Journal of Engineering and Applied Sciences 12 (3): 548-554, 2017
ISSN: 1816-949X


# A Comparative Analysis Study on Information Security Threat Models: A Propose for Threat Factor Profiling

[1]Fatimah Sidi, [1]A. Jabar Marzanah, [1]Lilly Suriani Affendey,
[1]Iskandar Ishak, [1]Nurfadhlina Mohd Sharef, [2]Maslina Zolkepli,
[2]Tan Ming Ming, [2]Muhammad Faidhi Abd Mokthi, [2]Maslina Daud,
[2]Naqliyah Bt Zainuddin and [2]Rafidah Abdul Hamid
[1]Faculty of Computer Science and Information Technology,
University Putra Malaysia, 43400 Serdang, Selangor Darul Ehsan, Malaysia
[2]Cyber Security Malaysia, Level 7, Sapura Mines No. 7,
Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor, Malaysia

**Abstract:** This study describes a comparative analysis study conducted on existing approaches, frameworks and relevant references used in field of information security. The purpose of this study is to identify suitable components in developing a threat factor profiling. By having a threat factor profiling, organizations will have a clear understanding of the threats that they face and enable them to implement a proactive incident management program that focuses on the threat components. This study also discusses the proposed threat factor profiling.

**Key words:** Threat model, security, threat factor profiling, frameworks, clear

## INTRODUCTION

In today's high technology environment and rapid growth of the internets, organizations are becoming more and more dependent on the information systems. The security issues become very important due to highly dependence of devices on computers and the engagement with internet services (Zulkernine and Ahamed, 2006). Organizations and individuals have many information assets which are subject to an increasing number of threats. Virtually, all organizations face increase of threats to their networks and the services that will lead to information security issues (Jouini *et al*., 2014).

Based on a survey by PWC in 2016, cyber related crimes have been ranked as the second most reported economic crimes that affected 32% of the organizations. The survey also reported that most companies in the survey are still not adequately prepared or understand the information security threat and risk posed to their organization. Statistics by the Malaysian Computer Emergency Response Team (MyCERT) reported that incidents of fraud and intrusion are among the top three ranked incidents in Malaysia since 2014.This statistic had raised the worries of management of organization because security issues of confidentiality, integrity and privacy had received serious attention in cyber security within organizations.

Due to increasing number of information security threats and incidents, many organizations have identify information security as an area of their operation that needs to be protected as part of their system of internal control. Threat is potential cause of an incident which may result in harm to a system or organization. Threats cause damage to information systems. Threats utilize vulnerabilities to enact this damage and security controls are implemented to attempt to prevent or mitigate attacks executed by threat actors. At the moment, the existing threat factor profiling is not efficiency for all organizations. Hence, we will propose a new threat model that combines components from existing threat models as well standards and guides that will have bigger focus on organizations needs to address information threat issues.

**Defense-in-depth strategy in securing information in an organization:** In information security, the strategy of implementing multiple layers of defense to combat multiple security issues is commonly referred as defense-in-depth. A defense-in-depth strategy has become increasingly important as a result of overall business and IT trends which may weaken an organization's control of information assets.

In view of defense-in-depth strategy, a threat factor profiling is propose here as a mechanism for dealing with

**Corresponding Author:** Fatimah Sidi, Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 Serdang, Selangor Darul Ehsan, Malaysia

information security and cyber threat within an organization. By having a threat factor profiling, organizations will have a clear understanding of the threats and enable implementation of proactive countermeasures that focuses on the threat components.

**Literature review:** In order to have a threat factor profiling, threat modelling technique is used by many organizations to secure their cyber network to prevent financial loss. Some organization also use risk management standard to handle threats in their organizations. The following sections presents a brief related works of existing threat approaches, risk management standards, methods and techniques.

**Existing approaches in handling threats for information systems**

**STRIDE:** Microsoft's STRIDE is the most popular approach for threat modelling (Torr, 2005). It is most widely used as a support tool (Hussain *et al*., 2014). Components of STRIDE are spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. A Data Flow Diagram (DFD) is presented and applied to the threat categories based on STRIDE method. The STRIDE Model also been used to ensure secure software during the design phase. In other words, STRIDE Model is believed to have the ability to identify the security weaknesses of the software system by threat categories that had been defined (Scandariato *et al*., 2015). STRIDE also provides guidelines for appropriate countermeasures to be adopted in order to reduce threat risk to an organization (Sultan and Abbas, 2015). Xin and Xiaofang (2014) had incorporated STRIDE Model and threat tree analysis in order to study the problem of security issues in online banking system. The results from this two model combination are successful to improve the efficiency of the threat analysis for online banking. STRIDE Model has been proven to be very useful to determine the six threat categories in an efficient way for number of areas including web services (Jiang *et al*., 2010) secure web application (Hussain *et al*., 2011), cloud security (Saripalli and Walters, 2010), secure Software using aspect-oriented (Sherief *et al*., 2010).

**DREAD:** DREAD is part of a system for risk-assessing computer security threats previously used at Microsoft. It has been comply with STRIDE Model for rating threats (Thompson *et al*., 2014). Rao and Pant (2010) using DREAD in Geospatial Weather Information. Geospatial Weather Information System (GWIS) is a web based tool for capturing, storing, retrieving and visualization of the weather climatic data. They claimed that that threats should be meet the security objectives, reduce the risks in the development and deployment stage. According to Jiang *et al*. (2010) and Thompson *et al*. (2014) DREAD Model is used to comply with STRIDE Model whereby the rating of the threats will be produced once the threats have been categorized, then the mitigation technique would be proposed.

**OCTAVE:** OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) is a risk and mitigation management of information security risks method for organizations. It could be used for deriving the impact values to the critical assets of an organization (Feng *et al*., 2014). It has 5 components that including assets, access, actor, motives and outcome. OCTAVE moves an organization toward an operational risk-based view of security and addresses technology in a business context. OCTAVE is suitable when there is a need to implement and control an organizational risk management (Zhang *et al*., 2010). It is also useful to deal with a fundamental reorganization which include when an employer does not have a working risk methodology in area. OCTAVE requires a strong risk management framework to be carried out. OCTAVE need to implement with many worksheets and practices to fulfillment. It does not offer a list of "out of the box" practices for assessment and mitigation for security risk.

**CVSS:** CVSS (Common Vulnerability Scoring System) is a risk rating and ranking system. It is a comprehensive scoring and assessments risk model. The component of CVSS is Attack Vector (AV) Attack Complexity (AC) Privileges Required (PR) and User Interaction (UI). CVSS is composed of three metric groups that refer to base, temporal and environmental. CVSS is the best application to measure the risk. However it not minimized the attack surface area, (i.e., layout flaws) or assist enumerate risks inside any arbitrary piece of code as it is only a scoring system, not a modelling methodology. It is more complicated than STRIDE/DREAD as it objectives to calculate the risk of vulnerabilities to deployed software and environmental factors. CVSS is a complex risk ranking that need a spreadsheet in calculating the risk components. The CVSS is often used in laboratory which to study the framework (Gallon, 2011) attack graph (Gallon and Bascou, 2011), environmental scoring (Ibidapo *et al*., 2011), vulnerability across cvss metrics (Tripathi and Singh, 2011) and it also used in secure software for aspect-oriented stochastic petri nets (Sherief *et al*., 2010).

Vocabulary for Event Recording and Incident Sharing (VERIS) provides a common language for sharing cyber security events. VERIS also enables organizations to collect, classify, analyse, compare and share information security incident data (Alberts *et al*., 2003). VERIS produces a set of metrics designed to provide a common language for describing security incidents in a structured, repeatable, anonymous and secure manner. The VERIS mostly applicable in organization (Fisk *et al*., 2015) and cyber security domain.

**AS/NZS 3100:2009:** AS/NZS (The Australian/New Zealand Standard) is the first formal standard for documenting and managing risk. It is flexible and iterative. AS/NZS Model is widely adopted by industries for their operational risk management and to improve the organization's operations and competitiveness. Meanwhile, Coras is based on AS/NZS 4360:2004. The operation of Coras is based on the five activities in AS/NZS (Hussain *et al*., 2014). It is used to develop a structure that uses the methods of risk analysis and computer tools for assessing the risks (Chandrashekhar *et al*., 2015). The application of AS/NZS as a standard to manage risk by organization (Shedden *et al*., 2006) is very useful and effective. However, this standard does no longer practically perceive the threats to each critical information asset, nor the particular vulnerabilities for each asset (Lalanne *et al*., 2013). Coras risk modeling is a free available model-driven risk analysis tool that derived from AS/NZS .

**ISO/IEC 27005:** ISO/IEC 27005 standard provides guidelines for information security risk management, supporting in particular the requirements of an Information Security Management (ISMS) according to ISO/IEC 27001:2005. This is a standard for assessing risk analysis (Lalanne *et al*., 2013) especially web and could services. This is a security mechanism to implement into information system. Leitner and Schaumuller (2009) had developed a new method based on this standard and found that new risk management and implementations are applicable and efficient. Arima approach was developed to assist risk evaluation. However, this Arima method needs further evaluation and testing. In addition Mayer and Fagundes (2009) had used the Maturity Model in information security which tie with this standard to provides a proper framework to handle the information security risk management in an organization. This approach is achievable because each activity in the risk management is well presented to secure the organization. ISO/IEC 27005 version 2011 had better improvement compare with previous version. The best improvement is it allowed users to select the process which is appropriate for them. That is it is not required to follow the all steps given in this standard (Lalanne *et al*., 2013).

**NIST Special Publication (SP) 800-39:** Special publication 800-39 is a general standard that gives a structured and easy way for organization to managing security risk. It provides a guide lines in supporting NIST security standard which involved several processes such as the specific details of assessing, responding to and monitoring risk on an organization management. The prototype Aurum is developed for the idea ontology and interaction decision support (Ekelhart *et al*., 2009). The implementation of NIST SP is particularly focus on risk in IT systems. It could provide the information security knowledge to the risk manager and ensure the resources are well modeled for risk identification and risk mitigation. The next section will provide a comparison of existing approaches based on overview in the literature review.

## MATERIALS AND METHODS

**Comparison**: A comparison of existing approaches and methods will be addressed in this section. The comparison is based on the objective of each approaches, processes involved and key components. Table 1 and 2 summarized the comparison of the approaches that currently being used in industry and academia.

**Objectives:** From our study, the objective is different based on the each approach that presented. Veris is used to collect security incident data, OCTAVE identifying critical information asset and their security requirements, AS/NZS 3100:2009 is developed to a perceived need for practical assistance in applying risk management in public sector and private sector organizations, DREAD is rating model and CVSS is an open framework to gives a severity score to each vulnerability. The objective of risk management standards such as ISO/IEC 27005 and NIST SP 800-39 is to provide guidelines for organization to manage risk including threats towards web services.

**Processes:** Most of the threat models consist of similar processes such as identifying assets and threats that exists in STRIDE and OCTAVE Model. However, each model executes the identification task differently where CSVV using the numerical approaches to identify threat by calculating the impact.

AS/NZS 3100:2009, ISO/IEC 27005 and NIST SP 800-39 are different from the other compared models due to its objective that focusing on managing risk and not specifically for cyber threats. We also found out that STRIDE is more advanced than other models because it includes the process of counter measuring threats which is not available in other models.

Table 1: Summary of components by existing approaches 1

| Types | Microsoft-STRIDE | Microsoft-DREAD | CVSS | VERIS framework |
|---|---|---|---|---|
| Type (Model/framework/ Standard, etc.) | Classification scheme for characterizing known threats | Classification scheme to calculate risk/threat-risk ranking model | Open framework for communicating the characteristics and severity of software vulnerabilities | Framework/taxonomy on information security incident |
| Objective/purpose | To develop an understanding of risks to a system and how to mitigate them; | To assign threat severity and priority level of identified threats | To provide a robust and useful scoring system for IT vulnerabilities | To enable organizations to collect, classify, analyze, compare and share information security incident data in a structured, repeatable, anonymous and secure manner |
| Processes/task | Identify assets<br>Identify threat (STRIDE)<br>Recommend counter measures/mitigation | Identify damage potential<br>Identify reproducibility<br>Identify exploitability<br>Identify affected users<br>Identify discoverability | Calculate impact to CIA, attack vector, attack complexity<br>Determine temporal metrics<br>Implementation environmental metrics | Whose actions affected the asset<br>What actions affected the asset<br>Which assets were affected<br>How the asset was affected |
| Key components | Asset<br>Threat sources<br>Counte rmeasure | Asset | Asset<br>Threat sources | Asset<br>Threat agent<br>Threat actor<br>Threat sources |

Table 2: Summary of components by existing approaches 2

| Types | OCTAVE framework | AS/NZS ISO 31000: 2009, risk management | ISO/IEC 27005 | NIST Special Publication (SP) 800-39 |
|---|---|---|---|---|
| Model/framework/standard, etc. | Framework for identifying and managing information security risks | Formal standard for documenting and managing risk | Guidelines for information security risk management | A standard and guidelines that developed by NIST for information security risk management |
| Objective/purpose | To identify the information assets that are important to the mission of the organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats | To provide a common approach in support of standards dealing with specific risks and/or sectors | To support the security risk based on management approach | To give a guidelines to integrate organization-wide program into organization risk security operations |
| Processes/task | Identify assets<br>Identify access<br>Identify actor<br>Identify motives<br>Identify outcome | Establish context<br>Identify the risks<br>Analyze the risks<br>Evaluate the risks<br>Treat the risks | Context establishment<br>Identification of assets<br>Identification of threats<br>Identification of vulnerabilities | Risk assessment<br>Risk mitigation<br>Risk evaluation |
| Key components | Asset<br>Threat agent<br>Threat actor<br>Threat outcome | Asset | Asset | Asset<br>Threat sources |

**Components:** STRIDE Model is derived from the following six threat categories. Various activities could be categorized the threats according to STRIDE. When a threats has been identify, it would be categorized based on the criteria. For instance, if there is an illegal use of user authentication information, the threat could be categorized into spoofing. By considering threats of these various categories for each single element in the DFD, STRIDE greatly supports the identification of threats within the application. STRIDE Model has an asset which refers to cyber-attack that could bring loss to an organization. The threat sources could be referring to the way that may cost vulnerability. It could be refer to any category of the STRIDE Model.

DREAD Model focuses only on asset and information related to it that includes capability, advantage, feature, a financial or a technical useful resource that may get from any damage, loss or disruption. The damage to an asset might also affect the normal functionality of the system as well as the people or agencies involved with in the systems. Meanwhile, the other component such as threat agent, threat actor and threat source could not be obtained in DREAD. This is because this model is mainly for rating purposes.

CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. It was to provide a robust and useful scoring system for IT vulnerabilities and its process was based on impact to CIA, attack vector, attack complexity, Temporal and environmental. Therefore, the key component for this framework is asset and threat sources.

VERIS had also the entire component such as asset, threat agent, threat actor and threat sources compare with others method. There are five asset including ownership, management, hosting, accessibility and cloud in the VERIS framework. Threat agent also cloud is referring to

impact assessment. Furthermore, the threat actor is including the internal actor and external actor. This meaning that internal actor is referring to who are originating come from the organization. This may involve company full-time employees, independent contractors, interns and other staff. External actor could be referring to the outsider sources of the organization. This may refer to criminal groups, lone hackers, former employees and government entities.

OCTAVE is having assets for the threats identification. The OCTAVE assessment identified five critical information infrastructure assets for backup process, including three data assets, a personnel asset and an application asset. The category of the assets is data, personal asset, people and application. The threat actor from inside and outside also been consider in OCTAVE. The threat agent could refer to the motive of the actor (Alberts and Dorofee, 2001). Meanwhile, the threat sources cloud refers to disclosure, modification, disruption and the interaction. However, others component such as counter measure could not be obtain from OCTAVE.

AS/NZS 3100:2009 is a standard for applying risk management analysis. It contents a critical asset in threat identification that seeks to identify the information assets. This is very important to organizations daily operations via various information-collecting strategies such as brainstorming, interviewing of key stakeholders, simulations, situation consideration and organizational documentation evaluations (Padyab *et al*., 2014). However, among the limitation of AS/NZS is management processes and human error or mistakes (Shedden *et al*., 2010).

ISO/IEC 27005 is an international standards but it do not promise to solve the security problems. This ISO/IEC 27005 just includes the component of asset which refer to 'Service" in cloud computing. NIST SP 800-39 is applicable to assess for the risk in IT system (Ekelhart *et al*., 2009). It is more effectives in examining the risk. The component of this standard is asset which refer to information such as hardware, software, system connectivity and responsible division (Syalim *et al*., 2009). The threat sources also as an important component in this standard for assessing security risk effectively.

## RESULTS AND DISCUSSION

**Proposed conceptual threat factor profiling model:** Based on the comparison made in previous section we found out that each model has different approaches and components because of the differences on their objective. Previous research has indicates that combination of different threat model could help better in identify risk threat and mitigate it (Hussain *et al*., 2011; Xin and Xiaofang, 2014). As a result of our comparative analysis, combination of the components from the reviewed models can produce a threat factor profiling model. In this study, we propose a threat factor profiling model based on important component found in this study. Our propose model will include components namely threat sources; threat motive; threat outcomes; threat agents and threat.

This study has provided an overview of the several approaches namely STRIDE, OCTAVE, CVSS, AS/NZS 3100:2009, VERIS, DREAD, ISO/IEC 27005 and NIST SP 800-39 in computer security domain. We also conducted a comparative analysis on all the models. We found out that STRIDE and CVSS has captured a major share of attention in terms of threat identification and management for organization. However, the component and the processes of the reviewed model are different and it requires the combination of multiple models to manage cyber threat in an organization. In this study, we propose a threat factor profiling model that based on combination of component from the reviewed models. As future works, we will enhance and implement our proposed model through prototyping.

## CONCLUSION

Hence, this study was conducted to analyze existing information security threat approaches, frameworks and other relevant references. Based on the study, the suitable components for the proposed threat factor profiling will be adapted or adopted for the development of threat factor profiling. By establishing the threat factor profiling, an organization can be better equipped in managing information security risks and more alert on the current threats situation (Feng *et al*., 2014). Our propose model will be built to analyze and better understand the cyber threat in organizations.

## ACKNOWLEDGEMENTS

This research is supported by Ministry of Science, Technology and Innovation (MOSTI) under a special grant scheme programme. The National Policy on Science, Technology and Innovation (DSTIN) Flagship Programme. This research project is a collaboration work between Cyber Security Malaysia and Universiti Putra Malaysia (UPM) to jointly develop the National Integrated Information Security Threat Factor Profiling Model (NIISTFP). Any opinions, findings and

conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the MOSTI.

## REFERENCES

Alberts, C. and A. Dorofee, 2001. OCTAVE SM threat profiles. Pittsburgh Softw Eng. Inst., 2001: 1-14.

Alberts, C., A. Dorofee, J. Stevens and C. Woody, 2003. Introduction to the OCTAVE Approach. Carnegie Mellon University, Pittsburgh, Pennsylvania.

Chandrashekhar, A.M., Y. Huded and S.H.S. Kumar, 2015. Advances in information security risk practices. Int. J. Adv. Res. Data Mining Cloud Comput., 3: 47-51.

Ekelhart, A., S. Fenz and T. Neubauer, 2009. Aurum: A framework for information security risk management. Proceedings of the 42nd Hawaii International Conference on System Sciences, January 5-8, 2009, IEEE, Austria, Vienna, ISBN: 978-0-7695-3450-3, pp: 1-10.

Feng, N., H.J. Wang and M. Li, 2014. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inform. Sci., 256: 57-73.

Fisk, G., C. Ardi, N. Pickett, J. Heidemann and M. Fisk *et al.*, 2015. Privacy principles for sharing cyber security data. Proceedings of the Workshops on 2015 IEEE Security and Privacy, May 21-22, 2015, IEEE, Los Alamos, New Mexico, ISBN: 978-1-4799-9933-0, pp: 193-197.

Gallon, L. and J.J. Bascou, 2011. CVSS attack graphs. Proceedings of the 2011 7th International Conference on Signal-Image Technology and Internet-Based Systems, November 28-December 1, 2011, IEEE, Mont-de-Marsan, France, ISBN: 978-1-4673-0431-3, pp: 24-31.

Gallon, L., 2011. Vulnerability discrimination using cvss framework. Proceedings of the 2011 4th IFIP International Conference on New Technologies, Mobility and Security, February 7-10, 2011, IEEE, Mont-de-Marsan, France, ISBN: 978-1-4244-8704-2, pp: 1-6.

Hussain, S., A. Kamal, S. Ahmad, G. Rasool and S. Iqbal, 2014. Threat modelling methodologies: A survey. Sci. Int., 26: 1607-1609.

Hussain, S., H. Erwin and P. Dunne, 2011. Threat modeling using formal methods: A new approach to develop secure web applications. Proceedings of the 2011 7th International Conference on Emerging Technologies, September 5-6, 2011, IEEE, Sunderland, England, ISBN:978-1-4577-0768-1, pp: 1-5.

Ibidapo, A.O., P. Zavarsky, D. Lindskog and R. Ruhl, 2011. An analysis of CVSS v2 environmental scoring. Proceedings of the 2011 IEEE 3rd International Conference on Privacy, Security, Risk and Trust (PASSAT) and Social Computing, October 9-11, 2011, IEEE, Edmonton, Alberta, ISBN: 978-1-4577-1931-8, pp: 1125-1130.

Jiang, L., H. Chen and F. Deng, 2010. A security evaluation method based on STRIDE model for web service. Proceedings of the 2010 2nd International Workshop on Intelligent Systems and Applications, May 22-23, 2010, IEEE, Changsha, China, ISBN: 978-1-4244-5874-5, pp: 1-5.

Jouini, M., L.B.A. Rabai and A.B. Aissa, 2014. Classification of security threats in information systems. Procedia Comput. Sci., 32: 489-496.

Lalanne, V., M. Munier and A. Gabillon, 2013. Information security risk management in a world of services. Proceedings of the 2013 International Conference on Social Computing, September 8-14, 2013, IEEE, Pau, Pyrenees-Atlantiques,France, ISBN:978-0-7695-5137-1, pp: 586-593.

Leitner, A. and B.I. Schaumuller, 2009. ARIMA-A new approach to implement ISO/IEC 27005. Proceedings of the 2nd International Conference on Logistics and Industrial Informatics, September 10-12, 2009, IEEE, Hagenberg, Algeria, ISBN:978-1-4244-3958-4, pp: 1-6.

Mayer, J. and L.L. Fagundes, 2009. A model to assess the maturity level of the risk management process in information security. Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management-Workshops, June 1-5, 2009, IEEE, São Leopoldo, Brazil, ISBN:978-1-4244-3923-2, pp: 61-70.

Padyab, A.M., T. Paivarinta and D. Harnesk, 2014. Genre-based assessment of information and knowledge security risks. Proceedings of the 2014 47th Hawaii International Conference on System Sciences, January 6-9, 2014, IEEE, Luleå, Sweden, ISBN:978-1-4799-2504-9, pp: 3442-3451.

Rao, K.R.M. and D. Pant, 2010. A threat risk modeling framework for Geospatial Weather Information System (GWIS): A DREAD based study. Int. J. Adv. Comput. Sci. Appl., 1: 20-28.

Saripalli, P. and B. Walters, 2010. Quirc: A quantitative impact and risk assessment framework for cloud security. Proceedings of the 3rd International Conference on Cloud Computing (CLOUD), July 5-10, 2010, IEEE, Coral Springs, Florida, ISBN:978-1-4244-8207-8, pp: 280-288.

Scandariato, R., K. Wuyts and W. Joosen, 2015. A descriptive study of Microsoft's threat modeling technique. Requirements Eng., 20: 163-180.

Shedden, P., T. Ruighaver and A. Ahmad, 2006. Risk Management Standards Œ The Perception oF Ease of use. University of Melbourne, Melbourne, Victoria.

Sherief, N.H., A.A.A. Hamid and K.M. Mahar, 2010. Threat-driven modeling framework for secure software using aspect-oriented Stochastic Petri nets. Proceedings of the 7th International Conference on Informatics and Systems, March 28-30, 2010, IEEE, Alexandria, Egypt, ISBN: 978-1-4244-5828-8, pp: 1-8.

Sultan, R. and S.Q. Abbas, 2015. Web services threats, vulnerabilities and countermeasures. Int. J. Adv. Res. Comput. Sci. Manage. Stud., 3: 243-252.

Syalim, A., Y. Hori and K. Sakurai, 2009. Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. Proceedings of the International Conference on Availability, Reliability and Security, March 16-19, 2009, Fukuoka, Japan, pp: 726-731.

Thompson, D.R., J. Di and M.K. Daugherty, 2014. Teaching RFID information systems security. IEEE. Trans. Educ., 57: 42-47.

Torr, P., 2005. Demystifying the threat modeling process. IEEE. Secur. Privacy, 3: 66-70.

Tripathi, A. and U.K. Singh, 2011. Analyzing trends in vulnerability classes across CVSS metrics. Int. J. Comput. Appl., 36: 38-44.

Xin, T. and B. Xiaofang, 2014. Online banking security analysis based on STRIDE threat model. Int. J. Secur. Appl., 8: 271-282.

Zhang, X., N. Wuwong, H. Li and X. Zhang, 2010. Information security risk management framework for the cloud computing environments. Proceedings of the 10th International Conference on Computer and Information Technology, June 29-July 1, 2010, Bradford, UK., pp: 1328-1334.

Zulkernine, M. and S.I. Ahamed, 2006. Software Security Engineering: Toward Unifying Software. In: Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues; Managerial and Technical Issues, Merrill, W. (Ed.). Mississippi State University, Starkville, Mississippi, pp: 215-232.