Misuse Case Modeling for Secure E-tendering System

Haslina Mohd, Mohd Afdhal Muhammad Robie, Fauziah Baharom, Nazib Nordin, Norida Muhd Darus, Mohamed Ali Saip, Azman Yasin, Azida Zainol and Nor Laily Hashim

School of Computing, College of Arts and Sciences
Universiti Utara Malaysia
haslina@uum.edu.my; mafdhal3@gmail.com; fauziah@uum.edu.my; nazib@uum.edu.my; nor854@uum.edu.my;
mdali@uum.edu.my; yazman@uum.edu.my; azida@uum.edu.my; laily@uum.edu.my

ABSTRACT

Tendering process is utilized by principal to invited capable tenderer to participate in competitive bid for winning a large project. Due to advent of IT infrastructure, E-tendering is introduced and adopted in many countries. Yet, an electronic environment did not promise curbing collusion between principal and certain tenderers. Other than common threats to system like security breaches by malicious parties, security issue related to ethical issue like fraud and repudiation issue where no evidence existed to denied it. In this paper, common threats for e-tendering process altogether with security countermeasure are described. This three interrelated attribute (consist of tender phase, threat and security countermeasure) are illustrated in misuse case for better understanding of the risk that may occurs in particular tender phase. Furthermore, it sought to ease the system developer for designing and constructing a secure e-tendering system.

Keyword: e-Tendering, Security threats and counter measure; misuse case.

I. INTRODUCTION

The emergences of information technology (IT) have been affecting all of organization activities including tendering. Construction industry has changed in order to keep up to grow of technology. Information and communication technology (ICT) help and ease most business and government institution. In business, the parties used to communicate and enter in contract. Hence, electronic tendering was introduced. E-tendering is adopted through many countries. This system serves as electronic environment. Compare to base tender process document archiving are more efficient and effective.

Although electronic based systems provide opportunities for improved business processes which are lead to paperless, reduced reliance on human capability during transaction, reduced costs and shortened evaluation period (Lou &Alshawi, 2009), these systems still remain uncertainty in issues relating to legal and security compliance perspectives (Betts et al., 2006), vague security framework, ownership of intellectual property, and the capture/management of the knowledge generated during the project, as well as issues of trust transaction (Rezgui*et al,* 2004; Brewer, *et al* , 2005; Pasupathinathan&Pieprzyk, 2008; Kumar Dey, Noor Nabi & Anwer, 2009). In addition, the major risks factors relating to electronic transactions on the internet such as hacking, viruses, pirating, illegal trading, fraud, money laundry, defamatory libel (Darlington, 2006) have very destructive impacts on trust and transparency in the process of tendering (Dara&Gundemoni, 2006) and also undermining of tendering data (Oyediran&Akintola, 2011).Thus, to make an e-tendering process totally secure, identifying all possible threats and determining potential solution to discover the threats are absolutely vital.

Currently in Malaysian practice, open tendering is applied for procurements above RM200,000.00. For tenders that target for local suppliers, the bidding period is 21 days and if the required goods or services are not available locally, the bidding will be opened to international tenderers for 56 days. As mentioned by Hui, Othman, Omar, Abdul Rahman and Harun (2011), tendering system is always involved with issues of accountability, transparency, corruption, integrity and cronyism. As example in cronyism and corruption, there are occurrence of information leakage to closely relative or friend as a hint to win a tender competition. However, the existing e-tendering system is still lack in addressing integrity, confidentiality, authentication and non-repudiation in e-tendering requirements. Thus, one of the challenges in developing an e-tendering system is to ensure the system requirements include the function for secure and trusted environment.

II. OVERVIEW OF TENDERING PROCESS

Tendering is an invitation to relevant parties to make an offer to the principal, which must be capable of accepting the offer thereby creating a legally binding contract (Thrope and Bailey, 1996 & Atlas et al, 1993). There are two parties that involve in this tendering process: 1) *Principal.*Any party inviting and receiving tenders. A principal may include contractor or sub contractor (AS 4120, 1994).And 2) *Tenderer.*Any party submitting tenders, including contractor, subcontractor and supplier (AS 4120, 1994).

Basically there are four (4) stages in the tendering process: Qualification and compilation of the tender list, tender invitation and submission, tender assessment and tender acceptance (Working Group 3, 1997). Meanwhile,according to Australian Standard Code of Tendering (AS 4120-1994), a standard tendering process contains seven (7) components which are the extension from the basic tendering phase. Those components are Pre-qualification and Registration, Public invitation, Tender Submission, Close of Tender, Tender Evaluation, Award of Tender, and Archiving.

III. E-TENDERING PROCESS

E-tendering is described as the electronic publishing, communicating, accessing, receiving and submitting of all tender related information and documentation via the internet, thereby replacing the traditional paper-based tender processes, and achieving a more efficient and effective business process for all parties involved (NT Government; NSW Department of Commerce) (AS 4120, 1994).

E-tendering process is very familiar with the traditional tender process, but the procedure of tendering for particular system may vary. This common feature of e-tendering are mapped against the general component of conventional tender process as shown in the Table 1.

Table 1. Correlation between E-Tendering System Components and Australian Standard Code of Tendering procedures

Tendering System Component	E-tendering Basic System Function
Pre-qualification & registration	Pre-Qualification Registration
	Issue user name and password
Public Invitation	Tender Advertisment
	Tenderer views tender advertisement and notice
Tender submission	Tenderer Registration to Tender for a Project
	Download tender document
	Tenderer submit tender
Close of tender	Close tender
	Principal Opens Tender
Tender evaluation	Tender Evaluation Process
	Request for Information
	Award Tender/Acceptance of tender
Award of Tender	
	Sign the Formal Agreement
Archiving	Retention of Document

IV. E-TENDERING SECURITY THREAT

Threat is the potential activity that could lead to vulnerability of the system (Gregory, 2010). To develop a secure system, threat identification is important in eliciting the security requirement of the system. Basically, there are nine (9) basic threats in information system (McGuire, 2000). However, through the deep finding in common threat in e-commerce (Songtao, 2011) and e-tendering article (Betts et al, 2006), there are six (6) main threats particularly in e-tendering (Dawson et al, 2006) and there are 1) Integrity violation:Malicious party change, alter or delete the information or document that should or have been done by qualified tenderer or principal committee; 2) Confidential violation:Malicious party view sensitive information of qualified tenderer or principal progress unauthorized; 3) Impersonate:Commonly in term of identify fraud, malicious party gain access of real qualified tenderer activities or impersonating as principal host for tender; 4) Non-verifiable evidence:The tenderer may claim that they are unable to prepare document due to lack of notification or clarification allowing to claim their right to be treated fairly as other tenderer; 5) Denial of service:Service host maybe unable to process user request or submission due to technical problem; 6) Repudiation: Either principal or tenderer may able to deny content or deadline of tender document causing a dispute principal and tender. When one of side of party claim this denial, the opposition cannot deny the claim. State when this of threats may occurs during tender process.

V. COUNTERMEASURE FOR SECURITY THREATS

The basic security requirement components are confidentiality, integrity and availability. Apart from that, there are also some paper that been indentify the security requirement that specifically for e-Tendering. Research that been done by Du et al (2006) identify there are 4 security services that need to provide to the protocol. There are confidentiality, data origin authentication, original integrity confirmation and system reliability. Meanwhile Mohammadi and Jahanshahi (2009), they found that e-tendering security requirement are non-repudiation and authentication, secure time and secure record keeping. Although several legislation mostly focus on integrity, confidentiality and some on availability, Non-repudiation (Rodriquez et al, 2011, Hu, 2011; Mohd Mahfuzur, Karim & Aliar, 2010) is crucial in order to handle legal compliance in case of providing evidence to negate or officially accept a business transaction on agreement is fulfill legally.

In e-Tendering process, keeping the confidential in communication is important. Confidentiality in computer system aims to avoid leaking of sensitive information during communication (Betts et al, 2006). Cryptography encryption mechanism can be utilize to ensure the confidentiality of the system. There are two type of encryption; symmetric key encryption and asymmetric key encryption. This mechanism enable only the authorized person to view the data transaction by using their own private key which is use to decrypt and encrypt the message. Integrity of system is property to make the protected data from original source cannot be manipulated by malicious party. In legal perspective, it is vital for a system such like e-Tendering system to maintain the integrity ensuring the reliability of the system. For instance, keeping the integrity of the tender box by not comprising the flouting the rules of confidentiality. For instance as the data transmitted on a network, it is trivial to change or accidentally change the value of byte in the message. To ensure the data is genuine the integrity property is maintained by allowing the recipient of message to identify the message has change or not (Betts et al, 2006). The security tools that can ensure the integrity such as digital timestamping to provide timestamp integrity (Betts et al, 2006), digital signature and biometric for integrity of record (Betts et al, 2006) and secure sockets layer (SSL) for communication integrity (Betts et al, 2006).

Availability ensuring that authorized parties can enter the system and access the data. In e-Tendering, the availability of computer system to hold the tender offer is essential. The availability of the tender box is crucial in the e-Tendering process (Betts et al, 2006). The reliability of the electronic tender box should exceed that of the physical tender box. One of the major concerns which principals and tenderers have of moving to the e-Tendering process is the issue of the electronic tender box not being available at the close of the tender.

VI. OVERVIEW OF MISUSE CASE

Misuse case is the inverse of a use case (Sindre&Opdahl, 2000). Despite that,misuse case has a similar characteristic like original use case. Therefore it promotes a same benefit for allowing stakeholder with a non-technical background to involve in the security requirement development process (El-Attar & Ahmad, 2011). Similar to use case development, the misuse cases provides a systematic way for the elicitation of both functional and non-functional requirements (Alexander, 2003).

This modeling tool was introduced by Sindre&Opdahl (2000) to represent actions that the system should prevent together with those actions which it should support. Misuse cases have proven to be reliable in bringing out possible security requirement in the system (El-Attar & Ahmad, 2011) which is suitable when developing a secure system.

This model has two representations, graphical diagram and textual template (Matulevicius, Mayer & Heymans, 2008). Both of it come with a security requirements process (Sindre&Opdahl, 2000; Sindre&Opdahl, 2005) which consists of 1) identifying critical assets, 2) defining security goals, 3) identifying threats, 4) identifying and analyzing risks, and 5) defining security requirements.

*Graphical Misuse Cases.*The use case illustrate a set of actions during system take place, which yields an observable result that is of value for one or more actors, or stakeholders of the system. To show a use case contains the action define in another use case, include relationship are used. As the inverse of the use case, Fig. 3 represent a misuse case diagram consisting “a sequence of actions, including variants, which a system or user inadvertently or unintentionally interact with the subject that causing harm to some stakeholder if the sequence is allowed to complete” (Sindre&Opdahl, 2000). The misdeed are classified as threaten relationship while the mitigate relationship specify security countermeasure against a misuse case (e.g., digital certificate).

Textual template. The details of use cases are usually captured in the associated textual templates. Templates are important because they encourage developers to write clear and simple action sequences. A lightweight description is embedded in an ordinary template and extends it with additional entries for threat specification. An extensive description supports a detailed analysis of security threats in a dedicated template (Sindre&Opdahl, 2000).

VII. CONSTRUCTING WITH MISUSE CASES

In this section we demonstrate how misuse cases can be used for security risk management (Feather et al, 1997) in the e-tendering process for tender advertisement and tender submission only. Since, constructing all the process available in e-tendering will be tedious andcomplex. Therefore, this paper only focused on a few use cases such as Advertise Tender, View Tender Advertisement, Register Tender, Download Tender Specification, and Submit Tender Document. The possible threats that might attack the tendering processes are representing by misuse case. The misuse case is one of the Unified Modeling Language (UML) notation that can be used to represent threat in the use case diagram.

The steps of constructing misuse cases as follow:

(a)*Context and Asset Identification.*Figure 1 represent a context of advertisement and submitting tender process. The Principal will advertise the tender to inform the tender about available tender. Then tenderer, view the available tender and register to preferred tender. Next the system will let tenderer download the document specification at the same time the system will record the registration. After complete the tender document, tenderer will submit it through the system before the due date.

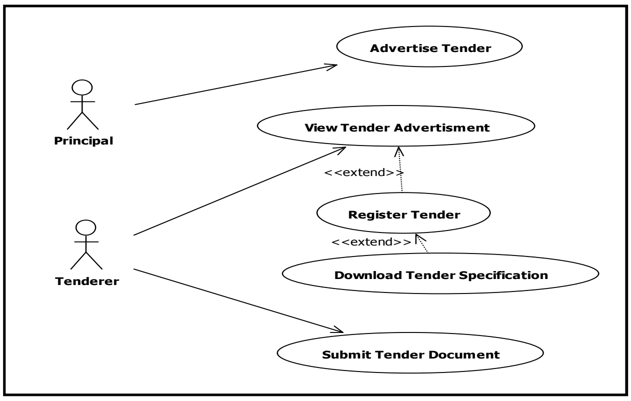

Figure 1. Tendering Process (Advertise and Submit Tender) Use Case Modeling

(b) *Security objective determination.* Use case cannot be use to show the vulnerable assets and security criteria in the diagram. It’s only can be used to tell the reason about the security criteria. This paper concentrating on threeprocesses: i)receiving tender document by principal; ii) ensuring the integrity of tender advertisement; and iii) tender submission, meaningthat once the tender advertisement is published, andthe tender document is submitted its cannot be changed.

(c) Risk analysis and assessment. In Figure 2 showsthe threat modeling in that might be happened in the tendering process specifically during the advertising and submitting tender process. The threats are represented by misuse casesfor. The Attacker in this misuse case threatens the identity of the principal and integrity of the advertisement which can lead to fake advertisement. The Attackermight threatening the confidentiality of the information duringtender submission process. They are not only stealing the submitted tender information but also can modifying the content. For the side of tenderer, the attacker stealing the tenderer's identity, submitting fake tender or stealing tender specification. The attacker also might change the tender closing time during the tender document submission. Therefore, the late tender document can be submitted into the principal database.

(d) *Risk treatment*. The misuse cases do not suggest any risk treatment. However mitigate relationship are use to specify treatment for each particular risk.

(e) *Security requirements definition*. The use case in Figure 2 shows the possible threats that might attacked the tendering process. The identified treats and possible solution for the e-tendering system are adapted from Haslinaet al.(2011). The security solution is not available for this misuse case.In Figure 3, each threat has its own mitigate relation. This mitigate relation act as countermeasure for specific threat that can reduce the effect of that venerability.

(f) *Control selection and implementation*. Misuse cases do not suggest any techniques to select and implement controls.

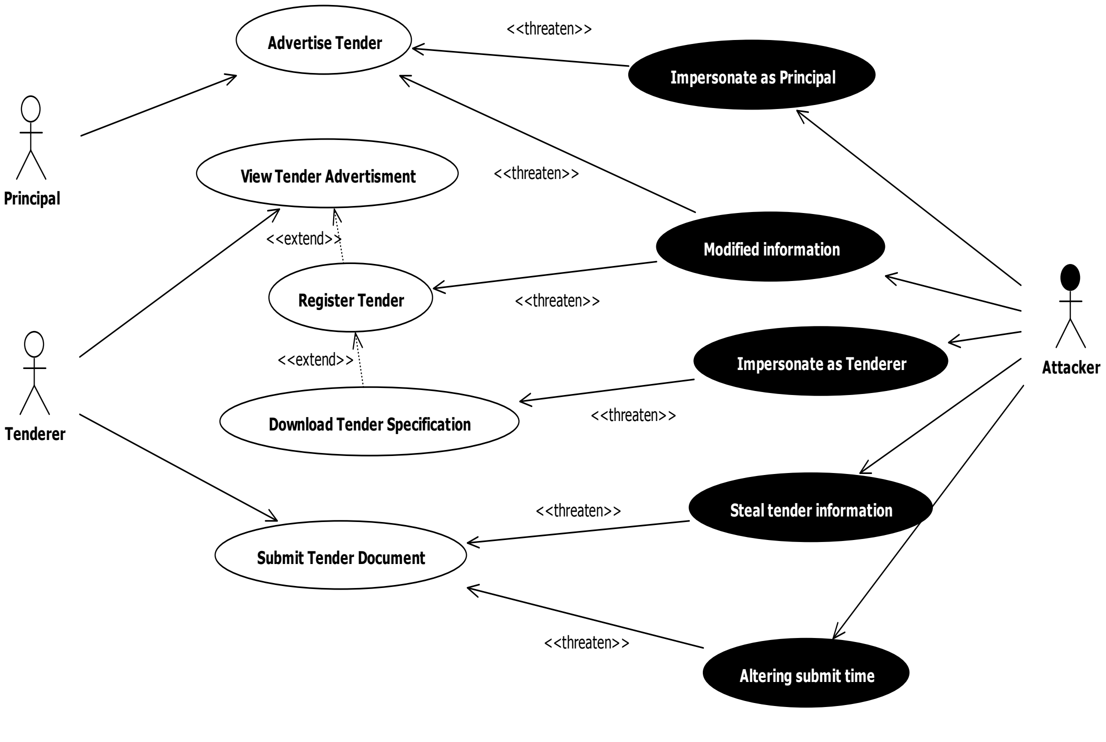

Figure 2.Threat Modeling of e-Tendering System.

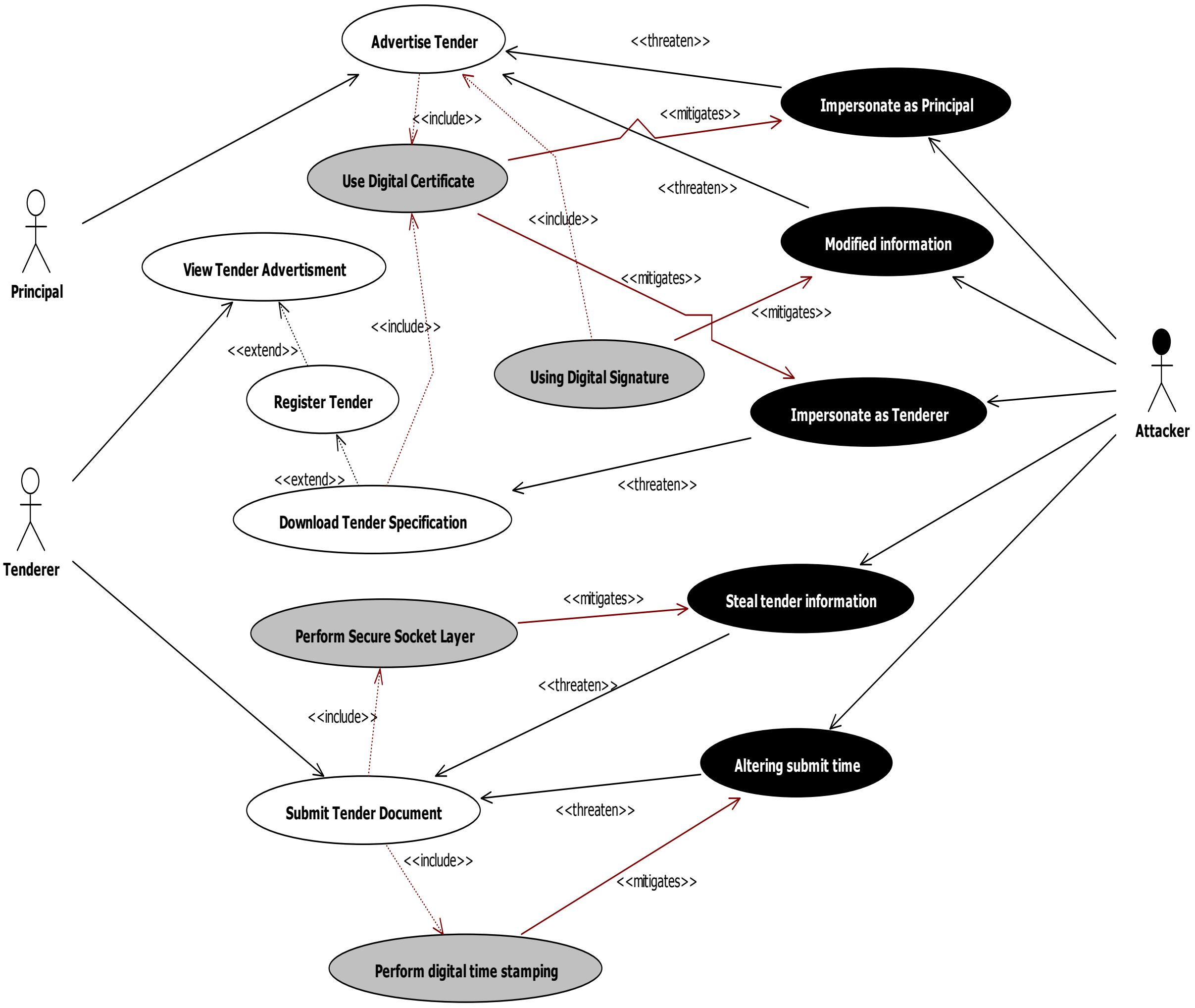

Figure 3. Modeling of Security Requirement of e-Tendering System

CONCLUSION

Retaining the accountability and security trust as conventional tendering process is important, therefore e-tendering system are required to be capable in deliver the same quality value. Apart of ethical issue threat, the developer should consider technological factor that may create hole for malicious party to invade or attack the system. In addition e-tendering system must consider several security mechanisms to curb several ethical issues like repudiation via applying digital signature and so forth. This research paper sought to integrate a secure practice in the available tender process body. These are only some examples of security issues in e-tendering that might need to utilize varietysecurity mechanisms to overcome this interrelated security problem. Without proper planning, the system might cause security hole and cost consuming. In whole view, the developer should consider on security issues and threat like confidentiality, integrity, availability, non repudiation and authentication which interrelated among itself and involving organization practice and regulations. In this paper, misuse case is designed to portray the mapping between the security risk in tendering phase and countermeasure to overcome the security problem. Thus by using mitigate relationship feature, it is able to show that what a user can do or enforce to curb these misdeeds. From this misuse case, the designer able to clarify and tell technical and non-technical people what happen in e-tendering system (similarly to the use case function) in enforcing security mechanism to produced a secure e-tendering system.

REFERENCES

AS 4120 (1994) Standard Australia Committee on Construction Industry Practices. Code of Tendering, Australia Standard. Standards Association of Australia, 1 the Crescent, Homebush, NSW 2140, 28 October 1994.

Atlas, I., Pitney, A., Curtis, J., Greenham, P., Hanly, G., Glodstein, D., Mansfield, J. & Grace, T. (1993), The Tendering Process. BLEC Business Law Education Center from the Training Division of Longman Cheshire

Alexander, I. (2003). Misuse Cases: Use Case with Hostile Intent. *IEEE Software* , 58-66.

Betts, D., Black, P., Christensen, S., Dawson, E., Du, R., & Duncan, W. (2006). Towards secure and legal e-tendering. *Journal of Information and Tecnology in Contruction, XI* , 89-102.

Dara, J., & Gundemoni, L. (2006). Credit card security and e-payment: Enquiry into credit card fraud in e-payment.

Darlington, R. (2006). Crime on the net.

Dawson, E., Christensen, S., Duncan, B., Foo, E., Du, R., Gonzalez, J., N., & Black, P. (2006).eTendering – Security and Legal Issues. Technical report, CRC Contruction Innovation, www.consruction-innovation.info.

Du, R., Foo, E., Boyd, C., Raymond, K. C. (2006). Formal Analysis of Secure Contracting Protocol for E-tendering, Australian Computer Society, pages pp 155-164.

El-Attar, M., & Ahmad, I. (2011). Improving Quality in Misuse Case Models: A Risk-Based Approach. *10th IEEE/ACIS International Conference on Computer and Information Science* .

Gregory, P. (2010). *CISSP Guide to Security Essentials.* Course Tecnology.

Haslina M., Nazib N., Fauziah B., Norida M. D., Nor Laily H., Zaharin M., Azman Y., Azida, Z. (2011). An Investigation of Possible Security Threats and the Proposed Secure Solution for Electronic Tendering Systems of Information Technology (IT) Projects.In Proceedings of the *International Soft Science Conference 2011(ISSC2011)*, 23-25 November, 2011 Ho Chi Minh, Vietnam.

Hu, Z. (2011). The Study of E-Commerce Security Protocol.

Hui, W. S., Othman, R., Omar, N. H., Abdul Rahman, R., & Haron, N. H. (2011). Procurement Issues in Malaysia. *International Journal of Public Sector Management, Vol. 24, No. 6* , 567-593.

Kumar Dey, S., Noor Nabi, M., & Anwer, M. (2009). Challenges in building trust in B2C e-Commerce and proposal to mitigate them: developing countries perspective. *12th International Coference on Computers and Information Technology* .

Lou, C. W., & Alshawi, M. (2009). Critical success factors for e-tendering implementation in construction collaborative environments: people and process issues. *ITcon Vol. 14* , 98-109.

McGuire, L. B., & Roser, N. S. (2000). What your business should know about internet security. *Strategic Finance, Vol 82, No 5* , 50-54.

Mohammadi, S., Jahanshahi, H. (2009). A Secure E-Tendering System, IEEE.

Oyediran, O. S., & Akintola, A. A. (2011). A survey of the state of the art of e-tendering in nigeria. *ITcon Vol. 16* , 557-576.

Pasupathinathan, V., & Pieprzyk, J. (2008). A fair e-tendering Protocol.

Pauli, J. J., & Xu, D. (2005). Misuse Case-Based Design and Analysis of Secure Architecture. *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC'05)* .

Qingping, G., Li, F., & Li, Y. (2009). Probe into E-commerce Security Technology.

Rodriguez, A., Fernandez-Medina, E., Trujillo, J., & Piattini, M. (2011). Secure business process model specification through a UML 2,0 activity diagram profile.

Rezgui, Y., Brown, A., Cooper, G., Aouad, G., Kirkham, J., & Brondon, P. (2004). An integrated framework for evolving construction models.

Sindre, G., & Opdahl, A. L. (2000). Capturing Security Requirements through Misuse Cases.

Songtao, H. (2011). Security Strategy of E-Commerce in China.

Thorpe, C. P. and Bailey, J. C. L.(1996), Commercial Contract. A practical guide to deals, contracts, agreements and promises.Woodhead, Cambridge England,

Working Group 3 (1997), Code of Practice for the Selection of Main Contractors, Construction Industry Board.