Advances and Applications in Mathematical Sciences
Volume 21, Issue 10, August 2022, Pages 5789-5799
© 2022 Mili Publications, India

A FRAMEWORK FOR IMPROVING PRIVACY AND SECURITY OF PUBLIC CLOUD-BASED ENTERPRISE RESOURCE PLANNING SYSTEMS

SAI KALKI JAJULA[1], TANYA AGRAWAL[2], ANIL KUMAR MISHRA[3], ASHIMA NARANG[4] and VED PRAKASH[5]

[1,2,3,4,5]Department of Computer Science
Amity University, Haryana, India
E-mail: saikalkij@gmail.com
tanyaagarwal.cool@gmail.com
akmishra2@ggn.amity.edu
ashimanarang04@gmail.com
vprakash@ggn.amity.edu

1. Abstract

The objective of this exploration is to research at and look at the potential security chances associated with cloud based Enterprise Resource Planning Systems, which may be present in both traditional ERP systems and Cloud Computing. This focus on security of Cloud based ERP.

This paper presents an information security framework for supporting corporate governance that can be implemented into an ERP system. Since most security managers are know about the structure, a conventional data security system can be utilized as a beginning stage for fostering a particular ERP security system. Individuals, Policy and technology are the three parts of the data security structure. To better fit ERP systems, these three components have been extended and enhanced. This paper I have included mapping of proposed ERP model to security framework and the included best existing framework like ITIL ISO 17799 for guiding service strategy and service design development stages in IT services life cycle. Researched best way of developing/creating ERP system and put my findings and dependency must use while developing an ERP Frame-work. The ERP security system is utilized to show the way that the three parts can be incorporated into an ERP model. The management/IT organization/corporate offices can utilize the ERP security structure to coordinate data security inside the ERP framework. The security architecture plan is independent on customers, vendors and products. This ERP can be utilized by any ERP system such as education, banking, logistics etc. We used separate DNS name for separate section of an ERP. It reduces the chance of compromising

2020 Mathematics Subject Classification: 68M12.

Keywords: Enterprise Resource Planning · Envelop Encryption · Identity Man- agement · Policy · Security Framework.

Received January 5, 2022; Accepted February 21, 2022

integrity of entire ERP system if one DNS record/ERP domain gets attacked as we are using separate DNS the ERP security structure ensures that data security is incorporated into the plan, execution, and activity of an ERP framework, guaranteeing that the information it produces is reliable.

2. Introduction

Information is one of the primary assets for an affiliation and ought to be suitably shielded. Data security joins designs, processes, and inward controls to guarantee the constancy and game plan of information and utilitarian structures inside a connection. The transparency of data is likewise critical for the connection [1]. If the dependability of the information is impeccable and the information is secret anyway not open to supported clients, it is worthless.

Enterprise resource planning (ERP) structure security should be tended to be near standards as standard data security. An ERP structure controls all the business related information of a relationship as well as the information connecting with the clients and supplier [2]. The security of the information and assurance of the information inside the ERP structure is thusly essential to the presence of the corporation. The motivation behind this research is to propose cloud based ERP framework for improving Privacy and security. Many ERP frameworks at last don’t adjust to corporate and IT administration prerequisites. The interaction used to give an answer for the above issue is as per the following:

A security structure is inspected to finish up the viewpoints that are legitimate to ERP frameworks.

The absences of this security structure are seen concerning an ERP frame- work.

The security structure of an ERP is cultivated that acclimates to collaborative and IT association necessities.

Created Terraform template to provision resources on cloud platform.

3. Security Framework Structure

Figure 1 depicts a conventional information security structure. The structure is ordered into 3 sections: individuals, innovation and strategy, which are dependent [3]. Change to any one part will intervene in with others.

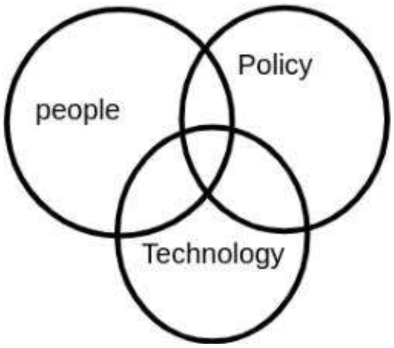


Figure 1. Generic information security framework.

People Component. Individuals part is confined into 2 get-togethers. The fundamental social affair contains people who set up security and sponsorship the communication. Two or three key positions integrate senior organization, security supervisors, IT heads and analysts. The resulting gathering is the genuine clients of the structures [4].

Policy component. Data security is a fundamental snippet of data improvement association. Different procedures are available to a relationship to make data security part of corporate association, for example, generally decides that incorporate CobiT, ITIL and ISO 17799.

CobiT. CobiT is an IT association control development and improvement frame-work that guarantees that IT assets are concurred with the genuine vision and systems.

ITIL. ITIL outline and portrays key cycles like change, issue and blueprint the board. It other than gives a construction to managing the cycles [5]. By driving a concentration toward changing and depicting a particular correspondence, the IT division can see open entrances for upgrades in capacity which can accomplish as far as possible over even more likely direct association transport and backing [6].

ISO 17799. ISO 17799 is an acknowledged worldwide standard that gives rules and ideas to security the board. It is disconnected into 10 components which are utilized to do security.

Technology Component. This component part of the Information security can be isolated towards 5 help focuses.

Identification and authentication

Authorization

Confidentiality

Integrity

Non-repudiation

4. Mechanism flow of an ERP System

The interaction stream part of an ERP framework manages manner in which data streams between the different programming modules.

Policy Component. ISO 17799 will influence the manner in which the various parts collaborate with one another. It will likewise decide the degree of data that streams between the different programming parts.

People Component. Individuals part doesn't assume a huge part since all data stream occurs behind the scenes of the ERP framework [7]. The main angle that should be thought about is that the clients should know about what the framework works and the mean for their activities could have later on.

Technology Component. The progression of data between the different programming parts should be constrained by the accompanying support points [8]:

Confidentiality-Information ought to stay private as no client straightforwardly collaborates with the data as it streams starting with one module then onto the next.

Integrity-The data that streams from one programming element or even inside an element should be an equivalent when it appears at its impartial. The data should not change in the course of the correspondence stream.

Availability-The ERP structure must be accessible to guarantee that data can stream in the middle of the various elements [9].

5. Configuration

Your DNS server may have the option to determine records in zones that it has assuming you select this choice. However long your organization is totally confined from the Internet, you can take advantage of this to its fullest potential. Set up as a web name server and recover the root server's arrangement data. DNS servers is used to host zones and check for the records/message on the net, this is very benefitting choice.

In the beginning, you may only see one zone icon-the root zone-if you are using BIND for the first time. Local domain and 127.0.0.l are used to resolve the local hostname and IP address of Linux distributions that include the BIND package. The BIND DNS Server module main page as given in Figure 2. Used separate DNS name for separate section of an ERP. It reduces the chance of compromising integrity of entire ERP system if one DNS record/ERP domain gets attacked as we are using separate DNS. If we have 5 domain of an ERP, one DNS gets attacked. Integrity Continuity of 80% of an ERP is still unaffected. Only 20% comprised which earlier case would be 100% compromised. Which is a great improvement.

Making another expert zone an expert zone is one for which your DNS server fills in as the essential wellspring of data, and it is the one to focus on. Multiple servers can host a single zone, but only one of those servers is the master, the rest are slaves.

SSL/TLS Certificate. Transport Layer Security (TLS) certificates-generally regularly known as SSL, or advanced endorsements-are the groundwork of a no problem at all web. TLS/SSL declarations secure web associations by scrambling information sent between your program, the site you're visiting, and the site server. SSL/TLS certificates can be requested as shown in Figure 3.

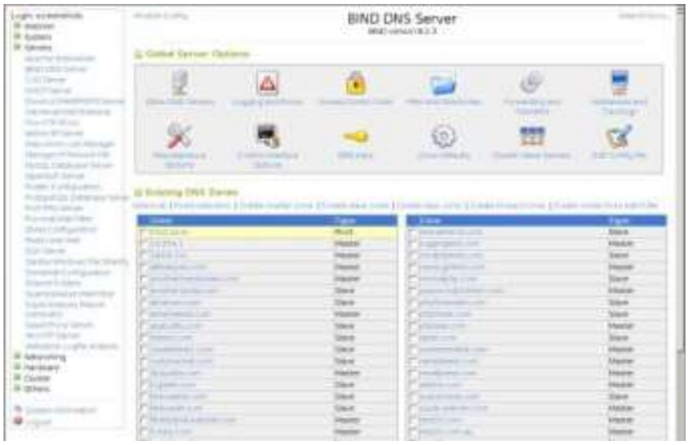
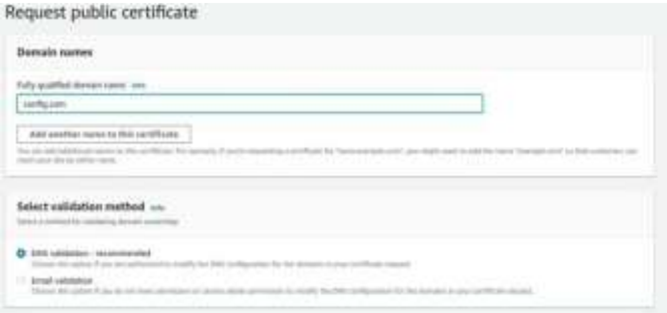


Figure 2. DNS Server.



Request public certificate

Domain names

Fully qualified domain name

config.com

Add another name to this certificate

Select validation method

● DNS validation - recommended

○ Email validation

Figure 3. Requesting SSL/TLS Certificate.

Identity Management. Identity management (ID management) is the authoritative cycle for guaranteeing people have the suitable admittance to innovation assets [10]. This makes sure that authorized users have proper access. We created User Access Management to give permissions, created Admin role and given permissions to use entire ERP system while some users given permission to one sub part of an ERP and lastly given read only permissions to the users who require to validate data only. Used json format to given permissions which are user friendly and easy to understand. Json is key value pair format. Two valid actions can be given-Deny and Permit as shown in Figure 4. If Actions given as anything else than above stated then it will be a Deny always until we have explicit Permit.

6. Methods

Policy Component. It is the obligation of the program head to guarantee that ITIL and CobiT are stuck to during and post the execution of the ERP structure. This abidance to in general rules and picks make sure that clients are content to handle the relationship since they fathom that an affiliation and organization are acclimating with the guidelines.

People Component. Individuals part will sort out that fact inside the coalition is committed for the security parts of an ERP framework. These obligations will be gotten from the general individuals a piece of the security plan and will be joined into ERP security framework.

Technology Component. As given in Table 1 the 7 mainstays of ERP security should be fused in the ERP framework. These points of support structure the underpinning of ERP security and figure out what clients and clients are permitted to do inside the framework. These support points likewise guarantee that the privacy, uprightness and accessibility of the data are beyond reproach.

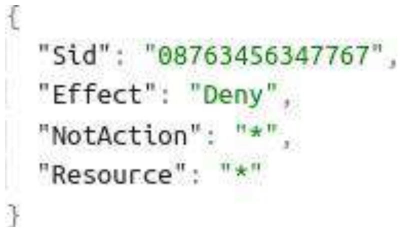
Table 1. Mapping of proposed ERP Model to security framework.

	Policy component	People Component	Technology component
Methodology	ITIL ISO 17799 -Personnel security -Communi Cations and Operations	Policy and procedures Risk analvsis Management Awareness Change	Identification and Authorisation Confidentiality Integrity Non-repudiation Availability Auditing

Factors involved in proposed secured cloud based ERP System are Business Requirement, Business Continuity, Accessibility using cloud, Security concerns around Cloud based ERP, make best use of existing security framework.

Policy. Utilize unequivocal deny and the strategy consents conclude whether the solicitation is supported or dismissed. Most of approaches are saved as JSON/XML records as given in Figure 4. Character based arrangements, asset based approaches, authorizations limits, Organizations SCPs, ACLs, and meeting strategies are upheld by most Cloud Providers. IAM arrangements characterize authorizations for an activity, no matter what the means used to do it. Permit is superseded by an express deny in any of these policies. Choose the approach astutely in light of the fact that it is first degree of safety.

ISO 17799 is a veritable by and large standard that gives rules and suggestion to security the executives [11]. It is separated into components that are utilized to execute security. This spotlights explicitly on the detail of finishing and con-trolling data security which can be utilized to address all approach related issues inside the ERP structure.



```
{
  "Sid": "08763456347767",
  "Effect": "Deny",
  "NotAction": "*",
  "Resource": "*"
}
```

Figure 4. Policy.

Data Security. Use Spring security, OpenID Connect and Auth 2 for Authentication and enable CSRF Protection. To Prevent XSS Attacks make use of content Security Policy [12]. This can be done while developing ERP system and can chose cloud Providers for hosting them. We used ‘org.springframework.security.oauth’ dependency to implement Data Security layer.

Encryption Component. When sensitive data is stored in a database or on a file system, it should be encrypted. This restricts direct access to data and guarantees that the application logic filters all accesses [13]. To get delicate in- formation in the cloud, the encryption part can utilize public-key or private-key encryption draws near. Since the encryption and unscrambling processes add handling above, non-delicate information ought to be saved in plaintext to set aside cash. Some related works on Cloud service applications and public network security encryption are referred [14-17].

Multi Level Encryption Solution. Used multi level to encrypt information. Encrypt Plain text data with data key then encrypting the data key under another key. Process to create is given below:

Produce a DEK locally. You could do this with an open source library like OpenSSL, indicating a code type and a secret key from which to produce the key.

Utilize this DEK locally to scramble your information.

Create another key in Cloud KMS, or utilize a current key, which will go about as the KEK. Utilize this key to scramble (wrap) the DEK.

Store the encoded information and the wrapped DEK.

7. Conclusion and Future Scope

The paper centers on security inside an ERP framework. It gives 25% better performance than compared to existing framework as it comprises policy and the dependency to use while developing ERP framework. Used separate DNS name for separate section of an ERP. It reduces the chance of compromising integrity of entire ERP system if one DNS record/ERP domain gets attacked as we are using separate DNS. It gives a security structure that can be used to address all material security focuses inside a connection and to ensure that it moves toward an indispensable part of an ERP framework. The security architecture is organized into the ERP model to equip the relationship with a conspicuous impression of which security issues should be watched out for inside which ERP section. It is direct given the over that security should move toward a critical piece of the ERP component. An ERP structure is in addition a basic piece of the connection and can't be treated as a free framework without pondering the cooperation's philosophies and strategies.

The paper gives a connection a development to guarantee that whole perspectives including IT and organization security are coordinated into the ERP framework. The alliance can rapidly figure out where an ERP framework is to be blamed concerning security and the inadequacy can be changed before it result in troublesome issues.

One more viewpoint that should not be dismissed is that ERP security is a determined cycle. The power association begins with the pre execution stage where security is organized and coordinated into the ERP structure. The power cycle stops with the execution of the ERP framework. As the design is kept conscious with the latest and new types of progress arise, security should be addressed as a typical occasion to keep the data great.

References

[1] M. Stamp, Information security: principles and practice, John Wiley Sons 2011.

[2] W. She and B. Thuraisingham, Security for enterprise resource planning systems, Information Systems Security 16(3) (2007), 152-163.

[3] A. Narang, D. Gupta and A. Kaur, Biometrics-based un-locker to enhance cloud security systems, International Journal of Cloud Applications and Computing (IJCAC) 10(4) (2020), 1-12.

[4] A. A. Al-Johani and A. E. Youssef, A framework for ERP systems in SME based on cloud computing technology, International Journal on Cloud Computing: Services and Architecture 3(3) (2013), 1-14.

[5] G. Dhillon, Guest Editorial: the challenge of managing information security, International Journal of Information Management: The Journal for Information Professionals 24(1) (2004), 3-4.

[6] C. Marnewick and L. Labuschagne, A security framework for an ERP system, In ISSA (2005), 1-15.

[7] R. Kashyap, Security Framework for Enterprise Resource Planning, In Metrics and Models for Evaluating the Quality and Effectiveness of ERP Software IGI Global (2020), 84-118.

[8] A. Narang, Analysis of the multitasking feature-Virtualization and virtual storage in Cloud, International Journal of Innovation Research in Computer and communication Engineering (2017), 9439-9443.

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

[10] F. Gibb and S. Buchanan, A framework for business continuity management, International Journal of Information Management 26(2) (2006), 128-141.

[11] K. Goel, C. Gupta, R. Rawal, P. Agrawal and V. Madaan, FaD-CODS Fake News Detection on COVID-19 Using description logics and semantic reasoning, International Journal of Information Technology and Web Engineering (IJITWE) 16(3) (2021), 1-20.

[12] P. K. Verma, P. Agrawal, V. Madaan and C. Gupta, UCred: fusion of machine learning and deep learning methods for user credibility on social media, Social Network Analysis and Mining 12(1) (2022), 1-10.

[13] A. Shankhdhar, P. K. Verma, P. Agrawal, V. Madaan and C. Gupta, Quality analysis for reliable complex multiclass neuroscience signal classification via electroencephalography, International Journal of Quality and Reliability Management, (2022).

[14] C. Gupta, D. Gaur, P. Agrawal and D. Virmani, HuDA_COVID Human disposition analysis during COVID-19 using machine learning, International Journal of E-Health and Medical Communications (IJEHMC) 13(2) (2021), 1-15.

[15] A. Narang and D. Gupta, A review on different security issues and challenges in cloud computing, In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) IEEE (2018), 121-125.

[16] M. Ali, S. U. Khan and A. V. Vasilakos, Security in cloud computing: Op-portunities and challenges, Information Sciences 305 (2015), 357-383.

[17] K. Fan, Q. Tian, J. Wang, H. Li and Y. Yang, Privacy protection based access control scheme in cloud-based services China Communications 14(1) (2017), 61-71.

[18] H. Kaur, P. Agrawal and A. Dhiman, Visualizing clouds on different stages of DWH-an introduction to data warehouse as a service, In 2012 International Conference on Computing Sciences (2012), 356-359.

[19] V. Madaan, D. Sethi, P. Agrawal, L. Jain and R. Kaur, Public network security by bluffing the intruders through encryption over encryption using public key cryptography method, In International Conference on Advanced Informatics for Computing Research (2017), 249-257.

[20] E. Torre, J. Durillo, V. De Maio, P. Agrawal, S. Benedict, N. Saurabh and R. Prodan, A dynamic evolutionary multi-objective virtual machine placement heuristic for cloud data centers, Information and Software Technology 128 (2020), 106390.

[21] A. Zabrovskiy, P. Agrawal, V. Kashansky, R. Kersche, C. Timmerer and R. Prodan, FSpot: Fast and Efficient Video Encoding Workloads Over Amazon Spot Instances, Computers, Materials and Continua 71(3) (2022), 5677-5697.