INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)
ISSN 2278 – 7631 (Print)

Modeling Security Concerns In Web Based ERP

Manoj Jhawar
MBA 2nd yr, IIT Kanpur, India
Deepak Nirwal
MBA 2nd yr, IIT Kanpur, India
Shashank Shivhare
MBA 2nd yr, IIT Kanpur, India

Abstract:
ERP provides the unified business process across the organization by integrating various business processes. Presently ERP is experiencing the transformation that will make it much more intelligent, collaborative, web enabled, highly integrated and may become wireless.ERP system are prone to high vulnerability and as the information is highly confidential , the ERP vendors have integrated their security solution but we need new technical approaches to secure an ERP systems. ERP solutions worked upon common use of distributed application which causes security problems. This paper describes various security models for Web ERP systems using web service technology. This paper discusses ERP technology from its development through architecture to its product and security models in WebERP. The security solution in ERP and directions for secure ERP systems are mentioned in this paper. The approach here mentions an open security model for distributed ERP systems and needs further research.

Key words: *Web Service, Web Service Security (WSS), security modeling, Peer-to-Peer (P2P) architecture, XML*

1. Introduction

ERP systems are integrated, configurable and tailor made information system which manages all the information in an organization and incorporates business across the organization's boundaries. An enterprise can automate its business process, reduces cost of collaboration and complexity. ERP induces business process reengineering to optimize its business transaction and operations and finally delivers an efficient business scenario.

Today's ERP system such as SAP R/3 or Oracle consists of many specific modules which provide specific functionality. Further such ERP depends upon very large scale infrastructure such as servers and networking which are very expensive to initially and in maintenance. Today a lot of effort is being given to develop a ERP architecture which will facilitates further reusability business components through a shared, non monolithic architecture based on a peer to peer (P2P) network.

As common use of distributed application is being done, it leads to security issues. The objective of this paper is to describe an open security model for a shared ERP package on web technology (internet). In this paper we will discuss ERP technologies and framework including the communication platforms such as ALE, EDI, and also Exchange Infrastructure. Some security aspects of SAP and emerging web services for ERP. The overview of the ERP security using a layered approach and the RBAC model for ERP .Further we will compare these security aspects with authorization function of SAP R/3 system and the Baan security method. Recent researches in ERP security are also discussed.

2. Background & Motivation

Today's ERP consists of various software component related to each other. Presently these components are administered using a single central application server. In regard to ERP system various complexities arise such as non requirement of all modules, investment in expensive networking infrastructure and expensive customization. All these problems lead to acquisition of ERP packages only by big enterprises.

A solution to above mentioned problem is to develop a distributed ERP package which will allow system components to reach over internet and this component combined will appear as singe ERP network for the user but in actual it consists of different individual

elements existing on different computers. Based on this concept it is possible for a company to access functionality components over a P2P network.

This approach will solve the mentioned problems:

- Separation of local and remote functions will save wastage of local resources for unnecessary components.
- To make single components execution possible on small computers.
- Maintenance and installation costs will decrease due to decreasing complexity of local sytem

In common use of distributed application i.e. on web erp, several security problems exists and these are

- Resource protection
- Data confidentiality
- Data integrity
- Authentication of user
- Non repudiation of transaction
- Reliability of user
- Anonymity of user

3. Security Concerns in WebERP

Various WebERP security concerns needs to be understand first before farming any model. Security issues that are specific to web based enterprise resource in enterprises are as follows.

3.1. Physical Security

The physical setting of software and data is an important part of a business plan as well as a software safekeeping plan. A physical security violate means that somebody with cruel intent has physical access to hardware where either our application is running or where our data is stored.

3.2. Transmission Security

Data transmissions can be intercepted when data is communicated between the user, server, and database. A simple way to prevent requires encrypting all communication between source and destination. But encryption comes at a price to performance. If we spend too many processing cycles encrypting and decrypting the data, we will have to purchase more costly hardware or endure delay

3.3. Storage Security

When ERP data is viewed by users, unauthorized access to users is limited due to requirement of business logic with the proper credentials. But a network administrator has direct access to data in the database. In such case, the data could be seen without going through business logic

3.4. Access Security

Access security is significant for checking unwanted users from capturing resources and sending unofficial queries to our servers. Generally this is achieved through the use of firewalls that prevent discarded traffic from communicating with our business applications. Further lack of access security could impact one's application availability and thus provide hackers a chance to make it easier to steal passwords or resources.

3.5. Data Security

Data security limits the access of data objects for specific individuals. Various levels of data security include insert, delete read-only and edit. One can be set the data security at the application or object level. Data security can be enforced either through business logic or at database layer. In most of the cases the business logic works towards authentication of users and provides them with certain rights to data objects. This means that only authenticated users can access to objects based on particular capabilities provided by the system. For e.g., a sales person may have read-only access to a product information so that he cannot change the commissions/ pricing/margins associated with product. Also a sales person might have access to customer records that he is managing, but not having access to customers managed by other people. To simplify management decision making, systems offer role-based security so that administrators can allocate broad security policies to particular individuals. Accounting, HR, marketing, sales, shipping, management, etc roles can be recognized and assigned to individual employees. Employees that are performing more than one role can get multiple policies. Administrators can make changes to security for many people by assigning different roles at once without the need of changing individual records.

3.6. Application Security

Application security includes two broad areas – firstly the way the application manages and secondly authenticates users and the way in which application code is controlled.

3.7. User Authentication

User authentication normally involves username and password to identify rightful users. User identity is critical for confirming data rights and also for creating an audit for follow up of activities for compliance requirements. Modern systems needs strong passwords, implement lock-out from excessive failures, and also give administrators the option to necessitate users to change their password at Specific time intervals. Beside these common security measures, administrators may also restrict access to the system by IP address to combat hackers that are trying to guess usernames and password from remote locations.

Authenticated users are granted access to particular data and processes. ERP application must provide security checks to prevent authenticated users from doing unauthorized work. For example, somebody only authorized to feed data should not be able to delete the data. If somebody is only authorized to fill out a form, then the data must be look at to prevent SQL and overflow injection issues.

3.8. Managing Code and Logic

All ERP software undergoes updates and revisions. The processes which manage these updates can be included as part of overall security plan provided by the vendor. For e.g., when compiling the final codes, processes are made to insure that rogue code is not put in into a production build.

As a WebERP uses shared hardware, shared operating system and a customer-specific application code, so the security issues are almost like to traditional ERP. Distances covered by transmission security are always longer, but it has little impact on overall security. When the WebERP is running a multi-tenant application process, the data security and application issues may be slightly dissimilar, but not necessarily less secure. Further in a multi-tenant deployment, the application must be designed so as to prevent client 1 looking client 2′s data. Usually all WebERP applications are designed in this way. The multi-tenant application must assign resources so that client 1 cannot take resources from client 2 during a heavy usage period

4. ERP Architecture

ERP systems have evolved widely over the years. Initially, ERP systems were used for simple jobs such as accounting and HR planning. With the introduction of Web technologies, companies now such as Oracle, SAP, Baan, etc began developing a group of applications for ERP systems. The rising technologies such as Web service, extensible Markup Language (XML) have had a major impact on security of ERP systems.

In enterprises, some systems may be developed by the enterprises itself but others may be developed by various vendors using different databases technologies and languages. ERP system differs from each other and this makes it difficult to upgrade the organization's businesses, information technologies and strategy effectively. Since communication infrastructure and ERP functionalities are combined in components so an ERP system can easily meet these requirements. A typical Web ERP system should have the following features:

- Integration—various components are integrated and seamless data flow occurs between components to collaborate as a single function.
- Flexible—system is flexible, compatible and expandable with the old systems, changes to the business processes and strategies are easy to accomplish.
- Real-time—different components works in online, real time and batch processing modes should be presented.
- Componentization—different business functional requirement are designed as different components.
- Tailor able—system should be simply configured according to the enterprise's requirements.
- Profitability—ERP system must have the capability to reduce the cost or increase profit, since it is a basic requirements and motivations for any company.
- Security—security plan has to be imposed to protect various enterprise resources not considering whether it is suitable or sufficient. The business sense in ERP system utilizes client/ server architecture to create a distributed computing situation. Generally, the 3-tier architecture is used. This contains three layers of logic:
- Front layer of Presentation Layer: A combined Graphical User Interface (GUI) or any browser that collects data, generates requests, and proceeds the results back to the user.
- Middle layer of Application: Application programs that collects the requirements from the Presentation layer and further routes the request based on the business function, rules or logic.
- Database Layer (Back): Data Base Management Systems that manages the business and operational data throughout the entire enterprise. As the user has access to this information, this layer may also contains the operating system and the associated hardware, since these are necessary for the system but visible to users.

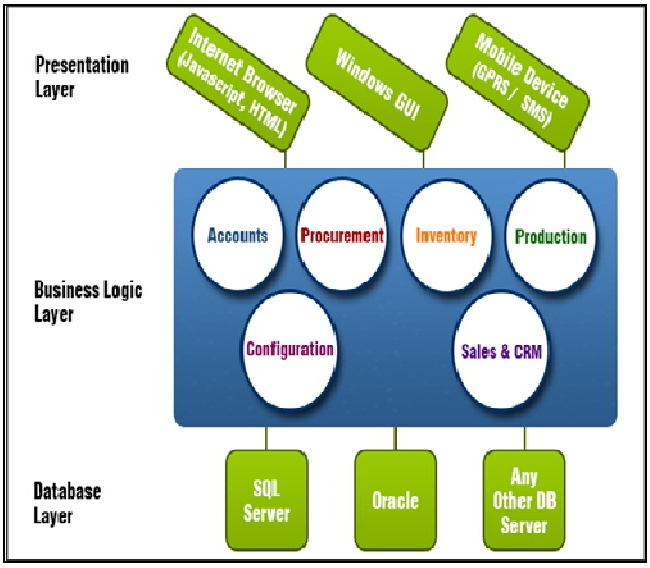

Figure 1: The Architecture Of Enterprise Resource Planning (Image Source: Emerladinsight.Com)

4.1. ERP Technology

Important technical elements of the visualized design in WebERP are a P2P system as a fundamental network design schema and a Web Service technology as approach to frame a top level interconnection of business mechanism. In regard to security aspects a lot of research is being already done by the World Wide Web Consortium (W3C) and Organization for the Advancement of Structured Information Standards (OASIS). The following definitions give a brief knowledge of the theoretical and technical foundations.

- **P2P systems**
  Peer-to-peer' (P2P) refers to a category of systems and applications that use distributed resources to perform a critical function in a decentralized way
- **Web Services**
  Web Services are encapsulated software-components, self-descriptive which allows an interface for distantly calling their functionality and can be loosely attached by the exchange of messages. For achieving universal interoperability, regular internet technology is used for networking
  The use of Web services eases integration and reduces costs. Further clients want to access information without having to go through a ERP software. With the use of Web services and the composition of Web services, outsourcing vendors as well as clients can access many of the ERP applications seamlessly and easily.
- **Web Service Security (WSS)**
  WSS describes a set of existing extensible markup language (XML) standards and security mechanism and their grouping to a standard for securing messages being written in the Simple Object Access Protocol (SOAP) format. XML is a flexible text format standard developed by the World Wide Web Consortium (W3C) and is a simplification of Standard Generalized Markup Language (SGML) for large-scale electronic publishing .A major advantage of XML over other description languages such as HTML is its ability to represent data format using Document Type Declaration (DTD) schema or XML schema. This is the reason that XML is applied in many ERP applications developed in recently.

5. Shared ERP Architecture

In above discussion we mentioned the division of the ERP system is based on a P2P architecture. In P2P architecture each peer can communicate with the rest of the contributing network nodes. Apart from other forms of P2P structuring, illustration below use a complete P2P architecture whereas the addition of a centralized control is discarded.

The responsibilities and duties of every network node are divided into two sections. First section has the service providing peers and second section has the ones which utilize theses services establishing the basis for exchanging software components, but the over-all functionality of system will be available to the whole ERP network. SOAP (Simple Object Access Protocol) messages which are mentioned in Web Service Description Language (WSDL) build up the communicational basis of this situation. Further in a Web Services registry ERP mechanism can be searched out by applying Universal Description, Discovery and Integration (UDDI) standards. New providers can be involved easier because of integration of these standards and new system functions are added by applying new Web Services whereby high flexibility is provided.

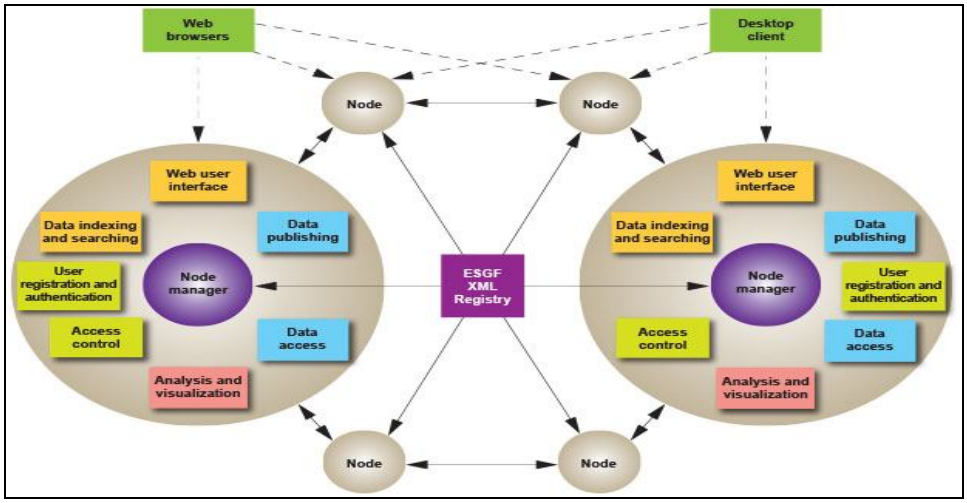

Figure 2: Various ERP Components in A P2P Network Are Based On Web Services Provided By ERP Peers (Image Source: Str.Llnl.Gov)

5.1. Peer Architecture in ERP

The contact between server and client is done by exchanging Web Service requests and responses as SOAP messages. Requests will include all the necessary input factors of the remote component boundary. Responses represent an occurrence of the pre-described return object. In figure below we can see message interchange.

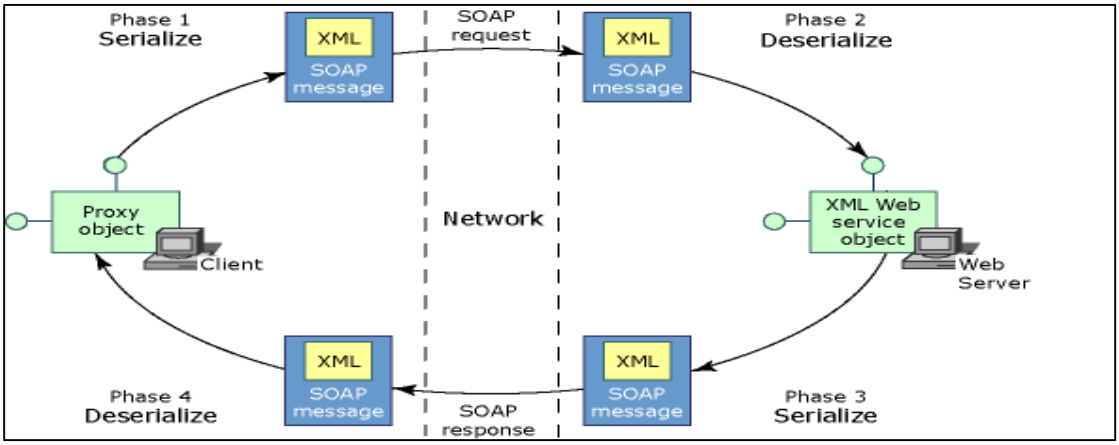

Figure 3: Communication between client and web service (image source: microsoft.com)

All incoming and outgoing messages must satisfy the hierarchic back end architecture of every individual peer. Corresponding with the motivation to incorporate standard methods, an ERP peer back end consists of the following elements:

- Webserver when Hypertext Transfer Protocol (HTTP) is using application layer basis
- Component repository which manages the local components
- UDDI registry for provision of offering public business component
- Central enterprise database management system (DBMS)

5.1.1. Features Of Peer Architecture

- Components are employed as independent elements of different computers as ERP peers.
- Every participant uses a basic standardized installation
- Components of other participants can be accessed by other participants
- Ensemble of various network nodes together that will appear as a single ERP system to the user
- Different components can be developed by different vendors
- ERP system consists of system components which are distributed within a computer network.

5.1.2. Advantages Of Peer Architecture

- Standardized technologies such as XML will facilitates integration of new components such as SOAP, WSDL, UDDI
- Self organizing peer to peer network causes decentralization and thus reduces organizational expenditures

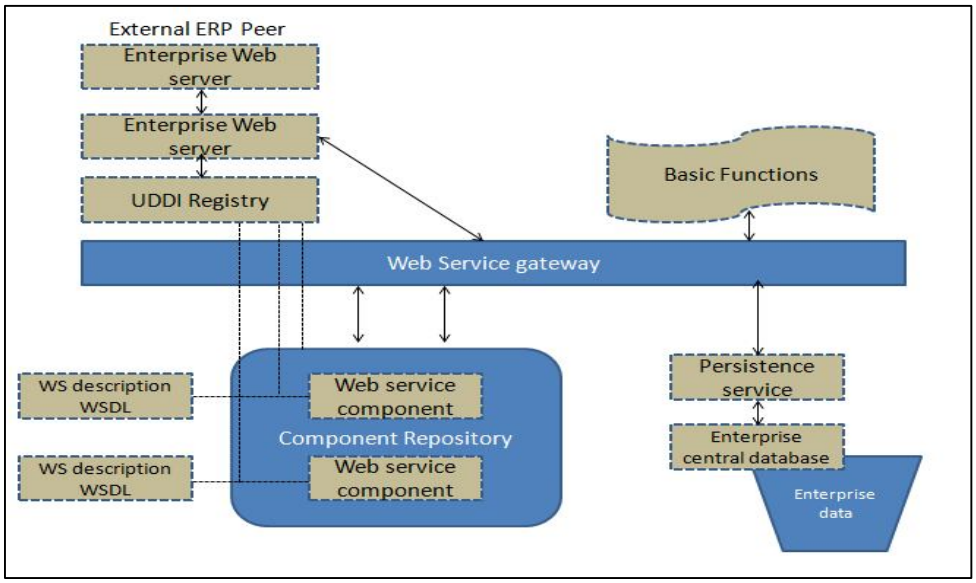

Figure 4: Schematic Diagram of Internal Peer Architecture- Controls Of the Whole Internal and External Access To Available Web Service Component by Web Service Gateway

6. Security in ERP

ERP systems are facing security problems, so security is important as ERP is used in numerous industries including defense, intelligence, financial and medical. Firstly, we need to develop a security policy and then a model for ERP systems. Many existing systems focus on confidentiality aspects of security. In this section, we will discuss the developments and current trends in security for ERP systems. We will discuss what needs to be secured, current developments, including security, for SAP. Further we will also discuss some of the next-generation security models. Also an overview of trends, security policies and Web services security are also discussed.

6.1. How to Approach Security in ERP

Security problem always exists in every component of an ERP system. These components can be classified into three categories- 1.network layer 2.presentation layer, and 3.application layer, which include internal interfaces, business processes and database. When a customer communicates with an ERP or various business components located in different places interact with each other, security problems in these cases are grouped into the network security domain. ERP experts will not deal with such cases directly and instead this function will be provided by purchasing from other vendors who are experts at fixing network security.

Application layer security needs large efforts of ERP experts to offer an effective way to secure the business processes and data. ERP technicians will also choose to activate or deactivate the security functions provided by the database vendor as per requirement of overall security solution

6.2. Current Security Solutions in ERP

- Role-Based Access Control
  Many of the current ERP systems are based on Role- Based Access Control (RBAC), although they may have different settings of either enhancements or simplifications. This model (Figure 2) defines roles and grants certain access rights. An RBAC model consists of the following components:
- Roles: A role is a named job function within a organization and a role may be hierarchical. For Example-an engineer role is also an employee role.
- Permissions: Permission is the access to one or more objects in the ERP system. Permission has different meanings in different environment. In a database system, if permission refers to the rights such as select, update, delete, or insert a record. Further if it is an accounting application then it may be the rights such as account creation/deletion, credit or debit, and transfer.

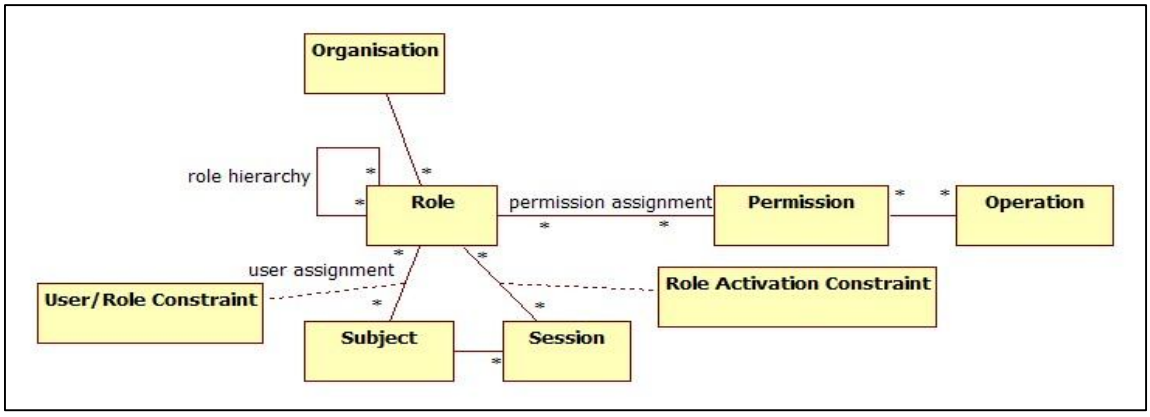

Figure5: Schematic Diagram Of Role Based Access Control (Image:Taggedwiki.Zubiaga.Org)

- Users: A user is a person who is assigned one or more roles.
- Constraints: In a system where there is only single administrator, then constraints may be meaningless. But if the administration is decentralized, means there are several administrators, then the constraints will be used by the senior administrator to restrict the junior's right to grant or deny the permissions.

7. Open Security Model

Constructing a new security layer and connecting it into the already existing architecture, requires considering different provision of individual security needs. Within the shown circumstance of a shared ERP system those necessities commonly correspond to message reliability, validity and data confidentiality of all interface calls and replies and thus of the entire network traffic. Since these strategic security objectives differ from each ERP peer to another one, it is crucial that the security model is open for virtually all security system and standards, which will allow the processing of basic definitions of security outline. Referring to the present security mechanisms a security outline describes the concrete security necessities of the appropriate network node together with the respective configuration parameters.

An appropriate profile processor is able to audit all the incoming messages for security fulfillments on the own security profile and also to extend all outgoing messages according to the security policy of remote ERP peer. Process sequence for this can be seen in figure below.

Same as in Web Service description (in WSDL), it is possible to create for related security profile and then to decide whether the remote guidelines are in accordance with the security needs of the possible caller and as result to communicate or not. For e.g., parts of those descriptions can be

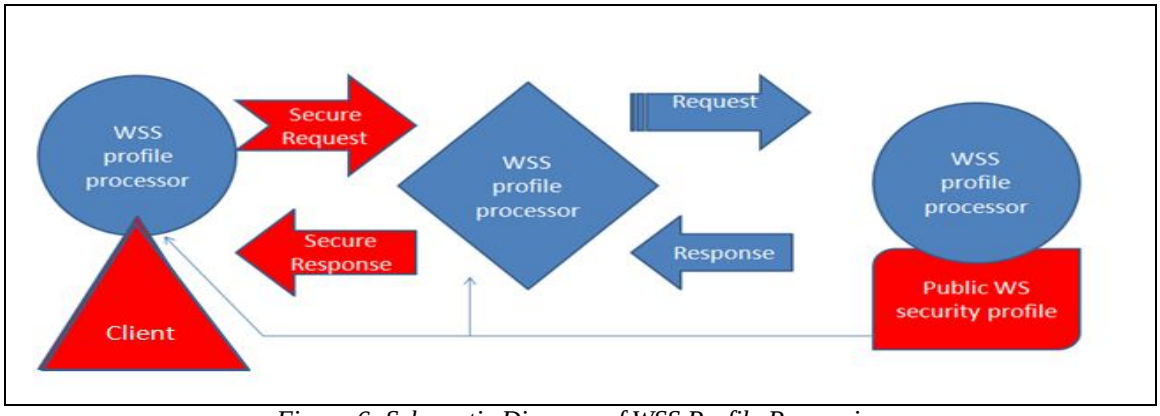

Figure 6: Schematic Diagram of WSS Profile Processing

1. XML encryption
2. XML signature
3. SAML-configuration parameter.

A Web Service Security (WSS) profile does not only contain security policy of a Web Service, but it also has a list of all supported security mechanisms. Such properties that are related to the remote system security could also describe the existence of a trusted environment according to a Trusted Computing Group (TC) which in turn would offer more important data privacy for non-public enterprise information.

The demands of the Web Service Security descriptions are satisfied and processed by a new security layer that we are calling security control gateway. It can be seen in the diagram below.

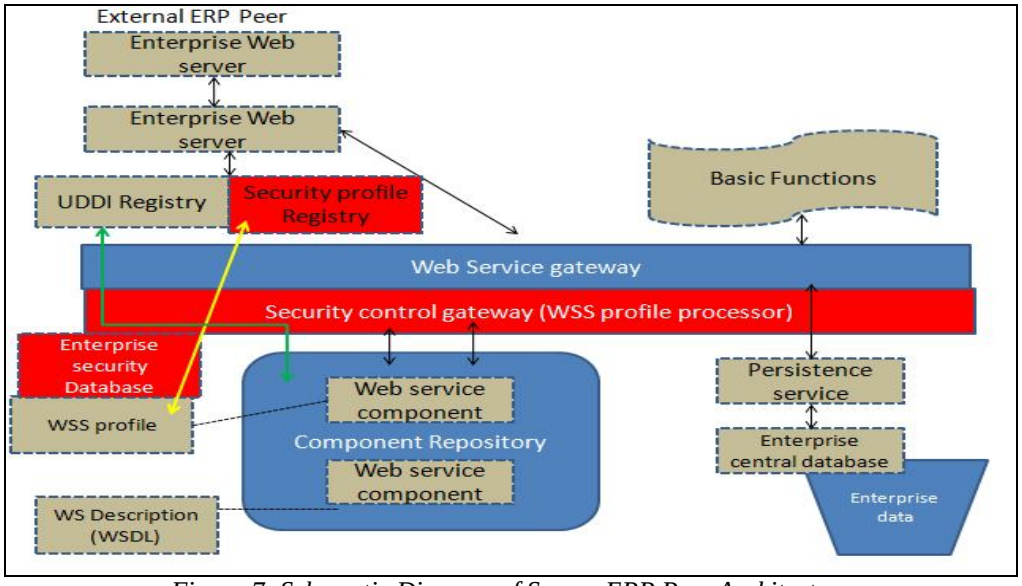

Figure 7: Schematic Diagram of Secure ERP Peer Architecture

8. Results & Discussion

Going deep into the history of ERP technology, it is easier to find out that the transformation from mainframe structure into client or server architecture is one of its biggest steps. This architecture makes it possible to develop a large system which will integrate a lot of functionalities. Further since ERP becomes the core of the operation and business in a company, ERP will not always remain the same in requirement as automation of business evolves. Future of ERP system may have the following features:

Feature	**Description**
Intelligent	ERP system in the future will have more components that perform the analysis, investigation and even advice on the strategic transformation. This feature says that more confidential information will move from within or out of an ERP system.
Knowledge-based	Enterprises are moving towards knowledge-based operation and so the ERP system that supports the daily business also needs to move towards knowledge-based management, operation and communication.
Heterogeneous	Heterogeneous means that the components from different vendors can coexist and cooperate in an ERP system. Normally it has two prerequisites-1.componentization and 2.integration. It is also true that some of the leading ERP vendors are going to make changes or have already done changes regarding these two aspects. Providing strong communication platforms to support heterogeneous applications and also the applications developed in the form of components is required.
Collaborative	This could be in the area of e-business. One can classify the business processes within an enterprise into two types- 1.enterprisecentric process and 2.collaborative process. Also processes such as accounting and payroll processing are enterprise-centric and others such as supply chain management are completely collaborative. Further in the future, more processes will be redesigned in a collaborative way. This implies that the ERP system will be more open and also more Internet-based.
Wireless	ERP system access from a mobile device.

Table 1: Future ERP Security Features

9. Conclusion

ERP is the technology which drives the reformation in the area of economy and impacts people's life style indirectly. Today ERP system is going towards a system with more coordination and collaboration and also higher heterogeneity and integrity, much more intelligent, highly operating on the level of knowledge, becoming wireless-enabled. Security issue within ERP has been there for a long time back, but today most of the solutions are based on the assumption that an ERP system is a closed environment system. Given the current trends, where ERP is more likely to become an open system, such solutions will be insufficient to provide the security. Even though many researchers are working in this area and some solutions are provided to better suites the open environment, but the security mechanism for ERP system has not yet been much brought to the open environment for further discussion. Besides, these existing security solutions like RBAC or SAP R/3 are based on the features of the current ERP system and since ERP reveals more and more new features that may be supported in the future, present security mechanism needs to be retrofitted and new security issues have to be identified.

In open security model proposed above we see that the division of transport data and content is the key-note area of the introduced security model. Furthermore, extended interface calls and responses sums up the respective information a network peer uses to serve or request ERP functional modules.

The prefixed article builds an open architecture which will not only considers the integration of existing security standards such as XML encryption or XML signature or SAML but will also aids future developments like Trusted Platforms. So before such a secure shared ERP system can be switched on we need further research into Web Service security (WSS) profile schemas must be done.

10. References

1. Date C J., 1986. An introduction to database systems. Addison-Wesley Publishing Company.
2. Davenport, T.H. (2000): Mission Critical: Realizing The Promise Of Enterprise Systems. Harvard Business School Press. Boston, MA.
3. Fabio Mulazzani, Barbara Russo, Giancarlo Succi,ERP Systems Development: Enhancing Organization's Strategic Control Through Monitoring Agents, Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on 1-3 June 2009
4. Fogg B. 2002. Persuasive Technology: Using Computers to Change What We Think and Do.
5. Fowler M. and Highsmith J. June 2001. The Agile Manifesto.Software Development Magazine. http://www.sdmagazine.com/documents/s=844/sdm0108a/0108a.html
6. Salimifard, K. Dept. of Ind. Management., Persian Gulf Univ., Bushehr, Iran Ebrahimi, M.; Abbaszadeh, M.A Investigating critical success factors in ERP implementation projects.
7. Somers. T.M. & K. Nelson (2001). The Impact of Critical Success Factors across the Stages of Enterprise Resource Planning Implementations, 34th Annual Hawaii International Conference on System Sciences (HICSS-34), Vol. 33. Issue 11 pp 805-812.
8. Somers T. M., and K.G. Nelson, 'A taxonomy of players and activities across the ERP project life cycle', Information and Management, 41(3):257–278, 2004.
9. Schwaber K. 2000. Against a sea of trouble: Scrum Software Development. Cutter IT journal.Vol. 13.Issue 11. pp 34-39.
10. M. Tarafdar, and R.K. Roy, "Analyzing the Adoption of Enterprise Resource Planning Systems in Indian Organizations: A Process Framework", Journal of Global Information Technology Management, Vol. 6, 2003, p. 31.
11. Weber, R. Information Svstems Control and Audit. Prentice Hall, New Jersey, USA, 1999
12. Davenport, T.H. (2000): Mission Critical: Realizing The Promise Of Enterprise Systems. Harvard Business School Press. Boston, MA.
13. Fogg B. 2002. Persuasive Technology: Using Computers to Change What We Think and Do.