International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

A Framework for Security of ERP System on Cloud

Shashank Bhushan Chaturvedi[Å*] and Prateek.Singh[Å]

[Å]Department of Computer Science & IT, SHIATS, Allahabad, India

Accepted 25 December 2013, Available online 30 December 2013, **Vol.3, No.5 (December 2013)**

Abstract

Enterprise Resource Planning (ERP) is a tool for integrating business activities across functional departments on different modules with the aim of improving the performance of the organization's resource planning, management and operational control. This is the service which is most widely used on cloud in these days. In nearly every survey done about cloud computing the top reason given for not adopting it is a concern over security. So it is very important to develop new techniques for security over cloud. This paper proposes a framework for security of an ERP system on cloud. This framework is used to improve service quality, the complexity to manage security and increase privacy of an ERP system.

Keywords: *ERPS Cloud, Cloud Trusted and Provisioning Domain (CTaPD), Security as a Service (SeaaS)*

1. Introduction

More and more companies are using cloud computing services in order to reduce costs and to increase the flexibility of their IT infrastructure. As observed in the techniques above, the approach proposed for preserving enterprise privacy mostly requires changing the cloud data and demand additional maintenance for each new set of user data that is generated or consolidated in the enterprise system. Security of enterprise data on retrieval in cloud is one of the most important properties that an IT solution system must satisfy. For this reason, several efforts have been devoted to incorporating data preserving techniques with data retrieval on cloud in order to prevent the disclosure of sensitive information during the knowledge discovery.

The aim of our work on cloud is to extract relevant knowledge from large amounts of data while protecting at the same time sensitive information. An important aspect in the design of such framework is the identification of suitable evaluation criteria and the development of related benchmarks. Recent research in the area has devoted much effort to determine a trade-off between the right to security and the need of knowledge discovery. It is often the ca se that no work exists that outperforms all the others on all possible criteria. Therefore, with the help of comprehensive view on an existing data security framework we can gain insights on how to design more effective one.

2. Proposed Framework

We present a cloud based ERP system Framework. In the past, companies have stored their records of their clients and venders on paper locally. This allowed a controlled environment with easy management of data privacy and security: keeping the paper records in a locked cabin at the office. Even the increasing use of personal computers and

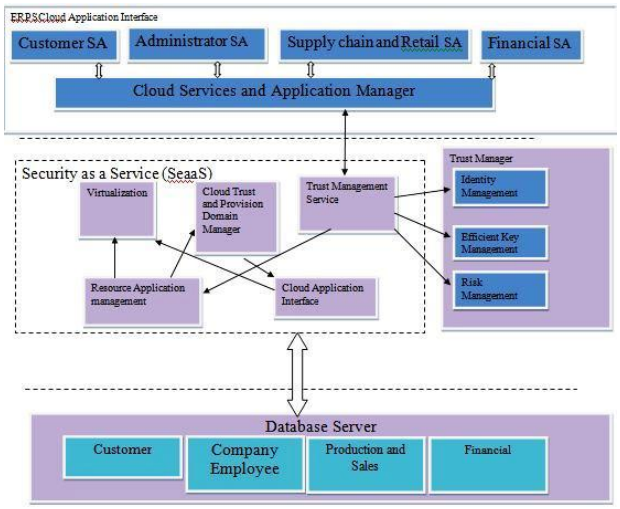

Fig.1 Proposed security framework for ERP system on cloud.

modern information technology in institutions allowed for a moderate effort to manage privacy and confidentiality of individual records. This was due to the decentralized and locally managed infrastructure of each organization. But nowadays outsourcing of IT infrastructure (e.g., cloud computing) and other services (e.g., billing processing and

*Corresponding author **Shashank Bhushan Chaturvedi** is a M.Tech Scholar and **Er. Prateek.Singh** is working as Asst. Prof

accounting for clients) leads to a complex system where privacy-sensitive data are stored and processed at many different places. Hence, it becomes attractive to store and process in the cloud (at outsourced data providers that can be accessed via the Internet). While such information processing systems promise improved service quality, the complexity to manage data security and increases privacy.

3. Enterprise Resource Planning Security Cloud (ERPS-Cloud) Architecture

In this research, we first describe the ERPS-Cloud architecture (shown in Figure) and its support for security service provisioning, resource and security isolation, and the integration of processing and operations of cloud. We then describe several services that can help both cloud and ERP to achieve the proposed system-level functionalities, such as identity management, key management, policy enforcement, and context-aware routing and risk assessment.

A.ERPS-Cloud Security Services Architecture

ERPS-Cloud Architecture: Figure shows the conceptual infrastructure for ERPS-Cloud. ERP user's node can leverage hardware farms on cloud to augment its computing capabilities. Beyond this, we introduce a new type of service named cloud trusted and provisioning domain (CTaPD) to isolate information flows belonging to different security domains using programmable router technologies. Moreover, we provide fine-grained trust management and feedback/command capability to ERP users. In summary, ERPS-Cloud is designed to provide the following cloud services:

• Serve as an arbitrator for identity key and secure data access policy management.

• Provide security isolations to protect ERP users' information.

• Monitor ERP status for risk assessments, intrusion detection and response.

• Provide service composition and applications for ERP users devices.

Now, we describe the functionality and properties of each component of Fig.1. ERPS-Cloud uses Software Agents (SAs) (i.e., application components) to link the cloud services and ERP user's devices. Each device can have multiple SAs for different cloud services, which are managed by application manager of the device. Each device also provides sensing data about the device itself (such as processor type, utilization and location with GPS support), and about the neighboring ERP users nodes (such as neighbor's identity or addresses, link quality, neighboring durations, etc.). On the cloud side, the ERPS-Cloud Application Interface (EAI) exports services that can be consumed by to user devices. In addition, the EAI also provide interfaces to CTaPD manager and Resource and Application Manager (RAM). Middle-ware based solutions are required when the cloud components do not use web-based interfaces. Several unique cloud components and constructions are proposed for ERPS-Cloud. We introduce multiple virtual domains: (1) security, a user's device may run multiple applications at different security domains, e.g., its simultaneous communication with two individuals with from administrative domains; and (2) context-awareness, it may be necessary to separate services for different local and network settings. For example, ERPS-Cloud can simulate the operations using different system parameters or routes selection algorithms to compare different approaches for utilizing cloud computing and communication resources. This approach provides a comprehensive overview of operations and provides information to ERP solutions and system managers for decision making. In each CTaPD, one or more SAs are used for every node. A Node Manager (NM) is responsible for managing the loading and unloading of SAs in the system.

The ERPS-Cloud Resource and Application Manager (RAM), constructs CTaPD when it is directed by ERPS-Cloud CTaPD manager and ERPS-Cloud Trust Manager Server (TMS). They form the core for providing Security-as-a-Service (SeaaS). With SeaaS, ERPS-Cloud can offer security service composition capability according to requests from ERP applications. In our SeaaS service model, the CTaPD manager plays the central role since it collects context-awareness information from the ERP applications and used it for intrusion detection and risk management. The ERPS-Cloud TMS is the Trust Authority (TA) for ERPS-Cloud. It handles the attribute-based key distribution and revocation. It provides identity search and federation services for ERP belonging to multiple administrative domains. It also performs policy checking and enforcement functions to provide a unified trust management system for ERPS-Cloud. Finally, the ERPS-Cloud Service and Application Store (ESAS) serve as the repository for SAs and applications. When service composition is needed, the MSAS will install the required SAs or applications through the EAI. In this scenario, the SAs for the new drivers and authentication module will be installed. This operation needs collaborations between TMS and ESAS.

Secure Isolation through CTaPD: *C*TaPD are established to provide data access control and information protection. We must note that the framework may not need/imply the division of the administrative domain into CTaPD.

Resource isolation: The actual administrative work is handled by the ERPS-Cloud CTaPD manager. Every node that belongs to a particular CTaPD will have the complete routing information for CTaPD in which it resides, but not others. Each node can reside a different physical system. Each node would have to support our communications framework which includes secure group communication to sending data to all the ESSIs in the same CTaPD. The bandwidth for a communication link can be divided by using different encryption/ decryption/ authentication keys. An advantage of the ERPS-Cloud framework that provides network virtualization through multiple CTaPDs is that it facilitates prioritization of critical/emergency services in a network. For example, using the proposed virtualization approach, prioritized and normal service

classes can be defined using different CTaPDs. They can share the same physical cloud but prioritized based on the CTaPD. MANET operations and communications can be migrated into the cloud when peer-to-peer communication is under stress either from insufficient bandwidth or attacks.

Data access control: In addition to the isolation provided by CTaPD service domain, ERPS-Cloud also needs to integrate data access control and information isolation using a cryptography based approach. Besides the traditional security concerns (i.e., authentication, authorization, audit etc.), additional security risks are introduced by ERP users who share the same application instance and resources. In cloud related literature, this referred to as multi-tenant environments. Each ERP users ESSI can be considered as his/her tenancy in the ERPS-Cloud. In the multi-tenant environment, data access control is one of the most critical security concerns that need to be addressed. Data isolation mechanisms prevent users from accessing resources belonging to other tenants. There are generally two kinds of access control isolation patterns: implicit filter and explicit permission. We further generalize the two patterns to provide access control for other resources:

• Implicit Filter Based Access Control Isolation: In this pattern, when one client requests to access shared resources, a common platform level account (i.e., the ESSI identity with corresponding SA and cloud resource requests) is delegated to handle this request. The delegated account is shared by all clients and has the privileges to access resources of all clients. However, the key of this mechanism is to implicitly compose a client-oriented filter that will be used to prevent one user from tapping into resources of other client. This can be achieved by using a cryptography-based solution, i.e., group key management based solutions to secure information flow through different CTaPDs that share the same physical system.

• Explicit Permission Based Access Control Isolation: In this pattern, access privileges for the resources have been explicitly pre-assigned to the corresponding tenant accounts by using the Access Control List (ACL) mechanism. Therefore, there is no need to leverage an additional common delegated account across tenants.

B. ERPS-Cloud Trust Management

Several interrelated components of trust management in ERPS-Cloud will be addressed including identity management, key management, efficient data access control, and security context-aware-based risk assessment. Moreover, we will present an approach to incorporate cloud computing techniques to address several research issues considered very difficult problems of cloud computing.

ERPS-Cloud Identity Management: The user-centric identity management, which is also frequently referred to as identity, allows an individual to have multiple identifiers. For example, the identifier carried on a national ID card becomes just one of many of an individual's identifiers, which can also include passport ID, club card ID, military ID, email ID, unique IP address, etc. There are many research problems may in this area. How to provide convenient secure single sign-on to multiple distinct entities? How to give individuals fine-grained control for the sharing specific personal identities between entities when it is to their advantage to do so? How do we know what identity information to share when two users meet? To address these questions, we propose a novel Attribute-Based Identity Management (ABIDM).

The major benefit of using this identity representation is the standardization of identity management. In practice, the numbers ERP user node should not be many. They can be assigned to ERP users as predefined attributes that that do not changed frequently. We call these attributes as static attributes.

Efficient Key Management for Secure and Private Data Access Control:

Each attribute can have multiple secret components for different users. We must note that users can share an attribute; however the corresponding private key components for that attribute are different. The internal nodes of the attribute tree are logical gates, such as AND, OR. They are implemented using threshold secret sharing scheme at the bottom level the encryption is performed using a construction similar to identity-based encryption (IBE). During encryption, in order to satisfy the AND gate, the decrypter must have all the secrets under it to reconstruct the higher level secret; to satisfy the OR gate, the decrypter is only required to have one of the secrets. The encryption algorithm is performed in a top-down and decryption algorithm is performed in a bottom-up manner using the users' pre-distributed secrets to reconstruct higher level secrets until they reach the root. In this presented example, based on the pre-distributed secrets, $u1 \square u3$ can decrypt the secret S and thus they can access the data encrypted by using the DEK S.

Efficient Key Management for Secure and Private Data Access Control:

Each attribute can have multiple secret components for different users. We must note that users can share an attribute; however the corresponding private key components for that attribute are different. Existing key management solutions usually consider the key management and Identity Management (IDM) as different issues. We use a novel key management solution, to integrate key management and IDM. In this, we can simply consider all the attributes belong to an entity as its public key. Each attribute can be considered as a public key component, and each of the attributes is also paired with a private key component. The private key, which is in turn is formed by multiple private key components, is distributed from a TA. We must note that component is basically an extended version of identity-based cryptography, in which the identity can be considered multiple descriptive attributes and the attributes can be used to represent descriptive policies through logical operators such as AND and OR. Moreover, the data access can be very flexible, where the data sender does not need to know the identities of receivers. In fact, this approach is very effective for secure group communication, where a

group of receivers may satisfy the specified data access policies. Furthermore, a policy tree can be used for secure group communication since attributes can be used to specify a group of users, which make the approach appealing in large-scale ERP systems.

Context-aware Risk Management in ERPS-Cloud:

Risk management calls for the identification, assessment, and prioritization of risks followed by a coordinated and economical application of available resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. The methods, definitions, and goals vary widely in cloud computing according to whether the risk management method is in the context of the mission supporting functions, operations, or security.

4. Conclusion

The proposed framework shows the trust management services, which manages security of identity, efficient key and risk. This substantially improved the overall security of the ERP system.

However, we must note that there is no recipe to complete security when it comes to ERP systems. The weakest element is still the people component where no security measures can guarantee the confidentiality level of the people of the company, regardless of the awareness and procedures that are put in place. As mentioned previously, security is an ongoing process where the security measures have to be tuned every time the system is updated. What matters even more, of course, is the price/performance ratio, meaning that security measures will always try to first comply with a higher performance ratio and then to advantage the security of the system.

5. Scope for Further Research

In the future, this small set of security measures could be extended and reevaluated with different security scanner applications to confirm the effectiveness of the same in the ERP system architecture. There always should be balance between the price/performance ratio and the security level applied to the ERP system, since usability is directly connected to the performance of the system. In this way one would define a baseline set of security measures which will successfully increase the security of the ERP system while maintaining at the same time a satisfying level of performance.

Nevertheless, critical and sensitive modules should always get a security base line measures applied regardless of the effect they have on the system performance, as data security and protection is the foundation of today's ERP web-based systems.

References

Binu Sumitra, Meenakumari J (Aug/Sept 2012) , A Security Framework For An Enterprise System On Cloud, *IJCSE*.

Brehm, N., Gómez, J.M. & Rautenstrauch C. (2005), Web service-based ERP systems and an open security model'. *Proceedings of 16th IRMA*

Dans E. (2011), Benefits and Disadvantages of Cloud Computing,http://algramrandomramblings.blogspot.com/2011/01/benefits-and-disadvantages ofcloud.html

Eskeli, J. *et al*.(2010), Challenges and Alternative solutions for ERP's

Gil P., (2010), What is Cloud Computing

Halton G., Deepak S., Cloud Computing Essay(2009), http://www.scribd.com/doc/23743963/Cloud-Computing-Essay 1.1

Lombardi Flavio, Pietro Roberto Di (July 2011), Secure Virtualization for Cloud Computing, Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, *Academic Press Ltd.* London, UK.

Motiwalla, L.F. & Thompson, J. (2011), 'Enterprise systems for management, *Prentice Hall*.

Marnewick C., Labuschagne L.(2006), A Security Framework For An ERP System, Article University Of Johennesbusg.

Netsuite,(2011), The Customizable Cloud-How The Cloud Provides The More Flexible Alternative to Legacy ERP Platforms.

Ogren Eric (Sept 2009), Whitelists SaaS modify traditional security, tackle flaws

Rane Pradnyesh (2010), Securing SaaS Applications: A Cloud Security Perspective for Application Providers, Information Security Management Handbook, Vol. 5, vhttp://www.infosectoday.com/Articles/Securing_SaaS_Applications.htm

Suuburah J. (2010), Security Issues in Cloud Computing, http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-omputingsecurity-issues.htm

Wei She and Bhavani Thuraisingham (2007),Secutiry For Enterprise Resourse Planning System, Information System Security, 16:152-162.

Kulkarni Gurudatt, Gambhir Jayant. (Jan-June2012) Security In Cloud Computing, IJCET

Zhang, D.B. (2005), ERP Definition - What is ERP. Available at http:// www.sysoptima. com/erp/erp_definition.php.