Advanced Computing: An International Journal (ACIJ), Vol.8, No.5, September 2017

IMPROVING PRIVACY AND SECURITY IN MULTI-TENANT CLOUD ERP SYSTEMS

Djamal Ziani and Ruba Al-Muwayshir

Department of Information Systems, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

This paper discusses cloud ERP security challenges and their existing solutions. Initially, a set of definitions associated with ERP systems, cloud computing, and multi-tenancy, along with their respective challenges and issues regarding security and privacy, are provided. Next, a set of security challenges is listed, discussed, and mapped to the existing solutions to solve these problems. This thesis 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, ERP system, ERP problems, ERP security challenges, ERP security solutions, ERP and cloud computing

1. INTRODUCTION

This section focuses on the main purpose of securing cloud enterprise resource planning (ERP) systems, a new proposed model to secure the cloud ERP environment. The primary focus is on the services provided by SaaS, PaaS, and IaaS to discuss the main problems and issues associated with the security and privacy thereof. The current research provides an in-depth understanding of the cloud-based ERP and the multi-tenancy architecture. Furthermore, this research addresses the issue of how to improve the privacy and security in a multi-tenant cloud system for higher education. The security of data storage and user authentication are our primary research concerns.

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

DOI:10.5121/acij.2017.8501

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 analyze 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.

This paper is organized as follows: Section 2 details the background of ERP systems, cloud computing, cloud ERP, and multitenancy architecture. Section 3 is a literature review of prior works related to the above-mentioned subjects. Section 4 describes the proposed model to secure data storage in cloud ERP systems.

2. BACKGROUND

In this section, we present a theoretical background of both main topics of this paper, namely ERP and cloud computing. We provide detailed descriptions of the ERP lifecycle, ERP platform, cloud computing service models, cloud computing modes, cloud ERP, and the multitenancy model.

2.1. ENTERPRISE RESOURCE PLANNING (ERP)

With the advent of E-Business and the need to leverage multiple sources of information within the enterprise, ERP (enterprise resource planning) software has appeared as a major area of interest for many businesses. ERP systems are currently concerned about every aspect of organization as they provide a highly integrated solution to meet the information system requirements. ERP has become a basic business information processing requirement for large leading companies. 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. 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 [31].

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 [35].

2.1.1 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 [33].

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 [33].

2.2. CLOUD COMPUTING

Cloud computing changes the way enterprises and industries create a new brand of opportunity to conduct their processes over the internet in dynamic scalable resources virtualized and provided by the internet [36].

Cloud computing refers to both the applications delivered as services over the internet and the hardware and systems software in the datacenters that provide these services. Cloud computing offers the major opportunities known as X-as-a-Service offerings. This utility-based payment model is considered one of the main benefits of cloud computing [26]. There is no need for up-front infrastructure investment, such as investment in software licenses, i.e., no risk of unused but paid software licenses; and investment in hardware infrastructure and related maintenance and staff. Users of cloud services only use the volume of IT resources required, and only pay for the volume of IT resources used. They take advantage of the scalability and flexibility of the cloud. Cloud computing enables easy and fast scaling of the required computing resources on demand [1][6][10][23].

Commercial cloud computing typically includes three divisions: platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS). Different service models of cloud computing aid understanding of cloud communications. PaaS allows customers to deploy

their own applications by accessing the different platforms of clouds. At the lower level, IaaS allows access to network requirements, systems, operating system management, and storage services. SaaS is the most well-known segment and allows customers to purchase the service hosted in the cloud by accessing an application [39].

ERP software that is deployed in a cloud environment becomes "Cloud ERP Software". Most (if not all) cloud environments are built using virtualization and load balancing technology that allows applications to be deployed across multiple servers and database resources. Cloud ERP is positioned as a revolutionary approach to deploy ERP solutions. It provides solutions that are scalable, flexible, affordable, adaptable, and efficient. Cloud ERP as a business management software has delivered critical business data with immense success [14][18].

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 [34].

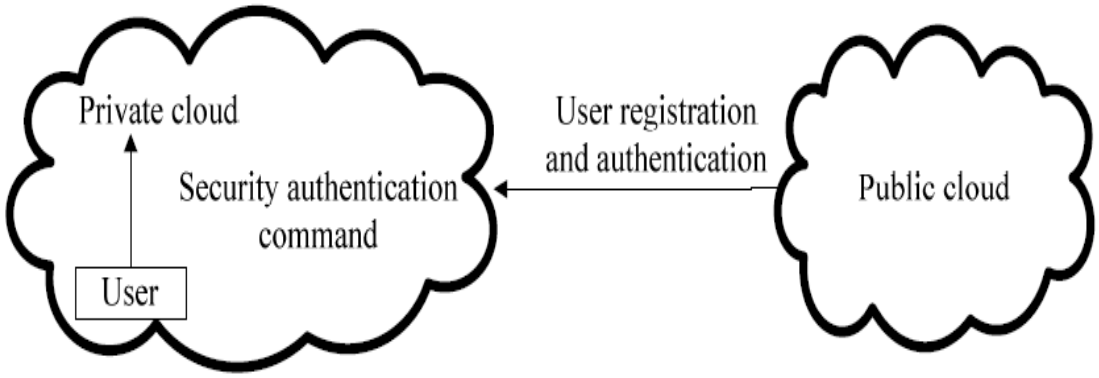

Figure 1: Structure of cloud computing security [34]

2.2.1 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 [36].

Analysis of the convergence of computing trends and the evolution of several cloud computing technologies have resulted in them being considered as multidisciplinary research fields,

including utility computing, distributed computing, internet delivery, virtualization, storage, grid computing, and content outsourcing. Cloud computing could be considered as the grid computing evolution of business oriented services, shifting business and IT infrastructure to be implemented using cloud computing with data storage, services, and computing power provided to customers by a third party [36].

2.2.2 CLOUD COMPUTING DEPLOYMENT MODELS

The models of deploying cloud computing are: private, public, cloud of community, and cross-clouds, providing a single point of access for ubiquitous cloud services suitable for different situations and models. The public model of cloud computing can be employed in multi-tenant cloud environments by sharing the third-party services and infrastructure located in the off-site provider. In contrast, the private model of cloud computing can be employed in a single-tenant environment by sharing the provider's infrastructure and the services of the organizations. The private cloud is suitable for storage of critical mission and core business applications of enterprises, whereas the cloud of community is not sufficiently protected because it supported by a specific community that shares the most common concerns and interests, and can be shared by various enterprises.

The fourth cloud model is the hybrid cloud which contains several private and public clouds, making the provision of cloud services more challenging owing to the added complexity of distributed applications determination across internal and external clouds [36].

2.3. CLOUD ERP

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 [38]. SaaS supports cloud computing services for business embedded with capabilities of communications, for example, ERP systems [39].
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 [38].

Cloud-based ERP is a development of integrated business suites supporting ERP, CRM, and E-Commerce capabilities where application modules can be accessed using the software as a service (SaaS) delivery model, and where application users have flexibility to configure and subscribe to a set of application modules based on an architecture called multi-tenancy [12][25].
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 [49].

2.4. MULTI-TENANCY ARCHITECTURE

The concept of multi-tenancy defines the main goal of increasing resource sharing between SaaS application clients, and reducing the clients' operational costs. Clients can apply different strategies of multi-tenant architecture to accomplish multi-tenancy [40].

The client, called a tenant, pays according to a certain subscription package with remote hosting on the internet by the SaaS model of software delivery. SaaS has a high reliability of provided services at low cost to give clients freedom and the ability to own, host, and maintain the infrastructure and software application of the hosting environment [41].

Multi-tenancy on the application level is an example of a SaaS application, and includes an architectural design principle that allows multiple customers to be hosted by a single application instance or server. The current models of multi-tenant application design are not flexible, despite the operational cost and maintenance benefits of the application-level multi-tenancy that provides multiple software variations to multiple customers. Multi-tenancy architecture is designed for SaaS applications, which allow multiple customers (tenants) to share the same application. However, this application is sufficiently flexible for the tenants to customize to their specific needs. It is based on a predictable monthly subscription; tenants only pay for what they use [7][8][40].

Limited PaaS solutions provide a support for building multi-tenant applications; however, they do not directly support tenant specific customization without offering the same flexibility as SaaS solutions. The mechanism of multi-tenancy provides application data partitioned between tenants, including the ability to offer a unique namespace string ID for each tenant supported by various vendors of multi-tenancy services, such as data isolation, data store, and caching service [40]. The aim of multi-tenancy is to reduce operational costs, and to increase the sharing resources of SaaS applications between customers [40].

3. 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 [20], the authors mentioned that providing an ERP platform for small and medium-sized enterprises raises numerous new questions. Most of them are concerned with the appearance of multi-tenancy. Thus, mastering multi-tenancy is one of the keys to provide an efficient and customizable platform for business applications. They identified two cornerstones of a multi-

tenancy aware infrastructure in the context of customization, namely dynamic instance composition and abstraction from the persistency layer.

In [21], 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 [29], 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 [27], 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 [2], 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 [24], the authors presented a cloud computing architecture focused on SaaS called multi-tenant, 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.

In [4], the authors stated that security is a key requirement that must be addressed when engineering new SaaS applications or re-engineering existing applications to support multi-tenancy. They proposed a model called TOSSMA, a tenant-oriented SaaS security management architecture. TOSSMA mitigates four main problems in multi-tenant cloud applications: loss of security control, integration of SaaS application security, customization of SaaS applications security, and the provision of isolation between the tenants' data.

In [3], the authors proposed a distributed scheme through a homomorphism token with distributed verification of erasure-coded data. Many companies are not yet ready to implement cloud computing technology owing to lack of proper security control policies and weakness in protection which lead to numerous challenge in cloud computing. Additionally, their technique provided a process to avoid collusion attacks of server modification by unauthorized users.
In the study of [44], the authors aimed to understand data confidentiality by reviewing the encryption techniques . This study concluded that the most common approaches for data encryption are based on RSA, indicating that most researchers of the cloud computing environment are interested in RSA encryption techniques. The revealing result of this study showed that the proposed approaches have a lack of validation in cloud computing, which needs to be addressed to improve confidence and trust [44].

In [45], the authors focused on the security of data storage in the cloud. They evaluated several modern encryption techniques tested randomly in the cloud computing environment using the pseudo random number generator (PRNG) according to NIST statistical testing. The results of this study showed that there are some differences between algorithms and techniques, without any strong indication of statistical weakness of the selected algorithms in the cloud environment.

In [46], the primary contribution was to securely motivate multi-tenancy to design and implement multi-tenancy without modifications. The discussion of multi-tenant design and implementation evaluates the architectural performance of multi-tenancy, including clustering architecture into tenants and sharing data across them. In detail, multi-tenancy can be used as a major component of PaaS services, including resource sharing in private clouds.

The study of [43] analyzed security threats and opportunities to provide secure cloud services. It presented the requirements of secure cloud services, which assists in introducing a new research attitude in the context of security. This study investigated security technologies to establish a secure environment of cloud computing. It analyzed security threats, security technologies, and security requirements of cloud computing services from the aspect of providers and end users.
The authors of [42] provided an overview of the essential differences between multi-tenancy architecture and other related concepts. The primary contribution was the discussion of multi-tenant applications and their architectural implementation concerns from the aspect of vendors. It discussed the relationships between the major architectural concerns of multi-tenancy design. In addition, this study discussed and classified the concepts of performance isolation, quality of service, customizability, and persistency.

The authors of [49] aimed to present an investigation of probable security issues of cloud ERP deployment inherited from ERP and cloud computing from the customer and provider perspectives. This study used the methodology of qualitative research by interviewing professional ERP, cloud computing, and cloud ERP. The results of this study categorized the security issues of architecture, threats, authentication, authorization, and data security into three groups: ERP and cloud ERP security issues, contemporary challenges in cloud ERP, and cloud ERP solutions.

The study of [37] demonstrated that the configuration of the SaaS environment with ERP multitenancy can change all the application layers. The authors proposed a secure multi-tenant

environment using a central configuration with flexibility to solve security and privacy issues. Additionally, they addressed the performance issue using different techniques of configuration isolation and tenant data base isolation, providing a high-performance solution for multi-tenancy SaaS environments.

Despite the numerous advantages of cloud ERP systems, there are many probable challenges, issues, and drawbacks. In [32], the major cloud ERP system issues include: flexibility, ownership of data, security issues, customization, and provider issues. Other issues such as system, performance, system reliability, and security concerns were addressed in [30]. Customers should make a trade-off between different provisions of cloud ERP, such as storage scalability, security, performance, interoperability, and network services [28]. In [22], a set of cloud ERP solutions was discussed to determine the advantages of adopting in-house enterprise solutions.

In this paper, the authors motivate large companies to employ in-house ERP solutions owing to their increased customization ability. Additionally, cloud ERP solutions are limited to their vendors. Cloud ERP solutions are difficult to change according to organizations' needs because their flexibility remains inadequate. ERP systems require heavy customization to handle complex and distinct business processes for better performance of these solutions [17]. Multi-tenancy solutions increase the complexity of ERP systems, despite their provided advantages. The customization of cloud ERP multi-tenancy is partially solved. Moreover, all tenants can be updated simultaneously; however, the configuration of tenant-specific is more difficult because it requires the redeployment of every tenant of configuration data [16].

PaaS and SaaS cause data security challenges and issues. The challenges of SaaS applications are similar to those of web applications, but protecting them from attacks requires more than traditional security solutions. SaaS providers should secure their provided software and PaaS should secure the platforms of these services and new approaches to security are required [15]. Limited resources regarding cloud ERP security issues are provided in the literature. Some cloud services use multi-tenant architecture for accessibility by several users. The security of data associated with cloud applications is the responsibility of the providers, whilst data need to be secure during processing, transferring, and storing [15].

One practical solutions is to use dynamic credentials to change their values according to the user's location or data packets [15]. An alternative solution is to use digital signatures for data security using recognizable RSA algorithms of data transferred over the internet in the cloud environment [13]. At the same time, strong encryption techniques such as SSL and AES can be used to secure the sending and storage of sensitive data in clouds. Some encryption algorithms are used to mitigate attacks of cloud storages [11]. The use of data prevention tools aims to prevent leakage of sensitive data from clouds through data transmission. Additionally, they can assist in addressing the most important data to be secured, and identifying users' rights and actions regarding the sensitive data stored in the clouds.

Data integrity is a further concern in clouds services providers; to ensure the data is up to date, integrated, and available in a way that satisfies users' needs and expectations. The provider of clouds services can improve the security by continually keeping a backup for each update. Thus, a set of protocols can be used to integrate the network security; however, the backups can

maintain different versions, partially or fully based on a specified amount of time. From a physical security perspective, the cloud service provider should support the physical access with strong security measures and a disaster recovery. In contrast, each user should be responsible for his/her duties to ensure traceability and to use data logs for data recovery from data loss.

Tenant authentication in cloud computing has modern opportunities and challenges. Some parties such as cloud providers and users in the cloud environment share overall responsibility. In this context, the network security is the responsibility of the user to access the services over the internet, whereas physical security and additional network security policies, such as firewall rules, are the responsibility of the cloud [9].

Data storage in cloud ERPs should be secured by the security management module to allow users to access stored data. Moreover, business logic is available in the systems used by users and they should be open only to legal users, and should be separated from other users' data. The security management module of the cloud data storage includes three significance components: encryption component, privacy component, and backup component. First, the encryption uses private or public keys to encrypt sensitive data stored in the cloud database to ensure that direct access is prevented by business and application logic. However, the encryption process requires decryption and both are costly for the clouds; thus, to minimize remaining costs, non-sensitive data can be stored without encryption. Second, the privacy component should restrict a clear border between the different users' data to permit several users to concurrently save their data in a location that can be used by other users. The multi-tenancy enables cloud computing to be accepted by major users, but the interruption between different users' data makes them accessible [5].

Third, the backup component ensures that if all data stored for a specific enterprise is backed up periodically to allow the cloud-based enterprise system in disaster recovery to restore all stored data. Further, all stored backup data should be encrypted to prevent illegal access to sensitive data.

4. 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 manage data access. 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. In cloud infrastructure, all channels used to communicate to data owners, clients, and cloud service providers are protected to securely exchange public keys between partners. However, all client devices are unable to perform expensive computations and operations because they have inadequate processing capabilities. All clients trusted to access data only have accessibility to the encrypted index of accessible data.
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 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. Clients must be granted privileges by the data owner with respect to the private keys to allow them to access external cloud data. Clients can download data from the clouds by decrypting the data locally after a successful

authentication process. The distribution of data is another mechanism provided to the tenant to save and secure his/her data. The tenant can select which database table he wants in his company database and which database table will be on the provided database side.

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. By using the distribution technique, the tenant will have better privacy on his data, without losing the performance, because all the data will be on memory.

4. CONCLUSIONS

This research studied several problems in multi-tenant cloud applications: loss of security control; integration of the SaaS application security; customization of SaaS applications security; and provision of isolation of tenants' data. One of the main purposes is to secure cloud ERP systems using a new proposed model to secure the cloud ERP environment. The primary focus was on the services provided by SaaS, PaaS, and IaaS and the main problems and issues associated with the security and privacy. The main problems that limit the performance of ERP systems are networking requirements, large storage requirements, and employee training requirements. Additionally, there are a set of disadvantages, including privacy concerns, prohibitive costs against low budgets of small businesses, 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.

ACKNOWLEDGEMENTS

I would like to thank everyone.

REFERENCES

[1] M.A. Vouk, (2008) "Cloud computing–issues, research and implementations", CIT. Journal of Computing and Information Technology, Vol. 16, No. 4, pp235-246.

[2] A. 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.

[3] D.P.D.S. Abburu, (2012). "An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, No. 2.

[4] M. Almorsy, J. Grundy, & A.S. Ibrahim, (2012, June) "Tossma: A tenant-oriented saas security management architecture", In Cloud computing (cloud), 2012 IEEE 5th international conference on (pp. 981-988). IEEE.

[5] S. Subashini & V. Kavitha, (2010), "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, Vol. 34, No.1, pp1 -11.

[6] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, Konwinski, A., ... & M. Zaharia, (2010) "A view of cloud computing", Communications of the ACM, 53(4), 50-58.

[7] A. Azeez, S. Perera, D. Gamage, R. Linton, P. Siriwardana, D. Leelaratne, ... & P. Fremantle, (2010, July), "Multi-tenant SOA middleware for cloud computing", In Cloud computing (cloud), 2010 ieee 3rd international conference on (pp. 458-465). IEEE.

[8] D. Banks, J. Erickson, & M. Rhodes, (2009), "Multi-tenancy in cloud-based collaboration services", Information Systems Journal. BCG (2012).

[9] M. Armbrust et al., (2009), "A view of cloud computing", Communications of the ACM, 53(4), p.50. Available at: http://inst.cs.berkeley.edu/~cs10/fa10/lec/20/2010-11-10-CS10-L20-AF-Cloud Computing.pdf [Accessed July 30, 2012].

[10] S.L. Dinesh Kumar Saini, Yousif,, J.H. Sandhya, & V. Khandage, (2011), "Cloud Computing and Enterprise Resource Planning Systems", Proceedings of the World Congress on Engineering, Vol. 4.

[11] D. Harnik, B. Pinkas, A. Shulman-Peleg, (2010), "Side channels in Cloud services: deduplication in Cloud Storage", IEEE Security Privacy, Vol. 8, No. 6, pp40–47.

[12] E. Fathi Kiadehi, & S. Mohammadi, (2012), "Cloud ERP: Implementation of Enterprise Resource Planning Using Cloud Computing Technology", Journal of Basic and Applied Scientific Research, Vol. 6.

[13] U. Somani, K. Lakhani, M. Mundra, (2010), "Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing", In: 1st International conference on parallel distributed and grid Computing (PDGC), IEEE Computer Society Washington, DC, USA, pp211–216.

[14] G. F Fathima Haseen Raihana & J. A. Jamal Mohamed College, (2012), "CLOUD ERP– A SOLUTION MODEL", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN, Vol. 2, No. 4, pp4.

[15] S. Xiao & W. Gong, (2010), "Mobility Can help: protect user identity with dynamic credential", In: Eleventh International conference on Mobile data Management (MDM), IEEE Computer Society, Washington, DC, USA, pp378–380.

[16] R. Mietzner, T. Unger, R. Titze, & F. Leymann, (2009), "Combining Different Multi-Tenancy Patterns in Service Oriented Applications," presented at the IEEE Enterprise Distributed Object Conference, Auckland.

[17] E. Kimberling, (2011), "Is SaaS ERP right for your organization," 360° ERP Blog.

[18] A. Lenart, (2011), "ERP in the Cloud–Benefits and Challenges", In Research in systems analysis and design: Models and methods, pp39-50, Springer Berlin Heidelberg.

[19] Md Asif Mushtaque, R. Sindhu, (2014), "A New Innovation On User'S Level Security For Storage Data In Cloud Computing", International Journal of Grid Distribution Computing 7.3, pp213-220.

[20] J. Müller, J. Krüger, S. Enderlein, M. Helmich, & A. Zeier, A, (2009), "Customizing enterprise software as a service applications: Back-end extension in a multi-tenancy environment", In Enterprise Information Systems, pp66-77. Springer Berlin Heidelberg.

[21] 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.

[22] 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.

[23] M. Okuhara, T. Shiozaki, & T. Suzuki, (2010), "Security architecture for cloud computing", Fujitsu Sci. Tech. J, Vol. 46, No. 4, pp397-402.

[24] Z. Pervez, S. Lee, & Y.K. Lee, (2010, February), "Multi-tenant, secure, load disseminated SaaS architecture", In Advanced Communication Technology (ICACT), 2010 The 12th International Conference on (Vol. 1, pp214-219). IEEE.

[25] P.S. Petra Schubert, & A.F. Femi Adisa, (2011), "Cloud Computing for Standard ERP Systems: Reference Framework and Research Agenda", Arbeitsberichte aus dem Fachbereich Informatik, Vol. 4, No. 27, pp29.

[26] L. Qian, Z. Luo, Y. Du, & L. Guo, L, (2009), "Cloud computing: An overview", In Cloud Computing, pp626-631. Springer Berlin Heidelberg.

[27] 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.

[28] P. Hofmann, (2010), "Cloud Computing: The Limits of Public Clouds for Business Applications", IEEE Internet Computing, Vol.. 14, No. 6, pp90–93.

[29] A. Satapathy, & J. Badajena, (2013), "A Secure Model and Algorithms for Cloud Computing based on Multicloud Service Providers", International Journal Computational Intelligence and Informatics, Vol. 3, No. 1.

[30] B. McCrea, "Putting the spotlight on ERP," Logistics Management, pp32 – 35, Jun-2011.

[31] Y. Xu, N. Rahmati, & V. Lee, (2008, June), "A review of literature on Enterprise Resource Planning systems", In Service Systems and Service Management, 2008 International Conference on (pp1-6). IEEE.

[32] S. Salleh, S. Maliza, T. Yen, & C. Chan, (2012), "Cloud Enterprise Systems: A Review of Literature and its Adoption", presented at the PACIS 2012 Proceedings, Hochiminh City, 2012.

[33] J. Esteves, & J. Pastor, (2001), "ENTERPRISE RESOURCE PLANNING SYSTEMS RESEARCH: AN ANNOTATED BIBLIOGRAPHY", Communications of AIS, Vol. 7, No. 8.

[34] N. Sahin, (2013), "Cloud ERP Security: Guidelines for Evaluation", Department of Computer and Systems Sciences.

[35] J. Umble, R. Ronald, M. Haft, & U. Michael, (2003), "Enterprise resource planning: Implementation procedures and critical success factors", European Journal of Operational Research, Vol. 146, pp241–257.

[36] X. Xun, (2012), "From cloud computing to cloud manufacturing", Robotics and Computer-Integrated Manufacturing Vol. 28, pp75–86. New Zealand.

[37] S. Walraven, E. Truyen, W. Joosen, F. Kon, & A. Kermarrec, (2011), "A Middleware Layer for Flexible and Cost-Efficient Multi-tenant Applications", IFIP International Federation for Information Processing, pp370–389.

[38] W. Voorsluys, J. Broberg, & R. Buyya, (2011), "Introduction to cloud computing", Cloud computing: Principles and paradigms, 2-44.

[39] L. Bangfan, Z. Huihui, & W. Meng, (2014), "How to Design the Cloud Computing Used in E-government's Information Security?", Applied Mechanics and Materials, Vol. 536-537, pp616-619.

[40] A. Bezemer & C. P., Zaidman. (2010), "Multi-tenant SaaS applications: maintenance dream or nightmare?", in In Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), pp88–92.

[41] M. Kapuruge, A. Colman, J. Han, A. Bouguettaya, M. Hauswirth, & L. Liu, L, (2011), "Achieving Multi-tenanted Business Processes in SaaS Applications", Springer-Verlag Berlin Heidelberg. pp143–157.

[42] E. Shehab, M. Sharp, L. Supramaniam, & T Spedding, (2004), "Enterprise resource planning An integrative review", Business Process Management Journal, Vol. 10 No. 4.

[43] J. Ju, Y. Wang, J. Fu, J. Wu, & Z. Lin, (2010), "Research on Key Technology in SaaS", in 2010 International Conference on Intelligent Computing and Cognitive Informatics, pp. 384–387.

[44] H. Wang & Z. Zheng, (2010), "Software architecture driven configurability of multi-tenant SaaS application", in Web Information Systems and Mining (WISM), 2010, pp418–424.

[45] D. Johnson, (2010), "Multi-tenant versus Single-tenant ERP – a comparison," [Online]. Available: http://erpcloudnews.com/2010/06/multi-tenant-versus-single-tenant-erp-a-comparison/. [Accessed: 28-Aug-2013].

[46] D. Banks, J. Erickson, & M. Rhodes, (2009), "Multi-tenancy in Cloud-based Collaboration Services", Hewlett-Packard Development Company, L.P.

AUTHORS

Djamal Ziani has been an associate professor in the Computer Sciences and Information Systems College at King Saud University since 2009. He is also a researcher in ERP and a member of the data management group of CCIS, King Saud University. He received a Master's degree in Computer Sciences from the University of Valenciennes, France in 1992, and Ph.D. in Computer Science from the University of Paris, Dauphine, France in 1996. From 1998 to 2009, he was a consultant and project manager in many companies in Canada, such as SAP, Bombardier Aerospace, and Montreal Stock Exchange.

Ruba Almuwayshir is a teaching assistant at AlJouf University and a master's student at King Saud University.