International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

A Fuzzy Based Analysis of Software Confidentiality at Specific Stage

Munindra Kumar Singh

Abstract*: Mostly software security flaws are most important for the customers and industry. Assessing software security is necessary to reduce faults. Various quantification methods are available include fault, errors, and vulnerabilities from various perspectives. It is a very difficult task to quantify security through a model. Experts develop a new innovative idea or constructive way of evaluating security attributes such as confidentiality. In this paper, the attention that how reduces the fault during the uses of a confidentiality environment. Experts evaluate the literature review with limitations and various quantification techniques that can develop a model. The proposed model uses fuzzy techniques to correlate their parameters with the software metric sat design level. In the developed model, one can generate the surface boundary with parameters and given the complete index value of the confidentiality index.

Keywords* : About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

Software security may be defined by different views. It may be defined in terms of the attributes or characteristics it should possess [2]. Software security can be defined as a safe degree, which is a system, component or process [6]. It is a planned and systematic set of activities to ensure the safety of the software. it consists of:

- Software Quality Assurance
- Software Quality Control
- Software Quality engineering

The quality is a difficult translation in the user's measurable characteristics of the future needs to be defined, to create a product to give satisfaction to the user as well as the price to pay.It is not easy and feels quite successful in the individual effort as He finds that the needs of the consumer have changed by competitors. Security is a property of software quality [10] .

Manuscript published on November 30, 2019.
* Correspondence Author
Dr. Munindra Kumar Singh, Dept. of MCA, VBSPU, Jaunpur, India.

It is based on the experience of the developer with the product or service. The magnitude of software security is not an issue of a single medial [8]. When a developer makes changes to the codebase, then it should have a way to verify that the reform changes the overall security, or at least not likely to open up new vulnerabilities.

II . BACKGROUND

This segment attention to methodology and approaches for software security. Firstly, researchers highlight the research objectives and detain the various methods to reduce the fault, how they relate to our goals. Second, describes the criteria for scoping the relevant research works. Third, advocate the parameters to retrieve the relevant research works. Fourth, explain the show will justify the questionnaires. Many methods and approaches are cons ice in table 1 by the experts.

III FUZZY BASED QUANTIFICATION

The fuzzy-based analysis illustrates the security sensitivity and provides a complete analysis from the fuzzy approach to statistical methodology [3]. These approaches and assessments of statistical analysis governed through a set of rules. Rules are presented in table 3.Fuzzy based rules have divided into four segments. Given the following analysis, the full or indirectly, the use of fuzzy sets in statistics, by far, given the variety of detail and comments. According to this analysis, the researchers focused on various security parameters of the complex relationship between the fuzzy theory and statistical analysis. All security features are considered separately, there is a conceptual and mathematical foundation and methodology development [4, 6] requires thorough insight from both perspectives In table 1 ranges are defined according to the data (from [7]) for confidentiality assessment with surface analysis. This data is most important to examine various perspectives with different parameters. These parameters have directly affected the confidentiality issues. We observe the best-suited metrics for design issues at confidentiality levels. Table 2 is the most important table due to confidentiality matters. Direct access methods, Cyclometric Complexity, and Cohesion among methods are played a vital impressive role in security issues. Rules and respective ranges are applied to forward enhance confidentiality and missing gaps with surface analysis. The metrics are categorized into four segments such as low, high, very low and very high.

Experts	Year	Contributions	Challenges/ Extensions
L. Dai and K. Cooper [1]	2007	Attention to methods and approaches software security	Quantification Aspects
J. Jensen and M.G. Jaatun [2]	2011	Establish to relationship with security and reliability	Only Theoretical analysis
Atrey [3]	2011	Develop new methodology for securing	Social Networking Perspective
B.R. Singh [4]	2013	Vulnerability discovery attentions	Stated for Vulnerability attention
Yuan Yifan [5]	2014	Analysis about Security Vulnerabilities	No attention on validation
Anshul Mishra et. al. [7]	2017	Proposed Confidentiality quantification model	With fault issues
Dr Devendra Agrawal et. al. [9]	2017	Proposed Security quantification model	Only Design level
Charles Weir et. al. [11]	2019	Explained software security terminology for developers	Missing Parameters

Table 2 Rules with various Design attributes

AND of	DAM(H)	AVG_CC(VL)	CAM(L)	Then	Confidentiality (N)
AND of	DAM(N)	AVG_CC(VL)	CAM(N)	Then	Confidentiality (VL)
AND of	DAM(VH)	AVG_CC(N)	CAM(VL)	Then	Confidentiality (L)
AND of	DAM-VH	AVG_CC-VH	CAM-VL	Then	Confidentiality(H)
AND of	DAM_VH	AVG_CC_VH	CAM_VH	Then	Confidentiality (VH)

IV CONCLUSION AND DISCUSSION

The Proposed analysis uses the various phases. Direct access methods, Cyclometric Complexity, and Cohesion among method whose analysis are controlled the fault issues and improved the confidentiality. Considerable reduction in the fault issues up to 90%. This analysis compared with the existing confidentiality paraments. The.developing fuzzy analysis is suitable for reduces fault, errors Fuzzy logic control uses the centroid method of defuzzification produces 4x 1 variable as the output. The output variable confidentiality represents the positive as shown in Table 2. The confidentiality impact is obtained based on the fuzzy rules and based on this observation. In the implementation of Fuzzy rules, the AND function is used. Table 2 represents the fuzzy rule base for nine different combinations. Fig.2, 3, 4, 5, 6 shows the confidentiality index, representation of the fuzzy rules used in the proposed system. Direct access method sare the first input, second input is Cyclometric Complexity and the third input is Cohesion among method and the output (confidentiality) is based on the fuzzy rule base. Fuzzy logic controllers yield reduced fault and better performance in comparison with conventional methods as it is insensitive to parameter variations. For sensitive analysis, the fuzzy logic-based based analysis to deal with the parameter variations (Direct access methods, Cyclometric Complexity, and Cohesion among method). In this paper, we consider the fuzzification level of parameters from various perspectives.

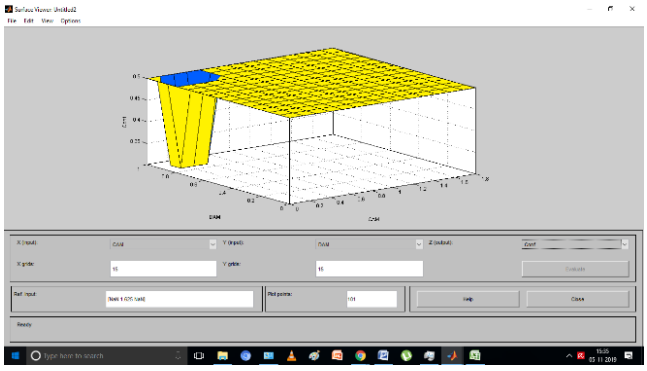

Fig 2 Confidentiality_DAM

Table 1 Parameters Range Table

Parameter_ DAM	**Range (0-1)**
V_Low	(0.0 to 0.2)
Low	0.3 to 0.4
Normal	0.5 to 0.6
High	0.7 to 0.8
V_high	0.9 to 1.0

Parameter_Avg_CC	**Range (0-3.25)**
V_Low	0.0 to 0.6
Low	0.7to 1.2
Normal	1.3 to 1.8
High	1.9 to 2.4
V_high	2.5 to 3.25
Parameter_CAM	**Range (0-1.8)**
V_Low	0.0 to 0.4
Low	0.5 to 0.8
Normal	0.9 to 1.1
High	1.2 to 1.5
V_High	1.6 to 1.8
Confidentiality	**Range (0-1)**
V_Low	0.0 to 0.2
Low	0.3 to 0.4
Normal	0.5 to 0.6
High	0.7 to 0.8
V_High	0.9 to 1.0

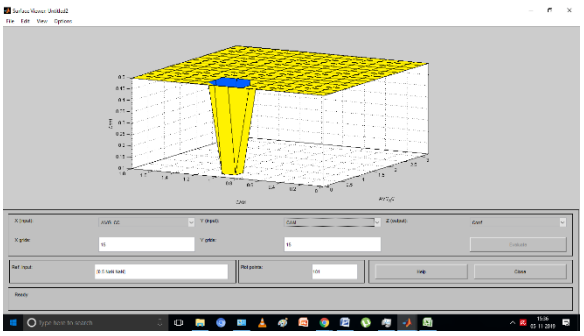

Fig 3 Confidentiality_AVG_CC

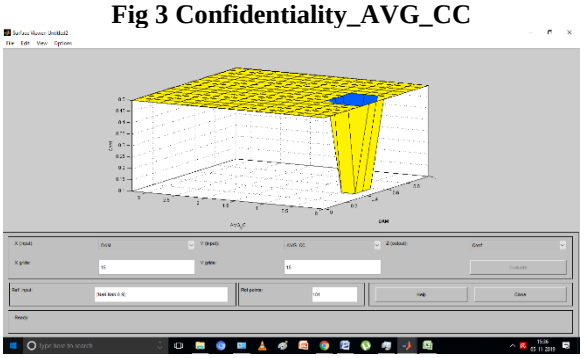

Fig 4 Confidentiality_CAM

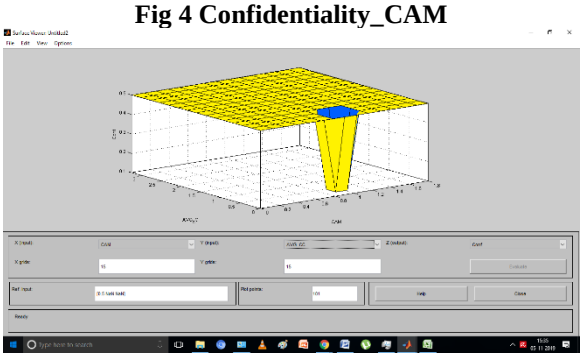

Fig 5 Confidentiality Output

REFERENCES

1. L. Dai and K. Cooper (2007), A Survey of Modeling and Analysis Approaches for Architecting Secure Software Systems. International Journal of Network Security, 5(2):187–198.
2. J. Jensen and M.G. Jaatun (2011), Security in Model Driven Development: A Survey. In Availability, Reliability and Security (ARES), Sixth International Conference on, pages 704 –709, august.
3. Atrey, P. K. (2011). A secret sharing based privacy enforcement mechanism for untrusted social networking operators. Proceedings of the 3rd international ACM workshop on Multimedia in forensics and intelligence, ACM. pp. 13-18, 2011.
4. B.R. Singh. (2013), Vulnerability discovery with attack injection software vulnerability discovery. International Journal of Advanced Research in Computer Science and Software Engineering, 3(9):451-456.
5. Yuan Yifan and Somjai Boonsiri (2015), Analysis of Security Vulnerabilities Using Misuse Pattern Testing Approach. Journal of Software, 10(5):650-658.
6. Rizvi et. al. (2017), Early Stage Software Reliability Modeling using Requirements and Object-Oriented Design Metrics: Fuzzy Logic Perspective. International Journal of Computer Applications, 162(2), 44-59.
7. Anshul Mishra (2017), Dr. Devendra Agarwal, Dr. M. H. Khan. Confidentiality Estimation Model: Fault Perspective. International Journal of Advanced Research in Computer Science, Vol 8 No 5.https://doi.org/10.26483/ijarcs.v8i5.4068
8. B. B. Madan, and K. S. Trivedi (2002), Modeling and Quantification of Security Attributes of Software Systems. Proceedings of the International Conference on Dependable Systems and Networks (DSN'02), IEEE.
9. D. Agarwal (2017), Availability Estimation Model: Fault Perspective. International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 6, June.
10. Bandar Alshammari (2010), Security Metrics for Object Oriented Designs. Software Engineering Conference (ASWEC), IEEE.
11. Charles Weir et. al. Interventions for Software Security: Creating a Lightweight Program of Assurance Techniques for Developers, https://2019.icseconferences.org/details/icse-2019-Software-Engineering-in-Practice/3/Interventions-forSoftware-Security-Creating-aLightweight-Program-of-Assurance-Tech

AUTHORS PROFILE

Munindra Kumar Singh, is working as lecturer in dept. of Computer Applications, Veer Bahadur Singh Purvanchal University, Jaunpur. His area of interest is Grid Computing, Computer Network, Fuzzy Logic and Software Engineering. He has published 07 papers in reputed International Journals. He has also presented papers in International Conferences.