


# Security Risk Assessment of Healthcare Web Application Through Adaptive Neuro-Fuzzy Inference System: A Design Perspective

This article was published in the following Dove Press journal:  
*Risk Management and Healthcare Policy*

Jasleen Kaur <sup>1</sup>  
Asif Irshad Khan <sup>2</sup>  
Yoosef B Abushark <sup>2</sup>  
Md Mottahir Alam <sup>3</sup>  
Suhel Ahmad Khan<sup>4</sup>  
Alka Agrawal <sup>1</sup>  
Rajeev Kumar <sup>1</sup>  
Raees Ahmad Khan <sup>1</sup>

<sup>1</sup>Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, UP, India;

<sup>2</sup>Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia; <sup>3</sup>Department of Electrical & Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah, Saudi Arabia;

<sup>4</sup>Department of Computer Science, Indira Gandhi National Tribal University, Amarkantak, MP, India

**Introduction:** The imperative need for ensuring optimal security of healthcare web applications cannot be overstated. Security practitioners are consistently working at improvising on techniques to maximise security along with the longevity of healthcare web applications. In this league, it has been observed that assessment of security risks through soft computing techniques during the development of web application can enhance the security of healthcare web applications to a great extent.

**Methods:** This study proposes the identification of security risks and their assessment during the development of the web application through adaptive neuro-fuzzy inference system (ANFIS). In this article, firstly, the security risk factors involved during healthcare web application development have been identified. Thereafter, these security risks have been evaluated by using the ANFIS technique. This research also proposes a fuzzy regression model.

**Results:** The results have been compared with those of ANFIS, and the ANFIS model is found to be more acceptable for the estimation of security risks during the healthcare web application development.

**Conclusion:** The proposed approach can be applied by the healthcare web application developers and experts to avoid the security risk factors during healthcare web application development for enhancing the healthcare data security.

**Keywords:** healthcare web application, security risk assessment, fuzzy systems, neural network, adaptive neuro-fuzzy inference system

## Introduction

Evaluating and mitigating the security risks in healthcare web applications has become the prime concern of researchers and security practitioners around the world. Several statistics have revealed that the instances of data breaches in the context of healthcare have jeopardised both the patients and the hospital management systems. Pilfering and poaching of any data is a grave crime; more so when the highly classified information of patient's medical report is breached and tampered with, it can result in fatal consequences as it would affect the patient's treatment procedures. Dedicated efforts are being made to enhance healthcare web application security in order to increase the accountability and determine whether and to what extent our investments in products and processes are making our systems more secure. In most of the cases, 'compromising on designs' has been observed to be one of the major security risks.<sup>1</sup> In order to reduce the "time-to-market", the developers tend to rush the designing phase. As a result, security is not often engineered into the product and is also not the elemental concern

Correspondence: Rajeev Kumar  
Email rs0414@gmail.com

during the developmental process of the web applications. This norm presents before us a dire need to consider security during early developmental stages. According to Gary McGraw,<sup>2</sup> the three pillars of the application security are risk management framework, Touchpoints and knowledge. So, if one wants to upgrade security, risk management is one of the fundamental approaches to be emphasized upon. Risk management helps in proper planning of the possible security risks at the time of application development, thereby helping the developers in prioritizing risks and taking proactive measures to avoid them.<sup>3</sup>

There are several risk assessment approaches; however, each is imbued with a set of limitations that often hamper the efforts of security practitioners. Different risk assessment approaches include preliminary hazard analysis (PHA), failure mode and effects analysis (FMEA), failure mode, effects and criticality analysis (FMECA), event trees, fault tree analysis (FTA), critical incident technique, decision tree analysis (DTA) and probabilistic risk assessment.<sup>4</sup> PHA is deployed in an organization to determine the risks associated with events that occurred in the past. FMEA is not applicable at the initial phases of development,<sup>5</sup> while the FMECA can only be performed after performing FMEA, and FTA is mostly considered as a reactive approach. The Critical Incident Technique is not very illustrative.<sup>6</sup> DTA results are dependent upon the planning and decisions; therefore it is prone to errors.<sup>7</sup> ANFIS, on the other hand, is a hybrid system consisting of both fuzzy logic and neural networks. Being a hybrid system, it contains the connectionism and adaptivity of neural networks with the human-like reasoning of a fuzzy system. At present, it is being deployed in several medical prognosis and treatment procedures. For instance, ANFIS technique is used to: determine the blood sugar levels of a diabetic person<sup>8</sup> predict the duration of stay in ICU at the time of cardiac arrest<sup>9</sup> assure security in web-based neuroscience applications;<sup>10</sup> predict chronic kidney disease<sup>11</sup> and assess the risk in software projects which find their application in healthcare scenario.<sup>12</sup> The empirical study undertaken in this research endeavour also found that the proposed ANFIS provides a better estimation of the security risks at early developmental phases.

The paper starts with the problem formulation section followed by the research contributions made by the authors. The next section discusses the various studies conducted in this domain and then, the methodology for security risk evaluation during secure healthcare web application development has been discussed in detail. Further, the security risk factors of healthcare web application identified at design phase based on literature review and experts' suggestions are mentioned. Next section

enlists the empirical aspects and the findings. Finally, the obtained results are discussed followed by the conclusion of the research work.

## Problem Formulation

Risk may be defined as the potential for loss or damage when a threat exploits vulnerability.<sup>13</sup> For risk management, developers usually rely upon understanding and experience and do not apply proper risk management mechanisms. The need for the risk management can only be judged if one gets to know the extent of severity of the occurrence of any event. As per this research endeavour, the main concern of the researchers is to focus on the “security” risks that may affect the security of a healthcare web application. Healthcare data, being sensitive in nature, may lead to serious security issues. The healthcare information security breaches in 2016 have affected more than 27 million patients globally.<sup>14</sup> With an enormous increase in digitization, the healthcare stakeholders are largely dependent upon the Internet-enabled applications for their health. The demand for a secure application is thus the top priority for them. Assessing security risks at the design phase will nip the security risks in the bud and help in the development of a secure application. Therefore, as the first priority, the researchers of the present study have identified the security risks at the design phase by discussing with the experts. Thereafter, the impact of these risk factors has been gauged through ANFIS.

## Research Contributions

There are many classifications for security risk management in healthcare web application development. The key levels are: Literature review; Security Risk Identification; Security Risk Analysis, Security Risk Assessment; Security Risk Action; Review and revision.<sup>15</sup> The authors have also followed a similar workflow in this research work. Initially, the security risks existing at the design level have been selected through experts' suggestions from the Common Weaknesses Enumeration (CWE) list.<sup>16</sup> Further, the given risks have been quantitatively analysed through an adaptive neuro-fuzzy inference system (ANFIS) technique. Based on the above discussion, various research contributions made by the authors are as follows:

- (a) The authors have identified the different security risks that may exist during the early developmental phases of healthcare web application. Experts' opinions have been collated for compiling this list.

- (b) An adaptive neuro-fuzzy technique for security risk evaluation of web healthcare applications is proposed.
- (c) The different security risks are evaluated through the proposed ANFIS technique.
- (d) The estimation is validated with the help of fuzzy regression modelling .

## Related Work

Several noteworthy research initiatives have been undertaken in the context of security risk management and this domain continues to be the foci of the security experts and researchers.<sup>17</sup> However, the quantification of the security risk factors through the previous approaches is extremely challenging.<sup>18,19</sup> There are several studies that have implemented the neuro-fuzzy technique for estimating the results. For example, Wang et al<sup>20</sup> have stated that for assessing the actual security of any healthcare web application, proper quantification is mandatory which itself is a very complex procedure. Praynlin et al<sup>21</sup> and Sangaiah et al<sup>22</sup> divided the neuro-fuzzy into two major types of fuzzy models which are required for assessment of security risks. The models propositioned were traditional models and conceptual models based on fuzzy sets analysis.

Sonia et al<sup>23</sup> proposed a method for security risk evaluation. With the help of fuzzy numbers, the researchers have measured the security risks of healthcare web application. For example, Ming-Chang Lee has used sets during management of security risk.<sup>24</sup> Dark et al<sup>25</sup> have applied the fuzzy set theory that evaluates the cost and time performance, security risk management and utilization of healthcare web application development scheme. Shedden et al<sup>26</sup> utilized the structure of security risk for qualitative assessment of security risk of healthcare web application. Guan et al<sup>27</sup> proposed a fuzzy-based procedure for security risk evaluation and have used drawings for designing the security risk models.

Some researchers have also used the fuzzy inference idea for stating the unpredictability and analytic hierarchy process technique for making structure. Furthermore, they have used this structure for ranking the alternative risk factors security during the healthcare web application development.<sup>28</sup> Some have made use of assembled fuzzy based decision-making method for security risk assessment,<sup>29</sup> while others have used the fuzzy analytic hierarchy process technique for assessment of security risks.<sup>30</sup> However, these research studies also have their share of flaws. Most of these studies do not consider the inaccuracy of the experts while citing their opinions.

Existing models of security risk analysis for secure healthcare web application development are limited. Nowadays, many decision-making problems remain debatable for the developers.<sup>18-20</sup>

The nature of development of healthcare web application is accompanied by imposed uncertainties which largely depend upon a person's thought process about the security risk management during healthcare web application development. In continuation with the above issues, Jang et al<sup>31</sup> proposed the introductory study in neural network in the field of security risk in 1993. The researchers used the neural network for identification of security risk. van Staalduinen et al<sup>32</sup> have applied a network of neural fuzzy for evaluation of security risk during secure healthcare web application development. Gao et al<sup>33</sup> proposed a novel method for security risk evaluation that makes use of K-means clustering algorithm.

From the above discussion, it is obvious that the implementation of the hybrid neuro-fuzzy technique is expected to provide a better estimation of security risk in the early phases of development of a web application. The use of this technique would reduce the cost and effort invested in developing the security characteristics in a given healthcare web application. Therefore, the researchers have proposed a risk management hybrid scheme with the connectivity of neural networks and human-like behaviour of a fuzzy system, so as to reduce the security risks at the early stages of the healthcare web application development life cycle.

## Methodology

This research work aims at determining the systematic ranking of security risk factors more efficiently than the various existing methods. The approach is also intended to help the developers in executing sensitivity analysis for security risk factors. The accuracy is also claimed to be high. The methodology is as follows:

**Security risk factors identification:** Locating the security risks at design phase of healthcare web application development.

**Data collection:** Collecting the essential data related to the identified security risk factors.

**Security risk evaluation:** By implementing ANFIS.

**Performance evaluation:** Estimating the proposed ANFIS.

**Validation:** Validating the acquired results.

**Figure 1** maps the step-by-step methodology undertaken for this study. The first step involves the identification of the security risk factors with the help of the experts'

suggestions. As per the severity level of these risk factors, a Common Weaknesses Enumeration (CWE), a list of the common healthcare web application security weaknesses is developed. Secondly, the data for risk analysis are collected with respect to the identified security risks through the questionnaire. Then, the security risk is evaluated through ANFIS. Thereafter, the performance of the proposed ANFIS is estimated and lastly, the results obtained are validated with the help of the fuzzy multiple regression modelling.

The results obtained through ANFIS are compared with those obtained from Fuzzy Multiple Regression Modelling. Multiple regression equation for each security risk factor is then calculated in order to estimate the association between the results and the independent variables. The correlative results obtained thereby prove that ANFIS, the hybrid learning approach, may be considered as highly efficient and precise in estimating the healthcare web application security risk at the early stages of web development.

## Security Risk Factor Identification

In the proposed research work, the security risks that exist at the design phase of healthcare web application development life cycle have been identified.<sup>16</sup> For this, the researchers garnered the suggestions of the experts who cited the major causes of security risks that are likely to be introduced at the design phase. Table 1 consists of eight significant security risks with their detailed description and related security factor.

## Empirical Study

An empirical study is the collection and analysis of primary data based on direct observations. Moreover, the empirical approach may be regarded as a way to give quantified evidence to the usefulness of the methodology. The researchers have therefore adopted such a study so as to quantify the observations and legitimize the efforts devoted to accomplish the intended objective. Thus, this

section of research has been subdivided into the following sections which are enunciated below.

### Data Collection

The knowledge database includes knowledge of academia experts and cybersecurity professionals from the industry.<sup>42</sup> The questionnaires were distributed amongst 100 experts having experience of about 10 years and finally, 51 valid questionnaires were collected on the basis of completeness and precision (Appendix). As the knowledge obtained was usually linguistic in nature, a pre-processing was required in order to convert this knowledge to numerical data. It has been emphasized by various researchers that what cannot be measured, cannot be controlled.<sup>43</sup> Hence, meticulous calculations have been enlisted in this study to elicit corroborative results. The matrix representation of severity with respect to the probability of the security risk factors is in Table 2. For calculating the magnitude of security risk for each factor with respect to the linguistic variable, authors have used the fuzzy values table created from Chang and Lee.<sup>44</sup> Table 3 represents the fuzzified numeric values of security risks.

Further, the triangular fuzzy numbers (TFNs) are used for converting the linguistic values into the numerical values. In addition, Table 3 shows the linguistic values that are in the form of semantic variables including probability of occurrence; severity and security risk. Finally, after the conversion of the linguistic variables into TFNs, the Centre of Area (COA) method has been applied for de-fuzzifying the TFN into corresponding values of BNP, where BNP is the best non-fuzzy performance of the security risk and  $F = (f_i, f_m, f_h)$  shows a TFN and is evaluated using equation 1.

$$F = [(f_h - f_i) + (f_m - f_i)]/3 + f_i \quad (1)$$

The detailed description of these techniques has been illustrated further. The data based on the opinions of the first expert are presented in Table 4. Table 2 helps in quantifying the security risk factor (third column of Table 4). The



Figure 1 Methodology adopted.

**Table 1** Security Risk Factors at Design Phase

SN	Security Risk at Design Phase	Definition	Related Security Factor
1.	Access to Critical Private Variable via Public Method (ACPVPM)	A public method that can read or modify a private variable is defined by the healthcare web application. <sup>34</sup>	Access control
2.	Password in Configuration File (PCF)	Password is stored in the configuration file, thereby making it prone to be misused by any outsider. <sup>35</sup>	Authentication
3.	Critical Variable Declared Public (CVDP)	Any critical variable/field is declared as public when intended security policy requires it to be private. <sup>36</sup>	Confidentiality
4.	Unverified Password Change (UPC)	No authentication mechanism is followed while setting a new password for a user. <sup>37</sup>	Authentication
5.	Race Condition within a Thread (RCT)	If any resource is being used simultaneously then there is a possibility that resources may be used while invalid and this makes the state of execution undefined. <sup>38</sup>	Integrity
6.	Untrusted Search Path(USP)	An externally supplied search path is being used for critical resources that can point to resources that are not under the application's direct control. <sup>39</sup>	Confidentiality; integrity; availability; access control
7.	Download of Code Without Integrity Check (DCWIC)	An executable source code is downloaded from any remote location without checking the origin and integrity of the code. <sup>40</sup>	Integrity; confidentiality
8.	External Initialization of Trusted Variables or Data Stores (EITV)	The healthcare web application initializes critical internal variables or data stores using inputs that can be modified by suspicious actors. <sup>41</sup>	Integrity

**Table 2** Matrix Representation of Security Risk

<u>Severity</u>	<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Catastrophe</u>
<u>Prob.</u>					
Very Unlikely	L	L	M	S	S
Unlikely	L	L	M	S	H
Even	L	M	S	H	H
Likely	M	S	S	H	H
Very Likely	S	S	H	H	H
L = Low; S = Significant; M = Medium; H = High					

**Abbreviations:** L, low; S, significant; M, medium; H, high.

arithmetic values including probability of occurrence; severity and size of every factor of security risk can be evaluated with the collective help of Table 3 and BNP method.

The same procedure is then repeated for 51 experts, and the knowledge database is created. Here, the authors have assumed that the data is normally distributed. We know that if the data are assumed to be normally distributed, ie,  $N(0, \sigma^2)$ , its histogram should have a plot like normal distribution with mean zero.

Figure 2 represents the normal probability illustration and the probability illustration of residuals for “risk

probability” and Figure 3 is about the normal probability and residuals diagrams for “risk severity” for the first factor “ACPVPM”. The plots clearly represent that the opinions of experts convey normal distribution. A similar method has been implemented on the other seven security risk factors. The results in all cases depict that the observations are normally distributed.

### Security Risk Assessment and Prediction Through Fuzzy Regression Modelling

The authors have used the Multiple Regression Model as each of the inputs is found to be less correlated with the

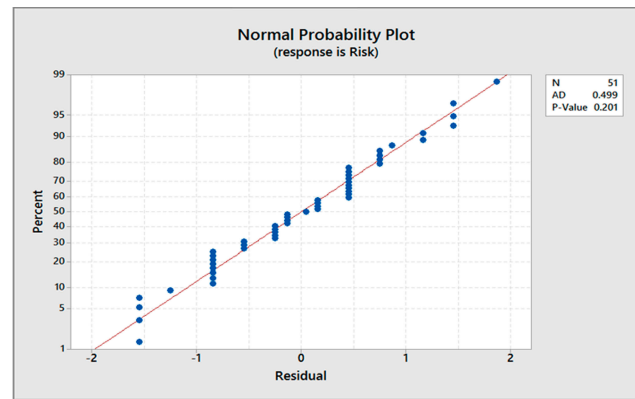
**Table 3** Linguistic and Fuzzy Values

Linguistic Value	Fuzzy Value
Linguistic Variables (Probability of Security Risk Occurrence)	
Very Unlikely (VU)	(0.0000, 0.1230, 0.2500)
Unlikely (U)	(0.1250, 0.2500, 0.3500)
Even (E)	(0.3250, 0.4800, 0.7500)
Likely (L)	(0.5500, 0.7000, 0.8500)
Very likely (VL)	(0.7500, 0.8720, 1.0000)
Linguistic Variables (Severity of Security Risk Occurrence)	
Very little (VL)	(0.0000, 1.2500, 2.5000)
Little (L)	(1.2800, 2.7500, 4.2500)
Medium (M)	(3.2400, 4.7500, 6.1800)
High (H)	(5.4600, 7.0000, 8.3000)
Catastrophic (C)	(7.5000, 8.7500, 10.0000)
Linguistic Variables (Security Risk Value)	
Low (L)	(0.0000, 0.1600, 0.3300)
Medium (M)	(0.1500, 0.3500, 0.5000)
Significant (S)	(0.3800, 0.5800, 0.7500)
High (H)	(0.6000, 0.8300, 1.0000)

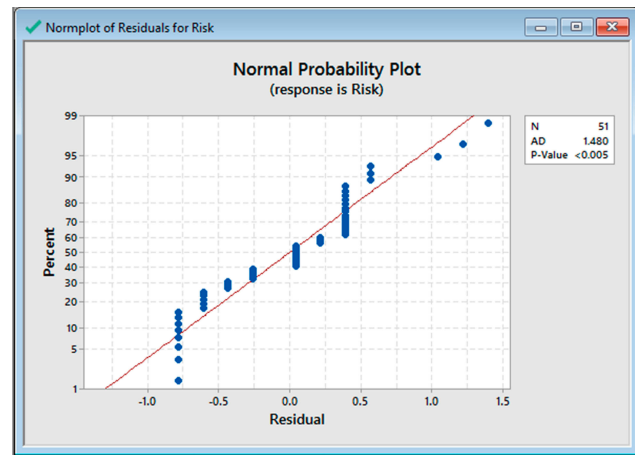
output variable. With the help of MINITAB 18, the step-wise regression technique evaluated the first security risk factor of “ACPVPM” during the healthcare web application development.<sup>45</sup> Figure 4 represents the recommended fuzzy system for assessment of security risk.

**Security Risk Assessment and Prediction by ANFIS**

As the quantification helps in analysing the effect of the risk outcomes on the security of the healthcare web application, we can say that the magnitude of each security risk is a function of probability of its occurrence.<sup>42</sup> Therefore,



**Figure 2** Normal probability plot for probability of security risk occurrence.



**Figure 3** Normal probability plot for severity of security risk.

for the procedure of fuzzy systems design through neural network, the researchers have considered the probability of security risk occurrence and its severity as the inputs, and the magnitude of security risk as the output of system.

**Table 4** Probability and Severity Given by Expert I for Each Security Risk Factor

Sec. Risk	Coded Linguistic Variable			Numerical Value		
	Probability	Severity	Security Risk	Probability	Severity	Security Risk
ACPVPM	4	4	4	0.7000	7.0000	0.8300
PCF	4	4	4	0.7000	7.0000	0.8300
CVDP	3	3	1	0.4800	4.7500	0.1600
UPC	3	3	1	0.4800	4.7500	0.1600
RCT	5	5	4	0.8720	8.7500	0.8300
USP	4	4	4	0.7000	7.0000	0.8300
DCWIC	4	4	2	0.7000	7.0000	0.8300
EITV	3	4	3	0.4800	7.0000	0.5800

Code  
 Probability: 1 – very unlikely; 2 – unlikely; 3 – even; 4 – likely; 5 – very likely.  
 Severity: 1 – very little; 2 – little; 3 – medium; 4 – high; 5 – catastrophic.  
 Risk: 1 – low; 2 – medium; 3 – significant; 4 – high.

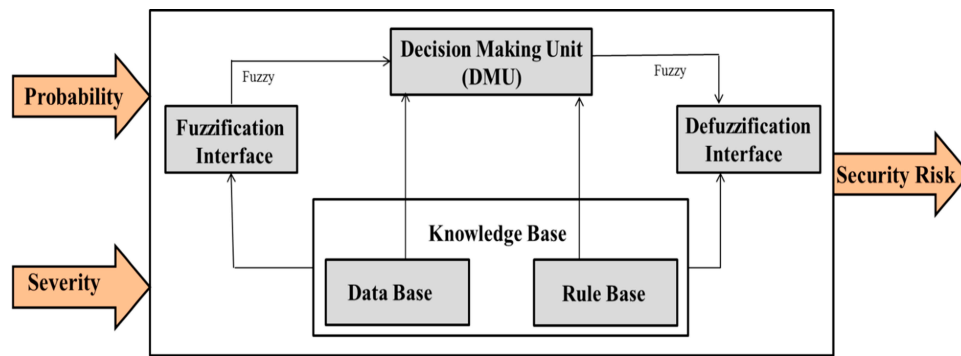


Figure 4 Security risk assessment using the proposed fuzzy system.

Figure 5 shows the diagrammatic representation of this fuzzy system with two inputs and one output.

Linear relation is used between these inputs; this is given in the equations (2) and (3):

$$\text{If (xis A1) AND (y is B1), then } \{f1 = p1x + q1y + r1\} \quad (2)$$

$$\text{If (x is A2) AND (y is B2), then } \{f2 = p2x + q2y + r2\} \quad (3)$$

where A1, A2, B1 and B2 are the membership functions of each of the inputs of x and y; and p1, p2, q1, q2, r1 and r2 are the linear parameters of then-part of the system.

ANFIS consists of five different layers that have their own respective significances. The nodes in the first and fourth layer are meant to adapt to the function parameter while every node in the second, third and the fifth layer is non-adaptive in nature.<sup>45</sup> The design of these systems is based on the information that system parameters and fuzzy values are calculated logically with the help of the neural network. Neuro-fuzzy systems utilize two algorithms including hybrid learning and error back-propagation so as to relate input and output values.<sup>46</sup> The basic flaw of this technique is that the system is required to be trained.<sup>47</sup> Further, the least square method has been used by the

authors to derive the best parameters. It is already known that if the membership functions of inputs are not known, the solution space will be very large. So, the convergence will turn out to be a time taking process because then it will be performed in two steps viz. forward step (for calculation of errors) and backward step (for operating the parameters).

### Performance Evaluation

In this section, the researchers have explained how the security risk is being assessed through the proposed technique and how its performance is being evaluated. The authors have used 80% (40) of these data for the training purpose and the remaining 20% (10) has been applied for testing the system.<sup>48</sup> The ANFIS structure of the proposed system has been shown in Figure 6. The logic operator, AND has been taken in joining the rules. A code has been programmed in MATLAB 18 healthcare web applications for the same.<sup>45</sup> Finally, the output of the program (the ideal membership functions for probability of occurrence, security risk severity, etc.) is obtained.

Minimum error occurrence has been considered as the basis for the selection of best membership function. The

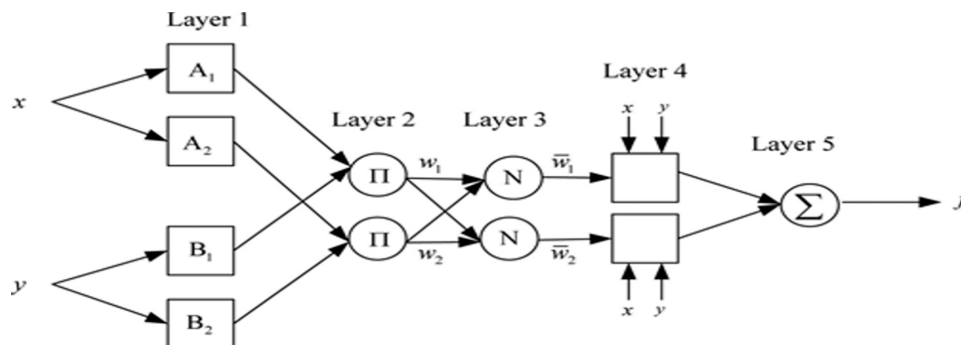


Figure 5 Layered structure of neuro-fuzzy system.

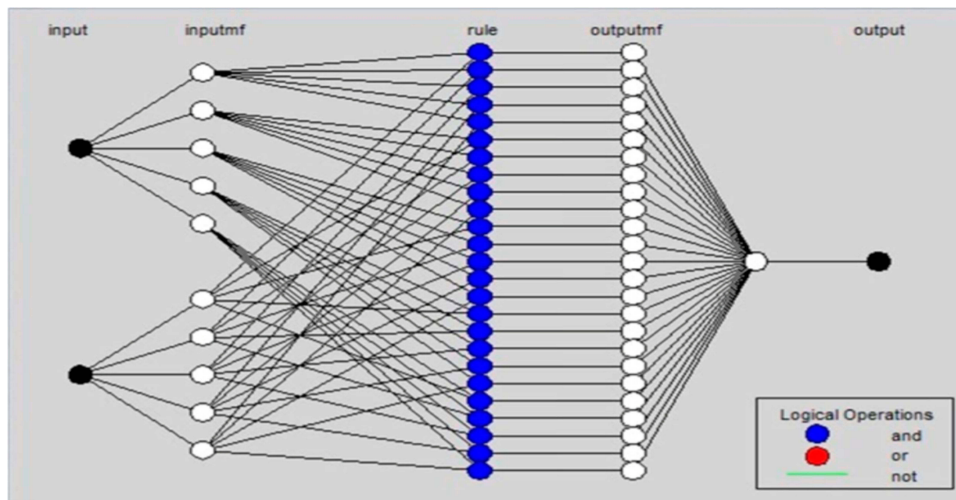


Figure 6 ANFIS structure.

performance of the designed fuzzy system has been evaluated on the basis of two types of errors, viz., RMSE (Root Mean Squared Error) and MSE (Mean Squared Error). The correlation coefficient, R between the obtained data and the data predicted by ANFIS has been calculated as per the given formulae (equations (4) to (6)).

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (X_{obs,i} - X_{model,i})^2}{n}} \tag{4}$$

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \bar{y}_i)^2 \tag{5}$$

$$R = \frac{[\sum_{i=1}^n (A_i - A') (F_i - F')]}{[\sqrt{\sum_{i=1}^n (A_i - A')^2 \sum_{i=1}^n (F_i - F')^2}]} \tag{6}$$

where  $A_i$ ,  $F_i$  and  $n$  denote the obtained data, predicted data and the frequency of observations, respectively. Similarly,

$$A' = \left(\frac{\sum_{i=1}^n A_i}{n}\right) \text{ and } F' = \left(\frac{\sum_{i=1}^n F_i}{n}\right)$$

Table 5 Performance of ANFIS for Security Risk Factors at Design Phase

Security Risk	RMSE	MSE	R
ACPVPM	0.0107	0.01145	1.0000
PCF	0.0277	0.000767	1.0000
CVDP	0.018	0.000324	1.0000
UPC	0.0049	0.00002401	1.0000
RCT	0.0242	0.00058564	1.0000
USP	0.0696	0.004844	1.0000
DCWIC	0.0296	0.00087616	1.0000
EITV	0.11080	0.01227664	1.0000

Table 5 shows the implementation of alternative situations with their errors.

### Prediction and Sensitivity Analysis

The significance of prediction is that it helps in estimating the intermediate as well as the overall outcome of the proposed analysis. Table 6 shows the security risk prediction of each security risk factor and the overall security risk of the proposed model. Sensitivity analysis provides the researchers with the test of robustness of the model. The overall sensitivity analysis, ie, probability and severity of the occurrence of each security risk have been clearly shown in Table 7.

### Validation of Security Risk Assessment Through Fuzzy Multiple Regression Modeling

Validation and verification of the technique being used for solving any problem needs comparison of obtained results.

Table 6 Prediction of Overall Security Risk Through ANFIS

Security Risks	Probability	Severity	Security Risk	Security Risk Prediction	
				Security Risk Factors Model	Overall Security Risk
ACPVPM	2.7255	2.6862	2.3529	3.0387	3.0343
PCF	3.0196	3.0392	2.8235	3.0008	
CVDP	3.2156	3.0392	2.9607	3.0760	
UPC	2.9803	3.1372	2.8431	2.8745	
RCT	3.0588	2.8627	2.7647	2.9196	
USP	2.8823	2.6862	2.6078	3.0534	
DCWIC	2.8823	2.9607	2.6274	2.8169	
EITV	3.0980	2.7450	2.7843	3.4937	



**Table 7** Sensitivity Analysis of the Factors of Security Risk

Prob. of Occurrence			Severity of Occurrence		
Probability	Severity	Security Risk	Probability	Severity	Security Risk
0.1250	5.0000	2.7375	0.5000	1.2500	0.4747
0.2250	5.0000	2.7849	0.5000	2.2500	1.1255
0.3250	5.0000	2.8322	0.5000	3.2500	1.7763
0.4250	5.0000	2.8796	0.5000	4.2500	2.4271
0.5250	5.0000	2.9269	0.5000	5.2500	3.0779
0.6250	5.0000	2.9743	0.5000	6.2500	3.7287
0.7250	5.0000	3.0216	0.5000	7.2500	4.3795
0.8250	5.0000	3.0690	0.5000	8.2500	5.0303
0.9250	5.0000	3.1163	0.5000	8.7500	5.3557
1.0000	5.0000	3.1519			

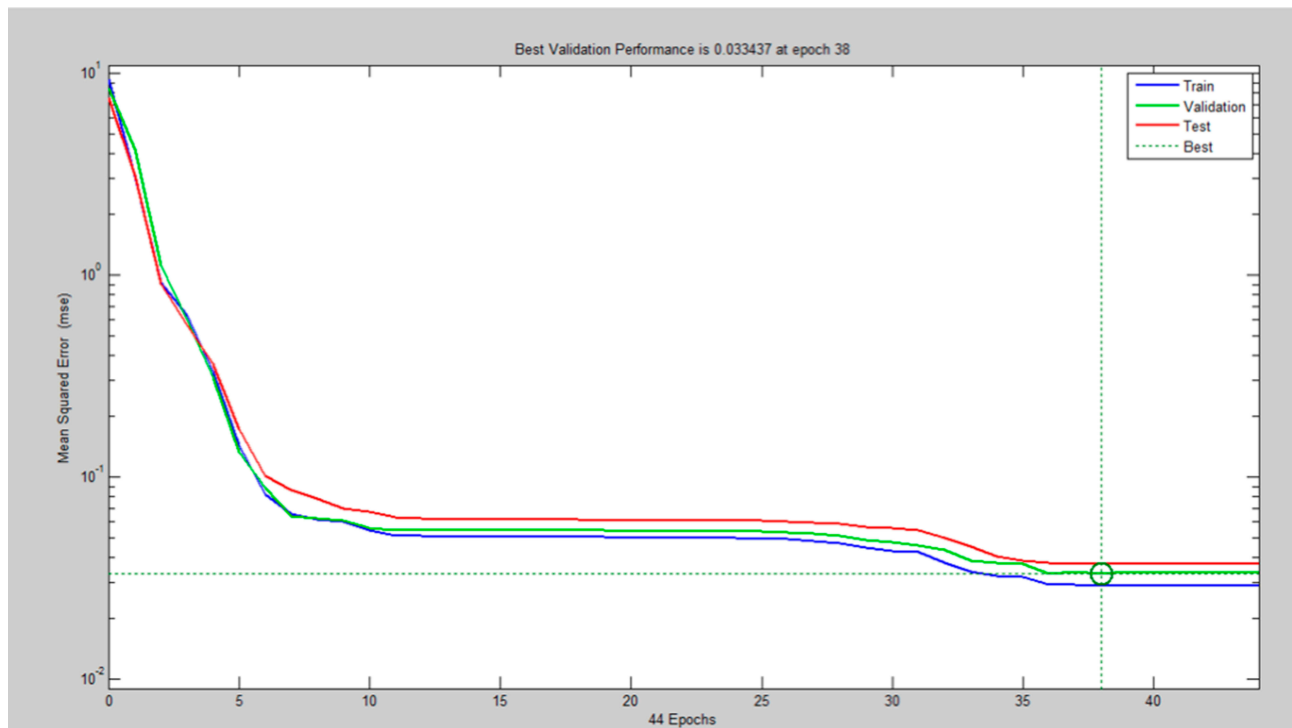
This comparison has to be between the method employed at present and the alternative methods that have already been enlisted earlier in the previous research studies. In the above case study, the authors have taken the ANFIS for assessment of security risk. The plot for validation against the training data has been shown in Figure 7. The circle in the plot clearly depicts that the validation plot lies exactly between the actual data plot and the observed data plot. Hence, the research work is said to be validated. Similarly, all the other security risk factors identified in Security Risk Factor Identification section of this paper have been analysed.

Normally, multiple regression equations (MRE) can be shown as equation (7).

$$\text{Security Risk} = b_0 + b_1 \times \text{Probability} + b_2 \times \text{Severity} \tag{7}$$

where  $b_0$  is a constant value, and  $b_1$  and  $b_2$  represent regression coefficients.

Table 8 shows the Multiple Regression Equations for each identified security risk factor, whereas Table 9 consists of the Multiple Regression Equation for security risk through the hierarchy. Table 10 depicts the prediction of overall



**Figure 7** Plot of validation against training data.

**Table 8** Multiple Regression Equation for Each Security Risk Factor

Security Risk	Multiple Regression Equation	R Squared Value
ACPVPM	Security Risk (ACPVPM) = -0.851+ 0.4741 Probability + 0.7117 Severity	90.99%
PCF	Security Risk (PCF) = -0.539+ 0.4571 Probability + 0.6521 Severity	84.01%
CVDP	Security Risk (CVDP) = -0.287+ 0.4410 Probability + 0.6021 Severity	81.52%
UPC	Security Risk (UPC) = -0.579+ 0.4549 Probability + 0.6558 Severity	87.71%
RCT	Security Risk (RCT) = -0.780+ 0.5457 Probability + 0.6552 Severity	87.90%
USP	Security Risk (USP) = -0.737+ 0.5063 Probability + 0.7017 Severity	88.41%
DCWIC	Security Risk (DCWIC) = -0.650+ 0.4170 Probability + 0.7008 Severity	90.72%
EITV	Security Risk (EITV) = -0.150+ 0.4555 Probability + 0.5550 Severity	89.25%

Security Risk through Fuzzy Multiple Regression Modelling. Table 11 shows the comparison of the obtained results through ANFIS and Fuzzy Multiple Regression model.

**Table 9** Multiple Regression Equation for Security Risk Through the Hierarchy

	Multiple Regression Equation	R Squared Value
Security Risk Evaluation Model	Security Risk = -0.5756+ 0.4735 Probability + 0.6508 Severity	87.03%

**Table 10** Prediction of Overall Security Risk Through Fuzzy Multiple Regression Modelling

Security Risks	Probability	Severity	Security Risk	Security Risk Prediction	
				Security Risk Factor Model	Security Risk Model (Overall)
ACPVPM	2.7254	2.6862	2.3529	2.3530	2.4631
PCF	3.0196	3.0392	2.8235	2.8231	
CVDP	3.2156	3.0392	2.9607	2.9610	
UPC	2.9803	3.1372	2.8431	2.8490	
RCT	3.0588	2.8627	2.7647	2.7648	
USP	2.8823	2.6862	2.6078	2.6072	
DCWIC	2.8823	2.9607	2.6274	2.6268	
EITV	3.0980	2.7450	2.7843	2.7846	

Figures 8–15 show the residual plots for individual security risk factors as identified in the previous sections. Figure 16 shows the residual plot for the security risk through hierarchy. Table 12 depicts the correlation between the results through ANFIS and multiple fuzzy regression modelling.

### Discussion

The medical data include information from vital signs such as heart rate, temperature, respiratory-rate, and blood-tests. If this data falls prey to any kind of cyber-attack, it can lead to serious security issues. As per a healthcare data security breach reported in January 2019, 1.57 million patients’ data of Inmediata Health Group were exposed because of misconfigured database.<sup>49</sup> A similar breach was notified by the University of Washington, Medicine, in February 2019 that affected 974,000 individuals. The reason behind this breach was also a misconfigured server.<sup>49</sup> The common loophole in both the breaches was misconfiguration of database/server and that could have been avoided if the security risks were evaluated at the design phase. Therefore, this research work intends to afford solutions for all security practitioners by propounding the use of ANFIS technique to assess the security risks at the time of designing a healthcare web application. The proper quantification of each security risk in the early stages will help the developers prioritize the risks and will result in the development of a more secure healthcare web application.

This study commenced its objective by identifying the eight major security risks that may persist during the design phase itself and are likely to affect the security of any healthcare web application. In the ensuing part of the study, these risks were assessed through the ANFIS technique. The overall security risk was calculated to be 3.03425. For corroborating and authenticating the efficacy of the proposed

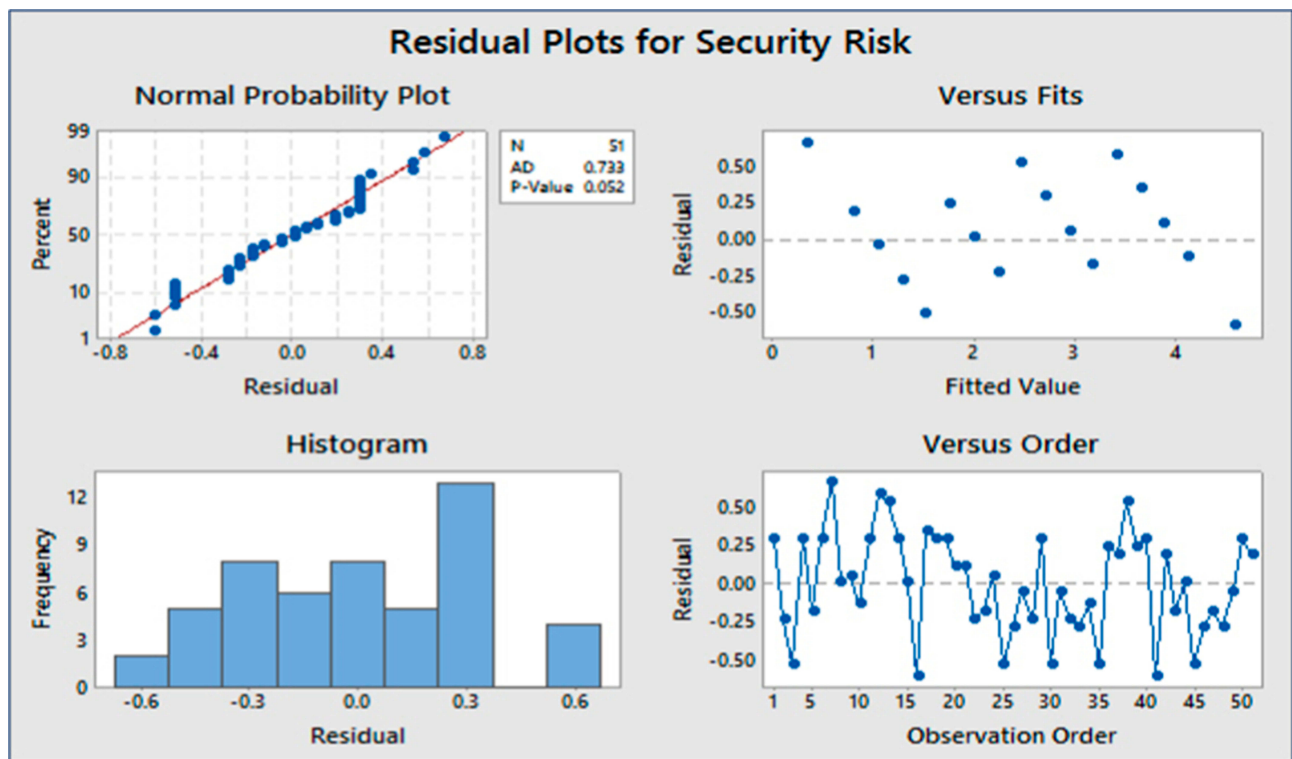
**Table 11** Comparison Between ANFIS [AS] and Fuzzy Multiple Regression Modelling [FM]

Security Risks	Probability	Severity	Security Risk	Security Risk Prediction			
				Security Risk Factor Model		Security Risk Model (Overall)	
				AS	FM	AS	FM
ACPVPM	2.7254	2.6862	2.3529	3.0387	2.3530	3.03425	2.4631
PCF	3.0196	3.0392	2.8235	3.0008	2.8231		
CVDP	3.2156	3.0392	2.9607	3.0760	2.9610		
UPC	2.9803	3.1372	2.8431	2.8745	2.8490		
RCT	3.0588	2.8627	2.7647	2.9196	2.7648		
USP	2.8823	2.6862	2.6078	3.0534	2.6072		
DCWIC	2.8823	2.9607	2.6274	2.8169	2.6268		
EITV	3.0980	2.7450	2.7843	3.4937	2.7846		

approach, the overall security risk value was estimated through multiple fuzzy regression modelling (2.4631) and the values obtained were compared (Table 11). The results obtained through both the approaches were found to be highly correlated (Table 12). This conclusively proves that employing the proposed ANFIS technique for security risk estimation at the initial stages of any healthcare web application would be highly effective. The only limitation of this study could be the unintentional exclusion of any important security risk factor as the selected risks are not all-inclusive.

### Conclusion

The proposed approach is basically for the security risk quantification so that the management of security risks existing at the design phase becomes easier for the developers. The advantages of the designed system are that this method is based upon the opinions of security professionals and experienced researchers. The implementation of artificial intelligence makes it a learning system. It can learn from past experiences and hence escalate its performance. It can be applied for both quantitative and



**Figure 8** Residual plot for ACPVPM.

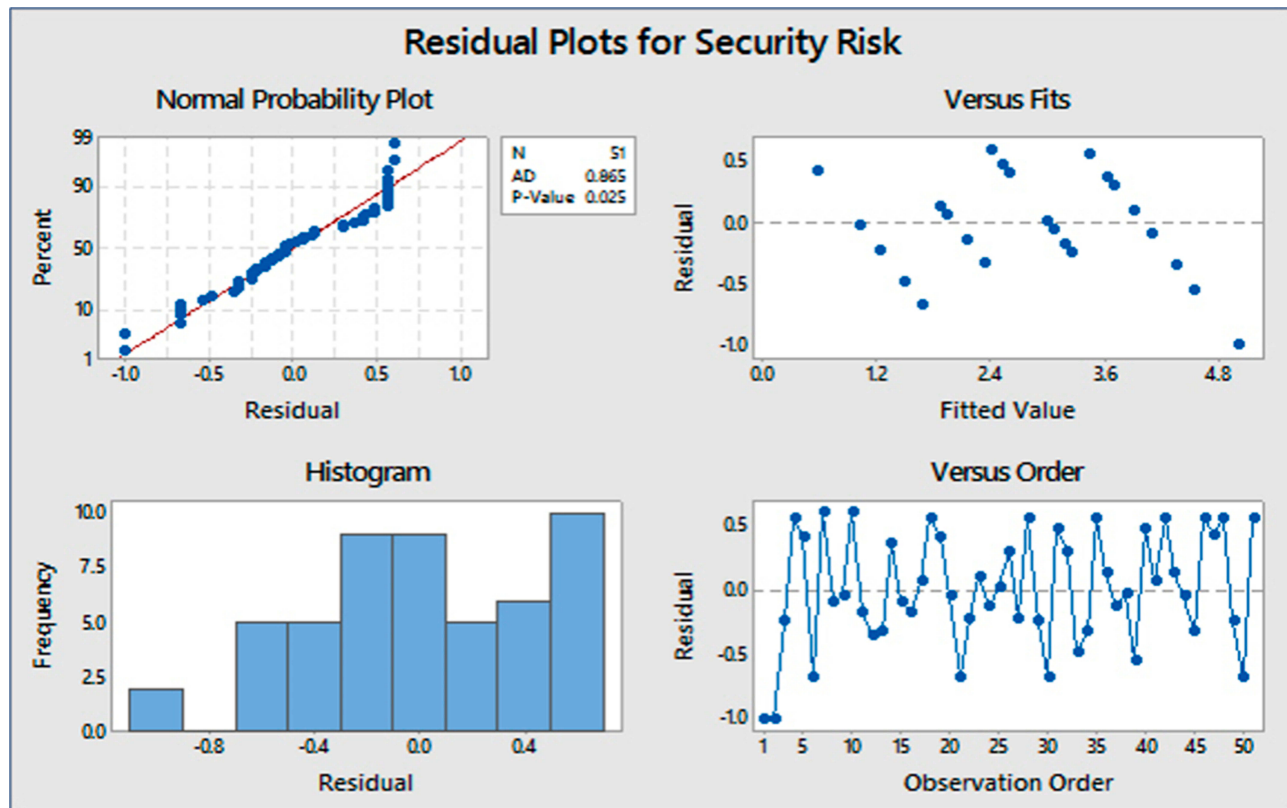


Figure 9 Residual plot for PCF.

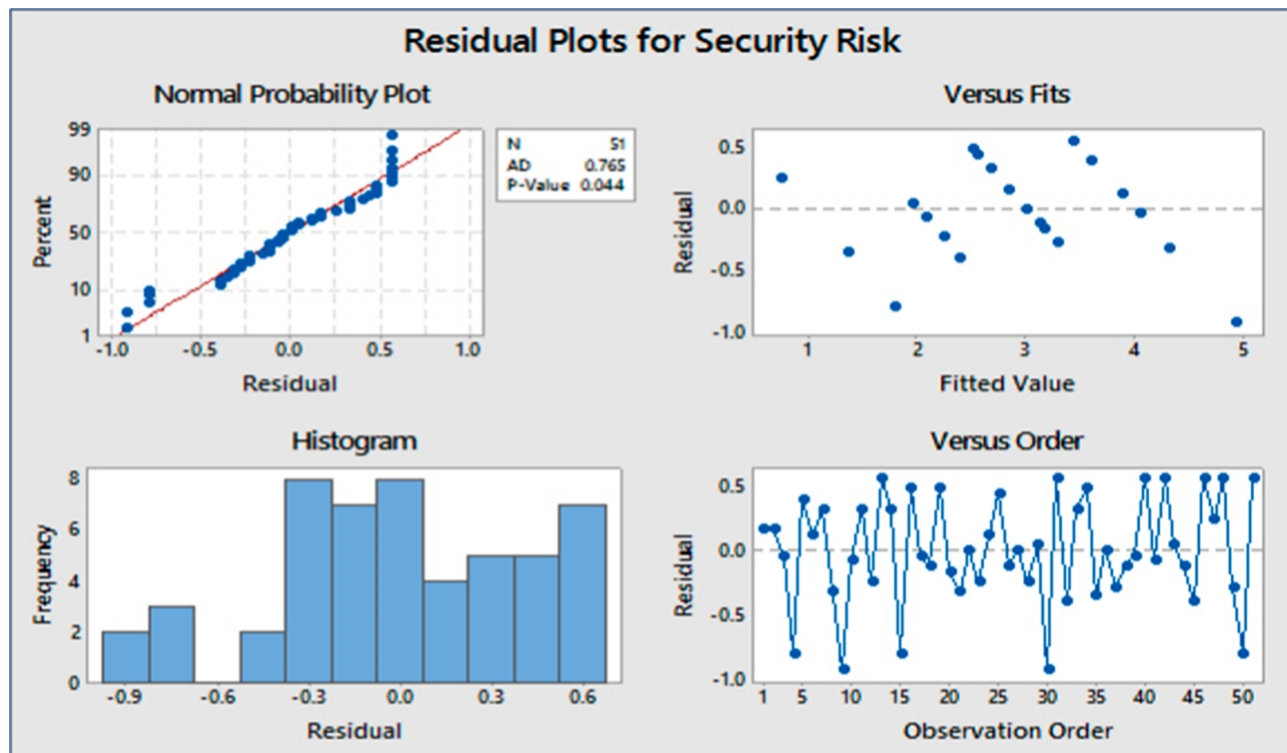


Figure 10 Residual plot for CVDP.

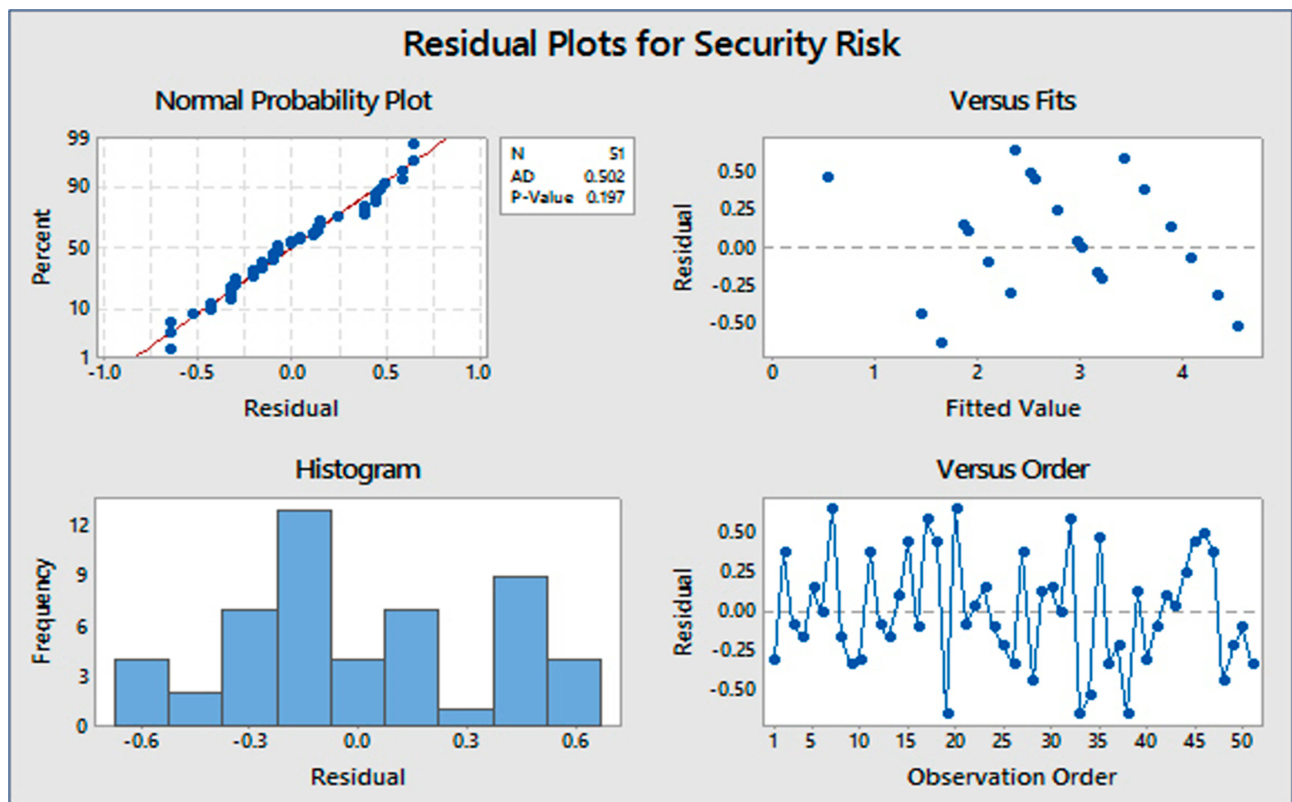


Figure 11 Residual plot for UPC.

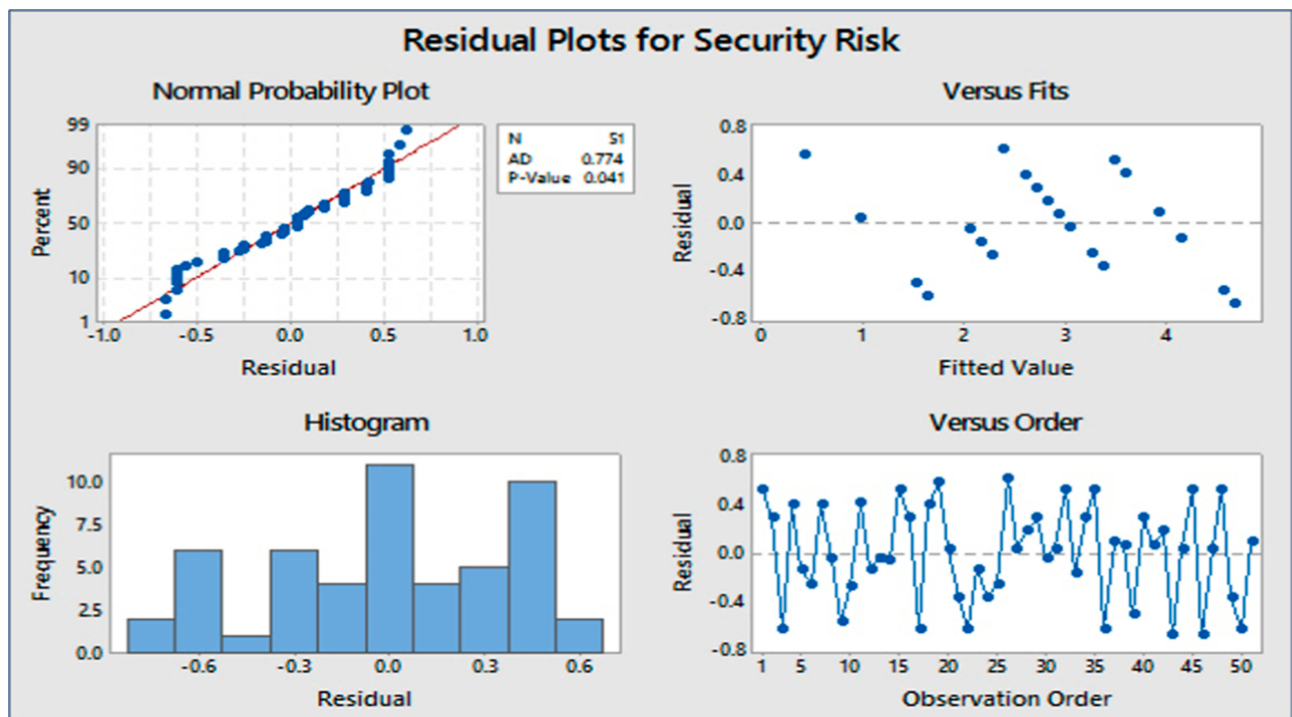


Figure 12 Residual plot for RCT.

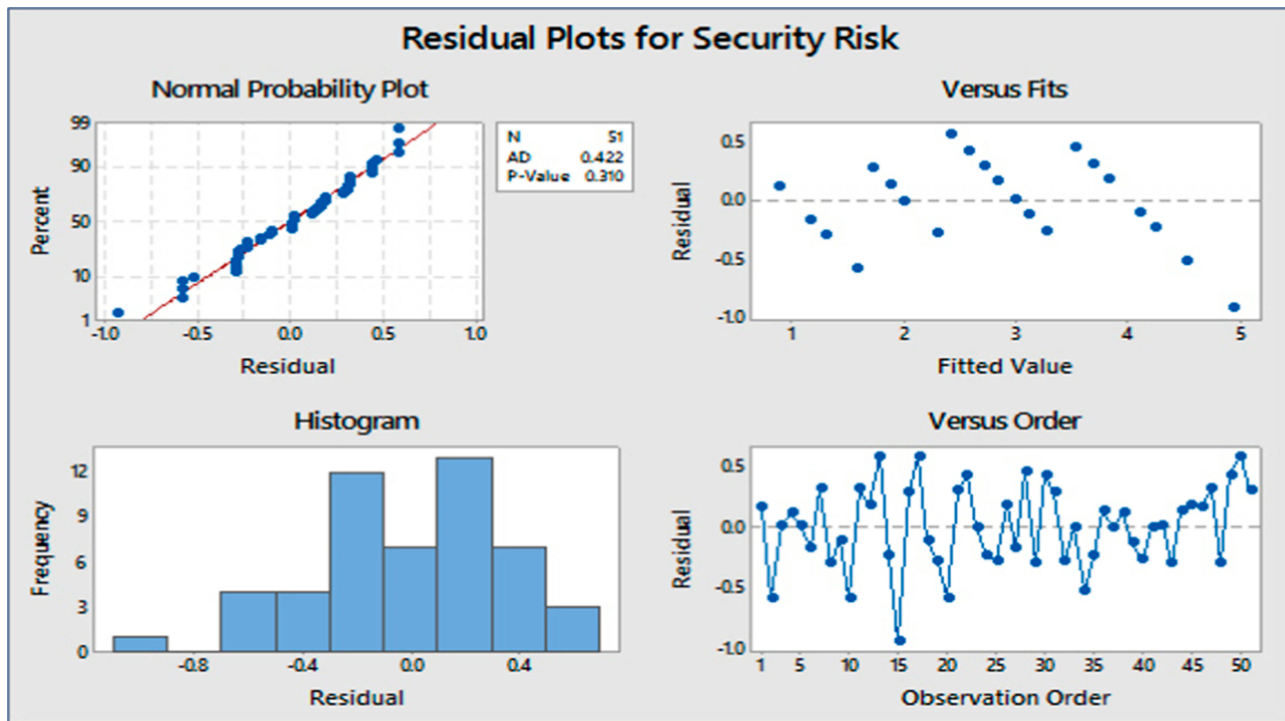


Figure 13 Residual plot for USP.

qualitative factors and thereby help in technical planning of security risks. The ranking of risks will be a major contribution of this system which will further help in

arranging the various risks into a proper hierarchical structure. The limitation of this research work is that the list of security risks identified by the researchers is not

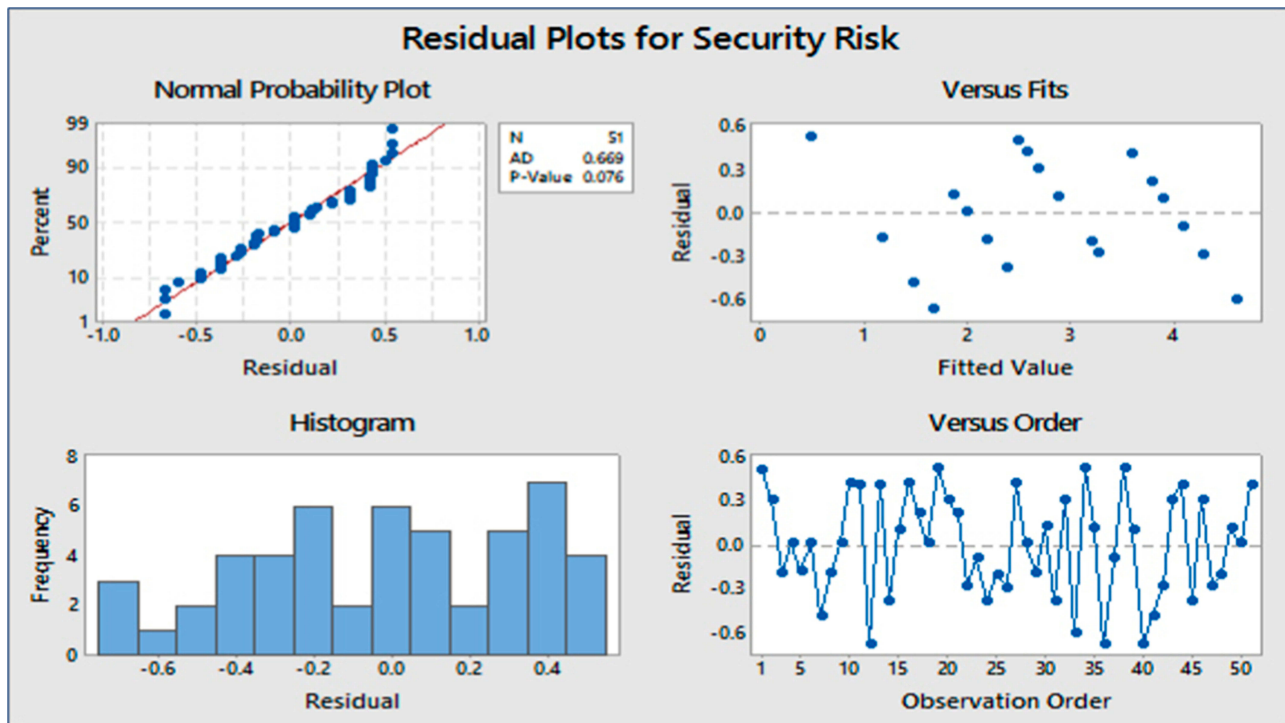


Figure 14 Residual plot for DCWIC.

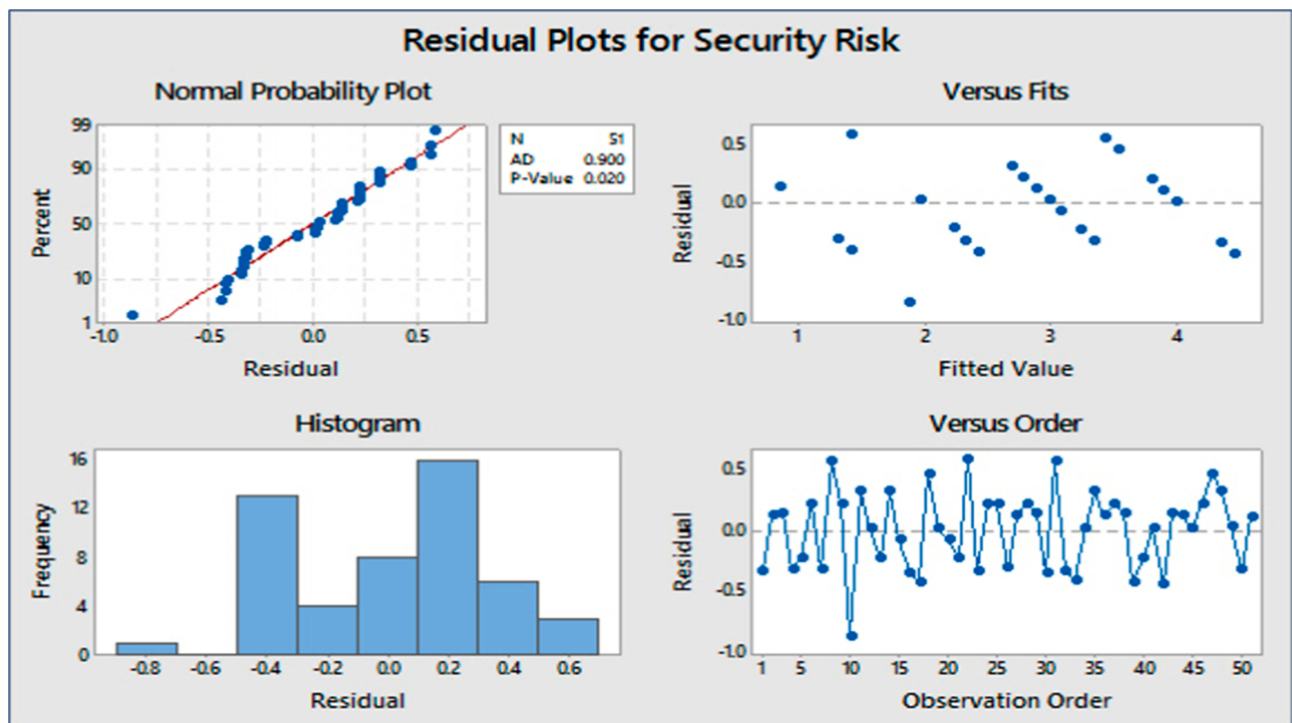


Figure 15 Residual plot for EITV.

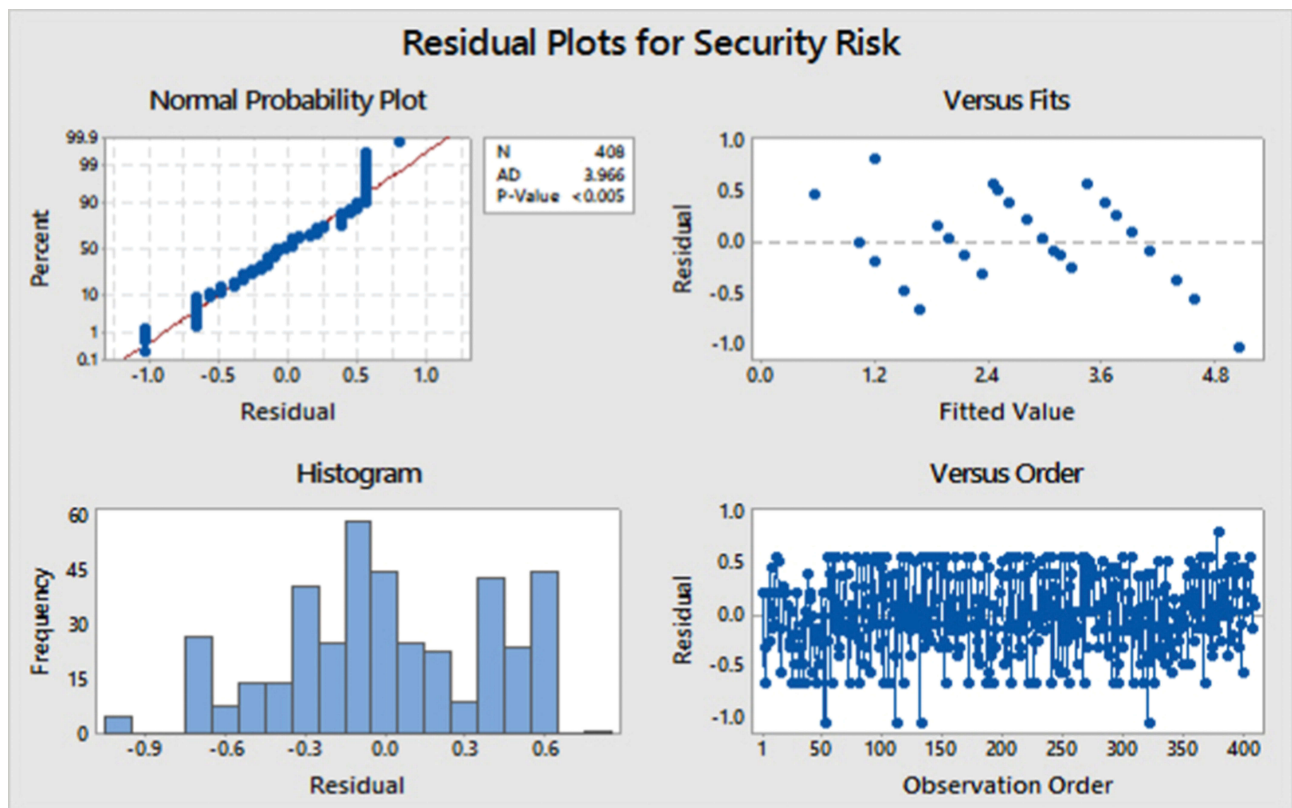


Figure 16 Residual plot for security risk through the hierarchy.

**Table 12** Correlation Between Both Results

	Probability	Severity	Security Risk
Probability	1.0000		
Severity	0.2790	1.0000	
Security Risk	0.6333	0.8617	1.0000

exhaustive. Some of the security risk factors might have been left unselected; making room for some error. The future study of the proposed work may include its comparison with the traditional risk assessment approaches.

## Acknowledgments

This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. (D-596-611-1441). The authors, therefore, gratefully acknowledge DSR technical and financial support.

## Disclosure

The authors report no conflicts of interest in this work.

## References

- Top 10 software development risks; [Cited July 10, 2019]. Available from: <https://www.itproportal.com/2010/06/14/top-ten-software-development-risks/Last>.
- McGraw G, editor. *Software Security: Building Security In*. Boston: Addison-Wesley Professional; 2006.
- Adaptive neuro-fuzzy interference system. In: Suparta W, Alhasa KM, editors. *Modeling of Tropospheric Delays Using ANFIS*. Berlin: Springer International Publishing; 2016. doi: 10.1007/978-3-319-28437
- Ostrom LT, Wilhelmens CA. *Risk Assessment: Tools, Techniques, and Their Applications*. John Wiley & Sons; 2019.
- FMEA. Weaknesses of a risk management tool that calculates a risk priority number. [cited Dec 27, 2019]. Available from: <https://www.brighthubpm.com/risk-management/72064-weaknesses-of-fmea/Last>.
- Critical incident technique. [Cited Dec 27, 2019]. Available from: [https://en.wikipedia.org/wiki/Critical\\_Incident\\_Technique](https://en.wikipedia.org/wiki/Critical_Incident_Technique).
- A review of decision tree disadvantages. [Cited Dec 27, 2019]. Available from: <https://www.brighthubpm.com/project-planning/106005-disadvantages-to-using-decision-trees/Last>.
- Nata'ala A, Muazu HD, Goni I, Jingi AM. Adaptive neuro-fuzzy system to determine the blood glucose level of diabetic. *Math Comput Sci*. 2019;4(3):63. doi:10.11648/j.mcs.20190403.11
- Maharlou H, NiakanKalhori SR, Shahbazi S, Ravangard R. Predicting length of stay in intensive care units after cardiac surgery: comparison of artificial neural networks and adaptive neuro-fuzzy system. *Health Inform Res*. 2018;24(2):109–117. doi:10.4258/hir.2018.24.2.109
- Mahmud M, Kaiser MS, Rahman MM, et al. A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications. *Cognit Comput*. 2018;10(5):864–873. doi:10.1007/s12559-018-9543-3
- Yadollahpour A, Nourozi J, Mirbagheri SA, Simancas-Acevedo E, Trejo-Macotela FR. Designing and implementing an ANFIS based medical decision support system to predict chronic kidney disease progression. *Front Physiol*. 2018;9. doi:10.3389/fphys.2018.01753
- Suresh K, Dillibabu RA. Novel Fuzzy Mechanism for Risk Assessment in Software Projects. *Soft Computing*. 2020;3:1–23.
- IT Security vulnerability v/s threat v/s risk: what's the difference? [cited July 10, 2019]. Available from: <http://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/>.
- Importance of data security in healthcare. [Cited December 27, 2019]. Available from: <https://insightscare.com/importance-data-security-healthcare/Last>.
- Risk Assessment Framework (RAF). [cited July 11, 2019]. Available from: <https://www.techopedia.com/definition/14010/risk-assessment-framework-raf>.
- Kaur J, Alka R, Khan A. Major software security risks at design phase. *ICIC Express Lett Int J Res Surv*. 2018. (ISSN 1881-803X).
- Wei G, Xhang X, Zhang X, Huang Z, Research on e-government information security risk assessment-based on fuzzy AHP and artificial neural network model. In: First International Conference on Networking and Distributed Computing (ICNDC) IEEE; 2010:218–221. Available from: <https://ieeexplore.ieee.org/document/5645431>. doi:10.1109/ICNDC.2010.52
- National Institute of Standards and Technology NIST. *Framework for Improving Critical Infrastructure Cyber Security, Version 1.0*. February 2012.
- National Institute of Standards and Technology NIST Special Publication 800-39. *Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View*. March 2011.
- Wang H, Wang B, You L, Zhang W. Software risk assessment method based on fuzzy neural network. In: 2015 International Conference on Computer Science and Intelligent Communication. Atlantis Pres; 2015. Available from: <https://www.atlantispress.com/proceedings/csic-15>.
- Praynlin E, Latha P. Estimating development effort of software projects using ANFIS. In international conference on recent trends in computational methods, communication and controls (ICON3C 2012), 2012. *Int J Comput Appl*. 2012.
- Sangaiah AK, Samuel OW, Li X, Abdel-Basset M, Wang H. Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm. *Comput Electr Eng*. 2018;71:833–846. doi:10.1016/j.compeleceng.2017.07.022
- Sonia A, Singhal H, Banati H. Fuzzy logic approach for threat prioritization in agile security framework using DREAD model. *IJCSI Int J Comput Sci Issues*. 2011;8(4).
- Lee M-C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *Intl J Comput Sci Inf Technol IJCSIT*. 2014;6(1):29–45. doi:10.5121/ijcsit.2014.6103
- Dark MJ, Assessing student performance outcomes in an information security risk assessment, service learning course. In: Proceedings of the 5th Conference on Information Technology Education. ACM; 2004:73–78. Available from: <https://dl.acm.org/doi/proceedings/10.1145/1029533?tocHeading=heading5>. doi:10.1145/1029533.1029552
- Shedden P, Smith W, Ahmad A, Information security risk assessment: towards a business practice perspective, Proceedings of the 8th Australian Information Security Management Conference; 2010; Perth Western, Australia. Edith Cowan University. doi:http://ro.ecu.edu.au/ism/98.
- Guan JZ, Lei MT, Zhu XL, Liu JY. Knowledge-based information security risk assessment method. *J China Univ Posts Telecommun*. 2013;20:60–63. doi:10.1016/S1005-8885(13)60220-4
- Feng N, Li M. An information systems security risk assessment model under uncertain environment. *Appl Soft Comput*. 2011;11(7):4332–4340. doi:10.1016/j.asoc.2010.06.005
- Lee ZJ, Chang LY. Apply fuzzy decision tree to information security risk assessment. *Int J Fuzzy Syst*. 2014;16(2):265–269.
- Eren-Dogu ZF, Celikoglu CC. Information security risk assessment: Bayesian prioritization for AHP group decision making. *Int J Innov Comp Inform Control*. 2012;8:8001–8018.



31. Jang JSR. ANFIS: adaptive-network-based fuzzy inference system. *IEEE Trans Syst Man Cybern.* 1993;23(3):665–685. doi:10.1109/21.256541
32. van Staalduinen MA, Khan F, Gadag V, Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliab Eng Syst Safe.* 2017;157:23–34. doi:10.1016/j.ress.2016.08.014
33. Gao GH, Li XY, Zhang BJ, Xiao WX. Information security risk assessment based on information measure and fuzzy clustering. *J Software.* 2011;6(11):2159–2166. doi:10.4304/jsw.6.11.2159-2166
34. CWE-767: access to critical private variable via public method. [cited July 15, 2019]. Available from: <https://cwe.mitre.org/data/definitions/767.html>.
35. CWE-260: password in configuration file. [cited July 21, 2019]. Available from: <https://cwe.mitre.org/data/definitions/260.html>.
36. CWE-766: critical variable declared public. [cited July 16, 2019]. Available from: <https://cwe.mitre.org/data/definitions/766.html>.
37. CWE-620: unverified password change. [cited July 10, 2019]. Available from: <https://cwe.mitre.org/data/definitions/620.html>.
38. CWE-366: race condition within a thread. [cited July 17, 2019]. Available from: <https://cwe.mitre.org/data/definitions/366.html>.
39. CWE-426: untrusted search path; [cited July 10, 2019.] Available from: <https://cwe.mitre.org/data/definitions/426.html>.
40. CWE-494: download of code without integrity check; [cited July 12, 2019.]. Available from: <https://cwe.mitre.org/data/definitions/494.html>.
41. CWE-454: external initialization of trusted variables or data stores; [cited July 12, 2019.] Available from: <https://cwe.mitre.org/data/definitions/454.html>.
42. Ebrat M, Ghodsi R. Construction project risk assessment by using adaptive-network based fuzzy inference system: an empirical study. *KSCE J Civ Eng.* 2014;18(5):1213–1227. doi:10.1007/s12205-014-0139-5
43. Baker WH, Rees LP, Tippett PS. Necessary measures: metric-driven information security risk assessment and decision making. *Commun ACM.* 2007;50(10):101–106. doi:10.1145/1290958.1290969
44. Chang LY, Lee ZJ, Applying fuzzy expert system to information security risk assessment -a case study on an attendance system. In: International Conference on Fuzzy Theory and Its Applications (iFUZZY). IEEE; 2013:346–351. Available from: <http://www.proceedings.com/22305.html>.
45. Hospital management system in java using NetBeans with source code; 2018 [cited August 02, 2019.]. Available from: <https://code-projects.org/hospital-management-system-in-java-using-netbeans-with-source-code/Last>.
46. Ting JSL, Tsang AHC, Kwok SK. Hybrid risk management methodology: a case study. *Int J Eng Bus Manag.* 2009;1(1):25–32. doi:10.5772/6783
47. Takagi T, Sugeno M. Fuzzy identification of systems and its applications to modeling and control. *IEEE Trans Syst Man Cybern.* 1985;15(1):116–132. doi:10.1109/TSMC.1985.6313399
48. Pant M, Ray K, Sharma TK, Rawat S, Bandyopadhyay A. Soft computing: theories and applications. *Proc SoCTA.* 2016;2.
49. The 10 biggest healthcare data breaches of 2019, so far; [Cited Dec 29, 2019.]. Available from: <https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far>.

## Risk Management and Healthcare Policy

Dovepress

### Publish your work in this journal

Risk Management and Healthcare Policy is an international, peer-reviewed, open access journal focusing on all aspects of public health, policy, and preventative measures to promote good health and improve morbidity and mortality in the population. The journal welcomes submitted papers covering original research, basic science, clinical & epidemiological studies, reviews and evaluations,

guidelines, expert opinion and commentary, case reports and extended reports. The manuscript management system is completely online and includes a very quick and fair peer-review system, which is all easy to use. Visit <http://www.dovepress.com/testimonials.php> to read real quotes from published authors.

Submit your manuscript here: <https://www.dovepress.com/risk-management-and-healthcare-policy-journal>