# A Fuzzy Analytic Network Process for Security Risk Assessment of Web based Hospital Management System

**Nawaf Rasheed Alharbe**

***Abstract:*** ***Software applications have revolutionized human lives. As healthcare industry becomes digitalized, more and more hospitals are now dependent on effective and user-friendly software applications for efficacious management. However, this progressive increase in the use of software applications has led to several security issues. Security risk has probably become the biggest and most sensitive concern in this era for hospital management systems. Assessment of security risk may help in acquiring the level of security that the end user wants. Security assessment needs identification and prioritization of its attributes for publishing guidelines to maintain that level, as security risk is a multidimensional problem. This study has used the Fuzzy ANP methodology to solve this multi criteria based problem. This work also emphasizes on increasing security by assessing the security risk in hospital management system. A real time case study of hospital management system has also been used for validating the results. The acquired results will help in mapping the guidelines and developing new mechanism as per the high prioritized attributes of security risk.***

***Keywords: Security Risk; Web Applications; Fuzzy Logic; Analytic Network Process.***

## I. INTRODUCTION

Software has become one of the essential needs of users in all the important fields such as medical, engineering, airlines, etc. Given the integral role of software applications and the increasing reliance of the users' in facilitating their tasks through software, it is imperative to ensure optimum security of the software in use. Developers cannot ignore the risk of having insecure software. Hence, the developers need to find newer techniques and adopt necessary action at the time of security risk assessment. In fact a report by the National Institute of Standards (NIST) in 2002 stated that more than $59.5 billion was consumed on repairs of faulty software annually [1]. Such reports are a forewarning for all software developers to research on security risk-management activities and create safeguard mechanisms in both cyber security and software security. Most of the times it is seen that ignorance of security is caused by the cost and time spent on it. The generation and development of a security tool for making software systems risk free at the time of design in SDLC is a highly extensive and costly task for any organization. Security risk analysis is an inseparable part of development process. Also, the assessment of security risk includes seven attributes that include: Human and organization factors, security requirements, insecure design, integrity, availability, resilience and non-repudiation. These attributes are the so called keystones to identify the risk and vulnerabilities in security and to mitigate them [2, 14-16].

Healthcare organizations and security of its applications is a booming and an expansive field for researchers nowadays. Also, patients' data is considered to be highly sensitive information. The trespassers are always ready to target the applications whether it is that of the system or the user's [3, 17-19]. Any organization that is developing any application for hospital management should manage the security risks associated with it. Furthermore, security risk assessment is a growing area which includes the development and assessment of new tools and technologies for security risk mitigation. The main aim of security breakers or the intruders is to exploit the vulnerabilities and acquire all the sensitive information of the hospitals and patients through which they can control the running system. Hence to avoid all the possible disruption, security risk assessment provides a mechanism through which security risk can be mitigated before delivering the application to the end stakeholder. An enactment of security risk assessment plays an important role for enhancing the security. Security risk assessment along with the planned process of software development improves the understandability for security and predicts the upcoming vulnerabilities which may occur at any time [2, 4, 20-22].

At the same time, growth of security issues or happenings is a rising concern amongst the investors and the IT industries. The organizations which do not focus on the security risk assessment during the development phase of software deliver applications that can contain dangerous vulnerabilities that may pose enormous risks to the users. Aligning with this contextual framework, the second section of the research paper focuses on the needs and importance of the security risk assessment using MCDM techniques. The third section describes the analytic process in detail. The fourth section demonstrates the assessment of security risk using fuzzy ANP. The fifth and the sixth section discuss the results and conclude the article.

## II. NEEDS AND IMPORTANCE

The fundamental aim of this paper is to find the priorities based on weightage and ranking of the security risk attributes by applying multiple criteria choice making process under which the use of analytical network process is shown. The idea is to provide more security and reliability to the application software.

**Revised Manuscript Received on November 02, 2019.**
***** Correspondence Author
**Nawaf Rasheed Alharbe***, Department of Computer Science and Information, Community College, Badr, Taibah University, KSA Email: nrharbe@taibahu.edu.sa, anawafrasheed@gmail.com

Since very few attempts have been made for prioritizing and ranking the attributes of security risk for hospital management system which may affect the success of software security and their trade-offs, the fuzzy ANP techniques can be used for prioritizing the attributes of all the security risk. The hybrid technique of Fuzzy ANP gives more accurate results in comparison to the classical ANP technique because it is helpful in eliminating the problem of uncertainty and vagueness in the decision making process. This process of analysis of prioritization of security risk attributes is a type of Multi-Criteria Decision Problem because of the multiple attribute contribution in it [5, 6, 23-24]. Multi-Criteria Decision Analysis (MCDA) is helpful for performing various evaluations of conflicting elements like Multi-Attribute Utility Theory and Analytic Network Process [7]. Objectives, alternative weights and their ranks are three different parts of MCDA process which are used in ANP technique.

Further, it is important to underline in this context that the Analytic Network Process (ANP), introduced by Thomas L. Saaty, is a generalized network form of the AHP or in other words ANP is an increased clarification of AHP. Also, Saaty recommended the use of AHP for solving the independent criteria formed in a hierarchy. Whereas, ANP can be used in dependent criteria formed in a network [8, 9]. The figure-1 describes the actual differences between AHP and ANP which are given below:

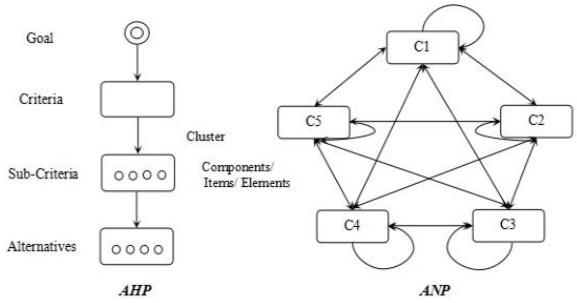


**Figure-1. Difference between AHP & ANP**

There are some real world problems of decision-making criteria which cannot be systematized as a hierarchy. This is because of the interdependence of criteria on each other for forming a network type of a structure rather than a hierarchical one. Furthermore, ANP is crucial in creating network organization equally in AHP, attributes in the lesser layer may impact on the advanced level of attributes. There is one more concept different from AHP which is called the "super matrix". It is present in ANP and not in AHP [11].

## III. METHODOLOGY

Several recent applications and research works are available in literature in which ANP method has been employed and it gives better results. For example, Rajeev Kumar et al. uses ANP method for the security of software [5]; Goztepe et al. used fuzzy ANP process towards prioritizing six sigma projects [2]. Dagdeviren et al. also used fuzzy ANP model to classify faulty behaviour risk in system [4], etc. Chang et al. [3] used the fuzzy ANP method to assess the risk level of intra organizational cultures and found that the security risk attribute is related to the enterprise resource planning system. Chinho Lin in 2014 applied Fuzzy ANP for supplier selection at an electronics company. The results showed one of the attributes called triple bottom line as an important attribute among the others [4].The methodology used in ANP is shown below and all the defined stages of ANP method are as follows:

In this process, all the attributes, sub-attributes and its alternatives that were taken have been elaborated upon. After these steps, the groups of all the items which are taken for prioritization and ranking are determined. Since, ANP is purely based on network process so the association is formed amongst the groups and within each group also more associations are created. As a result, some associations which are different are formed and these have their own properties [14]. Items that show self-interaction is also an effect which provides more flexibility and the last one is a mutual effect in which inter-dependencies among criteria is shown.

**Step1:** After taking linguistic values from the experts and practitioners, authors convert it into crisp numbers and Triangular Fuzzy Number (TFN). TFN can be defined as (p, q, r), where p, q, and r ($p \le q \le r$) are parameters indicating the smallest, the middle value, and the largest value in the TFN, respectively. In addition, a fuzzy number M on F is called TFN, if its membership functions is given in equations (1-2) and shown in Figure 2.

$$\mu_a(x) = F \rightarrow [0,1] \quad (1)$$

$$\mu_a(x) = \begin{cases} \frac{x}{q-p} - \frac{p}{q-r} x \in [p,q] \\ \frac{x}{q-r} - \frac{r}{q-r} x \in [q,r] \\ 0 \quad Otherwise \end{cases} \quad (2)$$

Experts allocated scores to the attributes affecting the values in a quantitative way conferring to scale which is shown in table 1.

**Table 1. Linguistic terms and the corresponding TFNs**

| Saaty Scale Definition | Fuzzy Triangle Scale | |
|---|---|---|
| 1 | Equally important | (1 ,1, 1) |
| 3 | Weakly important | (2 ,3, 4) |
| 5 | Fairly important | (4 ,5, 6) |
| 7 | Strongly important | (6 ,7, 8) |
| 9 | Absolutely important | (9 ,9, 9) |
| 2<br>4<br>6<br>8 | Intermittent values between two adjacent scales | (1 ,2, 3)<br>(3 ,4, 5)<br>(5 ,6, 7)<br>(7 ,8, 9) |

Using the equations (3-6) numeric values are transformed intoTFN [14] and signified as ($l_{ij}$, $mi_{ij}$, $u_{ij}$) where, $l_{ij}$ is said to be lower value, $mi_{ij}$ is middle value and $u_{ij}$ is called as uppermost level values. Moreover, TFN [ṇij] is recognized as the following:

$$\eta_{ij} = (p_{ij}, q_{ij}, r_{ij}) \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$where\, p_{ij} \le q_{ij} \le r_{ij}$$

$$p_{ij} = min(J_{ijd}) \ldots\ldots\ldots (4)$$

$$q_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}} \ldots\ldots\ldots\ldots (5)$$

$$and\, r_{ij} = max(J_{ijd}) \ldots\ldots (6)$$

$J_{ijk}$ in the above equations indicates the values given by expert d and the comparative importance of the values between two criteria also in which i and j signify a pair of criteria given by expert d. Assessment $\eta_{ij}$ .i.e;

TFN is calculated using the geometric mean of expert's opinions for a specificjudgment. Further, equations (7-9) help to aggregate TFN values. Consider two TFNs M1 and M2, M1= ($p_1$, $q_1$, $r_1$) and M2= ($p_2$, $q_2$, $r_2$). The rules of operations on them are as:

$$(p_1, q_1, r_1) + (p_2, q_2, r_2) = (p_1 + p_2, q_1 + q, r_2 + r_2) \quad (7)$$

$$(p, q_1, r) \times (p_2, q_2, r_2) = (p_1 \times p_2, q_1 \times q_2, r_1 \times r_2) \quad (8)$$

$$(p_1, q_1, r_1)^{-1} = \left(\frac{1}{r_1}, \frac{1}{q_1}, \frac{1}{p_1}\right) \quad (9)$$

**Step 2:** Prepare the pair-wise comparison matrix by using the responses received from the decision makers. Calculation of the Consistency Index (CI) using the formula in equation 10 as follows:

$$CI = (\gamma_{max} - Q)/(Q - 1) \quad \text{…….(10)}$$

where CI: Consistency Index and Q : is the number of compared elements.

Further, calculation of the Consistency Ratio (CR), using a random index is as following:

$$CR = CI/RI \quad \text{……..(11)}$$

where RI = random index (CI of the randomly generated pairwise comparison matrix). Random index is derived from Saaty [9]

**Step 3**: Next step is the construction of the comparison matrix. Also, defuzzified values are calculated to create a numeric value based on the produced TFN values. The defuzzification method used in this article has been taken from [12] as formulated in equation (12-14) which is said to as the alpha cut method.

$$\mu_{\alpha,\beta}(\eta_{ij}) = [\beta.\eta\alpha(l_{ij}) + (1 - \beta).\eta\alpha(h_{ij})] \quad (12)$$

where $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$

Such that,

$$\eta\alpha(l_{ij}) = (m_{ij} - l_{ij}).\alpha + l_{ij} \quad (13)$$

$$\eta\alpha(h_{ij}) = h_{ij} - (h_{ij} - m_{ij}).\alpha \quad (14)$$

α and β in these defuzzification equations are said as preferences of number of experts respectively.α and β values vary between 0 and 1.

**Step 4**: Next step is the formation of the super-matrix which is the result of the priority vector from the paired comparisons between groups including goal, criteria, sub-criteria, and alternatives.

## IV. ASSESSMENT OF SECURITY RISKS

Classical Analytical hierarchy process and Analytical network process techniques do not help in gaining unambiguous and clear results in complex and imprecise situations. Hence the use of fuzzy ANP in situations where decision makers are uncertain regarding the level of weights becomes important to overcome the problem of uncertainty. This makes FANP an efficient method of decision making in problems having multiple criteria. Security risk has been a thrust area for different fields. Ensuring data integrity of immensely classified information like the patients' record, diseases and medication, etc., are important for hospital management application. Hence, the assessment of security risk and its attributes is important for mitigating the risks at early phases of development. Assessment needs attributes of security risk have to be identified. The elements discussed in the proposed paper for security risk prioritization incorporate the following **7** attributes [3]:-

- Human and Organization Factor (F1);
- Security Requirements (F2);
- Insecure Design (F3);
- Availability (F4);
- Integrity (F5);
- Non-repudiation (F6) and
- Resilience (F7)

Security risk attributes are usually a qualitative measure. So, it becomes a stimulating task to assess the security risk attributes quantitatively. Thus, the weightages and ranks of security risk factors help in gaining high software security. For the development of secure software, prioritization of security risk attributes used a multi-criteria decision-making (MCDM) process [8-9].

The authors have used fuzzy ANP which gives a newer approach while considering the interdependence of attributes over each other [12-13]. In reality, there is interdependence among the nodes and the alternatives in the real-world scenario. Hence, fuzzy ANP provides a network framework among the various attributes and the many alternatives that could be undertaken when it comes to problems related to decision making. This research is focused on choosing the best and highly prioritized attribute among the number of attributes of security risk by using a hybrid methodology of multi criteria decision methods for security risk attributes.

For identification of security risk attributes we have used a questionnaire session with a group of experts specifically for hospital management system, aggregated the attributes in seven groups as shown in table 2. Alpha-cut method for Defuzzification of local priorities of security risk attributes and formation of super matrix from all the local priority vectors are shown in table 3 and table 4, respectively. Further, weighted matrix is obtained from super matrix as shown in table 5. This is followed by limit supermatrix obtained from weighted supermatrix which has been shown in table 6. Finally, in table 7 we obtained global priorities of security risk attributes.

**Table 2. Pair wise comparison matrix**

| Security Risk Attributes | F1 | F2 | F3 | F4 | F5 | F6 | F7 |
|---|---|---|---|---|---|---|---|
| F1 (Human and Organization Factor) | 1.0000, 1.0000, 1.0000 | 1.0640, 1.5290, 1.9900 | 0.5110, 0.5980, 0.8590 | 1.7290, 2.3110, 2.9010 | 1.6920, 2.4140, 3.1470 | 1.5760, 2.0930, 2.6130 | 0.5520, 0.6390, 0.9050 |
| F2 (Security Requirements) | - | 1.0000, 1.0000, 1.0000 | 1.1820, 1.4740, 1.8720 | 0.7910, 0.9600, 1.1350 | 1.4590, 1.8590, 2.2150 | 1.3330, 1.5230, 1.7970 | 1.5530, 2.2000, 2.8500 |
| F3 (Insecure Design) | - | - | 1.0000, 1.0000, 1.0000 | 1.0850, 1.3430, 1.8720 | 1.6050, 2.3360, 3.1470 | 0.3350, 0.4270, 0.5740 | 1.3990, 1.8160, 2.4460 |
| F4 (Availability) | - | - | - | 1.0000, 1.0000, 1.0000 | 1.4960, 1.9280, 2.3540 | 0.9450, 1.0810, 1.6370 | 1.2500, 1.6390, 2.0280 |
| F5 (Integrity) | - | - | - | - | 1.0000, 1.0000, 1.0000 | 1.1870, 1.5350, 2.0280 | 1.1920, 1.4890, 1.8980 |
| F6 (Non-repudiation) | - | - | - | - | - | 1.0000, 1.0000, 1.0000 | 0.3980, 0.5110, 0.6620 |
| F7 (Resilience) | - | - | - | - | - | - | 1.0000, 1.0000, 1.0000 |

**Table 3. Defuzzification and Local Weights**

| Security Risk Attributes | F1 | F2 | F3 | F4 | F5 | F6 | F7 | Weightage |
|---|---|---|---|---|---|---|---|---|
| F1 (Human and Organization Factor) | 1.0000 | 1.0000 | 0.8920 | 2.5630 | 2.6670 | 2.3440 | 0.9340 | 0.2190 |
| F2 (Security Requirements) | 0.5620 | 1.0000 | 1.7510 | 1.2120 | 1.8530 | 1.7940 | 2.4150 | 0.1800 |
| F3 (Insecure Design) | 1.1210 | 0.5710 | 1.0000 | 0.9890 | 2.6060 | 0.6910 | 2.1200 | 0.1560 |
| F4 (Availability) | 0.3900 | 0.8250 | 1.0110 | 1.0000 | 2.1770 | 0.7710 | 1.8900 | 0.1340 |
| F5 (Integrity) | 0.3750 | 0.5400 | 0.3840 | 0.4590 | 1.0000 | 1.8210 | 1.7670 | 0.1030 |
| F6 (Non-repudiation) | 0.4270 | 0.5570 | 1.4470 | 1.2970 | 0.5490 | 1.0000 | 1.4360 | 0.1190 |
| F7 (Resilience) | 1.0710 | 0.4140 | 0.4720 | 0.5290 | 0.5660 | 0.6960 | 1.0000 | 0.0910 |
| | | | | | | | | CR= 0.0720 |

**Table 5. Weighted Supermatrix**

| | F1 | F2 | F3 | F4 | F5 | F6 | F7 |
|---|---|---|---|---|---|---|---|
| F1 (Human and Organization Factor) | 0.5000 | 0.1340 | 0.0650 | 0.1360 | 0.1180 | 0.1520 | 0.1110 |
| F2 (Security Requirements) | 0.1460 | 0.5000 | 0.1530 | 0.1270 | 0.1420 | 0.1170 | 0.1160 |
| F3 (Insecure Design) | 0.1240 | 0.1250 | 0.5000 | 0.1060 | 0.0760 | 0.1100 | 0.1100 |
| F4 (Availability) | 0.1150 | 0.1140 | 0.1160 | 0.5000 | 0.0640 | 0.0300 | 0.0590 |
| F5 (Integrity) | 0.0760 | 0.0800 | 0.0440 | 0.0830 | 0.0490 | 0.0350 | 0.0130 |
| F6 (Non-repudiation) | 0.0340 | 0.0500 | 0.0120 | 0.0440 | 0.0370 | 0.5000 | 0.0900 |
| F7 (Resilience) | 0.0000 | 0.0000 | 0.1100 | 0.0000 | 0.0690 | 0.0550 | 0.5000 |

**Table 7. Final Weights and Ranks of Security Risk Attributes**

| Security Risk Attributes | Global Priorities | Ranks |
|---|---|---|
| F1 (Human and Organization Factor) | 0.1890 | 2 |
| F2 (Security Requirements) | 0.2170 | 1 |
| F3 (Insecure Design) | 0.1850 | 3 |
| F4 (Availability) | 0.1620 | 4 |
| F5 (Integrity) | 0.1120 | 5 |
| F6 (Non-repudiation) | 0.0720 | 6 |
| F7 (Resilience) | 0.0640 | 7 |

In this paper, an application of fuzzy ANP has been proposed on security risk factors for hospital management system. The authors in this work proposed a network structure of multitudes of security risk attributes through which a complete relationship and inter-dependencies among these attributes is realized. The data was collected from different academicians and experts form the area and twenty valid responses were collected for assessment. According to the results achieved from the assessment, it is clear that security requirements (R2) have the highest priority among the seven attributes of security risk.

## V. CONCLUSION

The process of assessing security risk contains multiple attributes within it. In this paper, we have identified suitable attributes for hospital management system and we have proposed Fuzzy ANP methodology for assessing security risk. The subjective judgments of experts have been defined using TFN and then converted to crisp values using steps in Fuzzy ANP. We have also studied the interdependencies between different attributes of security risk. This assessment will help the developers to mitigate security risk early in the development life cycle by generating guidelines which could prove to be instrumental for the software developers.

## REFERENCES

1. Davis, Noopur., Samuel T. Redwine Jr., GerlindeZibulski, Gary McGraw, Watts Humphrey"Processes for Producing Secure Software – Summary of US National Cyberscevurity Summit subgroup Report" IEEE Security & Privacy May/June 2004
2. Saaty, T. L. (2004). Fundamentals of the analytic network process—Dependence and feedback in decision-making with a single network. Journal of Systems science and Systems engineering, 13(2), 129-157.
3. Boran, Semra&Yazgan, Harun&Goztepe, Kerim. (2011). A fuzzy ANP-based approach for prioritising projects: A Six Sigma case study. Int. J. of Six Sigma and Competitive Advantage. 6. 133 - 155. 10.1504/IJSSCA.2011.039715.
4. Dağdeviren, M., &Yüksel, İ. (2010). A fuzzy analytic network process (ANP) model for measurement of the sectoralcompetititon level (SCL). Expert systems with applications, 37(2), 1005-1014.
5. Chang, B., Kuo, C., Wu, C. H., &Tzeng, G. H. (2015). Using fuzzy analytic network process to assess the risks in enterprise resource planning system implementation. Applied Soft Computing, 28, 196-207.
6. Lin, C., Madu, C. N., Kuei, C. H., Tsai, H. L., & Wang, K. N. (2015). Developing an assessment framework for managing sustainability programs: A Analytic Network Process approach. Expert Systems with Applications, 42(5), 2488-2501.
7. Kumar, R., Zarour, M., Alenezi, M., Agrawal, A., & Khan, R. A. (2019). Measuring Security Durability of Software through Fuzzy-Based Decision-Making Process. International Journal of Computational Intelligence Systems, 12(2), 627-642.
8. Avizienis, A., Laprie, J. C., & Randell, B. (2001). Fundamental concepts of dependability (pp. 7-12). University of Newcastle upon Tyne, Computing Science.
9. Available online at https://www.sebokwiki.org/wiki/Reliability,_Availability,_and_Maintainability
10. Wang, C. N., Thanh, N. V., & Su, C. C. (2019). The Study of a Multicriteria Decision Making Model for Wave Power Plant Location Selection in Vietnam. Processes, 7(10), 650.
11. Kahraman, C. (Ed.). (2008). Fuzzy multi-criteria decision making: theory and applications with recent developments (Vol. 16). Springer Science & Business Media.
12. Sipahi, S., & Timor, M. (2010). The analytic hierarchy process and analytic network process: an overview of applications. *Management Decision*, *48*(5), 775-808.
13. Kumar, R., Khan, S. A., & Khan, R. A. (2016). Analytical network process for software security: a design perspective. *CSI transactions on ICT*, *4*(2-4), 255-258.
14. R. Kumar, S. A. Khan, R. A. Khan, Revisiting software security: durability perspective, in: inter. jour. of hyb. info. tech. (SERSC) 8(2), (2015), pp. 311-322.
15. Alenezi, M., Kumar, R., Agrawal, A., & Khan, R. A. (2019). Usable-security attribute evaluation using fuzzy analytic hierarchy process. *ICIC Express Lett.*-An *Int. J. Res. Surv.*, *13*(6).
16. Alharbe, N., Atkins, A. S., (2014). A Study of the Application of Automatic Healthcare Tracking and Monitoring System in Saudi Arabia, International Journal of Pervasive Computing and Communications , Vol. 10, Issue 2, pp. 183-195.
17. Rajeev Kumar, Mohammad Zarour, Mamdouh Alenezi, Alka Agrawal, Khan R.A., (2019), Measuring Security-Durability through Fuzzy Based Decision Making Process, International Journal of Computational Intelligence Systems, June, 2019.
18. Alka Agrawal, Mamdouh Alenezi, Suhel Ahmad Khan, Rajeev Kumar, Khan R.A., (2019), Multi-level Fuzzy System for Usable-Security Assessment, Journal of King Saud University - Computer and Information Sciences, April 2019.
19. Kavita Sahu, R. K. Srivastava, Revisiting Software Reliability, Advances in Intelligent Systems and Computing, Springer, 2019.
20. R. Kumar, S. A. Khan, R. A. Khan, (2016) Durability Challenges in Software Engineering, Crosstalk-The Journal of Defense Software Engineering, pp. 29-31.
21. R. Kumar, S. A. Khan, R. A. Khan, (2015) Revisiting Software Security Risks, British Journal of Mathematics & Computer Science, Volume 11, Issue 6, 2015.
22. Kavita Sahu, Rajshree, Rajeev Kumar, (2014) Risk Management Perspective in SDLC", International Journal of Advanced Research in Computer Science and Web based healthcare management system Engineering, pp. 1247-1251.
23. R. Kumar, S. A. Khan, R. A. Khan, (2015) Durable Security in Software Development: Needs and Importance, CSI Communication, pp. 34-36, Oct 2015.
24. Kavita Sahu, R. K. Srivastava, Soft Computing Approach for Prediction of Software Reliability, ICIC Express Letters-An International Journal of Research and Surveys, , pp. 1213-1222, 2018.

## AUTHOR PROFILE

**Dr. Nawaf R. Alharbe** is an assistant professor with the Community College at Taibah University in Saudi Arabia. He got PhD degree in health informatics from Staffordshire University, UK and an MSc degree in advanced computing science. Dr. Alharbe is a passionate researcher and has also published a number of research papers in national and international journals both. He has research/ teaching experience of more than 10 years. His areas of research include knowledge management, RFID, Zigbee, Digital transformation and sensor technology in healthcare environment.