Model to Quantify Security For Adoption Of 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 - As all we know that e-procurement process has great reliance on software to achieve quality process and excellence in the domain. When software is concern then no one can deny the role of security aspects in software development especially in the early stage of development life cycle. So, it is a must to focus on security, because customer's priority is to have the secure software. In this paper software security is considered in the design phase of development life cycle. By considering these issues of customer and developer we need to assess security of software with the help of quantitative assessment method.

Index Terms: Security, Authorization, Authentication, Confidentiality, Integrity, Assessment Model .

I. INTRODUCTION

The design of secure software isn't an easy task. It certainly requires deep understanding of different aspects of security, like e-security measurement, e-security categories, and security policies [12].

As Author Lord Kelvin states "we can't control in the event that we can't measure". At the design time, a system must present incorporated security design that take well into explanation of security principles [3]. Design time is most malleable phase of software [2]. The best way to develop systems with required functionality and performance that can likewise withstand malicious attack is to design and implement them to be secure [13, 1].

Utilizing the concept of software security estimation amid development of software, security can be measured by breaking down object oriented design characteristics, measurement of security attributes like confidentiality, integrity, authorization and authentication its effect on software, security team may improve/control software security [14].

This will affect the quality and performance of the software. There is need to develop a scientific structured way to deal with an expression of secure software design to ensure that application software are secure and stable.

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

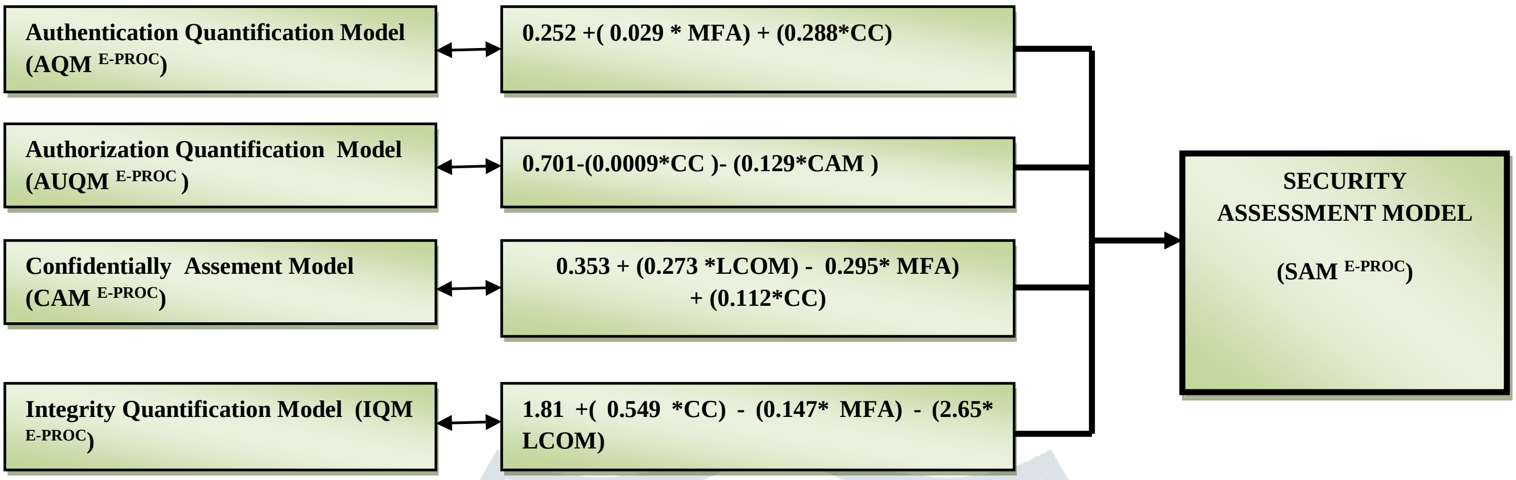
Where

- **Y is dependent variable**
- **X1, X2, X3 ... Xn are independent variables.**
- **α_1, α_2,… α_n are the regression coefficient of the respective independent variable.**
- **α_0 is the regression intercept**

To develop the security assessment model for e-procured object oriented software the authorization, confidentiality, authentication and integrity is prerequisite, and the generic quality models have been considered as a premise to develop the Security Model. The data have taken from [4, 6,7,8,9 and 10] for quantification and analysis. Author have developed a comparative chart in order to established the correlation between security and their security attributes are shown in figure 1 .

In order to developed model multiple regression line technique has been used to get the coefficients of regression variables and regression intercepts shown in developed equation .Identified security factors for e-procured software will work as a independent variable while security will taken as dependent variable . Assement of Security Model is very useful to get security index value for the e-procured software design for high quality product. Multivariate regression equation is given in Equation 1 which is as follows .In the previous paper we already applied the regression method technique for formulate the **Authentication Quantification Model (AQM $^{\text{E-PROC}}$) [9]** , **Authorization Quantification Model (AUQM $^{\text{E-PROC}}$)[10], Confidentially Assement Model(CAM $^{\text{E-PROC}}$) [8] , Integrity Quantification Model (IQM $^{\text{E-PROC}}$) [11]** which shown in the figure 1

Figure 1 Show relationship security index and their parameters


Authentication Quantification Model (AQM $^{E-PROC}$)
0.252 +(0.029 * MFA) + (0.288*CC)
Authorization Quantification Model (AUQM $^{E-PROC}$)
0.701-(0.0009*CC)- (0.129*CAM)
Confidentially Assement Model (CAM $^{E-PROC}$)
0.353 + (0.273 *LCOM) - 0.295* MFA) + (0.112*CC)
Integrity Quantification Model (IQM $^{E-PROC}$)
1.81 +(0.549 *CC) - (0.147* MFA) - (2.65* LCOM)
SECURITY ASSESSMENT MODEL
(SAM $^{E-PROC}$)

III QUANTIFICATION AND STATISTICAL SIGNIFICANCE

It is evident from review [6,11] that security is not a new term; rather it has been in discussion among the industry professionals at various forums ,but there is no commonly accepted comprehensive and complete model or framework available to estimating the security of the e procurement software at design phase, that motivate to develop the ***"Security Assessment Model for E-Procurement software (SAM $^{E-Proc}$) ",*** using object oriented design approach based on its internal design property at an initial stage of development life cycle.

Using SPSS Software the model computed table 1 , table 2 model summary ,and table 3 Security Assement model table is calculated which can be concluded that Security model is statistically significant at a confidence level of more than 95% and also the values of R2 and Adjusted R2 are also satisfactory. All of the metrics in Eq. (1) are also statistically significant.

Table 1 Model Computed Table

Project	Standard Authentication AQM $^{E-PROC}$	Standard Authorization AUQM $^{E-PROC}$	Standard Integrity IQM $^{E-PROC}$	Standard Confidentiality CAM $^{E-PROC}$	Standard Security SAM $^{E-PROC}$
P_1	0.682	0.581	0.534	0.465	0.461
P_2	0.518	0.659	0.425	0.479	0.47
P_3	0.503	0.606	0.46	0.564	0.519
P_4	0.472	0.59	0.524	0.53	0.518
P_5	0.659	0.564	0.469	0.494	0.519
P_6	0.564	0.65	0.35	0.636	0.955
P_7	0.472	0.635	0.463	0.674	0.977
P_8	0.592	0.642	0.598	0.675	0.848
P_9	0.465	0.584	0.54	0.841	0.931

$$SAM^{E\text{-}Proc} = (-\ 1.55) + (0.716 *AQM^{E\text{-}Proc}) + (1.70 *AUQM^{E\text{-}Proc}) - (0.654 * IQM^{E\text{-}Proc}) + (1.89 *CAM^{E\text{-}Proc}) \qquad \text{Equation (1)}$$

Table 2 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.998ª	.996	.994	.014236
Predictors: (Constant) Confidentiality CAM $^{E\text{-}PROC}$, Authentication AQM $^{E\text{-}PROC}$, authorization AUQM $^{E\text{-}PROC}$, Integrity IQM $^{E\text{-}PROC}$				

Table 3 Security Assessment Table

Project	Authentication AQM $^{E\text{-}PROC}$	Authorization AUQM $^{E\text{-}PROC}$	Integrity IQM $^{E\text{-}PROC}$	Confidentiality CAM $^{E\text{-}PROC}$	Calculate Security	Standard Security
P_1	.725	.656	.350	.384	.582	.519
P_2	.465	.614	.466	.604	.664	.672
P_3	.682	.639	.537	.669	.939	.971
P_4	.640	.569	.195	.660	.996	.961
P_5	.512	.640	.077	.323	.465	.429
P_6	.540	.613	.410	.565	.633	.619
P_7	.869	.676	.677	.610	.931	.934
P_8	.884	.650	.785	.624	.855	.874
P_9	.472	.614	1.202	.974	.885	.861
P_{10}	.747	.642	.403	.528	.810	.829
P_{11}	.495	.603	.668	.828	.958	.937
P_{12}	.792	.641	.005	.417	.892	.831
P_{13}	.636	.659	.831	.530	.484	.461
P_{14}	.540	.571	.712	.661	.591	.544

Security model has also been statistically validated using the statistical sample tryouts. Here also 25% of the data has been used for developing the model, while remaining used for model validation.
Calculated values between the calculated security using the developed model (2) and the reference security (already known) are shown in Table 3. It is evident from the values, that the estimated security values by the developed model (2) are strongly correlated with the already known actual security values. Therefore the security assessment model, quantifying security efficiently for UML diagrams not participated in the development of the model. It is ensure to check the validity of proposed work. So apply **2t tests** for check the validity.

Table 4 2t- test between Standard Security and Calculate security

	Mean	N	Std. Deviation	Std. Error Mean
Calculate Security	.76331	14	.185986	.049707
Standard Security	.74586	14	.197689	.052834

Null hypothesis (H_0): There is no significant difference between Standard Security and Calculate Security.**H_0: $\mu 1-\mu 2 = 0$**

Alternate hypothesis (H_1): There is significant difference between Standard Security and Calculate Security.**H_1: $\mu 1-\mu 2 \neq 0$**

In the above hypothesis µ1 and µ2 are treated as sample means of population. Mean value and Standard Deviation value have been calculated for specified two samples and represented in table 4.
The hypothesis is tested with zero level of significance and 95% confidence level. The p value is 0.05.

IV. CONCLUSION

The structure that we have shown here is being used for producing security index at design stage. It supports a security of activities in development of system. Overall, the availability of security index at design time will help the development team at later stage to overcome the cost of with a visible structure is very useful in the development of secure software. The paper has developed model to quantify security of the class diagrams. Security model estimates the security of class diagrams in terms of their Authentication, Authorization, Confidentiality and Integrity. The model have been developed using the technique of multiple linear regression. The paper also validates the quantifying ability of developed model.

References

1. G.McGraw, "Software Security". IEEE Security &Privacy, IEEE, vol.2, pp.80-83, 2004.
2. A. Agrawal, R. A. Khan and S. Chandra, "Software Security Process – Development Life Cycle Perspective", CSI communications, August 2008, pp. 39-42.
3. L Bass, P Clements and R Kazman, "Software Architecture in Practice", Second edition, SeiSeries in Software Engineering.
4. A. Mishra, D. Agarwal and M. H. Khan, "Security Estimation Model: Fault Perspective", International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS), 3 rd Special Issue on Engineering and Technology, Vol. VI, Issue VII, July 2017.
5. Liu, L. and E. Mylopoulos, "Analyzing Security Requirements as Relationship among Strategic Actors", 2nd Symposium on Requirements Engineering for Information Security (SREIS'02) Raleigh, North Carolina, October 16, 2002.
6. 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.
7. 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 .
8. 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.
9. 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 .
10. 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 .
11. S. Saxena , D Agarwal , " Integrity Quantification Model to Estimate Security During Effective E-Procurement Process ", Volume 7 , Issue 3 , pp-147-151 , March 2018 .
12. M. Jureczko and L. Madeyski, "Towards identifying software project clusters with regardto defect prediction", IEEE, 2010.
13. R. Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology", International Conference on Software Engineering Advances (ICSEA 2007), IEEE, Cap Esterel, French Riviera, France August, 2007. pp.60-60.
14. 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.
15. Pankaj Jalote. An Integrated to Software Engineering. 2nd Edition. Narosa Publication Home. 2002.
16. Alshammari, Bandar and Fidge, Colin J. and Corney, Diane (2009) "Security metrics for object-oriented class designs". In: QSIC 2009 Proceedings of: Ninth International Conference on Quality Software, August 24-25, 2009, Jeju, Korea. (In Press).

17. S.Saxena, D.Agarwal, “Filling a Gap in Existing Model for the Adoption of Effective Model of E-Procurement System in India ”, International Journal of Engineering and Techniques (IJET) , Volume 4 , Issue 2 , pp 374-379 , Mar-April ,2018

18. Surabhi Saxena , Devendra Agarwal , “ Traceability Assessment Model to Estimate Quality of the Effective E-Procurement Process in Adoption”, International Journal of Engineering Trends and Technology (IJETT) , Volume 58 , Issue 4 – April 2018 , pp – 177 – 180 .

19. Surabhi Saxena , Devendra Agarwal , “ Completeness Assessment Model to Estimate Quality of the Effective E-Procurement Process in Adoption”, International Journal of Management, IT & Engineering (IJMIE) Vol. 8 Issue 6, June 2018, pp- 369-380 .

Author Details

Surabhi Saxena received the MCA degree from Rajasthan Technical University, Jaipur in 2013. She is enrolled as Full time Ph.D. Research Scholar in BBDU, Lucknow in Department of Computer Application. 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 the Computer Science from Mangalore University in 1993, M.Tech from the U.P. Technical University, Lucknow in 2006, and Ph.D. from Shobhit University, Meerut in 2013. He has over 20 research papers with 4 students pursuing Ph.D.