IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Issue-1 E-ISSN: 2347-2693

# Confidentiality Assessment Model to Estimate Security during Effective E-Procurement Process

**Surabhi Saxena[1*], Devendra Agarwal[2]**

[1]Department of Computer Application, Babu Banarasi Das University (BBDU ), Lucknow (U.P.)India
[2]Department of Computer Application, Babu Banarasi Das University (BBDU ), Lucknow (U.P.)India

**Corresponding Author: saxenasurabhi1987@gmail.com*

**Available online at: www.ijcseonline.org**

Received: 04/Jan/2018, Revised: 10/Jan/2018, Accepted: 22/Jan/2018, Published: 31/Jan/2018

***Abstract-*** Building high secured software components is very important for component-based software projects. The confidentiality of software is one of the important factors determining the security of components. Estimating confidentiality near the beginning in the software development life cycle, particularly at design phase, may help the designers to integrate required highly secured for improving overall security of the developed software. In this paper researcher introduced a metric based model "Confidentiality Assessment Model (CAM$^{OOD}$)". This model measure the confidentiality induced by the use of various object-oriented design concepts like data hiding, aggregation, inheritance, coupling and cohesion. Herein, we compared our measurement results with various contributions.

***Keywords*** Software E-Security, Confidentiality, Security Factors

## I. INTRODUCTION

Software security is one of important concepts in secured software program and components. Building programs and components with high security always simplifies confidentiality, reduces security cost, and increases software quality.

As pointed out by Author Chowdhury [3], there is a set of program characteristics that lead to secured software, including confidentiality, integrity, availability, authentication and so on. According to the Author Bharat B. Madan [5] and Author Anshul et. al. [4] views software security is one of three pieces of the security puzzle. They pointed out that software confidentiality analysis is useful to examine and estimate the security of software using an empirical analysis approach. In the software engineering paradigm, software development of component-based software, engineers have several questions concerning component security [7]. What is component security and related factors? How to check, measure, or evaluate the security of software components? How to design and develop secured components to achieve good security?

At high stage software security consists of mainly two types of activities: one is the confidentiality of software components, including the number of requirement, categorization, and retrieval of existing secure components; the other is component integration that involves the integration of the complete secured components into an application [2, 14]. Over the past several years, a large number of methods, class have been developed to deal with these confidentiality issues. A current software engineering gives attention towards only security with assumption that all faults can be removed during development [10]. Building secured systems is one of the main challenges for software developers, who have been concerned with confidentiality-related issues as they assessment and developed.

## II CONFIDENTIALITY: SECURITY FACTORS

Wide area network of internet has become the integral part of our day to day life. Everyday various information is exchanged over the internet. So security of the information, data, and user creditability is highly sensitive issue now-a-days [12, 16]. For the security of internet & network security there are more basic principles. They are Authentication, Confidentiality, Integrity and Non-repudiation much more.

User authentication is referred as 'Provision of Assurance that the message is originated from Authorized user' [21]. Data confidentiality refers to limiting information access & disclosure to authorized user and preventing access or disclosure to unauthorized one. For data confidentiality is used to a great extent. A variety of researchers in the area suggested that confidentiality as a major attributes of security and their view is summarized in table1.

**Table 1 Critical View Of Security Factors By Experts**

| Sr. No. | Security Issues →<br>Author ↓ | Confidentiality | Integrity | Availability | Authorization | Non-Reputations | Authentication | Durability | Access Control |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Anshul et. al. (2017) [4] | √ | √ | √ | √ | √ | √ | ✓ | √ |
| 2 | R. A. Khan et. al. (2015) [9] | √ | √ | √ | √ |  | √ | ✓ | √ |
| 3 | Suhel et.al.(2015) [7] | √ | √ | √ |  | √ | √ | ✓ | ✓ |
| 4 | Bokhari et. al. (2014) [11] | √ | √ | √ | √ |  |  |  |  |
| 5 | Nikhat et.al. (2014) [17] | √ | √ | √ | √ | ✓ | √ | ✓ | ✓ |
| 6 | Danijel et.al (2012) [6] |  | √ |  |  |  |  | ✓ |  |
| 7 | Soham et. al. (2013)$^{sm}$ [ 7] | √ | √ | √ | √ | ✓ | √ | ✓ |  |
| 8 | Shalini et. al. (2011) [13 ] | √ | √ | √ | √ |  |  | ✓ | √ |
| 9 | Amjan Shaik (2010) [18] | √ | √ | √ | √ |  | √ |  |  |

## III. CORRELATION ESTABLISHMENT

Security is an important quality attribute. The index of security is identified by a number of various steps. It can be measured confidentiality index at design stage through the entire development process by its attributes. In order to developed confidentiality as a security attributes associated to design properties are shown in figure1, which demonstrate the Estimation method of software security.

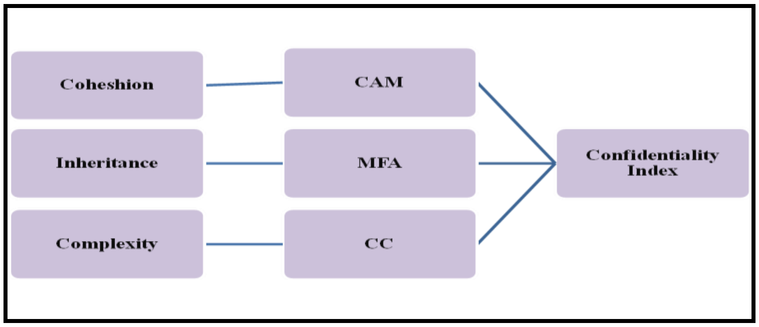

Fig 1 Correlation between Confidentiality and suited parameters of E-procured software

## IV. MODEL DEVELOPMENT

The generic metrics values have been considered as a foundation to develop the Confidentiality Assessment Model (**CAM$^{OOD}$)** for object oriented software design [7]. Estimation of class diagram's is prerequisite for the accurate confidentiality values. For this reason prior to developing **(CAM$^{OOD}$)** the study has developed model for Confidentiality. Correlation has been established and shown in figure 1.

Using SPSS, values of coefficient are calculated and confidentiality model is formulated as given below**.** The data used for establishing integrity model is taken from [19, 20, 15] that have been collected through large commercial object oriented e-procurement systems. In order to establish a model for confidentiality, multiple linear regression techniques have been used and showing in table 2. Multivariate linear model is given below in equation (1) which is as follows.

**$Y=\alpha_0 + \alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \ldots\ldots.. \alpha_n X_n$ (1)**

Where

- **Y is dependent variable**
- **X1, X2, X3 ... Xn are independent variables.**
- **$\alpha_1, \alpha_2, \ldots \alpha_n$ are the regression coefficient of the respective independent variable.**
- **$\alpha_0$ is the regression intercept**

Table 2 Confidentiality Calculated Table

| Project | KNOWN VALUES | LCOM | MFA | CC |
|---|---|---|---|---|
| $P_1$ | 0.793 | 1.10000 | 0.00000 | 0.6667 |
| $P_2$ | 0.389 | 0.62500 | 0.70000 | 0.6000 |
| $P_3$ | 0.588 | 2.00000 | 1.00000 | 0.0000 |
| $P_4$ | 0.600 | 0.80000 | 0.00000 | 0.8750 |

**Developed Equation $^{CAM}$ = 0.353 + 0.273 *LCOM - 0.295* MFA + 0.112*CC (2)**

Summary table 3 for Confidentiality Quantification Model proves that all the three selected metrics are statistically significant at confidence level of 95%.

Table 3 Model Summary $^{E\text{-}ConM}$

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| **1** | **.997$^a$** | **.994** | **.992** | **.011821** |
| **Predictors: (Constant), LCOM, MFA, CC** | | | | |

## V. EMPERICAL VALIDATIONS

An empirical validation proves that how significant proposed study and research, where metrics and model are able to estimate the confidentiality index of object oriented design at design time. The empirical validation is important phase of research to evaluate the proposed confidentiality assessment model for high level acceptability. Empirical validation is the fine approach and best practice for claiming the model acceptance [1, 8]. In order to validate developed confidentiality assessment model the data has been taken from the [4, 15, 19, & 20] and shown in table 4.

Table 4 Known and Calculated Confidentiality Index Values

| Project | LCOM | MFA | CC | Calculated Confidentiality Index | Known Index |
|---|---|---|---|---|---|
| $P_1$ | .667 | .769 | 1.400 | .465 | .455 |
| $P_2$ | .817 | .811 | 1.273 | .479 | .462 |
| $P_3$ | .762 | .844 | 2.250 | .564 | .545 |
| $P_4$ | .619 | .682 | 1.867 | .530 | .504 |
| $P_5$ | .775 | .897 | 1.427 | .494 | .489 |
| $P_6$ | .386 | .000 | 1.583 | .636 | .629 |
| $P_7$ | 2.000 | .952 | .500 | .674 | .678 |
| $P_8$ | .667 | .000 | 1.250 | .675 | .635 |
| $P_9$ | 2.000 | .957 | 2.000 | .841 | .813 |
| $P_{10}$ | 2.000 | .937 | 1.333 | .772 | .793 |

## VI. EXPERIMENTAL TRYOUT

No issue how powerful a theoretical result may be, it has to be empirically validated if it is going to be of any practical use. This is correct in software engineering, including software engineering.

Therefore, in addition to the theoretical validation, an experimental tryout is equally important in order to make the claim acceptable. It is essential to test the validity of proposed model for acceptance. So we used 2 sample t tests apply for check the impact between calculated and known confidentiality shown in table 5.

Table 5 2T- test for Model

| | Mean | Std. Deviation | Std. Error Mean | t | P value |
|---|---|---|---|---|---|
| **Calculated And Known Confidentiality** | .0144652 | .0203076 | .0064218 | 2.253 | 0.051 |

**Null hypothesis (H0):** There is no significant difference between Standard Confidentiality and Calculate Confidentiality

**H0: $\mu1-\mu2 = 0$**

**Alternate hypothesis (HA):** There is significant difference between Standard Confidentiality and Calculate Confidentiality.

**HA: $\mu1-\mu2 \neq 0$**

The hypothesis is tested with zero level of significance and 95% confidence level. The p value is 0.050. Therefore alternate hypothesis directly discards and the null hypothesis is accepted. The developed equation used for confidentiality estimation is accepted.

## VII. CONCLUSION AND FUTURE WORK

Confidentiality is an important factors and one of the most significant parameters of the software security. The lack of confidentiality aspect often leads to fault prone that may in turn lead to credibility, unauthorzation issues and hence to faulty development results. This paper highlighted the importance of confidentiality in general and as a factor of software security in particular. Result analysis shows that the '**calculated values**' of confidentiality computed through model are highly correlated with the '**standard values**'. It plays a significant role as far as the issue of secured software is concerned. However, the model has been validated on a small data set and it is to be done further on large dataset and assessment to other attributes for security purpose. We analyse the next attribute of security is evaluate and validate in coming research work.

## REFERENCES

[1]. S. Chandra & R. A. Khan, “A Methodology to Check Confidentiality of a Class Hierarchy”, Elsevier, Vol. 10, Issue 3, 2010.

[2]. Vineet Kumar Maurya, Santhosh Babu G, Jangam Ebenezer, Muni Sekhar V, Asoke K Talukder, Alwyn Roshan Pais, “*Suraksha:* A Security Designers’ Workbench”, presented in Hack.in 2009, IIT Kanpur, India, 17-19 March 2009.

[3]. I. Chowdhury, B. Chan, and M. Zulkernine, "Security metrics for source code structures," in Proceedings of the Fourth International Workshop on Software Engineering for Secure Systems Leipzig, Germany: ACM, 2008.

[4]. A. Mishra, D. Agarwal and M. H. Khan, “Integrity Estimation Model: Fault Perspective”, International Journal on Recent and Innovation Trends in Computing and Communication, Vol 5, Issue 5, pp 1246-1249, May 2017.

[5]. Bharat B. Madan, Katerina Goˇseva-Popstojanova, Kalyanaraman Vaidyanathan and Kishor S. Trivedi “Modeling and Quantification of Security Attributes of Software Systems”, Proceedings of the International Conference on Dependable Systems and Networks (DSN’02), IEEE, 2002, pp: 505-514.

[6]. Danijel et. al., “Software Fault Prediction Metrics:A Systematic Literature Review”, ACM, 2013.

[7]. Soham H. “Security Metric for Object Oriented Class Design-Result Analysis”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013.

[8]. Dr. Linda Rogenberg, Dinnis Brennan, “Principle Components of Orthogonal Object Oriented Metrics (323-08-14)”, White Paper Analyzing Results of NASA Object oriented Data, Oct 2001.

[9]. Raees Ahmad Khan, “Security Improvement of Object Oriented Design using Refactoring Rules”, I.J. Modern Education and Computer Science, 2015

[10]. Finding Accessibility and Interaction vulnerability of Rational Rose Class Design Using Design Metrics Soham H. Gandhi, D. R. Anekar, Mahevash A. Shaikh, Ajinkya A. Salunkhe.

[11]. Ubaidull et. al., “Security Requirement for Software Quality - A Survey of Engineering Discipline”, International Journal of ICT and Management, 2014.

[12]. Shazia Yasin, Khalid Haseeb, "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012.

[13]. Shalini Chandra, “Availability state transition model”, ACM SIGSOFT Software Engineering Notes · May 2011

[14]. Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

[15]. A. Mishra, D. Agarwal and M. H. Khan, “Confidentiality Estimation Model: Fault Perspective” International Journal of Advanced Research in Computer Science (IJARCS), Volume.8 Issue. 4, June 2017.

[16]. Steve Counsell, Stephen Swift, Jason Crampton “The interpretation and Utility of Three Cohesion Metrics for Object – Oriented Design” (ACM Transactions on SE & Methodology, Vol. 15, No. 2, April 2006.

[17]. P.Nikhat, S. Kumar and M. H. Khan, “Model to Quantify Integrity at Requirement Phase”, Indian Journal of Science and Technology, Vol. 9, Aug 2016.

[18]. Amjan Shaik, “Statistical Analysis For Object Oriented Design Software Security Metrics”, International Journal of Engineering Science and Technology Vol. 2(5), 2010

[19]. Suhel Ahmad Khan, “Confidentiality Quantification Model at Design Phase”, International Journal of Information and Education Technology, Vol. 2, No. 5, October 2012.

[20]. M. Jureczko & L. Madeyski, “Towards identifying software project clusters with regard to defect prediction”, IEEE, 2010.

[21]. Leslie Lamport, Password Authentication with Insecure Communication. Technical Note. Communication of the ACM, 1981.

## Author Profile

**Surabhi Saxena** received the MCA degree from Rajasthan Technical University , Jaipur in 2013. She is enrolled as Full time research scholar in BBDU , Lucknow in Department of Computer Application . His research interests include Software Engineering , Quality Models, ISO Standards, E-Commerce , E-Governance , E-Procurement , ERP **,** E-Security

**Dr. Devendra Agarwal** is currently working as HOD , Department of Computer Science in BBDU , Lucknow. He has over 18 years of teaching & 5 years of industrial experience. He has done his B.Tech in Computer Science from Mangalore University in 1993, M.Tech from U.P. Technical University, Lucknow in 2006, and Ph.D. from Shobhit University, Meerut in 2013. He has over 13 research papers with 4 students pursuing Ph.D.