Authentication Quantification Model To Estimate Security During Effective E-Procurement Process

Surabhi Saxena¹, Devendra Agarwal²

¹Ph.D. Research Scholar, Department of Computer Application, Babu Banarasi Das University (BBDU)

Lucknow, Uttar Pradesh, India

²Head of Department, Department of Computer Science, Babu Banarasi Das University (BBDU)

Lucknow, Uttar Pradesh, India

ABSTRACT

Security is a standout amongst the most impressive spaces of e-procurement based software development. It gives a solid system to oversee and blend security parameters for valuable estimation at design stage. The structural and behavioural design properties of classes, objects and their connections are assessed to create metric for authorization. The appraisal of security utilizing the model is more proper and its validation signifies the legitimate effect of basic and utilitarian data of object oriented design programming. The authorization evaluation model is created utilizing multiple linear regression strategy on object oriented design develops. The connected factual examination on this investigation closes its measurable importance commented that figured information is profoundly adequate. A solid hypothetical premise has been created for designing the measurements required for unpredictability factors and security qualities.

Keywords: Authentication, Security Attributes OO Design Metrics.

I. INTRODUCTION

As indicated by McGraw, software has numerous favourable circumstances. It gives its administrations which cover territories from running auto controlling, wireless and performing money related framework and administrations in banks [1]. However designer ought to dependably keep in their mind the security understanding since this unstable zone needs most astounding concern. Accordingly the product engineer society must concentrate on it as much as they could [4]. In the event that they don't do as such it will come about unsafe and perilous. While creating programming engineer ought to dependably focus on its security measures. All things considered, its weakness and inadequacies may demolish every one of our expectations and desires. Our web administrations are taken into account the drivers of the entire world through various programming programs. So avoidance measures ought to dependably be through as our most elevated concerning zones [6]. At whatever point software design specialists will introduce the parts in framework, they ought to guarantee that the development is done deliberately and precise with no replication of mix-ups [5].

A few focuses ought to be remembered while building up a safe programming control point ought to be parasite less as well as various and different. Mix, consistency and synchronization of free and individual parts ought to be produced with least blunder or blame. Each measure must be adjusted to sum up the inconvenience and complexities. As the business and different business are expanding,

so expect of programming affirmation is hugely felt. As it referred to so far that product is as delicate as glass. On the off chance that it doesn't deal with

precisely, it will damage our expectations amid its execution bringing about disappointment of the framework functionality [2, 14].The extent of programming ought to be with the goal that it might obtain multitudinous information and data regardless of its travel estimate. Authentication is a training to confirm whether a client on the framework is permitted to execute an express activity inside a confidence in domain. The utilized system working together with authentication as a part of an entrance control approach. Confirmation discovers who a client is, and Authentication concedes to what that client is allowed to do [3].Programming ought to be designed and developed in such way that can be limit or amplify its effect as indicated by expected recipe or proposed models. There have been no logical investigations that approve the claim to evaluate authentication of object oriented programming at design organize. It is regardless a firmly held conclusion among different specialists that object-oriented programming is less demanding to change than customary programming [16,11]. Quantitative appraisal of class chain of importance for Authentication security traits gives a method, how to oversee/control assets for security change. Along these lines dependability, wellbeing and security are an unquestionable requirement for programming advancement [12].These inescapable segments will upgrade client confidence in fabricated or created software's. Its protection capacity should likewise be kept up no matter what to convey imperfection free items [2].

II. E-AUTHENTICATION: SECURITY ATTRIBUTE

Authentication is the capacity of determining access rights to assets, which is identified with data security and COMPUTER security when all is said in done and to get to control specifically. Assets incorporate individual records' or things' information, COMPUTER programs, COMPUTER gadgets and functionality gave by computer applications [7]. The getting to of assets by clients through Authentication concentrates on parts and consent of software applications. On the off chance that applying any level of security, you ought to characterize an application class for each hunt definition. The application class is in charge of bringing a rundown of runtime esteems in view of the security properties [8].There are different recommended designs are accessible for get to control frameworks including optional access control, obligatory access control, and part based access control. What's more, various innovations are accessible for unifying access control into different structures, working frameworks, and libraries. Due to the intricacy of various accesses control conspires, it's best to start by taking a gander at Authentication from an expansive point of view. Authentication process is much the same as to demonstrate the personality at the season of checking. In multi client computer framework, Authentication gives the benefits to get to process or assets went before by Authentication [9].

III. AUTHENTICATION AND OBJECT ORIENTED PROPERTIES

The correspondence and mapping between the identified security attribute, Authentication, complexity and design constructs revealed that all metrics have relevance with respect to a class. This indicates that 'class' is the fundamental concept of object oriented software and hence all the metrics should eventually conduct measures taking classes as a basis. The proposed metrics will be used to compute Authentication cogency of OO design with the help of complexity using the class diagram. It has been observed that each of the design construct i.e., Encapsulation, inheritance, cohesion, coupling, & polymorphism having an impact on certain complexity factors and security attributes [12]. The significance of this study is to estimate Authentication cogency with an optimized set of object oriented class design features with their relationship in depicted in Figure 1.The correspondence and mapping between the distinguished security property, e- Authentication,

multifaceted nature and design builds uncovered that all measurements have importance as for a class. This shows 'class' is the crucial idea of object oriented software and thus every one of the measurements ought to inevitably direct measures taking classes as a premise. The proposed measurements will be utilized to process Authentication cogency of OO design with the assistance of many-sided quality utilizing the class outline. It has been watched that each of the design develop i.e., Encapsulation, inheritance, cohesion, coupling, & polymorphism affecting certain many-sided quality elements and security properties [10, 3, 15]. The noteworthiness of this investigation is to evaluate authentication cogency with a streamlined arrangement of object oriented class design highlights with their relationship in delineated in Figure 1.
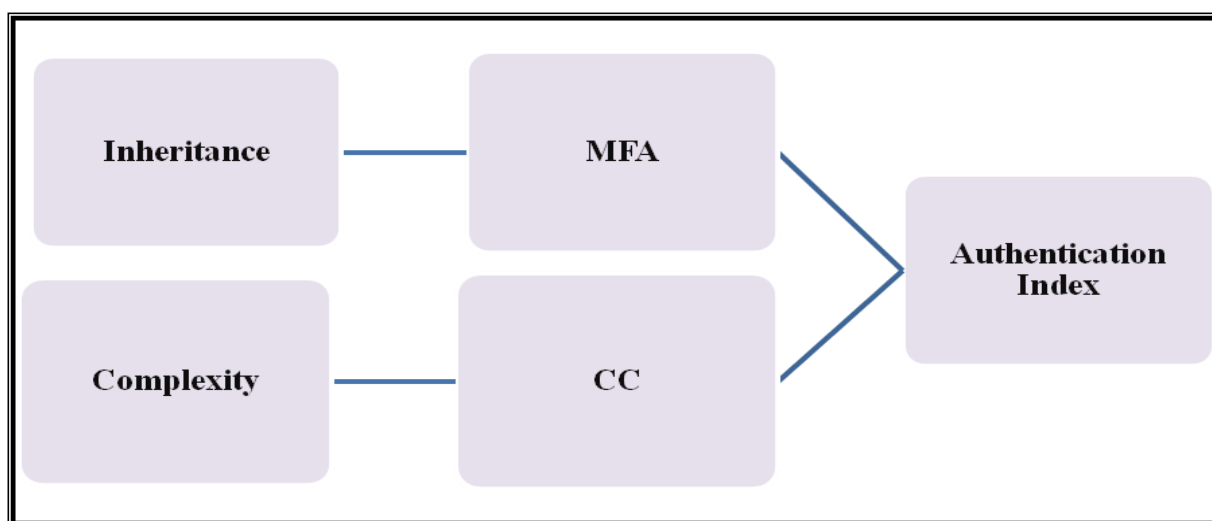

Figure 1. Association between security factors and Object oriented design property

Objects get to the assets to play out their undertaking through proper administrations. The predefined client acts as indicated by their part with legitimate consent to get to the assets for object oriented design progressions. In the event of object oriented design approach the key substance like objects, properties, techniques and classes are orchestrated to frame the design of the software through design qualities including legacy, coupling,

attachment, embodiment, polymorphism, and so forth [12]. In this regard the object characteristic goes about as part and Authentications act as performing activities for classes. Keeping in mind the end goal to gauge the Authentication cogency of object oriented design, the principle concentrate ought to be on the choice taken for getting to ensured assets that work on trust and propriety.

The conduct of classes is characterized by part and consent. Administrations are given by classes to perform or finish a specific undertaking for a client or head. The administrations are to a great degree security concern issues in light of the fact that their execution exceedingly relies on need and one line activity from passage to end point for each approved framework [3].

IV. DEVELOPMENT OF AUTHENTICATION QUANTIFICATION MODEL

The procedure of Authentication allows that perceived entity has appropriate to utilize a specific asset. The object oriented classes are characterized as far as their traits, techniques and connections. The classes connect with each other through generalization, aggregation, coupling or cohesion.

The part based task to develop Authentication framework settle the essential plan to evaluate Authentication to quantify general administrations for the client to finish the operations in the design

chain of command is portrayed in Figure 3. The generic models have been considered as a premise to build up the **Authentication Assessment Model (AAM)** for object oriented design demonstrated which includes the accompanying advances in various steps shown in figure 2.

The general depiction for Authentication is said in Table 3.Multivariate regression equation is given in Equation (1) which is as follows :-

It has been broadly reviewed and discussed in [18].

$$Y = \alpha_0 + \alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \ldots \ldots \alpha_n X_n \quad (1) \text{ Equation}$$

Where

- Y is dependent variable
- $X_1, X_2, X_3 \ldots X_n$ are independent variables.
- $\alpha_1, \alpha_2 \ldots \alpha_n$ are the regression coefficient of the respective independent variable.
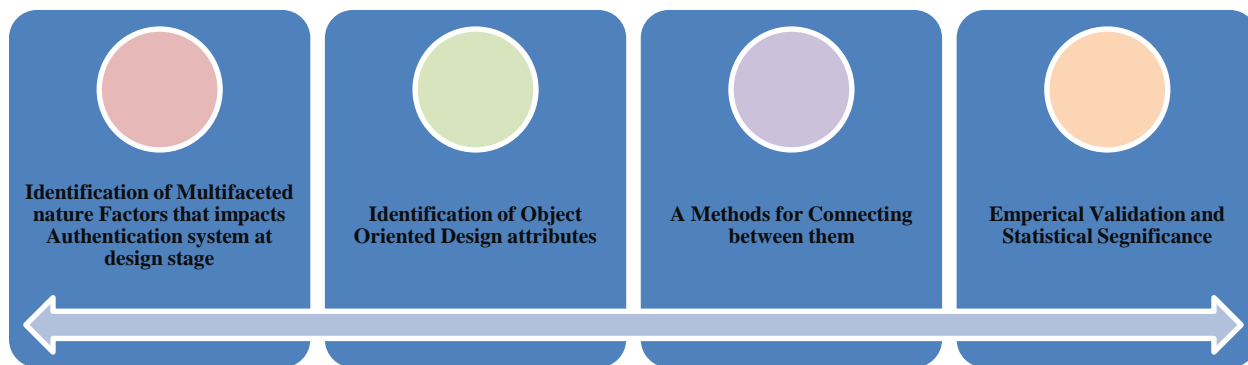- α_0 is the regression intercept.

Figure 2. Steps during Development of Model

In light of the relationship of the Authentication security variables and intricacy factors, the relative criticalness of individual factors that has significant effect on security at design stage is weighted relatively. A different direct relapse procedure has been utilized to get the coefficients. This procedure sets up a connection between dependent variable and various independent factors. The data used for developing model has been taken from [17] that have been collected through large commercial object oriented systems. The data essential for accepted authentication values is being used from [3].The computed data table and equation are shown in table 1 and equation 2.

Table 1. Model Computed Table

Project	MFA	CC	Known
P_1	0.950617	1	0.614
P_2	0.917647	1.375	0.5914
P_3	0.925	0.75	0.448
P_4	0.72549	1.4	0.864
P_5	0.454545	0.8	0.457
P_6	0	1	0.537
P_7	0.685185	2	0.784

$$\text{Developed Equation}^{\text{Authentication}} = 0.252 + 0.029 *MFA + 0.288* CC \quad (2)\text{Equation}$$

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.998ᵃ	.997	.996	.005491
Predictors: (Constant), MFA, CC				

Table 2.Model Summary Table

Model summary table (table 2), which provides information about regression line's ability to account for the total variation in the dependent variables. R Squared is goodness of fit measure for model. Descriptive statistics are useful for describing the basic features of data. It measures the central tendency of depended and independent variables.The measure of central tendency measures the average values of the model are shown in table3.

Table 3.Descriptive Statistics

	MEAN	STANDARD DEVIATION	N
Calculated	.57036	.085394	13
MFA	.79542	.151853	13
CC	1.03066	.301660	13

V. MODEL VALIDATION

Empirical studies are used to investigate software development and practices for understanding, evaluating, and developing in proper contexts. It allows the analyst to test out the theories with the support of empirical observations. This study based on empirical evidence. It is a way of gaining knowledge by means of direct and indirect observation or experience. Empiricism values such research more than other kinds. Empirical evidence can be analyzed quantitatively or qualitatively. Regardless of how capable a hypothetical outcome might be, it should be exactly approved to build up its handy utilize, viability and effectiveness. An experimental validation of the developed authentication index at design phase has been carried out using tryout data [3, 17]. In order to validate developed model, the value of metrics are available by using above data set for following projects in table 4.

Table 4.Authentication Data Table

Project	MFA	CC	Calculated Index	Known Index
P₁	.771	1.417	.682	.664
P₂	.881	.833	.518	.511
P₃	.581	.813	.503	.513
P₄	.949	.667	.472	.450
P₅	.708	1.412	.659	.619
P₆	.841	1.000	.564	.552
P₇	.949	.667	.472	.405
P₈	.804	1.100	.592	.559
P₉	.714	.667	.465	.454

P$_{10}$	.455	.857	.512	.517
P$_{11}$	.885	1.273	.644	.614
P$_{12}$	.822	1.444	.692	.698
P$_{13}$	.981	1.250	.640	.669

VI. STATISTICAL SEGNIFICANCE

It is required to check the accuracy of the proposed for acceptance. A 2t test has been acquainted with test the significance of **Calculated Index** respect to **Known Index**. An assumption test in view of 2-test t test is being performed and certainty interim is being seen by the distinction of two standard means. The t test history of Authentication is specified in table 5.

Null hypothesis (H0): There is no significant difference between **Calculated Index** and **Known Index** H0: μ1-μ2 = 0

Alternate hypothesis (HA):There is significant difference between **Calculated Index** and **Known Index**. HA: μ1-μ2 ≠ 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 5.The correlation outcomes is 0.964.The hypothesis is tested with zero level of significance and 95% confidence level. The p value is 0.055. Therefore alternate hypothesis directly discards and the null hypothesis is accepted. The developed equation used for Authentication estimation is accepted.

Table 5. 2t- test between Calculated Index and Known Index

	Mean	N	Std. Deviation	Std. Error Mean	T Value	P Value
Calculated Index	.57036	13	.085394	.023684		
					2.122	0.055

VII. CONCLUSION AND FUTURE WORK

A metrics based approach may be used to assess authentication and their positive impact of security. Based on the empirical result of these measurements fault of software can be minimized, and hence, security can be more improved.This paper defines the conceptual concept of authentication at design stage, which captures new and complementary dimensions of security, it

compared to a host of existing software security. Highly authentication needs to have a proper design that ensures a strong security among its software modules.

VIII. REFERENCES

1. G. McGraw, "Software Security: Building Security In", Addison Wesley Professional, ISBN:978-0-321-35670-3, 2006.

2. M. Dowd and J. McDonald, "The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities", Addison Wesley Professional, ISBN: 978-0-321-44442-4, 2006.

3. S. A. Khan et.al, "Estimating Authentication Object Oriented Design", IAJIT, 2015.

4. S. R. Chidember and C. F. Kemerer, "Towards A Metric Suite for Object Oriented Design", OOPSLA'91, ACM, 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. R.A. Khan, K. Mustafa,"Metric Based Testability Model for Object Oriented Design(MTMOOD)", SIGSOFT Software Engg. Notes, Vol. 34 Number 2,March 2009.

7. P. H. Meland, J. Jenesen, "Secure Software Design in Practice", ARES., IEEE, 2008.

8. C. Wang and W.A. Wulf, "A framework for security measurement" Proc. of National Information Systems Security Conference, 7-10 Oct 1997.

9. B. B. Madan, Trivedi, "Modelling and Quantification of Security Attributes of Software Systems", Dependable Systems and Networks DNS'022, IEEE.

10. B. B. Madan et.al., "Modeling and Quantification of Security Attributes of Software Systems", Proceedings of the International Conference on Dependable Systems and Networks (DSN'02), IEEE, 2002.

11. G. H. Walton, T. A. Longstaff and R.C. Linder, "Evaluation of Software Security Attribute's", IEEE, 1997.

12. S. R. Chidamber and C.F. Kemerer, "A Metric Suite for Object Oriented Design", IEEE Trans. On Software Engineering, IEEE, vol. 20, 1994.

13. C. Wang and W. Wulf, "A Framweork for Security Measurement", Proc.of National Information Systems Security Conference, (1997) October 7-10, pp. 522-533.

14. A. Mishra, D. Agarwal and M. H. Khan, "Availability Estimation Model: Fault Perspective", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 6, June 2017.

15. Dr. L. Rogenberg and Dinnis Brennan, "Principle Components of Orthogonal Object Oriented Metrics", White Paper Analyzing Results of NASA Object oriented Data, 2001.

16. S. Hernan, S. Lambert, T. Ostwald and A. Shostack, "Threat Modeling: Uncover Security Design Flaws using the STRIDE Approach", 2014.

17. M. Jureczko and L. Madeyski, "Towards identifying software project clusters with regard to defect prediction", IEEE, 2010.

18. Surabhi Saxena , Dr.Devendra Agarwal,. "A Systematic Literature Review on Software Reliability Estimation Model for Measuring the Effectiveness of Object Oriented Design", International Journal of Advanced Research in Computer and Communication Engineering, Volume 6 , Issue 6 , June 2017.

19. Surabhi Saxena , Dr. Devendra Agarwal,. "A Systematic Literature Review and Implementation of Software Usability Estimation Model for Measuring the Effectiveness ", International Journal of Emerging Technology and Advanced Engineering, Volume 7 , Issue 7 , July 2017.

20. 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.

21. Surabhi 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 .

22. Surabhi 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.

23. Surabhi 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 Ph.D. 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.