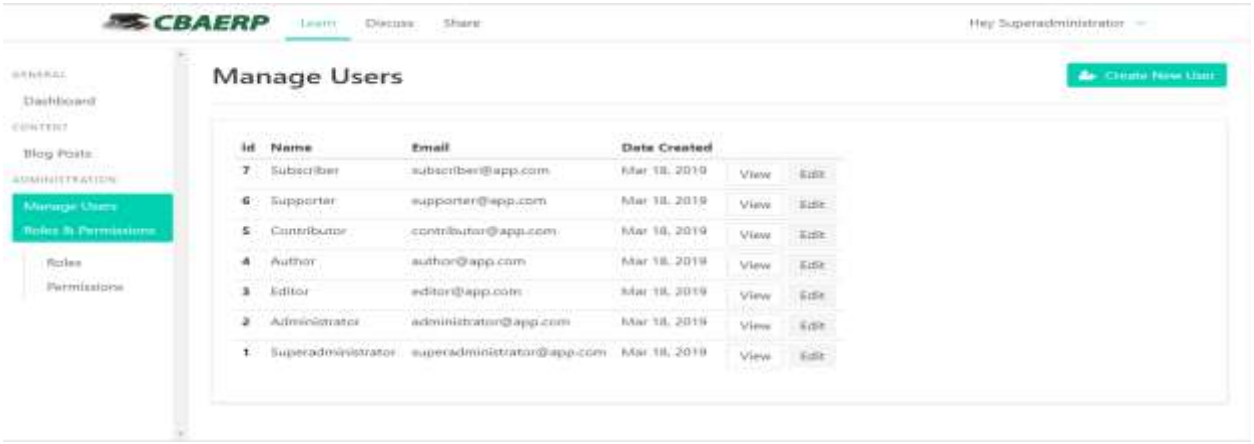

Figure 6: Users management

Controls against Delivery Model Threats

There are various intertwined security and privacy problems affecting cloud delivery models (IaaS, PaaS, and SaaS). Controls for these problems require, among others, secure end-to-end encryption, and a trust management scheme. Each delivery model (IaaS, PaaS, and SaaS) requires authorization in a public cloud to prohibit unauthorized access. Integrity is additionally a vital requirement for checking knowledge correctness. The high availability and integrity of the services require active security mechanisms in the underlying network (Fashoto SG, Ogunleye, GO, Adabara, 2018).

Table 1: Provides further insights for cloud problems for delivery models and their solutions.

Problem	**Effects**	**Affected Cloud Services**	**Solutions**
Abusive use of cloud computing	Loss of validation, service fraud, stronger attack due to unidentified sign-up	PaaS, IaaS	Observe the network status, provide robust registration and authentication technique
Data Loss and Leakage	Personal sensitive data can be	PaaS, SaaS, IaaS	Audit configuration and vulnerability, for

	deleted, destructed, corrupted or modified		administrative task use strong authentication and access control mechanisms and Provide data storage and mechanisms
Different service delivery/receiving model	Loss of control over the infrastructure of the cloud	PaaS, SaaS, IaaS	Offered services under the control and monitored
Insecure Interface and API	Improper authentication and authorization, wrong transmission of the content	PaaS, SaaS, IaaS	Data transmission is in encrypted form, strong access control and authentication mechanism
Malicious Insiders	Penetrate organizations resources, damage assets, loss of productivity, affect an operation	PaaS, SaaS, IaaS	Observe the network status, provide robust registration and authentication technique,
Service/Account Hijacking	Stolen user account credentials access the critical data of the cloud, allowing the attacker to compromise the security of the services	PaaS, SaaS, IaaS	Adoption of strong authentication
Shared Technology Issues	Interfere with one user services to other user services by compromising the hypervisor	IaaS	Use agreement reporting and breach notifications, security, and management process is transparent

Conclusion and Recommends

Cloud computing is a paradigm of computing that offers many valuable services to end-users, including processing, storage, and data management. However, it brings many security and privacy problems that require to be self-addressed. The security and privacy model was developed to assist higher institutions in Implementing or migrating to cloud-based ERP systems. Cloud-based ERP systems help the higher institution to provide a secure environment, costs in terms of hardware, software, and upgrades, as well as reduce up-front expenses.

The higher institution should enlighten staff and students on Cloud computing awareness, its security challenges, mitigation and should be made mandatory for them to appreciate the importance of utilizing cloud computing in improving performance.

The study recommends that academic institutions who have moved to the cloud should comply with the ISO27002 security standard, i.e. Limit the data a higher institution collects, Limit the use of the PII (Personal Identifiable Information), Set policies for retention, Set policies for destruction, Know where your data is stored and Make someone accountable

References

A Al - Shqeerat, K. H., A Al - Shrouf, F. M., Hassan, M. R., & - Jordan Hassen Fajraoui, A. (2017). Cloud Computing Security Challenges in Higher Educational Institutions - A Survey. *International Journal of Computer Applications*, *161*(6), 975–8887. https://doi.org/10.5120/ijca2017913217

Alharthi, A., Alassafi, M., Alzahrani, A., J Walters, R., & Wills, G. (2017). Critical Success Factors for Cloud Migration in Higher Education Institutions: A conceptual framework. *International Journal of Intelligent Computing Research*, *8*(1), 817–825.

https://doi.org/10.20533/ijicr.2042.4655.2017.0100

Bishop, M. (2003). *Computer Security: Art and Science*. Addison Wesley.

Fashoto SG, Ogunleye, GO, Adabara, I. (2018). Evaluation of Network and Systems Security Using Penetration Testing in a Simulation Environment. *GESJ: Computer Science and Telecommunications*, *2*(2), 91–100. https://www.researchgate.net/publication/327070756_EVALUATION_OF_NETWORK_AND_SYSTEMS_SECURITY_USING_PENETRATION_TESTING_IN_A_SIMULATION_ENVIRONMENT

Hansche, S., Berti, J., & Hare, C. (2003). *Official (ISC)^2 guide to the CISSP exam*. Auerbach Publications.

Higher Education | Pearson. (n.d.).

Ibrahim Adabara, Sanni Shamsudeen, Ajiboye Adeleke Raheem, H. N. N. (2018). Cloud-Based ERP Systems used in Higher Education Institution: Benefit, Challenges and Selection. *International Journal of Engineering and Information Systems (IJEAIS)*, *2*(7), 1–9. http://ijeais.org/wp-content/uploads/2018/07/IJEAIS180701.pdf

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. Lo. (2009). On Technical Security Issues in Cloud Computing. *2009 IEEE International Conference on Cloud Computing*, 109–116. https://doi.org/10.1109/CLOUD.2009.60

Kattimani, S. L., & Mallinath, W. K. (2017). *Enterprise Resource Planning (ERP) for academic Architecture Framework using Cloud Computing*. *6*(7), 151–157. https://doi.org/10.17148/IJARCCE.2017.6726

Mircea, M., & Andreescu, A. (2012). Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis. *Communications of the IBIMA*, *2011*, 1–15. https://doi.org/10.5171/2011.875547

Mokia, R., & Rolen, R. (2012). LibGuides: Improving Student and Faculty Access to Information Literacy Grambling State University. *Codex: The Journal of the Louisiana Chapter of the ACRL*, *1*(4), 37–45.

Muli, E., & Kimutai, J. (2015). *Adoption of Cloud Computing for Education in Kenyan Universities : Challenges and Opportunities*. *4*(6), 2854–2860.

Sanchez-Puchol, F., Pastor-Collado, J. A., & Borrell, B. (2017). Towards an Unified Information Systems Reference Model for Higher Education Institutions. *Procedia Computer Science*, *121*, 542–553. https://doi.org/10.1016/j.procs.2017.11.072

Sandhu, R. S. (1994). *Handbook of Information Security Management (1994-95 Yearbook)*. Auerbach Publishers.

Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, *75*, 200–222. https://doi.org/10.1016/j.jnca.2016.09.002

Surendro, K., & Olivia. (2016). Academic Cloud ERP quality assessment model. *International Journal of Electrical and Computer Engineering*, *6*(3), 1038–1047. https://doi.org/10.11591/ijece.v6i3.9836

Vanbaelen, R., & Harrison, J. (2011). Good practices to ensure sustainable education for international students' success. *2011 IEEE International Professional Communication Conference*, 1–12. https://doi.org/10.1109/IPCC.2011.6087216

Venkatachalam, M., & Arts, E. (2017). *Privacy and security issues in cloud computing using DaaS models Publication History Indian Journal of Science COMMUNICATION The International Journal for Science Privacy and secur... December 2016*.

Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010). Cloud Computing Research and Development Trend. *2010 Second International Conference on Future Networks*, 93–97. https://doi.org/10.1109/ICFN.2010.58