Confidentiality Quantification Model at Design Phase

Suhel Ahmad Khan, *Member, IACSIT,* Raees Ahmad Khan

***Abstract*—Software security is one of the most significant factors of software development. The assessment of security using the model is more appropriate and its validation signifies the valid impact of structural and functional information of object oriented design software. The confidentiality quantification model is developed using multiple linear regression technique on object oriented design constructs. The applied statistical analysis on this study concludes its statistical significance remarked that calculated data is highly acceptable. A strong theoretical basis has been developed for designing the metrics required for complexity factors as well as security attributes.**

***Index Terms*—Software security, complexity, confidentiality, security quantification.**

I. Introduction

The design of secure software is not an easy task. It certainly requires deep understanding of various aspects of security, like security measurement, security categories, security policies etc. Though techniques are well developed, but secure software designing is still a challenging problem. The major challenge in this area is to know 'how secure is secure enough'. Lard Kelvin states 'we can't control if we can't measure'. At the design time, a system must present unified security design that take well into account security principles. Design time is most malleable phase of software. The only way to develop systems with required functionality and performance that can also withstand malicious attacks is to design and implement them to be secure. Using the concept of software security estimation during development of software, security can be measured by analyzing object oriented design constructs, measurement of security attributes like confidentiality, integrity and availability and its impact on software, security team may improve/control software security. This will affect the quality and performance of the software. There is need to develop a scientific structured approach to deal in a word of complex software design to ensure that application software are secure and stable.

Manuscript received April 15, 2012; revised June 2, 2012. This work is sponsored by UGC, New Delhi, India under F. No. 34-107\2008 (SR).

The authors are with the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Vidya Vihar, Raibareli Raod, Lucknow- 226025 (e-mail:ahmadsuhel28@gmail.com,).

Raees Ahmad Khan is with the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Vidya Vihar, Raibareli Raod, Lucknow- 226025 (e-mail:khanraees@yahoo.com).

II. Confidentiality at Design Time

Confidentiality refers unauthorized disclosure of information. It also limits the access of information in right direction and prevention of disclosure of information to unauthorized users. The confidentiality works as a security policy that insures no one can access the data or information outside of this system which insures that a protection technique is also implemented here. Confidentiality is a broader concept of privacy which limits access to individual's personal information which requires a trusted binding mechanism of design and its total supporting services and related components. It insures that there is no chance of leakage of information [1]. It strengthens the mechanism that data is preserved and intruder can't violate the sanctity of data. Any confidential data access or confidential data transmission bound with related components and its supporting services that provides a trusted authorization or trusted authentication mechanism to process data at design phase. At design time components or entities are bound to each other through coupling/aggregation. The applied protection on data must engage with total supporting services and applied behavior of entities to insure the unauthorized disclosure of information. These can be evaluated by direct measurement through object oriented design constructs including coupling, encapsulation, inheritance; polymorphism all affects the confidentiality at design time.

III. Quantification of Security

Quantification of security is possible. Most of approaches are either theoretical basis or can be used as best practices [2]. There is not even a single proof mechanism available for addressing security using object oriented design constructs. Quantification analysis of software security at early stage enables the evaluation and assessment of security and provides the basis for assessment security technologies. Quantification of security will help to trade off between security goals and cost. Complexity plays an important role in deciding design security. There appears an urgent need of finding out the normal acceptable level of design complexity for producing a secure design. A viable quantification model is needed to address design security through complexity. One of the best approaches may be to correlate complexity factors with security attributes in order to quantify security in terms of complexity with the help of design characteristics.

IV. Correlation between Security Attributes & Complexity

Security is multidimensional attribute. The values of security are not identified by single step. It can be measured

through the whole development process by of its attributes. Computer security is frequently associated with three core areas, which can be conveniently summarized by the acronym "CIA"[3].

Fig. 1. Relation diagram

In order to establish a contextual relationship between designs constructs with complexity factors are being examined [4], [5]. The significance of this study is to quantify security with optimized set of complexity attributes which is discussed in Fig. 1. The used metrics are helpful to minimize/control the intolerable design complexity which is taken from [4], [6], [7]. To gain maximum strength of protection it is mandatory to keep design complexity low by preventing unnecessary privilege grant to services. Privileges should be minimal according to interaction between services and requests. Most of the services are holding the dynamic behavior. The behavior of components is analyzed by counting services at run time environment when they demonstrate polymorphic behavior. Decomposition is the process of defining the generalizations and classifications that compose an abstraction [8]. Keeping in mind this assumption, decomposition is merged with higher level of abstraction to maintain the theoretical basis that larger the number of methods invoked from an object, increases the design complexity. The motivation of hierarchical decomposition of design is to provide free space and allows the designers to take design decisions independently to distribute complexity across multiple components with less interdependence.

V. Confidentiality Quantification Model

The generic quality models have been considered as a basis to develop the security quantification model form object oriented design [2], [3], [9]. A class hierarchy of Online shopping Management System depicted in Fig. 2 has been presented to quantify the confidentiality through given complexity attributes of design diagram. The Six versions of class hierarchies are being used for metric value depicted in Table1 and data needed for standard confidentiality values is taken from [10]. The multiple linear regression model is fitted for the minimal set of confidentiality metric and result is shown in equation (3).

The model summary of calculated data is mentioned in Table 1 which discusses the statistical interpretation of used data and high value of R Square represents that model is highly effective. Table II summarizes the results of the correlation analysis for confidentiality quantification model, and shows that for all the System, all of the design constructs are highly correlated with Confidentiality.

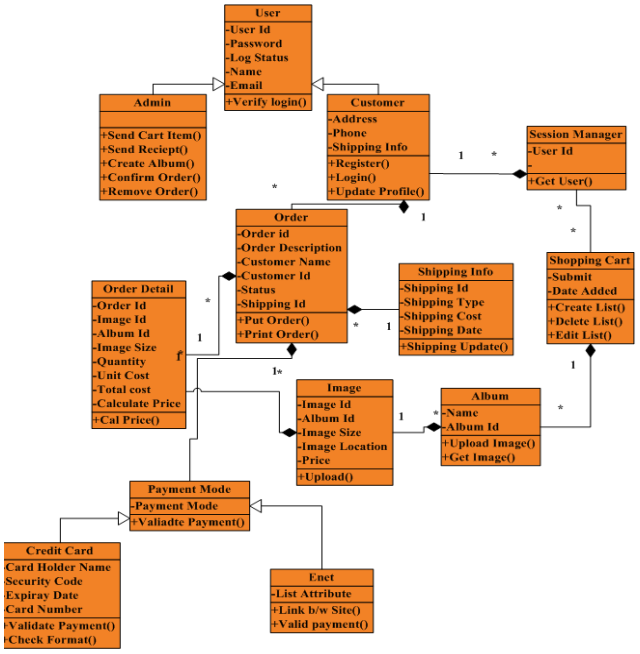

Fig. 2. Online shopping management system

$$\text{Confidentiality} = \alpha + \beta 1 * CP + \beta 2 * TSS + \beta 3 * MDH \quad (1)$$

$$\text{Confidentiality} = .599 - .623 * CP + .341 * TSS - 1.25 * MDH \quad (2)$$

TABLE I: Model Summary

Model	R	R Square	Std. Error of the Estimate	Sig. F Change
1	.965	.931	0.01452	0.331

TABLE II: Confidentiality Calculation Table

Class Diagram	Conf_Standard	CP	TSS	MDH
CD1	0.555	1.33	3.11	0.22
CD2	0.60	1.40	3.3	0.20
CD3	0.545	1.81	3.81	0.18
CD4	0.60	1.7	3.80	0.20
CD5	0.60	2.0	4.4	0.20

VI. Model Validation

No matter how powerful a theoretical result may be, it needs to be empirically validated to establish its practical use, effectiveness and efficiency. This is true in all Engineering disciplines, including Software Engineering. Therefore, in addition to the theoretical validation, an experimental tryout is equally important in order to make the claim acceptable. In view of this fact, an experimental validation of the proposed model namely complexity confidentiality quantification model (CQM) has been carried out using sample tryouts. Following sections describes the details of validations and data regarding validation for confidentiality formulation is carried out from six version of class diagram of online purchase system in Fig. 3 and taken data is depicted in Table III.

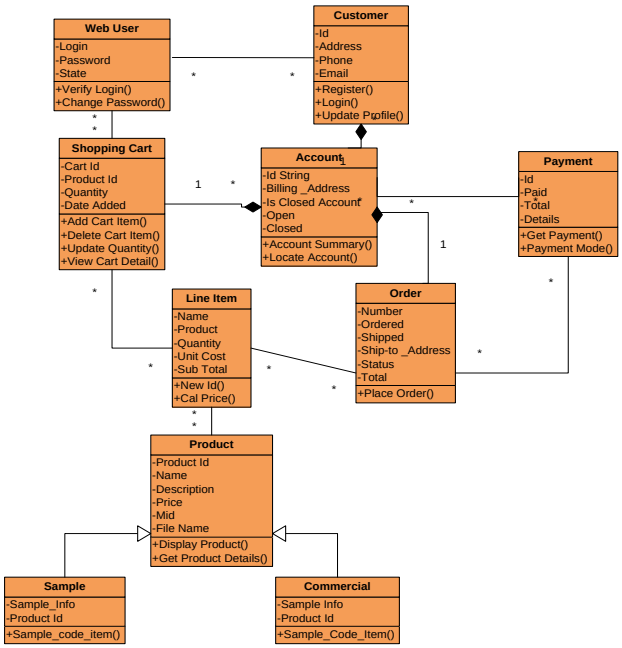

Fig. 3. Online purchase system

TABLE III: CONFIDENTIALITY DATA TABLE

Class Diagram	CP	TSS	MDH	Conf_Stand	Conf_Cal
CD1	1.0	3.45	0.54	0.454	0.477
CD2	1.83	4.41	0.16	0.583	0.763
CD3	2.18	4.45	0.18	0.455	0.533
CD4	1.78	4.0	0.28	0.50	0.504
CD5	1.38	3.30	0.30	0.462	0.489
CD6	2.0	4.33	0.16	0.588	0.629

It is mandatory to check the validity of proposed model for acceptance. A 2-sample t test has been introduced to test the significance of Conf_Stand values to Conf_Cal Values. A hypothesis test based on 2-sample t test is being performed and confidence interval is being observed by the difference of two standard mean. The t test history of confidentiality is mentioned in Table Ⅳ.

TABLE Ⅳ: T TEST OF CONFIDENTIALITY

	N	Mean	Std Div	Std Err
Conf_Stand	6	0.507	0.063	0.025
Conf_Cal	6	0.565	0.110	0.045

T Value=1.128
P Value=0.2853(Two Tailed)

Ho: (Null hypothesis): There is significant difference between Conf_Stand and Conf_Cal.

H1 :(Alternate hypothesis): There is no significant difference between Conf_Stand and Conf_Cal.

$$Ho: \mu1-\mu2=\delta0 \quad \text{verses} \quad H1: \mu1-\mu2 \neq \delta0$$

where μ1 and μ2 are the sample means and δ0 is the hypothesized difference (zero) between the two sample mean. Mean, Standard Div, Standard Error, Standard Error difference have been calculated for given two samples at Table Ⅳ. Given samples are trusted by 95% confidence with concluding remarks that samples means are same. There is no difference between tabulated data and calculated data. Therefore the null hypothesis is rejected and alternate hypothesis is accepted. The obtained equation through using design parameters for confidentiality calculation is highly accepted.

VII. CONCLUSION

This paper developed a multivariate linear model 'Confidentiality Quantification Model (CQM)' for object oriented software in design time. It estimates the security in terms of design complexity factors which are weighted according to their influence. Early quantification of confidentiality provides an opportunity to improve the security of design diagram. The proposed model has been validated through appropriate statistical measures and contextual interpretation has been drawn.

ACKNOWLEDGMENT

This work is sponsored by UGC, New Delhi, India under F. No. 34-107\2008 (SR).

REFERENCES

[1] G. H. Walton, T. A. Longstaff, and R. C. Linder, "Computational Evaluation of Software Security Attributes", *IEEE*, 1997.
[2] S. Chandra and R. A. Khan, "Software Security Metric Identification Framework (SSM)" *International Conference on Advances in Computing, Communication and Control, ICAC3'09, ACM*, 2009.
[3] C. Wang and Wulf, "A Framweork for Security Measurement," in *Proc. National Information Systems Security Conference*, pp: 522-533, 7-10 Oct. 1997.
[4] S. R. Chidember and C. F. Kemerer, "Towards A Metric Suite for Object Oriented Design," *OOPSLA'91, ACM*, pp:197-211, 1991.
[5] S. A. Khana and R. A. khan, "Securing Object Oriented Design: A Complexity Perspective," *International Journal of Computer Application*, vol. 8, no. 13, pp: 8-12, Oct 2010.
[6] K. Mustafa and R. A.Khan, "Quality Metric Development Framework," *Journal of Comp. Sci*., vol. 1, no. 3, pp: 437-444, 2005.
[7] Linda Rogenberg and Dinnis Brennan, "Principle Components of Orthogonal Object Oriented Metrics (323-08-14)," *White Paper Analyzing Results of NASA Object oriented Data*, Oct 2001.
[8] M. Dowd and John Mcdonald, "The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities," *Addison Wesley Professional*, 2007.
[9] R. G. Dromey, "A Model for Soft. Product Quality," *IEEE Transaction on Soft. Engg*. vol. 21, no. 2, pp: 146-162, Feb. 1995.
[10] S. Chandra and R. A, Khan, "Confidentiality Checking an Object Oriented Class Hierarchy, " *Network Security*, vol. 2010, no. 3, pp: 16-20, March 2010.

Suhel Ahmad Khan is pursing PhD in Information Technology form Babasaheb Bhimrao Ambedkar University (A Central University), Vidya Vihar,Raibareli Road, Lucknow. He has been completed his MCA degree from Uttar Pradesh Technical University, Lucknow. This Young, energetic Research Fellow, who has completed a Full Time Major Research Project funded by University Grants Commission, New Delhi. The funded research project entitled "Quantifying Security in Early Stage of Development Life Cycle: An Object oriented Software Perspective" has been successfully submitted to UGC. The author has more than 5 year of teaching & research experience. He is currently working in the area of Software Security and Security Testing. He has also published & presented papers in refereed journals and conferences. He is also member of IACSIT and Internet Society.