International Journal of Hybrid Information Technology
Vol.8, No.2 (2015), pp.311-322
http://dx.doi.org/10.14257/ijhit.2015.8.2.29

Revisiting Software Security: Durability Perspective

Rajeev Kumar[1], Suhel Ahmad Khan[2], Raees Ahmad Khan[3]

Department of Information Technology
Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India
rs0414@gmail.com[1], ahmadsuhel28@gmail.com[2], khanraees@yahoo.com[3]

Abstract

Security is a peak significant quality element in the pitch of software engineering. Software security improvement is easily done with the support of factors, models and metrics of security. Software security should be analyzed with the help of its security factors. Security dimension is the main attribute in evaluation, executing, and calculating security in the way to organize and develop quality of software. It is to be identified that qualifications of security factors increased through inspecting damages, discriminating susceptibility and attacks in design development process. This review is discussing the description and categorization of accessible security properties. Durability is an attribute of security that refers to the capability of software to conclude of a creation on time. Software security is affected with security attributes as well as durability. A stable state of the secure software enhances additional security.

Keywords: *Software Security, Security Factors, Security Durability, Object Oriented Design*

1. Introduction

The main aim of technology enhancement is to serve humanity with respect to social up gradation and security. Upcoming industries are increasingly more depends on the technology. This phenomenon has produced fresh security risks and security threats for the consumers [1-3]. Developing protected software is a problematical concern. Software security artifacts must be considered as an important tool in every level of software development. Design development process is a unique procedure in software development life cycle which brings beside noteworthy economic risks [4]. Design require a thoroughly preparation and enormous quantity of accountability during the software design development in security engineering.

Security attributes are developed into an incredibly vital surrounding in security engineering. Classification of security factors possibly will facilitate to expose susceptibility and moderate risks at the early stage of software development life cycle [5-7]. Timeliness of a secure software effects a lot in early stage of security. This phenomenon strengthens the fact that there must be an attribute which relates timeliness to security. In this concern durability is considered a security attribute and its effect on other security attributes is discussed later in this paper.

Identification of security factors help to improve security during software development [8-11]. These attributes prepare a core part in the security world. Here, introduces an untouched factor that is durability, which also plays a noteworthy responsibility with other attributes of security. At each phase of development life cycle, identification of security attributes may decrease the costs and prevent the effects from change at the final stage of life cycle [12-13].

ISSN: 1738-9968 IJHIT

This paper converse about software security at design level where software must be proficient to protect itself in a time period. Durability as a security factor makes a remarkable presence in software security as well as at the time while designing software.

2. Definitions and Literature Background

Software growth is impaired constantly from maintenance, interruptions, and unexploited methods[14]. This is not considering improvements in development skills, tools, and software mechanisms. Software security can be considered as an improvement to protect the software using its three attributes which are known as CIA [15-19]. Software security creates many techniques to protect software from illegal access and malicious occurrences. Security essentials are predictable methods that provide the uncracked methodologies [20]. Analysis of software security attributes is excited for unaffected information and satisfied customers.

Security requirements estimate, how properties of system's software essential would be protected of some threats [21-22]. This is clear from the scholar's review that the set of attempt has been prepared in the pitch of security. The researchers recognized usual security attributes which are being used to defend software at unusual step of operation. It is assumed that time dependencies of security is an attribute of software [23-25]. Privacy is distinct as the assurance that information is not publicized to prohibited processes. Integrity is distinct as the situation that occurs when information of data is unaffected from its source [26-29].

It has not been maliciously changed, transformed, or damaged. Integrity attentions on stopping unauthorized change of information. In difference to availability, confidentiality and integrity is the suitable, reliable access to information and data facilities for authorized consumers. These three attributes are the bases in the field of security [30-33]. With the enhancement of software security, a software can be protected from hazards, threats, etc. There happens an unboundedness of thinkable sources harm or loss of obtainability.

The problems of greatest concern of today relate to the durability as well as increased secure serviceability of software without maintenance. Human trusted software in present state, does not actual long-terms solutions for security perspective [34-38].The main aim of durable security of software is to provide security that can be trusted on keeping the information on the software as safe as possible from unwanted outside interaction. Originalities necessitate that approachability be delivered with the equivalent confidence related durability with confidentiality, availability and integrity.

3. Affiliation between Security and Durability

The budding information technology corporation of software has driven changes. Developing secure software has become a difficult task for the developers [39]. It definitely needs thoughtful subtle of security including security measurements, classifications and security attributes. Affiliations between software, security user's issues and core categories shown in Figure 1. Here, introduced a conceptual outline that measures observed effectiveness, simplicity of use with respect to security. Security as significant factor that affect user's acceptance. Highly related acceptance factors perform under numerous ideas and representations covering revolution acceptance and approval [40-41].

Security attributes are not only involved to generate strong cryptographic solutions, but also find out a way to provide secure requirements for designing [42]. Security rules motivate design and development to develop secure channels for transforming information. In the earlier years, security requirements are designed and arranged in a set of factors, designed into the secure software. Security is considered as a quality factor of software [43-45].

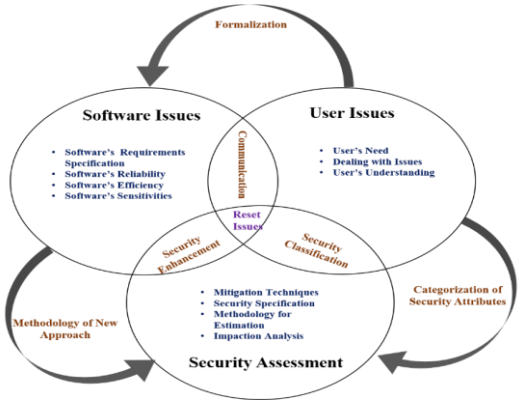

Figure 1. Affiliations between Software, Security and User's Issues

Security of software effectively increases the quality to meet its business requirements. As the time goes on viruses and malwares got active in the absence of any updated software. Study of security, experts says that process of identification of security factors is carried out through the reliability evaluations. Hence it seems that security accent changed to reliability of the software. The software that is secure and durable is considered as reliable. Now the question arises how the durability is a major factor of software security and how it improves reliability of software [46]. It can be related with the failure-free secure period, occasionally with the ability of the secure software to meaning after preservations, but the fact leftovers, the general description of durability is misplaced. Availability, survivability, reliability of security is parallel to each other as well as durability.

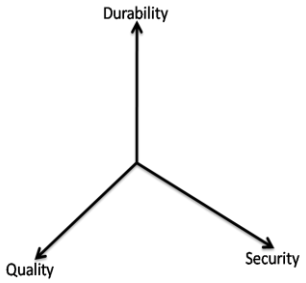

Figure 2. Affiliation between Security, Quality and Durability [50]

Time dependency appears in conceptual representation absolutely. It relies on software attributes that how much system's software is protect; exactly the durability decides for how longer software will be protected. Capacity of durability is signified by the interval of secure software. Affiliation between durability, security and quality, is shown in figure 2. Durability also discusses to the assurance that once the software has been notified of success, the security will continue, and not be unfinished. When the design security can be repaired, assessing durability is problematical and software will be recycled until it is no extended economical to control it.

Technically; durability can be distinct as the quantity of use one develops from a security before it declines. Durability is approximately what occurs when security of software goes out all over. Amplification in security may not be the outcome of practical developments. Fairly, the essential commercial environment basically may have transformed. Driven by market speed and feature demand, commercial software developers have high pressures to

deliver products rapidly, usually at the expense of quality as well as security [47-50]. Because of these market pressures and the increasing complexity of today's software, it is idealistic to assume total security and robustness [51]. The difficulty is that there is no perfect procedural description of durability.

4. Durability Relating with Security Attributes

The foremost weakness of developing application software in components or modules that it proceeds extra time-period for projection. Durability may be separate as the capacity of process of development depends on its secure design. Security factors are discovered with the essential requirements and recognized in a mannered way to use in software developments. Security is a stable element of software quality. Security parameters of the products represent the quality. Secure software cannot be valued if it is frequently interrupted and the preferred tasks lost for even a brief time [48]. Durability, human trust, dependability and trustworthiness are security features which relates to security in some means. Their relation to security and with each other is shown in Table 1 with brief introduction of them.

Table 1. Durability, Human Trust, Dependability and Trustworthiness

Concept	Durability	Trust	Dependability	Trustworthiness
Goal	Assurance or probability that an equipment, machine, or material will have a relatively long continuous usefu l life, without requiring an inordinate degree of maintenan ce.	Trust is defined as a willingness to rely on an ex-change partner in whom one has confidence.	Ability to deliver service that can justifiably be trusted. Ability of software or system to avoid failures that are more frequent or more severe than is acceptable to the user(s)	Assurance that software or system will perform as expected.
Threats Present	Attacks (e.g., intrusions, probes, denials of service). Failures (internally generated events due to, e.g., software or system design errors, human errors, corrupted data). Accidents (externally generated events such as natural disasters).	Physiological errors and social errors (nature of loyalty and betrayal in the context of organisational, cultural factors and changing economic).	Development faults (e.g., software flaws, hardware errata, malicious logic). Physical faults (e.g., production defects, physical deterioration). Interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)	Hostile attacks (from hackers or insiders). Environmental disruptions (accidental disruptions, either manmade or natural). Human and operator errors (e.g., software flaws, mistakes by human operators)
Reference	[29]	[27]	[28]	[30]

It is significant for security experts to distinguish what to expect for when they analyze security examination. This has foremost effects for the role of security factors and challenging their characters in the development of software security. Technology is fairly a vital portion relating to securing info of data assets. Attributes are accountable for design, enactment and process of scientific implements [50]. Durability factor is affected by other security attributes. Here, all security attributes are defined and described how they relate to durability as a security factor.

4.1. Durability Relating with Authentication

Software necessity to know the uniqueness of a consumer. Identification of user permits software to provide a modified contribution to access their data. Information about the user is returned in demand reverses on the client software. This permits you to modify your experience for that specific user. The techniques in which someone can be authenticated drop into three taxonomies, such as user knows, user has, and the user. This feature provides authentication with respect to trustworthiness against security failure for controllers when working with it.

For authenticated users it is an object containing the user's unique and potentially other data about the user. Authentication believes on the fact that only those users who privilege to be authentic and verified will be acceptable. In security terms, authentication is the process of attempting to verify the digital identity of the sender of a communication. It is often controlled at the interface stage [44-49]. Authentication is well effected by the user satisfaction and software effective evaluation. Software effective evaluation is to determine how well the software meets the needs of secure software. Authentication is effected like dependability and human trust, which in turn effects durability.

4.2 Durability Relating with Confidentiality

Confidentiality discusses of secure data whose disclosure may harm the information. Consumers classify conditions that categorizing, estimating the security and benefits of software. The consumer shall proceeds into justification whether informed third party would be potential to achieve. Considering all the definite truths and environments of effective evaluation to the consumer at that time. When you make the reputation of somebody who can be trusted on, construct philosophical relationships. In industry, trustworthy persons are more possible to make a longer consumer base, and appreciate earlier preferment.

The requirement to secure confidential information shall relate to the verification of both software and user. For this purpose, a classification security shall be introduced. This shall provide for clear criteria ensuring the enclosure of information into suitable categories of confidentiality. With durability the confidential information of data will be more secure for a specific period[45-48]. The interface which enables user for accessing some kind of data within timeliness is confidentiality. Confidentiality is effected by other security attributes as accessibility and user satisfaction which in turn effects dependability and human trust.

4.3 Durability Relating with Integrity

Consistently, persons who are extremely trusted understood to have constant integrity. In security perspectives, it is a replacement for ethics or attractiveness. It holds all the other ethical codes. Integrity is similarly frequently cast-off interchangeably with trustworthiness. Integrity essentials and justifies its actual own domain. There are four components to business integrity: individual principles, quantified values, effective values, and ethical codes. Persons of integrity are dependable because they improper their conclusions on ethical and moral codes, not on pragmatism. Integrity means maintaining and assuring the accuracy and consistency of information of data [48-51].

Integrity is a quality of attractiveness established by the ethical assurance and resolution essential to continue dependability between four components of consumer integrity such as physiological acceptability, user stasfication, business continuity, scalability. Integrity is violated when information is actively modified in transfer. This means that data cannot be modified in an unauthorized or undetected manner. Durability ensures that data meet with a significance hope of quality and that the data can be trustworthy [5-8]. When data is received by user it must be safe and should not be modified, than only it will satisfy user and may be trustworthy [51].

4.4 Durability Relating with Availability

The modern software architecture deals only partial assurances regarding availability. Specifically, the security architecture offers assurance that consumers who continue for long sufficient in trying to connect will be able to categorizes direct, limiting availability. This discusses to the dimension of the time interval during which the availability is determined[

52]. The fact availability is a function above time that can be calculated from the repair time and failure time distributions. Frequently it is concerned in availability of a software or system after necessary time has gone. Accuracy can be lost for the drive of the response time-periods [47].

Availability certifies that the consistent information of data and services will be conceivable, when it is demanded for duration of time. So many times loss of probability is considered as denial of service (DoS). Availability declares that software will not work everywhere without completion [37]. Availability effects the degree to which various kind of users can depend on that is dependability and trustworthiness. If there is improvement in the durable availability then security also works with less complexity as well as increases the security [42-52]. Being trustworthy and dependable is such an important to improving quality of secure software that it makes durability as a strong characteristic for consideration.

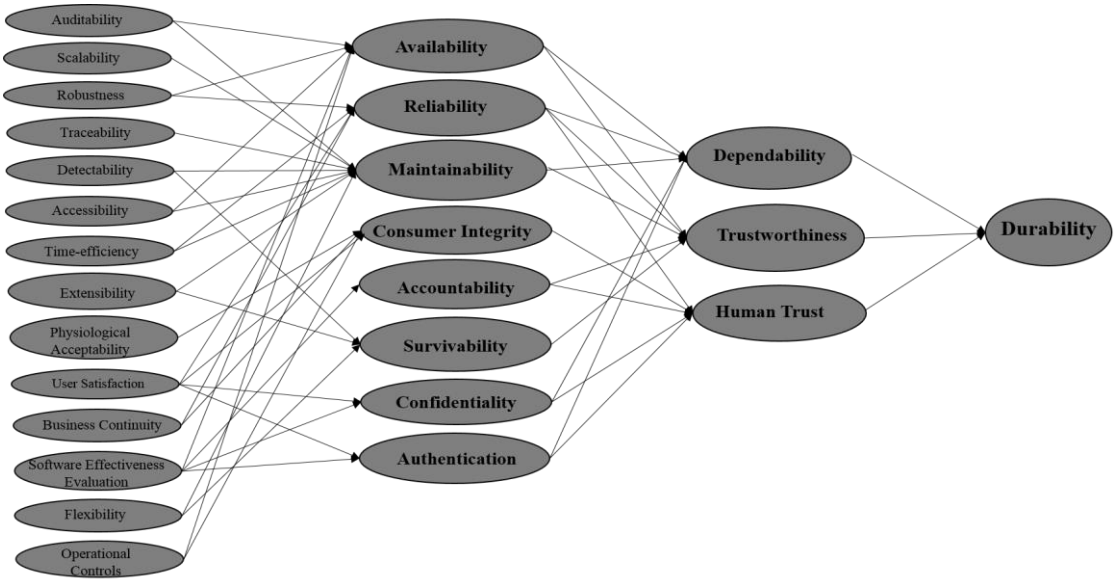

Figure 3. Affiliation between Security Factors and Key Determinants of Durability

4.5 Durability Relating with Survivability

Survivability ensures that software is providing vital properties to users even in the occurrence of an attack, software cannot have failure arguments. It certifies that security cannot have failure for specific time duration. Survivability, in the perspective of security, is the ability of a software to achieve its assignment in a timely manner, accidents, despite attacks or failures. As an idea and as a preparation, survivability should flood all stages of software or systems. Understanding of the significance of survivability contributes to lasting development and assignment completion. Survivability is concerned with energetic mission-critical facilities. Survivable security necessity continues to be delivered in unkindness of either malicious or accidental harm.

When developers tends to improve durable security, within this process survivability will also be improved [40]. Durability is the degree to which essential, mission-critical services continue to be provided in spite of either accidental or malicious harm [45]. Effect of detectability and movability strengthens the attribute survivability, which is to survive in presence of attacks. A secure software is flexible, means it can mould itself in occurrence of

malicious attacks. Timeliness, flexibility, user satisfaction are the attributes which effects survivability and ensures that software is trustworthy and dependable. A thorough understanding of the principles of survivability and assurance creates a firm educational foundation designed to address the knowledge gaps that arise in the area of security [46].

4.6 Durability Relating with Reliability

Reliability is one of the peak significant quality characteristics of mission-critical and safety-critical systems or software. Opposite to correctness, reliability discusses to the dynamic performance of a software as well as security. It is not a specific of the static source code. Traditional reliability models relations between software and hardware reliability. This difference is built on the hypothesis that software reliability is affected by design faults. Nowadays, the simple parting of software reliability is not legal any other. System software development process deals with software design faults as well. The execution environment effects the reliability of a software artifact as well as security.

Reliability is the degree to which a work product operates without failure under given conditions during a given time period. Reliability means to prevent security from failures and to make strategies to maintain its trustworthiness. So it can be estimated that durability enhances security with the help of reliability as well as human trust [46-47]. Reliability is the possibility of a system or software execution its drive sufficiently for the period of time planned under the operational situations faced. Being a reliable secure software means to maintain robustness and trust of user. A trustworthy software system is reliable and robust within a time duration that is if an error occurs it deals with it without any specific change in secure system of software.

4.7 Durability Relating with Accountability

Within a business, the codes and performs of accountability goal to increase both the interior ordinary of discrete and assembly behaviour as well as exterior issues, such as justifiable financial strategies. Also, accountability shows an increasingly significant role in hypothetical arenas, such as experimental research. Software effective evaluation is to ensure that the software is fulfilling the requirements of user and being trustworthy within a period. Accountability is an essential security concept. It means that every individual who works with a security should have specific responsibilities for information assurance that it is not easily accessible.

The tasks for which an individual is responsible are part of the overall security plan and are readily measurable by a person who has managerial responsibility for information assurance [46-50]. Characteristic that effects accountability is traceability, business continuity, software effective evaluation and operational controls. Traceability is attribute which ensures that errors which are interrupting of software are traced during an interval. Software which is fully secure is traceable as well as accountable.

4.8 Durability Relating with Maintainability

It may deal with many errors which occurs after the delivery of product. Unnecessary dependencies between modules, levels and incorrect coupling to existing programs, avoids informal replacement, modernizes, and modifications; and can cause alterations to actual classes to current through the whole software or system. Reflect designing software as well-defined levels, which openly describe the industry developments, and information of data access functionality. Maintainability is the facility of the software or security to experience modifications with a degree of simplicity. These modifications could influence mechanisms,

features, and interfaces when changing the software's functionality in direction to meet new business requirements as well as security requirements.

Maintainability is the simplicity with which a security can be maintained in demand to isolate defects, correct defects, repair or replace faulty components without having to replace still-working parts. Durability ensures that there is no need of maintenance of security in a specific duration of software execution. Maintainability is a factor by which defaults are corrected after the delivery of software. In the terms of security a system is as longer secure i.e., as much durable, it will need lesser maintenance [20-25]. Trustworthiness of a product is decided when system is secure, flexible, extensible.

Table 2. Definitions of Durability Sub Characteristics

Sub-characteristics	Definitions	References
Auditability	The capability of supporting a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.	[12]
Scalability	Scalability is the measure of how well a service or application can grow to meet increasing performance demands.	[11]
Robustness	Robustness is the ability of a software to cope with errors during execution.	[14]
Traceability	The ability to trace software design representation or actual program component back to requirements for secure design.	[25]
Detectability	Detectability is an application or a subsystem that is responsible for detection of node failures or crashes in a distributed system in duration of time.	[15]
Accessibility	Accessibility is the degree to which a service, or environment is available to as many people as possible.	[13]
Time - efficiency	The capability of the software to provide appropriate performance, relative to the amount of resources used understated conditions within specific time duration.	[29]
Extensibility	The ease with which an application or component can be enhanced in the future to meet changing security requirements or goals.	[16]
Physiological Acceptability	Acceptance in human psychology is a person's assent to the reality of a situation, recognizing a process or condition without attempting to change it, protest.	[26]
User satisfaction	User satisfaction, is a measure of how products and services supplied by a company meet or surpass customer expectation.	[52]
Business Continuity	Business continuity encompasses a loosely defined set of planning, preparatory and related activities which are intended to ensure that an organization's critical business functions will either continue to operate within a reasonably short period.	[27]
Effectiveness	Effectiveness is degree to which something is successful in producing a desired result; success.	[28]
Flexibility	The capability of a software to respond to potential internal or external changes affecting its value delivery, in a timely and cost-effective manner.	[3]
Operational Controls	The most difficult task of management concerns monitoring the behavior of individuals, comparing performance to some standard, and providing rewards as indicated.	[27]

It is already been identified that important security factors effects durability directly or indirectly. But there are some sub characteristics of software security like effectiveness, portability etc. which are affected or effects durability [28-29]. Durability is best defined with its characteristics. Durability has specific impaction on other characteristics of security factors. The sub-characters play very significant role in the measurement of security factors. The quantification of the security factors provides the help in the assessment of the overall

security of the software. The definitions of various sub-characteristics from the literature survey of durability are defined in the Table 2.

The design of security has a vital influence on the secure software. Principals of secure design constructed numerous views. It is significant to consider about the measures of security. Specific security attributes have optimistic or undesirable impact due to these software thoughts. When a design is prepared, it is to be prepared in modules to get quality product [33-36]. Then collected with every one, because of this probability of mistakenness is identical fewer. Security durability is distinct as the size of failure free process time-period. All failure is produced by functional stresses and process is established on actuality able to measure the stresses of attacks or causes.

5. Discussion

Security is one of the most significant quality factors that are concern to software designers as well as consumers. To achieve effective security of software detection of floating pathogenic bugs, the problem necessity be considered in standings of their timeliness size and ordinary characteristics [37-39]. The detection of vulnerabilities, ensuring sensitivity, cost efficiency, and manageability of security, using only three key components i.e. CIA is quite difficult to achieve. Use the commonality of these information as a foundation on which to build an asset-based, risk-driven danger analysis approach.

The approach which leads for trustworthiness, human trust and dependability which means durability. As the requirement arises security factors were identified and collected for their contribution in software development. Security is an essential part for getting quality product. The criterion for security estimation is a key to know the quality of that software. This course of study is being applicable at design of software development lifecycle and aiming to enhance one step in the security engineering of software. Following steps form one such process when performed iteratively, incrementally, and in parallel with the other activities and tasks:

- Develop a durability program plan that includes trustworthiness, human trust and dependability.
- Identify and highlight the valuable assets that are in hazard and thus may be affected.
- Conclude the negative influences that could happen to these valuable assets if the risks were to cause occurrences.
- Identify, classify, and highlight the hazards that may damage these valuable assets.
- Identify and investigate their potential sources.
- Estimate the associated risks to these respected assets
- Arrange them based on the degree of the negative impacts.
- Identify, investigate, and require durable security necessities as arrangements of the quality benchmark.
- Identify attributes of trustworthy secure software design.
- Identify the object-oriented design characteristics that required to diminish maintainability of a secure software for a duration.
- Identify attributes of trusted secure environments.
- Identify attributes to provide trustworthiness evaluation techniques for secure software within specific time-duration.

6. Conclusion

An essential security factor improves the security of software. Software security factors acts a major role in software security estimation. Durability as a security factor will contribute in security of software, if it is considered during Object oriented design making. Its feature depends on some security attributes and affects it directly. Durability has a significant impact on security attributes like, authentication, authorization, confidentiality, integrity, availability, reliability and survivability. Durability is parallel to availability, survivability, reliability etc. Here is a research which improvizes the fact that timeliness can be an important security factor and effects a lot in quality. This paper will give a view to show the effect of security factors with durability and impact of security attributes.

References

[1] G. McGraw, "Software Security", IEEE Security Privacy, vol. 2, (**2004)**, pp. 80-83**.**
[2] Definition of Accountability, Available at: http://en.wikipedia.org/wiki/Accountability last visit Oct 03 (**2014**).
[3] S. A. Khan and R. A. Khan, "Securing Object Oriented Design: A Complexity Perspective", International Journal of Computer Applications, vol. 8, no.13, October (**2010**).
[4] R. Kumar, S. A. Khan and R. A. Khan, "Software Security Durability", International Journal of Computer Science and Technology, vol. 5, no. 2, **(2014)** April - June, pp. 23-26.
[5] P. H. Meland and J. Jenesen, "Secure Software Design in Practice", ARES.(**2008)**, IEEE, 0-7685-3102-04/08., Copyright IEEE.
[6] C. Wang and W. A. Wulf, "A Framework for Security Measurement" Proc. of National Information System Security Conference, (**1997)** October 7-10, pp. 522-533.
[7] Definition of Availability, Available at: http://www.businessdictionary.com/definition/availability.html#ixzz3F3PBDSiZ, last visit Oct 03 (**2014**).
[8] What is Biometric Security? Available at: http://www.researchgate.net/post/What_is_Biometric_Security, last visit Oct 03 (**2014**).
[9] Authorize Requests, Available at: https://cloud.google.com/storage/docs/json_api/v1/how-tos/authorizing,last visit Oct 01 (**2014**).
[10] Global Information Assurance Certification Paper, Available at:http://www.giac.org/paper/gsec/835/clark-wilson-security-model/101747,last visit Oct 11 (**2014**).
[11] G. Hoglund and G. McGraw, "Exploiting Software: How to Break Code", Boston: Addison-Wesley, (**2004**).
[12] Engineering Safety Requirements, Safety Constraints, and Safety-Critical Requirements, Available at: http://www.jot.fm/issues/issue_2004_03/column3/ last visit Oct 17 (**2014)**.
[13] A. D. T. Amma, V. R. Pramod and N. Radhika, "ISM for Analyzing the Interrelationship between the Inhibitors of Cloud Computing", IJCAES, vol. 2, no. 3, (**2012**).
[14] A. D. T. Amma, V. R. Pramod and N. Radhika, "Synergic Impact of Inhibitors of Cloud Computing FISM and FMICMAC Approach", IJCA, vol. 87, no. 3, (**2014**).
[15] Security and Privacy Technologies in SOA, Available at: http://www.computer.org/portal/web/buildyourcareer/ts020last visit Oct 12 (**2014**).
[16] Web Services Security and Privacy, Available at: http://www.computer.org/csdl/proceedings/scc/2007/2925/00/2925xxxii-abs.html last visit Oct 12 (**2014**).
[17] O. Bloedorn, Available at: http://de.linkedin.com/pub/oliver-bloedorn/56/b9/31b last visit Oct 13 (**2014**).
[18] Secure Embedded Systems, Available at: http://seminarprojects.org/c/secure-embedded-systems last visit Oct 14 (**2014**).
[19] Network Security Essay, Available at: http://www.antiessays.com/free-essays/Network-Security-161531.htmllast visit Oct 15 (**2014**).
[20] PPT Network Security, Available at: http://boardreader.com/tp/ppt%20network%20security.htmllast visit Oct 15 (**2014**).
[21] Impact of Perceived Security on Consumer Trust in Online Banking, Available at: http://aut.researchgateway.ac.nz/handle/10292/491last visit Oct 16 (**2014**).
[22] Quality Assurance Resources, Available at:http://www.developmentguruji.com/monthly-human-resource-hiring/quality-assurance-resource.htmllast visit Oct 16 (**2014**).
[23] Example of Research Papers, Available at: http://examples-of research-papers.blogspot.in/2013/06/network-security.html last visit Oct 16 (**2014**).

[24] A. P. Martin and D. Khazanchi, "Information Availability and Security Policy", Pro. Twelfth Americans Conference on Information Systems, Acapulco, Mexico, (**2006**).
[25] S. Banerjee, C. A. Mattmann, N. Medvidovic and L. Golubchik, "Leveraging Architectural Models to Inject Trust into Software Systems", Available at http://sunset.usc.edu/~mattmann/pubs/sess05.pdf last visit Oct 18 (**2014**).
[26] S. S. Gokhale, "Architecture-Based Software Reliability Analysis: Overview and Limitations", IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 1, (**2007)**.
[27] S. Ghosh, S. K. Dubey and A. Rana, "Comparative Study of the Factors that Affect Maintainability", IJCSE, vol. 3, no. 12, (**2011**) December.
[28] R. Kumar, S. A. Khan and R. A. Khan, "Software Security Testing A Pertinent Framework", Journal of Global Research in Computer Science, vol. 4, no. 3, (**2014**).
[29] A. A. Ienis, J. C. Laprie and B. Randell, "Dependability and its Threats: A Taxonomy", Available at http://www.cs.newcastle.ac.uk/publications/inproceedings/papers/779.pdf last visit Oct 21 (**2014**).
[30] E. Haruvy and A. Prasad, "The Effect of Piracy on the Market Penetration of Subscription Software", Journal of Business, vol. 77, no. 2, (**2004**).
[31] I. Fléchais, "Designing Secure and Usable Systems", A Dissertation Submitted for the Degree of Doctor of Philosophy of the University of London, February (**2005**).
[32] Cyber Security and Information Assurance, Available at: http://www.cranfield.ac.uk/courses/training/cyber-security-and-information-assurance.html last visit Oct 25 (**2014**).
[33] ISO/IEC 9126-1, Institute of Electrical and Electronics Engineers, Part1: Quality Model, (**2001**).
[34] ISO/IEC TR 9126-3, Software Engineering Product Quality, (**2002**).
[35] D. G. Firesmith, "Common Concepts Underlying Safety", Security and Survivability Engineering, Technical Note CMU/SEI- 2003-TN033, Software Engineering Institute, Pittsburg, Pennsylvania, (**2003**), pp. 1-75.
[36] K. Sahu, R. Shree and R. Kumar, "Risk Management Perspective in SDLC" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 3, (**2014)**.
[37] D. N. P. Murthy and W. R. Blischke, "Warranty Management &Product Manufacture", Google Books, Business &Economics, (**2006**), pp. 1-302.
[38] J. E. Gaffney, "Metrics in Software Quality Assurance", ACM Press, no. 81, (**1981**), pp. 126-130.
[39] R. S. Pressman, "Software Engineering a Practitioner's Approach", McGraw-Hill Inc., (**1992**).
[40] A. Evesti, "Quality-Oriented Software Architecture Development", VTT Technical Research Centre of Finland, (**2007**).
[41] S. Kazuya, R. Koichiro, T. Dohi and O. Hiroyuki, "Quantifying Software Maintainability Based on a Fault Detection/Correction Model", 13th IEEE International Symposium on Pacific Rim Dependable Computing, (**2007**).
[42] R. L. Rogers, "Principles of Survivability and Information Assurance", © Carnegie Mellon University Pittsburgh, PA 15213, (**2004)**.
[43] Trustworthiness and Integrity: What It Takes and Why It's So Hard, Available at: http://josephsoninstitute.org/business/blog/2011/01/trustworthiness-and-integrity-what-it-takes-and-why-it%E2%80%99s-so-hard/ last visit Dec 13 (**2014**).
[44] D. B. Parker, "Restating the Foundation of Information Security", Proceedings of the Eighth International Conference on Information Security, Netherlands, (**1992**), pp. 139-151.
[45] R. Sandu, "Access Control: The Neglected Frontier", Proceedings of the First Australasian Conference on Information Security and Privacy, Australia, pp. 219-227.
[46] C. Schou, "Information Systems Security Organization", Glossary of INFOSEC related terms, Vols. I & II. Idaho: Idaho State University.
[47] J. Kelley, "Business Continuity: Battling High-tech Exposures", Risk Management, vol. 47, no. 5, p. 3133.
[48] ODI: On track Data International Cost of Data Loss, Available at: http://www.ontrack.com/understandingdataloss/ last visit Dec 13 (**2014**).
[49] S. Becker, M. Boskovic and A. Dhama, "Trustworthy Software Systems: A Discussion of Basic Concepts and Terminology", Graduate School Trustsoft, Carl-von-Ossietzky University of Oldenburg, Germany Sep (**2006**).
[50] Chapter 16: Quality Attributes, Available at: http://msdn.microsoft.com/en-in/library/ee658094.aspxlast visit Dec 13 (**2014**).
[51] Accountability, Available at: http://en.wikipedia.org/wiki/Accountability last visit Dec 13 (**2014**).
[52] A. A. Aziz, M. Nishazini, Azizan N. A. Noorashikin, "The Impact of Quality Standards and a Special Customer Service Program on Customer Satisfaction Index (Csi) for Kpj Seremban Specialist Hospital, Malaysia", IOSR Journal of Business and Management, Dec (**2013**).

Authors

Rajeev Kumar pursuing Ph.D. in Information Technology from Babasaheb Bhimrao Ambedkar University (A Central University), Vidya Vihar, Raibareli Road, Lucknow. He has been completed his master's degree in Information Technology from Babasaheb Bhimrao Ambedkar University Lucknow and bachelor's degree in Mathematics from MJP Ruhelkhand University, Bareilley. He is currently working in the area of Software Security, Security Testing and Software Risk.

Suhel Ahmad Khan has earned his Doctoral Degrees from Babasaheb Bhimrao Ambedkar University, (A Central University), Vidya Vihar, Raibareli Road, Lucknow. Dr. S. A. Khan is young, energetic researcher and has completed a Full Time Major Project funded by University Grants Commission, New Delhi, India. He has more than 5 years 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 a member of IACIT, UACEE, and Internet Society.

Raees Ahmad Khan has earned his Doctoral Degrees from Jamia Millia Islamia, New Delhi, India. Dr. R. A. Khan is currently working as an Associate Professor and Head in the Department of Information Technology, Babasaheb Bhimrao Ambedkar University, (A Central University), Vidya Vihar, Raibareli Road, Lucknow, India. He has more than 15 years of teaching & research experience. His area of interest is Software Security, Software Quality and Software Testing. He has published a number of National and International Books, Research Papers, Reviews and Chapters on Software Security, Software Quality and Software Testing.