A Critical Review of Fault Tolerance: Security Perspective
Anshul Mishra¹, Dr. Devendra Agarwal², Dr. M. H. Khan³

School of Computer Application, BBDU¹, Lucknow, India
Director (Engg.) at BBDNIIT, BBDU², Lucknow, India
Professor, Department of C.S. E., I.E.T³, Lucknow, India

Abstract—This Security is an important issue of any software system. Security factors play a valuable and appropriate role in software security estimation process. Software security is affected with security attributes as well as fault. An effort through fault perspective is to identify the involved factors of fault and its probable impact on design parameters to quantify security. Fault tolerance is taken as key concept to security assessment. It is to be identified that qualifications of security attributes improved through inspect indemnity, discriminating, vulnerability and attacks in design development process. This research bridges the gap between object oriented design parameters, faults and security factors. In this paper fault is discussed as a security factor of software security. A constant state of the protected software enhances additional security.

Keywords—Security, Fault, Fault Tolerance, Confidentiality, Integrity, Availability

I. INTRODUCTION
Security plays an increasingly important role for software system. Security concern must inform every phase of software development from problem domain to solution domain [22, 2]. Software security estimates provides the help for degree of protection and assess the impact. Microsoft has stated that above 50% of the security related problem for any firm has been found at design level of software development process. Software security touch points are based on good software engineering and involve explicitly pondering security throughout the software lifecycle. Security estimation of software may heavily affect to security of the final product. The experts made an effort in this regards to develop the security estimation guidelines, view and concept. There are some probabilities that original code segment may have some security flaws, anomalies that may influence security at different phase. To develop secure software system is the causative process of different steps and reflections of each phase are the matter of study to measure the perfect impacts of security. Security is a continuous process for every phase in development life cycle [6]. Security is a multidimensional attribute. Software security is about understanding software security risk and how to manage them. A quantitative approach can be much better than conceptual method to develop a technique which can assess the actual level of security assessment. Security enhancement techniques are extremely desirable for improving the internal structure, design simplicity and other feature of software. Before going for further discussion we will discuss about fault and try to drive relation between security and fault tolerance.

II. FAULT: SECURITY PERSPECTIVE
All Unscathed factor that is fault which determines the probability of occurrences attacks and also play a striking responsibility with other factors of security. Faults are common even today. Fault is the cause of software failure while failure is the effect that occurs as a result of the fault. Capability of fault is signified by the hiatus of unsecure software [3]. A security estimation process provides an accurate hint to measurement of software faults. The faults are found during the testing and the failure is when the system stops working. Fault attacks can be deployed in software which generally help to avoid, detect and correct faults. During development of software, faults and flaws are introduced either from the implementation or from the design of the software. It relies on software attributes that how much system’s software is protected; exactly the fault decides for how longer software will be protected. Fault is not only the factor that makes things hard to understand but with enough difficulty anything can become harder to understand. In this paper, we conduct a study regarding impact of fault to security estimation and their efficiency. There is need to develop a new approach to deal with a word of fault in software. Some other attributes of security is shown in figure 1. The required goal of security is to introduce measures and procedures that preserve confidentiality, integrity, availability, and other attributes such as authenticity, fault, and non-repudiation.

Figure 1. Security factors outlook
III. CORRELATION BETWEEN SECURITY AND FAULT TOLERANCE

The security assessment is helpful for software developers, risk management team and executives of the company. It definitely needs thoughtful subtle of security including security measurements, classifications and security attributes. Security attributes may decrease the cost and impinge between problem domain to solution domain at each phase of development life cycle [4, 5, and 20]. A level-2 heading must be in Italic, left-justified and numbered using an uppercase alphabetic letter followed by a period. For example, see heading “C. Section Headings” above.

Software Security is an external software attribute that reduces faults and effort required for secured software. Security must encompass dependable protection and secured the software system against all relevant concerns including confidentiality, integrity, availability, non-repudiation, survivability, accessibility despite attempted compromises, preventing, misuse and reducing the consequences of unforeseen threats [13, 15]. Fault tolerance is direct associated to security attributes such as confidentiality, integrity, availability, non-repudiations, and survivability. Fault tolerance thought will efficiently improve the security. Fault tolerance is frequently essential, but it can be riskily error-prone because of the added efforts that must be involved in the programme procedure. A consistent quantitative estimate of security is highly enviable at an early stage of software development life cycle. Fault tolerance is direct associated to reliability and security.

Fault prevention and fault tolerance intend to present the ability to deliver an accurate service. Controlling and Monitoring can work mutually to enforce the security policy. Fault tolerance is the ability of a system to continue secures the software module and presence of software faults. The development of high assertion software has been dominated by work on two split theme: security and fault tolerance. Here, we introduced a conceptual summarize in term of errors, fault, and attack surface that measures observed effectiveness and simplicity of use with respect to security mean shown in Figure 2.

Fault tolerance attributes as a fault masking, fault detection and fault consideration effective to security policy [16, 12]. Fault tolerance implies a savings in development time, cost and efforts; also it reduces the number of components that must be originally developed.

IV. RELATED WORK

The interest in software fault tolerance has been growing as software faults have become the major contributor to system failures. Study of security, experts says that fault, stability, complexity and reliability are an essential attributes which impinge on the depth of security. A long period of time fault tolerance has been used as a mean of improving and controlling the security of software system. Fault tolerance is the dynamic method that’s used to keep the interconnected systems together, sustain security and availability in systems [25]. Fault tolerance can be categorized in three level; Hardware, Software, and System faults [26].

Experts frequently supports and sustain that fault tolerance theory should be applied at early stage in the development process of software [10, 11]. Software fault tolerance is alarmed with techniques required to facilitate a system to tolerate software ‘bugs’ or faults. Fault tolerance is often old synonymously with graceful degradation which aims to detect, separate and resolve problems pre-emptively. Not all of the security faults existing in software systems are identifiable during the fault analysis [28, 40]. Many experts and researchers in the area recommended that fault tolerance is the ability of a system or component to continue normal operation despite the software fault and the similar is concise in table 1:

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Expert/Researchers</th>
<th>Contribution with Fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>D. B. Sharp, A. Nayak &amp; N. Goel 2007 [27]</td>
<td>Demonstrate a quantifiable definition for secure software with respect to integrity and fault</td>
</tr>
<tr>
<td>11.</td>
<td>R. Mehresh, Shambhu, J. Upadhyaya &amp;</td>
<td>Introduced a new approaches for analyzing the performance of a secure and</td>
</tr>
</tbody>
</table>
In the context of all this investigation fault tolerance is considered as a security solution and its effect the activist direction to other security attributes. A number of researchers addressed the fault tolerance in the context of security and design. Figure 3 illustrates the fault tolerance contribution in different perspective such as method, framework, algorithms and concept.

![Fault Tolerance Contribution Taxonomy](image)

**V. PURPOSE**

Security is key that helps to protect the data and resources. To improve security is to gain a better secured system. There is common agreement between researchers and security practitioners to integrate security at the preliminary stage of software development life cycle in order to develop secured software. [17]. Such as the necessity arises security factors were recognized and composed for their role in software development life cycle. Security estimation is achievable through the help of finding new security factors which directly and indirectly affect the security features of software. Security is associated with three important security pillars which can be conveniently concise by the acronym CIA (confidentiality, integrity, availability) [14]. Software practitioners, project managers, and developers remain under complete stress on account of their inability to deliver secure software system. This way of research is being appropriate at design process account of their inability to deliver secure software system. Figure 3 illustrates the fault tolerance and security. Fault tolerance is a noticeable matter researchers addressed the fault tolerance in the context of security attributes acquaintances to security. This research paper concludes that how will give a view to show the effect of fault tolerance factors having impact on security attributes and its behaviour are best suited in Object Oriented Design Perspective. Identify Design Parameters and related metrics. Analysis of best security practices. Establishing the co-relation between security factors and design parameters with fault tolerance mechanism. To establish a relation for quantified values.

**VI. CONCLUSIONS**

Security assessment must be a compulsory at early stage of development life cycle. As such no framework, models, and metrics has been available in the literature that estimates software security of object oriented design by taking fault into consideration. Fault is parallel to availability, survivability and reliability. Fault tolerance is a complete result of security which contributes in measure the fault. Fault is not a single measurable property some other attributes acquaintances to security. This research paper concludes that how will give a view to show the effect of security factors with fault.

**REFERENCES**


BIography

Anshul received the MCA degree from Dr. R. M. L. Avadh University, Faizabad, in 2008. He is enrolled as research scholar in BBDU, Lucknow. His research interests include Software testability, Software Quality Estimation, Data Dictionary.

Dr. Devendra Agarwal is currently working as Prof. & Director (Engg.) at BBDNIIT (BBD Group), Lucknow. He has over 17 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 10 research papers with 4 students pursuing Ph.D.

Dr. M. H. Khan, Professor, Department of Computer Science and Engineering at IET Lucknow UP. Obtained his MCA degree from Aligarh Muslim University (Central University) in 1991. Later he did his PhD from Lucknow University. He has around 28 years rich teaching experience at UG and PG level. His area of research is Software Engineering. Dr. Khan published numerous articles, several papers in the National and International Journals and conference proceedings.