Integrity Quantification Model to Estimate Security during The Effective E-Procurement Process

SURABHI SAXENA[1], DEVENDRA AGARWAL[2]
[1]Ph.D. Research Scholar,
Department of Computer Application, Babu Banarasi Das University
Lucknow (U.P.) India
[2]Head of Department,
Department of Computer Science, Babu Banarasi Das University
Lucknow (U.P.) India

ABSTRACT - Estimating Security is a most considered domain of software development. So the Integrity is a standout amongst the most significance factor of software development life cycle process which provides a strong mechanism to manage inappropriate Integrity factors. The integrity quantification model is more suitable and also validates the substantial effect in both structural and functional information of design phase development in e-procured software as well as security attributes. The Integrity Quantification Model ($IQM_{E\text{-}Proc}$) is developed by using multiple linear regression technique in procured software. The developed quantification model has been validated with realistic data to prove the significance. So that solid hypothesis premise has been created for outlining the measurement required for integrity factor in security perspective for measured effectiveness of e-procurement software **.**

Index Term - *Security Factor, Integrity Issues, Design Parameter*

I. INTRODUCTION

Now days, the Software development industry is confronting an issue in conveying secure procurement software [1, 6]. The Software developers, programmers, engineers, venture supervisors, and chiefs stay under weight because of their failure to convey secure procured software. It will be a bulky procedure and a costly undertaking for any product creating unit to execute security includes in the beforehand created application programs [8, 13]. The reasons might be: **a)** It isn't conceivable to rebuild and modify an application program completely with security modules **b)** Additional interest in making the already created programming secure isn't generally prudent and **c)** It isn't proposed to retrain software developers to be security specialists. It is essential for all product frameworks to perform appropriately under the nearness of security methodologies [12, 9]. So that framework ought to be equipped for working proactively, which means in this manner, it ought to act naturally guarded.

II. INTEGRITY AT DESIGN TIME

According to the various authors literature review and different - different study satisfies that the security feature cannot be add once software is ready to work [4]. So it must be added within the design phase in software life cycle process. If it is not done in design phase then the software industry will suffers genuine harms because of the absence of integrity quantification in security perspective in running and implementation phase. Later the result of that problem adverse effect in whole pillars of security attributes [5, 11 and 14].

III. ESTABLISHING RELATION

In order to established relationship between object oriented software characteristics and integrity factor. Therefore the main objective of software development is to delivered secure procured software that is correct, consistent and complete. In order to place the control integrity in security perspective. It is compulsory to settle on an exertion with measure it. The second objective of software development is work on design phase to start with step towards issue space should result space. With pictorial presentation are shown in figure 1. In the Software architecture modelling it is most appropriate stage to evaluate integrity quantification evaluation with respect to security perspective in the procurement software [10]. So that security and quality of e-procurement software is well maintained.

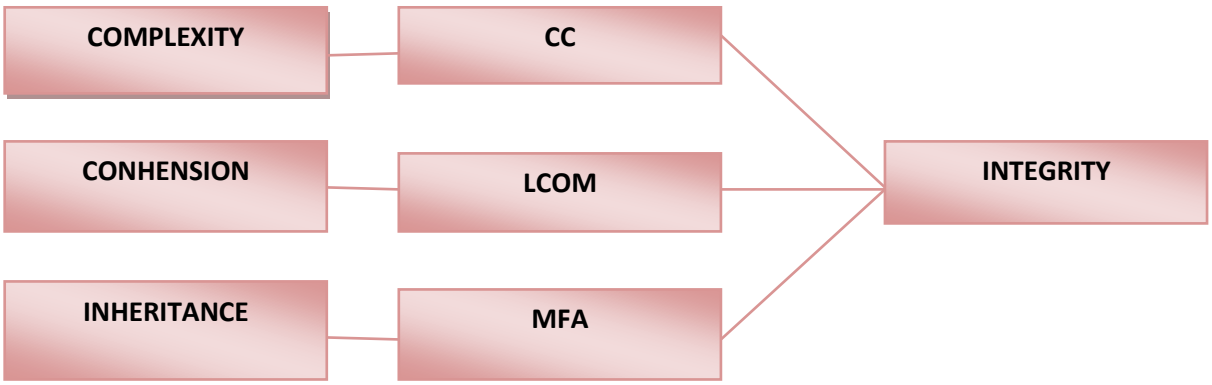

Fig1. Correlation between integrity and design parameters

IV. MODEL DEVELOPMENT

In order to established a model for integrity, multiple linear regression technique has been used . Multivariate linear model is given as follows :-

The data taken from [2, 3 and 7] for model development and quantification have been collected through the controlled experiment

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

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.**
- **α_0 is the regression intercept**

Developed Equation ^{IQM} (Y) = 1.81 + 0.549 *CC - 0.147* MFA - 2.65* LCOM - (eq. 2)

V. QUANTIFICATION AND VALIDATIONS

We present, in this section, the methodology of the empirical study used with regression line and we conducted in order to assess the relationship (fig 1) between the design issues and security factors. We performed statistical analysis and result in different perspective. We used the Pearson correlation coefficient. This technique, based on ranks of the observations, is widely used for measuring the degree of linear relationship between two variables.

It measures how tightly the closely related data clusters around a straight line. Correlation coefficient will take a value between -1 and +1. A positive correlation is increase together. A negative correlation is one in which the ranks of one variable increase as the ranks of the other variable decrease. A correlation of +1 or -1 will arise if the relationship between the values is exactly linear. A correlation close to zero means that there is no linear relationship..

Table1 Computed Table for Model Development

Project	Standard Index	CC	MFA	LCOM
P_1	.623	1.571	.740	.761
P_2	.354	.800	.902	.667
P_3	.395	.769	.000	.667
P_4	.527	1.375	.918	.714

P_5	.604	1.161	.000	.727
P_6	.375	.800	.455	.696
P_7	.333	1.250	.000	.805
P_8	.455	.500	.958	2.000

Table 2 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.995[a]	.990	.985	.009063
Predictors: (Constant), LCOM, MFA, CC				

Table 3 Descriptive Statistics

Descriptive Statistics			
	Mean	Std. Deviation	N
Calculate Integrity	.47640	.073954	10
CC	1.60190	.632400	10
MFA	.70780	.282368	10
LCOM	.79690	.125489	10

Table 4 Known and Calculated Integrity Index Values

Project	CC	MFA	LCOM	Calculated Integrity	Standard Integrity
P_1	1.000	.881	.640	.534	.569
P_2	.875	.841	.657	.425	.479
P_3	2.100	.804	.900	.460	.454
P_4	1.222	.919	.688	.524	.589
P_5	2.000	.685	.882	.469	.468
P_6	.800	.902	.667	.350	.395
P_7	1.476	.000	.814	.463	.454
P_8	1.950	.661	.835	.598	.584
P_9	2.750	.885	1.000	.540	.546
P_{10}	1.846	.500	.886	.401	.435

We performed statistical tests using correlation. The null and alternative hypotheses that our experiments have tested were:-

Null Hypothesis (H0): There is no significant correlation between **Calculated Integrity and Standard Integrity. H0: μ1-μ2 = 0**

Alternate Hypothesis- (H1): There is a significant correlation between **Calculated and Standard Integrity**. **HA: μ1-μ2 ≠ 0**

In this experiment, rejecting the alternate hypothesis indicates that there is a statistically significant relationship between the Calculated and Standard Integrity. The P value is 0.05 with 95% confidence level. It indicates that no differences with two values. So we accepted the null hypothesis and discard the alternate hypothesis. The developed equation used for integrity quantification is accepted.

Table 5 2 t- test between Calculated and Standard Integrity

Paired Samples Statistics					
		Mean	**N**	**Std. Deviation**	**Std. Error Mean**
Pair 1	**Calculate Integrity**	**.47640**	**10**	**.073954**	**.023386**
	Standard Integrity	**.49730**	**10**	**.068903**	**.021789**

VI. CONCLUSION AND FUTURE SCOPE

The conclusion in this paper should be viewed as exploratory and indicative rather than conclusive. Moreover, knowing that software security is affected by integrity, it would be interesting to extend the used suite of design metrics to better reflect the security effort. We hope, however, this study will contribute to a better understanding and characterizing of what contributes to integrity of classes in object oriented software. An appropriate notion of security should result if the integrity definition includes many views. In secured software one appropriate view could be integrity.

In the Future research the Security Assessment Model (SAM $^{E\text{-}PROC}$) is developed to estimate the security. Software Security estimation is the valuable technique of understanding for improving, guiding and controlling security integration at design phase . The Security Assessment Model (SAM $^{E\text{-}PROC}$) is a correlation relationship between the Authentication Quantification Model (AQM $^{E\text{-}PROC}$), Authorization Quantification Model (AUQM $^{E\text{-}PROC}$), Confidentially Assement Model (CAM $^{E\text{-}PROC}$), Integrity Quantification Model (IQM $^{E\text{-}PROC}$) .

REFERENCES

1. Flechais, Sasse and H. SMV. “Bringing Security Home: A Process for developing secure and usable systems”, ACM, pp 18-21, Aug 2003.
2. S. A. Khan and R. A. Khan, “Integrity Quantification Model for Object Oriented Design”, ACM SIGSOFT Software Engineering Notes, Vol 37, No.2, Mar 2012.
3. M. Jureczko and L. Madeyski, “Towards identifying software project clusters with regard to defect prediction”, IEEE, 2010.
4. P. H. Meland, J. Jenesen, “Secure Software Design in Practice”, ARES., IEEE, 2008.
5. Jagdish Bansiya, Carl G.Davis, “A Hierarchical Model for Object Oriented Design Quality Assessment” IEEE Transaction on Software Engg, Vol 28, No. 1, 2002.
6. Wang, C. and W.A., Wulf, A framework for security measurement.. Proceedings of national Information Systems Security Conference, 1997, Oct.
7. Anshul 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.
8. Clifford J. Berg, , High-Assurance Design: Architecting Secure and Reliable Enterprise Application Addison Wesley Professional,2005, ISBN: 0-321-37577-7
9. R.A.Khan, Suhel Ahmad khan, “A Roadmap for Security”, International Journal of Computer Science & Emerging Technologies (IJCSET), 5 Volume 1 Issue 1, June 2010.
10. N. Parveen , M. R. Beg and M. H. Khan, “Model to Quantify Availability at Requirement Phase of Secure Software”, American Journal of Software Engineering and Applications, Vol. 6, 2015.
11. R. Subramanyan and M.S. Krisnan, “Empirical Analysis of CK Metrics for Object-Oriented Design Complexity : Implications for Software Defects,” IEEE Trans. Software Eng., Vol. 29, No. 4, PP 297-310, Apr. 2003”.

12. McLeod, A., Pippin, S., & Catania, V. "Using technology acceptance theory to model individual differences in tax software use" , In Proceedings of the 15th Americas Conference on Information Systems, 2014.

13. Eckhardt, A., Laumer, S., & Weitzel, T., "Who influences whom? Analyzing workplace referents' social influence on IT adoption and non-adoption", Journal of Information Technology, 24(1), 11-24, 2009.

14. Liew, E. J. Y., Vaithilingam, S., & Nair, "M. Facebook and socio-economic benefits in the developing world", Behavior & Information Technology, 33(4), 345-360, 2014.

15. N. Praveen , M. Khaliq , " A General Study for Role of the Quality in the E-Procurement Process ", International Journal of Scientific Research in Computer Science , Engineering and Information Technology (IJSRCSEIT) January 2018.

16. S. Saxena , D Agarwal , " A Critical Literature Survey on factors that Effecting E-Procurement Software ", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) , Volume 7 , Issue 1, January 2018 .

17. S.Saxena, D.Agarwal, "Confidentiality Assessment Model to Estimate Security during Effective E-Procurement Process", International Journal of Computer Sciences and Engineering (IJCSE), Vol.6, Issue.1, pp.361-365,January 31, 2018.

18. S. Saxena , D Agarwal , " Authentication Quantification Model to Estimate Security During Effective E-Procurement Process ", International Journal of Scientific Research in Computer Science Engineering and Information Technology
(IJSRCSEIT) , Volume 3 , Issue 1,11th February 2018 .

19. S. Saxena , D Agarwal , " Authorization Quantification Model to Estimate Security During Effective E-Procurement Process ", IPASJ , International Journal of Computer Science (IIJCS) Volume 6 , Issue 2 , 28 February 2018 .

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 15 research papers with 4 students pursuing Ph.D.