American Journal of Applied Sciences, 10 (3): 253-258, 2013
ISSN: 1546-9239

doi:10.3844/ajassp.2013.253.258 Published Online 10 (3) 2013 (http://www.thescipub.com/ajas.toc)

A Model for Securing Sharing Information Across the Supply Chain

[1]Malihe Manzouri, [1]Mohd Nizam Ab Rahman and [2]Farshad Nasimi and [3]Haslina Arshad

[1]Department of Mechanical and Materials Engineering,
[2]Department of Electrical, Electronic and System Engineering,
Faculty of Engineering and Built Environment,
[3]School of Information Technology,
Faculty of Information Science and Technology,
University Kebangsaan Malaysia, Kuala Lumpur, Malaysia

Received 2012-02-27, Revised 2012-12-03; Accepted 2013-04-18

ABSTRACT

Supply Chain Management (SCM) is impacted by information technology both directly or indirectly. Sharing information across the supply chain not only supports internal operations but also collaboration among supply partners. So, securing information has a critical role in creating confidence in organizations to share their data across the supply chain. Purpose of this study is to propose an appropriate model for securing information across the supply chain. Reviewing the related literature, investigating the latest information technology and conducting interview with IT and SCM professionals expose the best technique of information security among supply partners. Active Directory Federation Service (ADFS) solution is proposed as the best method for securing information across the supply chain partners. The findings highlight the effective method of information security at the both level of network interconnections and software applications. This study would give invaluable information to all researchers and practitioner who investigate the information security among supply chain partners.

Keywords: SCM, Information Sharing, Security, Active Directory Federation Service (ADFS)

1. INTRODUCTION

In the today global market, organizations intend to adopt innovative technologies and strategies such as efficient Supply Chain Management (SCM) to achieve a sustainable competitive advantage (Olugu and Wong, 2009). Supply chain Managers always plan to design effective processes to meet customer demands better than competitors. Wang (2010) and Radhakrishnan *et al*. (2009) highlighted that optimising processes such as production, distribution and inventory improve organizational performance and decrease the overall cost.Besides, coordination and cooperation between processes are more crucial since Supply Chain Networks (SCNs) have become more and more global. So, the supply chain manager's focus is shifted from engineering efficient manufacturing processes to the managing of activities in the SCN (Hugos, 2006). SCM is impacted by Information Technology (IT) both directly or indirectly. IT supports internal processes and also collaboration between companies in a supply chain (Chong, 2006). With using high speed data networks and databases, companies can share data to better managing the supply chain as a whole and their own individual positions within the supply chain. The effective use of this technology is a key aspect of a company's success in managing their supply chain. All information systems are composed of technology that performs

Corresponding Author: Mohd Nizam Ab Rahman, Department of Mechanical and Materials Engineering, Faculty of Engineering and Built Environment, University Kebangsaan Malaysia, Kuala Lumpur, Malaysia

three main functions: data capture and communication; data storage and retrieval; and data manipulation and reporting. The first functional area is composed of systems and technology that create high speed data capture and communications networks (the internet, broadband, EDI and XML) (Hugos, 2006).

Every part of supply chain is deeply affected by information because each stage of supply chain makes proper decision to the daily operation based on this information. Although sharing information facilitates activities in implementing SCM (Wang, 2010), adapting IT tools is not free from obstacles and problems. Afsharipour *et al*. (2006) highlighted that the important problems in implementing e-procurement among Iranian automotive organisations are the lack of integration and inadequate IT infrastructure. Fawcett *et al*. (2007) believe that poor connectivity is less important than the lack of willingness to share essential information. In fact systems and technology signify only half of the information problems; the other one is the lack of willingness of managers to share information with the other members of supply chains. Using IT in the supply chain is associated with several risks which can be divided in installing new IT system and the operation of the IT systems. The higher risk might be created when the firms relies more on IT systems to make main decisions and execute processes. Any sort of IT problem, ranging from software and security breakdown to power outages to viruses, can entirely shut down the company's operations.

Manzouri *et al*. (2010) proposed a framework for sharing information across the supply chain. According to this framework each tier of a supply chain can predict its future orders and manage their future activities based on information which is shared across the supply chain. So, SCM can be implemented in these organizations more successfully. However, many managers were not willing to apply this framework in their organizations. They belived that since this framework accesses each organization to the database of its partners and all data of organization is available in its databese so, there is a possibility of information highjacking (Manzouri *et al*., 2010). So, lack of appropreate security solution in this framework makes it untrustable for managers to implement.

Hence, in this study authors are investigating the best method for securing information across the supply chain partners.

1.1. Security

The ability and willingness to share information essentially depends on the confidence in the security of the SCM system. The most challenging issues in information sharing are: incentives of different partners, prevention of the anti-trust implication and insurability of the timeliness and accuracy of information. In those organisations which Enterprise Resource Planning (ERP) solutions have been implemented, security plans of communications and information already exist. Inside of any ERP application the information security and SCM members' trust have been developed as an inevitable part. So, all members in the chain use a homologous application in which potentially all aspects of security have been applied in the flow of information among them.

On the other hand, security is a problematic issue for those organisations which act separately from each other with different software applications and information infrastructure (because of the lack of an ERP solution) which makes data and communications structures incompatible. In such discrete chain members, compatibility of feeding information from one member to the other and security in preserving these data transmissions (sharing information among networks) must be considered from several viewpoints. Security systems should be implemented and evaluated at both levels of network interconnections and software applications among each supply chain. Network communication security includes resources and sharing point accessibilities, users' accounting systems (for these access levels), proper routines and protocols for communications at both software and hardware level. Software applications security includes security features in databases and data structure varieties and data retrieval solutions.

2. MATERIALS AND METHODS

A research method is a system or procedure for conducting a study process. The data collection methods can be included the five categories: observation method, secondary data analysis, survey, interview and case study research. Research findings based on data collected by other investigators refers to secondary data analysis which may be applied for comparative purposes. Company records, government publications, articles, newspapers, journals and so on are known as the secondary data sources (Shuttleworth, 2008).

Fontana and Frey (2005) believed that three types of interview such as unstructured, semi-structure and structured interviews can be conducted through various means such as face-to-face communication, telephone or

computer online. In this research, a structured interview was considered by the authors because the authors enters the interview setting with a planned sequence of questions. Regarding to Fontana and Frey (2005) research, the objective of the structured interview is to express some issues so that the study can formulate a good idea of what variables need further in-depth investigation.

Four IT professionals who have more than 10 year's experiences in supply chain management were selected to be interviewed. Participants were asked to contribute to a meeting at the same time. So, there is possibility for all participants to discuss about their point of view. The interviews questions were based on the information sharing security and possibility of the information highjacking. Participants were asked to focus on the best method which can secure sharing information ascross all units of a chain. These professionals who were selected for the interview were chosen based on the following reasons: (1) The level of their experience in the field of IT and SCM implementation, (2) The degree of cooperation promised, (3) Location. Minimizing the interviewer's own bias in the interview was considered by authors. Interviewees bias and biased of the interviewer are known as the main constraints which affect in interview. Interviewee bias is when the physical appearance, race, facial expression, sex, age and dress of the interviewer (the authors) can influence the answers of the subjects. Meanwhile, biased of the interviewer exists when the interviewer (the authors) inappropriately influences respondents which may cause answers to be reported inaccurately. In this study data from face-to-face interviews was recorded by note taking. Notes were typed into computers as soon as possible after the interview to ensure that all the details were fully understood.

3. RESULTS AND DISCUSSION

Participants in interviews highlighted that it is necessary to build proper infrastructure to provide solution security components among supply partners. They emphasized the active directory and active directory fedration service as the solusions and considerdd that based on these technologies there is a need to defined some security policies inside each company and interconection among all members in supply chain.

3.1. Active Directory Federation Services Solution

The first and most important activity in any transmission and access to resources is implementing a unique security plan. The world of business suffers from two conflicting needs: (1) Enhancing the abilities of companies to collaborate and cooperate, even when crossing from one network to another. (2) Providing ever-tighter network security among those organisations. For this matter, Microsoft introduced Active Directory Federation Services (ADFS) as an integrated security solution. Since many organisations use Microsoft operating systems for their servers and PCs and many applications are mostly developed for and work on these platforms, it can be easy to implement the integrated security system. ADFS technology "interoperates across organisational boundaries and processes utilizing different technologies, identity storage, security approaches and programming models" (Pierson and Becker, 2005). Organisations need a standardized and secure method of expressing which technology it makes available to trusted partners (chain members) and runs based on policies such as what types of credentials and requests can be accepted, which organisations can be trusted and privacy policies. Implementing ADFS technology among organisations provides this opportunity to extend their existing Active Directory infrastructures to access the resources that are offered by trusted partners across the Internet. External third parties, other organisations and subsidiaries in the same enterprise are examples of those trusted partners. The claims that move among organisations can be created, secured and verified by ADFS. Moreover, ensuring secure transactions between organisations and departments can be audited and monitored by this technology.

3.2. Security Application Solution

In the software applications security level, the compatibility of data structure in various applications and databases are related tightly to the forms of security which they are using. However, naturally the security itself is an important implemented built-in feature in databases. Regarding this issue, Microsoft has also introduced an XML server to obviate all incompatibility issues between different data structures. Therefore, by using the XML server we have automatically solved security problems such as the misuse of trusted direct access or unauthorized access to the organisation database.

Currently, the Internet which is used in communication and collaboration across the SCM is the best solution for the infrastructure facilities. In this regard, all technologies of security and controlling of sharing information are suitable to be used on the Internet. General technologies for securing communication network through the Internet include: Secure Sockets Layer (SSL), multiple types of Virtual Private Network (VPN), firewalls, vulnerability assessment tools (scanners), intrusion detection systems and security auditing (logging) tools (Kros *et al*., 2005). On the other hand, new security technologies are generated which are appropriate for the security of internal SCM structures such as Role Based Access Control (RBAC) technology, Secure Supply-Chain Collaboration (SSCC) protocols suite and Radio Frequency Identification Technology (RFID) which provide secure information sharing across SCM (Zhang and Li, 2006).

After all, high levels of information sharing might also be faced with many security problems across the supply chain (Lee and Whang, 2004). Kros *et al*. (2005) and Autry and Bobbitt (2008) revealed that lack of productivity, revenues, loss of willingness and reduced competitiveness are the main consequences of breaking security in SCM. There are many possible security attacks which can threaten SCM systems information such as inference attacks (at the data management layer), password sniffing/cracking software (at the multiple layers), spoofing attacks (at the network communication layer), denial of service attacks (at the multiple layers) and direct attacks (at the multiple layers).

In the current framework proposed in this study each SCM system can use any or all of the above security solutions according to their IT infrastructure, funds, employees' knowledge and level of security which are necessary to apply on their data across sharing information. Moreover, a high level of security needs a high level of investment to implement security systems across the SCM.

Exploiting the perimeter devices, protocols and proxy servers are the most common security solutions for providing the confidentiality and privacy of the organisation's information sharing in the chain. Besides those mentioned well-known solutions, there is ADFS technology that is proposed as part of the information security. Basically in the area of enterprise and even global working size, we need to be more specific. In the proposed model that is shown in **Fig. 1** ADFS is responsible for preventing multiple accounting and the identification checking system to increase security, integrity and inter-operability among the trusted chain members. Moreover, by using some ADFS-related services such as Single Sign-On (SSO) and Web Service (WS) Federation, we can achieve the best-fit solution for medium to large companies in the suggested model. In addition for exploiting all possible and reasonable security solutions for interconnected networks, the model presents the necessary network element relationships. Obviously in such model which federation system has been applied (beside other technologies for the flow and sharing information), expected security would be done perfectly.

For better understanding of proposed model all tiers of a supply chain are summarized (**Fig. 1**) in four main companies (factory, distributer, wholesaler and retailer). According to this model when an employee from a manufacturer is going to access a Web application on the supplier company's website, the requested access at first must be verified by the manufacturer's Active Directory (AD) server itself. After authentication by local server, the request with gained credentials will redirect to the ADFS server which is already implemented in the manufacturer network and all chain members' networks as well. Then the request with specific added information will be redirected to the ADFS in the supplier network. After passing all these steps, the authenticated user request is transferred to the supplier's Web application and the user can log into the site. One of the greatest advantages of using ADFS is that the user by only one sign-in into the federation system can access the shared network of the whole chain. At last, we will have an integrated authentication system across the chain that not only prevents any interceptions and access of unauthorized users but also disposes the ability of monitoring all network transactions and managing resources by any individual member (on their own data and their partners). The key point in using ADFS is running global policy for the trust that all members are agreed on under their federation. Meantime, a user (company or individual) can be part of other federation systems too. So, this feature allows more flexibility for those companies who are involved with more than one supply chain because each ADFS has its own policy, routine and configuration.

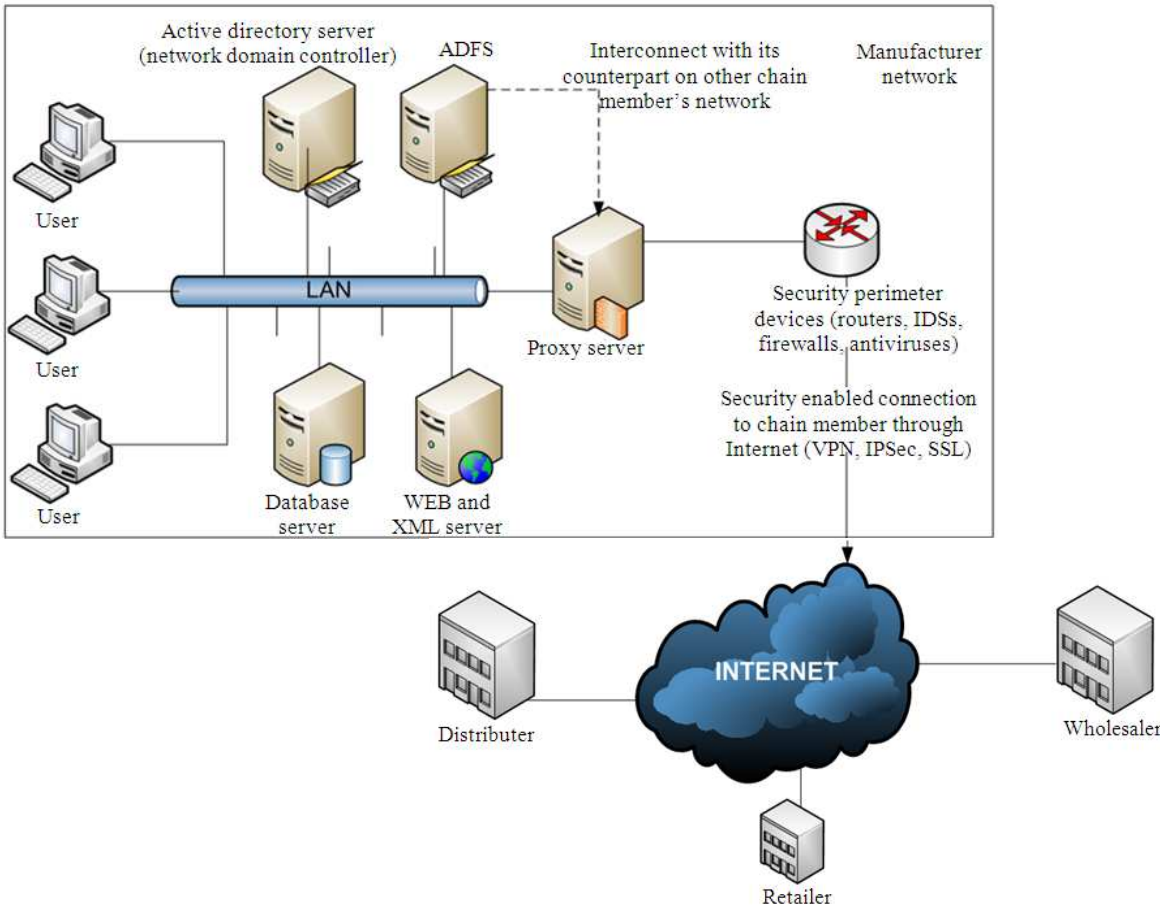

Fig. 1. Network diagram for security solution

4. CONCLUSION

Supply chain must be managed based on the flowing of information and material across the supply partners. So, organizations can be benefited from adapting IT in order to improve their overal performance. Managers are not willing to share their information across the chain unless they will be confident that they information is secured across the supply chain and there is not any possibility of infor‚mation highjacking.

Hence, in sharing information, security systems should be implemented and evaluated at both levels of network interconnections and software applications across the supply chian. Network communication security includes resources and sharing point accessibilities, users' accounting systems (for these access levels), proper routines and protocols for communications at both software and hardware level. Software applications security includes security features in databases and data structure varieties and data retrieval solutions. In addition, ADFS technology was suggested to be implemented among organisations to extend their existing Active Directory infrastructures to access the resources that are offered by trusted partners across the Internet.

5. REFERENCES

Afsharipour, A., A. Afshari and L. Sahaf, 2006. e-procurement in automotive supply Chain of Iran. MSc Thesis, Department of Business Administration and Social Science.

Autry, C.W. and L.M. Bobbitt, 2008. Supply chain security orientation: Conceptual development and a proposed framework. Int. J. Log. Manage., 19: 42-64. DOI: 10.1108/09574090810872596

Chong, A.C.Y., 2006. Migrating supply chain management process online: A study in Malaysian companies. INTI College Malaysia.

Fawcett, S.E., L.M. Ellram and J.A. Ogden, 2008. Supply Chain Management: From Vision To Implementation. 1st Edn., Prentice Hall, ISBN-10: 8131720691, pp: 600.

Fontana, A. and J.H. Frey, 2005. The Interview: From Neutral Stance to Political Involvment. In: The Sage Handbook of Qualitative Research, Denzin, N.K. and Y.S. Lincoln (Eds.), SAGE Publications, ISBN-10: 0761927573, pp: 695-727.

Hugos, M.H., 2006. Essentials of Supply Chain Management. 2nd Edn., Wiley, Hoboken, ISBN-10: 0471791512, pp: 288.

Kros, J.R., C.B., Foltz and C.L. Metcalf, 2005. Assessing and quantifying the loss of network intrusion. J. Comput. Inform. Syst., 45: 36-43.

Lee, H.L. and S. Whang, 2004. Information sharing in a Supply Chain. Int. J. Manufact. Technol. Manage., 1: 79-93.

Manzouri, M., M.N.A. Rahman, H. Arshad and J.A. Ghani, 2010. Cutting down the difficulties of SCM implementation: A comparison between iranian and malaysian companies. Appli. Mech. Mater., 44-47: 3652-3656. DOI: 10.4028/www.scientific.net/AMM.44-47.3652

Olugu, E.U. and K.Y. Wong, 2009. Supply chain performance evaluation: Trends and challenges. Am. J. Eng. Applied Sci., 2: 202-211. DOI: 10.3844/ajeassp.2009.202.211

Pierson, N. and J. Becker, 2005. Overview of Active Directory Federation Services (ADFS) in Windows Server 2003 R2. Microsoft Corporation.

Radhakrishnan, P., W.M. Prasad and M.R. Gopalan, 2009. Optimizing inventory using genetic algorithm for efficient supply chain management. J. Comput. Sci., 5: 233-241. DOI: 10.3844/jcssp.2009.233.241

Shuttleworth, M., 2008. How to choose from the different research method.

Wang, C., 2010. The influence of information sharing on supply chain management. Phys. Int., 1: 83-89. DOI: 10.3844/pisp.2010.83.89

Zhang, C. and S. Li, 2006. Secure information sharing in Internet-based supply chain management systems. J. Comput. Inform. Syst., 46: 18-24.