Covenant Journal of Informatics & Communication Technology. Vol. 9 No. 1, June, 2021
ISSN: *print* 2354 – 3566 *electronics* 2354 – 3507 DOI:

An Open Access Journal Available Online

Critical Factors Affecting the Efficiency of Information Security Risk Management in Business Organization: An Empirical Study

Arogundade Oluwasefunmi 'Tale T[1]http://orcid.org/0000-0001-9338-491X), **Mogaji Folashade**[2], **Ojo Oluwafolake**[3](http://orcid.org/0000-0002-1051-756X)
Alonge Christianah Yetunde[4](https://orcid.org/0000-0002-6901-1918) **, and Tobore Igbe**[5]

[1, 2, 3,4] Department of Computer Science, Federal University of Agriculture, Abeokuta.
[1] Department of Mathematical Sciences, Anchor University Lagos.
[5] Shenzhen Institutes of Advance Technology Chinese Academy of Sciences
[1]arogundadeot@funab.edu.ng, oarogundade@aul.edu.ng[1],
[2]temmydre@gmail.com[3]ojoeo@funaab.edu.ng, [4] alongecyetunde@gmail.com
[5]victor@siat.ac.cn

Received: 21.02.2021 Accepted: 30.05.2021

Date of Publication: June 2021

Abstract—One vital issue in the management of organization is the security of information. Managing information security is a methodical approach of addressing organizational security threats and risks. Considering the increasing cost of implementing and maintaining information security, organizations need to differentiate between the controls needed and those which are crucial that should also be in line with the organization goals and objectives. In this paper, we proposed to analyse critical factors affecting the efficiency of information security management using Artificial Neuro-Fuzzy Inference System (ANFIS) approach and also evaluate the performance of the scheme. We adopted the use of questionnaires to collect responses (dataset) for the study. The questionnaire was designed and categorized based on15selected major critical factors affecting the efficiency of information security management. There were 51 respondents from users of information technology product, professional workers, students and teachers. The results from the model were obtained after training with iteration of 8 epochs, the best training result for R is 0.7743 and the average testing result is 0.7767. Also, a similar result (values) was obtained as the one from the descriptive analysis and this indicate that the performance of ANFIS model can predict the level of risk severity. The results showed that cost has the highest risk level depending on the outcomes from the respondent and the ANFIS model.

Keywords/Index Terms—Artificial Neuro-Fuzzy Inference System (ANFIS); Information Security; Management (ISM); Risk Analysis.

1. Introduction

Information offers key support in the operation carried out by organization in making progressive decision, analysing critical record and provides a competitive advantage over competitors (Sivarajah*et al*., 2017). This information includes: sales data, transaction information, organisation profile record, performance record, election results, electronic health record and so on. In the real world, information needs to be securely protected and yet facilitate a controlled sharing of the resources. There have been great developments in the breadth and depth of concepts around Information Security. As a function, it has been embedded into the operations of many organisations, which makes overlaying strong management system needed for determining the way information is being shared and secured efficiently (Fan *et al*., 2018; Datta and Banerjee 2011).

Information is of great value and crucial to organizations but has its vulnerability to various attacks from both within and outside an organization such as hackers, viruses and worms, and data loss. Possible losses will take place as a result of security risks or threats are likely to lead to a number of actual and potential losses with monetary, legislative, and status consequences (Cavusgil*et al*., 2020; Yildirim *et al*., 2011).

In order to guard against these threats, the implementation of information security through; the set-up of firewall, security server, application of patches for fixing new vulnerabilities that are discovered in system software. It is important to determine what needs protection, the reason for the protection, the things that it should be secured from, and the approach for protecting it as long as it is in existence. Risk is the likelihood of facing harm or loss. The initial phase in the management of risk is to know which risks are threats to the information assets of organization. The understanding of this happens through conducting a full evaluation of the risk for identifying key organizational risks. By identifying these risks, security personnel in an organization makes decision on the best approach for addressing them. This process is what is considered as risk management (Culnan*et al*., 2008).

Some of the known vital factors affecting the information security risk management are cost, organizational structure, organizational size and philosophy of organization security. Organizational business practices have complementary support through information security risk management framework. A number of organizations focus their attention of information security risk management efforts on the system of evaluation. Information security risk assessments (ISRAs) give organizations the ability of identifying crucial information assets and security risks (Werlinger et al. 2009). In addition, information security management is technology dependent, process dependent and people dependent, but less attention have been considered for people involved in information security

(Glushenko 2017; Martin and Rice 2011). This is probably due to the tendency to view the problem from the approach of the organisation's requirement towards information security. Therefore, to handle these limitations, a questionnaire is constructed to gather information about factors influencing information security risk management from people directly and indirectly involved with organisational information structure. These factors are investigated and analysed with adaptive neuro-fuzzy inference system technique, machine learning method to reveal various critical factors affecting information security risk management. This approach will reveal critical factors affecting the efficiency of managing the risks of information security.

The rest of this paper is organized thus: the review of literature relating to the research work is done in Section 2, Section 3 describes the design of the questionnaire and proposed neuro-fuzzy method. The implementation, result and performance of the approach are discussed in Section 4. Section 5 gives the conclusion of the research.

2. Related Works

Table 1 shows a summary of the related work done in this area of research

Authors	**Approach**
Arogundade*et al.*, 2020	A semantically enhanced model for security management during the information system lifetime was proposed. The model supports the continuous collection of identified threat behaviours from the intrusion detection system, filtering and analysis of the threats for effective security risk control.
Abioye*et al.*, 2020	A life-cycle approach to ontology-based risk management framework for software projects was designed. The empirical investigation conducted showed that the scheme could assist the software developers in knowledge reuse during risk management processes.
Safa *et al.*, 2016	Model that shows how conforming to the information security policies of organisations and mitigating the risk of employee's behaviour is essential
Osho *et al.*, 2019	A data security system named "AbsoluteSecure" was proposed. The system combines the best features of biometric, cryptography, and steganography techniques. The experimental investigation conducted showed that AbsoluteSecure can provide confidentiality, integrity, and availability of data.
Alcaraz and Zeadally 2015	The threats and vulnerabilities faced by modern infrastructures that are critical were presented for the 21st century in the government, management of security and protected network architectures

Odun-Ayo *et al*., 2017	A new cloud-based security frame work for Human Resource Information System was implemented using the Google App Engine. The result was presented as a scalable application in which the data in storage is encrypted and visible on the Google Cloud Platform data store.
Lowry and Moody, 2015	A study was conducted on a control-reactance compliance model with an explanation of the motives that opposed the compliance with organisational information security polices
Jambhekar*et al*., 2016	Three-tier (and two-tier) security mechanism was designed. The scheme can effectively control the information security with the security key agreement and exchange protocol. The security system is suitable for low-bandwidth communication channel.
Chai, 2011	Computer-based learning and analysis was implemented and to achieve decreased response time and increased accuracy for monitoring and protecting the computer infrastructures of organizations from attacks proactively
Eweoya and Misra, 2014	The critical security incorporations that ensure a better security of software were explored. The investigation focused on information security in the software development life cycle to avoid tampering, endeavour integrity and authentication of information.
Dubois et al., 2010	An intense approach for building an ontology, or domain-specific model, of information system security risk management was implemented to handle specific challenges in ISM.
Arogundade et al, 2020	An agent based approach to resolve issues related to the collection and classification of software application anomalies and misuses to facilitate the reappraisal of security controls of information system
Azeez et al, 2020	A detailed analysis between the visual link and the actual link was carried out to determine the whitelist by taking final decision on the extracted information from the hyperlink, which can also be obtained from the web address provided by the user.
Jambhakar et al, 2016	A framework of collaborated technique was adopted which comprises the parallel and distributed encryption system to elaborate the working of cloud computing security.
Uneojo, and Misra, 2012	The study conducted a comprehensive survey on the characteristics of computer worms, the technique of using intrusion detection system behind firewalls in detecting worms and analysis of different reactive attack trace back approaches.

3. Methodology

Investigating information risk management involves solution strategies derived by using practice-based approach that is driven by organization policy and structure. In this section, a questionnaire is constructed to consider factors that affect organization's information security management. Artificial Neuro-Fuzzy Inference System (ANFIS) is constructed to analyse the critical factors affecting information security risk management. By investigating these factors, an organization can improve its security position over time.

3.1. Questionnaire for Information Security Risk Management

The questionnaire is constructed in hierarchical pattern which allows the factors to be arranged at different level of critical effect and influence. The hierarchy of the factor is designed to begin from the perceived information technological organizational factors such as cost, organizational size, organizational security philosophy, organizational structure and external influence. The complete list is described in Table 1. These factors are used to determine the success security risk management in organizations. Each factor is assigned five categories: Strongly Agree (SA), Agree (A), Indifference (I), Disagree (D), and Strongly Disagree (SD). The category describes user's option about each factor with respect to information management and risk management.

In this approach, the membership function representation is different from the usually expert system intervention procedures; the membership function is based on hierarchical factors architecture by categorizing the perception of respondents into discreet representation. The determinants of the factors gotten from the respondent which can either be: strongly agree, agree, indifferent and strongly disagree are categorized and measure discreetly are represented as values; 1,2,3,4 and 5 respectively. The reason for this categorization is as a result of the most perceived factor affecting the risk management trickle down to the users of the information technology product users. The risk level was determined based on the highest number of responses on SA and A compare to SD and D. The risk level was categorized into high, medium and low which are represented by 1, 2 and 3 respectively.

3.2. Adaptive Neuro-Fuzzy Inference System (ANFIS) Architecture

The ANFIS technique was originally presented by (Abdulrahman et al. 2014). It is a simple technique for learning data that employs fuzzy logic for transforming given inputs into a desired output through neural network processing elements (nodes) and information connections that are interconnected and have weight to map the numerical inputs to an output. ANFIS uses the combined benefits of two machine learning techniques (fuzzy logic and neural network) into a single technique (Abdulrahman et al. 2014). The operation technique with which ANFIS operates is via employing neural network learning methods for tuning Fuzzy Inference System (FIS) parameters; this technique enables the immense success of ANFIS (Jang 1993). It carries out a refinement of fuzzy IF-THEN rules for describing the behaviour of a complex system. This does not need a prior expertise of human, easy to implement, fast and precise learning, offer immense decision of membership functions, powerful generalization potential, and ease to incorporating linguistic and numeric knowledge to address problem. Rules that differ cannot share similar output membership function. The amount of membership function should be similar with the number of rules. In presenting the ANFIS architecture, two fuzzy IF-THEN rules based on a first order is constructed as:

Rule 1 : IF x is A1 AND y is B1 ; THEN f1 = P1 x +Q1 y + R1
Rule 2: IF x is A2 AND y is B2 ; THENf2= P2 x + Q2y + R2

where x and y are the inputs, Ai and Bi are the fuzzy sets, fiis are the outputs within the fuzzy region specified by the fuzzy rule, and Pi, Qi, and Ri are design parameters that are determined during the training process. We adopted ANFIS architecture of two rules and two inputs.

Table 1: Factors for questionnaire information risk management

S/N	Factors	Description
1	Cost	Cost of facilities discourages information technology (I.T) knowledge in the society.
2	External Influences	I.T improvement is hampered by the social and political influence
3	Agreement	I.T personnel and management find it difficult to produce software that are in accordance with what the society needs
4	Organization Structure	The organizational structure affects I.T products availability
5	Adaptability	Most I.T software are not adaptable to the social structure
6	Complexity	Most software are too complex to interact with
7	Level of Risks	The risk involved in the use of some software is too high
8	Organization Size	The larger an I.T organization, the more the availability of software in the society

9	Organization Security Philosophy	Organizational security philosophy or orientation determine the kind of software used by people
10	Consistency	Consistency in I.T has helped people using software
11	Usability	Usability of software could make I.T grow faster
12	Feasibility	Most real life problem are solved by I.T
13	Validity	Most I.T software are useful and valid for a long period of time
14	Credibility	I.T products have achieved a lot of credibility
15	Automation	Automation of real life activities are needed from I.T industry

The ANFIS has architecture with five layers. The detailed explanations for each individual layer are given. For Layer1, the nodes are adaptive. The outputs in Layer1 are the fuzzy membership grade of the inputs that are explained by the following equations:

$$O_{1,i} = \mu\_Ai(x)(1)$$

$$O\_(1,i) = \mu\_(Bi-2)\ (y) \qquad (2)$$

where x and y are inputs from factors considered in the questionnaire into node i, and *i=1,2.Ai* and *Bi* are the linguistic labels (high, low, and so on) associated with node function $\mu_Ai(x)$and $\mu\_(Bi-2)\ (y)$ can adopt any fuzzy membership function. For example, if the bell-shaped membership function is employed, $\mu\_Ai(x)$ is given by

$$\mu_{Ai}(x) = \frac{1}{1+\left[\left(\frac{x-c_i}{a_i}\right)^2\right]} \qquad (3)$$

Another membership function is the Gaussian membership function, which is given by

$$\mu_{Ai}(x) = exp\left[-\left(\frac{x-c_i}{a_i}\right)^2\right] \qquad (4)$$

Where a_i, b_i and c_i are the parameters of the membership function.

In Layer 2, the nodes are fixed. This layer involves the fuzzy operators; it uses the AND operator for fuzzifying the inputs. They are labelled with π, which indicates that they operate as a simple multiplier. The output of this layer can be represented as:

$$O_{2,i} = w_i = \mu_{Ai}(x) \times \mu_{Bi}(y) \qquad (5).$$

These are the firing strengths (weights) of the rules.

In Layer 3, the nodes are also fixed with the label, N, for indicating that they play a normalization role in firing the strength from the previous layer. The output of this layer can be represented as:

$$O_{3,i} = \underline{w_i} = \frac{w_i}{w_1 + w_2} \qquad (6)$$

Outputs of this layer are called normalized firing strengths.

In Layer 4, the nodes are adaptive. The output of each node in this layer is simply the product of the normalized firing strength and a first order polynomial. The output of this layer is given by:

$$O_{4,i} = \underline{w_i} f_i = \underline{w_i}(p_i x + q_i y + r_i) \qquad (7)$$

Where w is the output of Layer 3, p_i, q_i and $r_i$are the consequent parameters.

In Layer 5, there is only one single fixed node labelled with P. This node performs the summation of all incoming signals. The overall output of the model is given by:

$$O_{5,i} = \sum \underline{w_i} f_i = \frac{\sum_i w_i f_i}{\sum_i w_i} \qquad (8)$$

3.2.1 Hybrid Learning Algorithm

The algorithm used for learning in ANFIS is hybrid showing that it combines the gradient descent and least squares methods. In the forward pass, outputs of nodes go forward until Layer 4 and the resulting parameters are determined by the least squares. In the backward pass, the error signals propagate backward and the premise parameters are updated using gradient descendent. The hybrid learning approach converges much faster by reducing search space dimensions of the original back propagation method (Abdulrahman et al. 2014). The overall output is given by:

$$f = \frac{w_1}{w_1 + w_2} f_1 + \frac{w_2}{w_1 + w_2} f_2 \quad (9)$$

$$f = \underline{w}(p_1 x + q_1 y + r_1) + \underline{w}(p_2 x + q_2 + r_2) \qquad (10)$$

$$f = (\underline{w_1} x) p_1 + (\underline{w_1} y) q_1 + (\underline{w_1} r) + (\underline{w_2} x) p_2 + (\underline{w_2} y) q_2 + (\underline{w_2} r) \qquad (11)$$

Where p_1, q_1, r_1, p_2, q_2 and $r_2$are the linear consequent parameters. Hybrid algorithm has been shown to be is highly efficient in training ANFIS systems (Jang et al. 1995). The procedural step for its training steps is described in Figure 2.

3.2.2 Root Mean Square Error and Mean Square Error

These are employed in the model to minimize error during the process of training the model with the train dataset. The two methods can be defined as:

$$RMSE = \sqrt{\frac{1}{N} \sum_{j=1}^{N} (y_j - \hat{y}_j)^2} \quad , \qquad (12)$$

and

$$MSE = \frac{1}{N} \sum_{j=1}^{N} |y_j - \hat{y}_j| \qquad (13)$$

4. Results and Discussion

The gathered data through the questionnaire are extracted for forming dataset for pre-processing in the excel spreadsheet. This is necessary because the dataset should be in a specific format that can be usable in the MATLAB development environment. The ANFIS edit tool in the MATLAB is then used to process the neuro-fuzzy inference system. The result of this will return a prediction for the factors based on the inputs parameters and as well as show the effect of the variation in the input parameters to the prediction of the impact using the rule generated from the features inherent in the training dataset.Table 2 presents the results of the response obtained from the questionnaire, "Cost" has the highest score for SA with value of 47, "external influence" has a value of 42, and validity and usability both have the same score of 41 for SA. Figure 3 shows hierarchy of factors affecting efficiency of information security risk based on responses from SA criteria.

The training data was obtained from the original dataset extracted from the response collected from the questionnaire. This served as input into the ANFIS model followed by the measurement of the performance output. The dataset was pre-processed into a matrix form with inputs column and output column. This coded matrix represents the training data for the ANI development environment shown in figure 4.

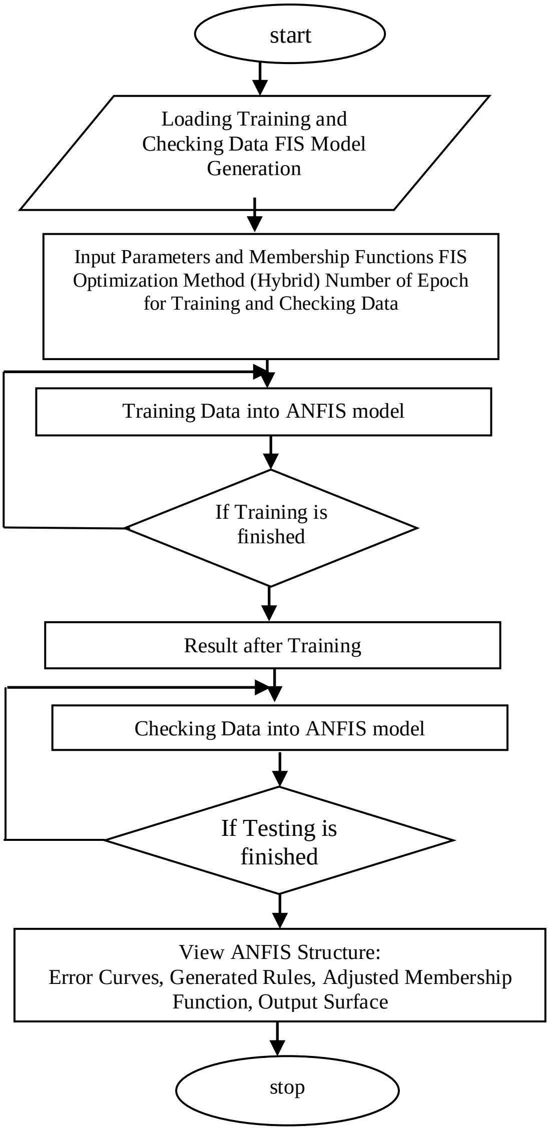

start
Loading Training and Checking Data FIS Model Generation
Input Parameters and Membership Functions FIS Optimization Method (Hybrid) Number of Epoch for Training and Checking Data
Training Data into ANFIS model
If Training is finished
Result after Training
Checking Data into ANFIS model
If Testing is finished
View ANFIS Structure: Error Curves, Generated Rules, Adjusted Membership Function, Output Surface
stop

Figure 1: Flowchart of ANFIS model

Table 2. Summary of the response obtained from questionnaire

S/N	Factors	Total Responses on (SA)	Total Responses on (A)	Total Responses on (I)	Total Responses on (D)	Total Responses on (SD)	Risk Level
1	Cost	47	1	3	0	0	1
2	External Influences	42	9	0	0	0	1
3	Agreement	0	0	0	29	22	3
4	Organization Structure	14	11	9	9	8	1
5	Adaptability	30	8	7	4	2	1
6	Complexity	24	9	7	6	5	1
7	Level of Risk	39	12	0	0	0	1
8	Organization Size	36	9	2	3	1	1
9	Organization Security Philosophy	33	12	4	0	1	1
10	Consistency	45	6	0	0	0	1
11	Usability	41	10	0	0	0	1
12	Feasibility	36	15	0	0	0	1
13	Validity	41	8	4	0	0	1
14	Credibility	32	16	1	0	5	1
15	Automation	36	11	3	0	1	1

The low, average and high membership category representation is given as: between 1.0 and 3.0 as low, between 3.0 and 5.0 as average, while above 5.0 as high. The number of inputs and output for the neural network training is shown in Figure 3. The Levenberge-Maquadt training is used and the mean square error performance is set at 1.19, with maximum iteration of 8 and having the gradient of 1.86. Figure 4 shows the correlation behaviour of high value 0.015 and low value of 0.003 described as Lag. The confidential limit is ±0.009, while the auto-correlation with error of 1 has the highest correlation of 19 and low correlation of 0.004. The confidential limit is±0.004 as seen in figure 5. Figure 6 describes the time series response for the training which suggests that the best output target is 0.33, validation target output of 0.25 with error of ±0.009. The summary of the results for training, validation and testing are shown in Figures 7 and 8. The error rate of ±0.04335 for validation and training result, at error instance of 12 and tested at high rate of 11 instances.

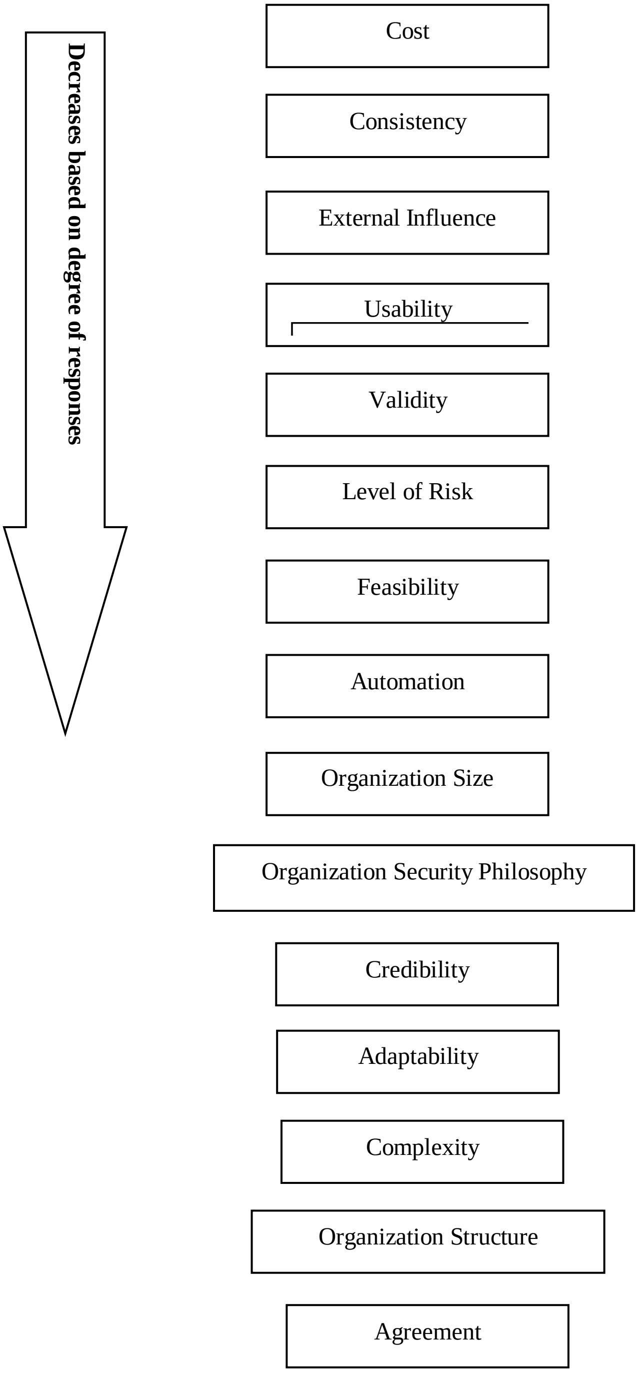
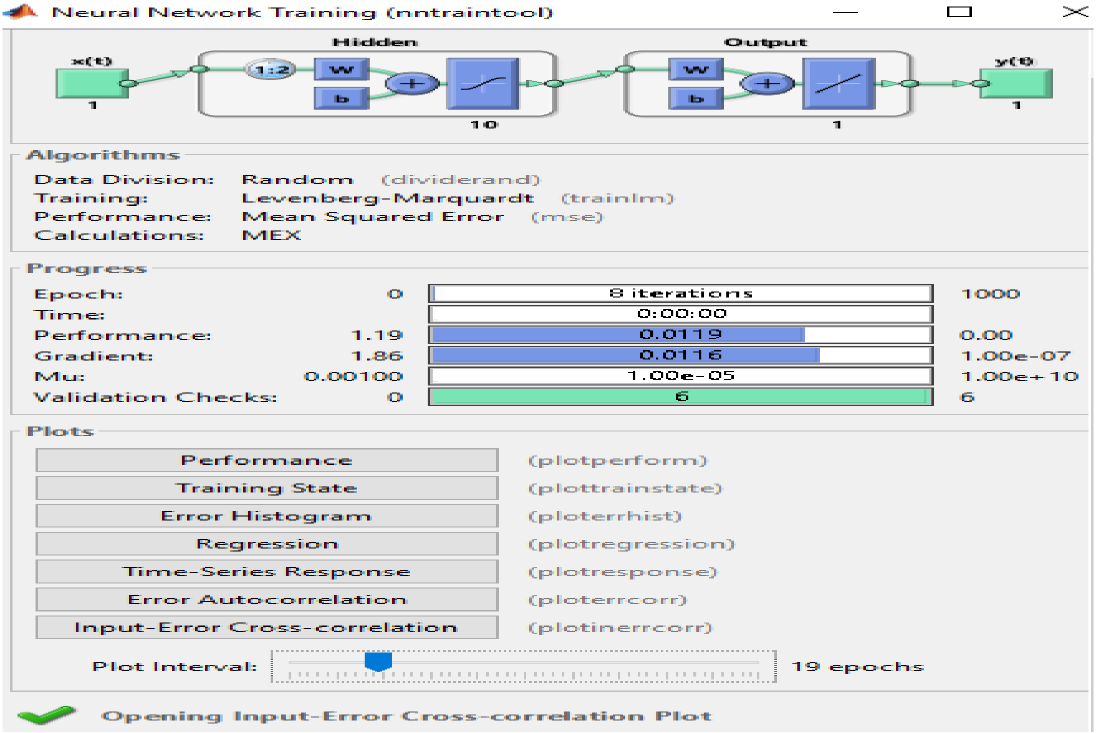


Figure 2: Hierarchy of critical factors affecting efficiency of information security risk



```
Algorithms
Data Division:    Random  (dividerand)
Training:         Levenberg-Marquardt  (trainlm)
Performance:      Mean Squared Error  (mse)
Calculations:     MEX

Progress
Epoch:                     0   8 iterations   1000
Time:                          0:00:00
Performance:            1.19   0.0119         0.00
Gradient:               1.86   0.0116         1.00e-07
Mu:                  0.00100   1.00e-05       1.00e+10
Validation Checks:         0   6              6

Plots
Performance                      (plotperform)
Training State                   (plottrainstate)
Error Histogram                  (ploterrhist)
Regression                       (plotregression)
Time-Series Response             (plotresponse)
Error Autocorrelation            (ploterrcorr)
Input-Error Cross-correlation    (plotinerrcorr)

Plot Interval:                   19 epochs

Opening Input-Error Cross-correlation Plot
```

Figure 3: MATLAB interface for neural network training with Levenberg-Marquadt method.

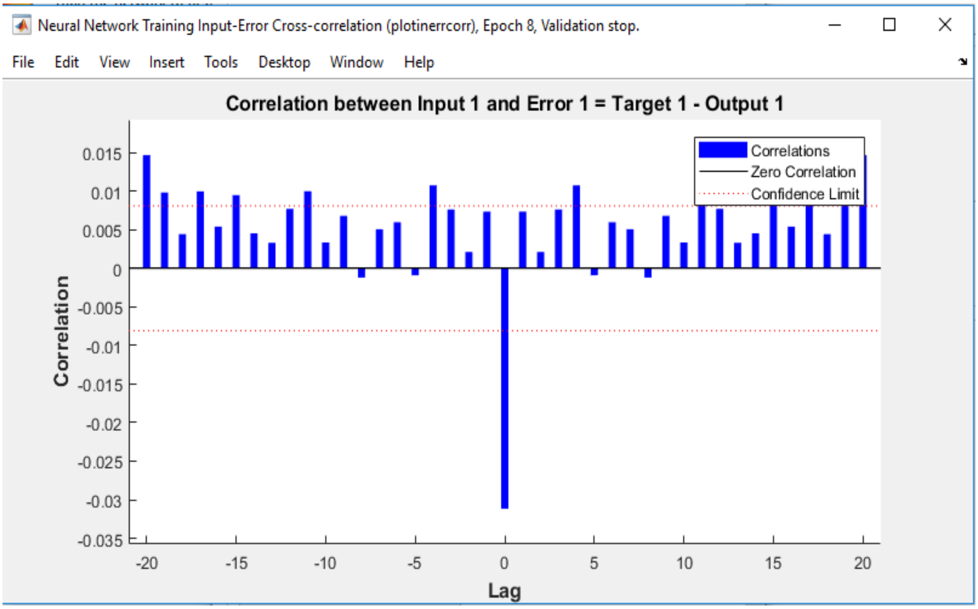


Figure 4: Result for neural network training with cross correlation analysis

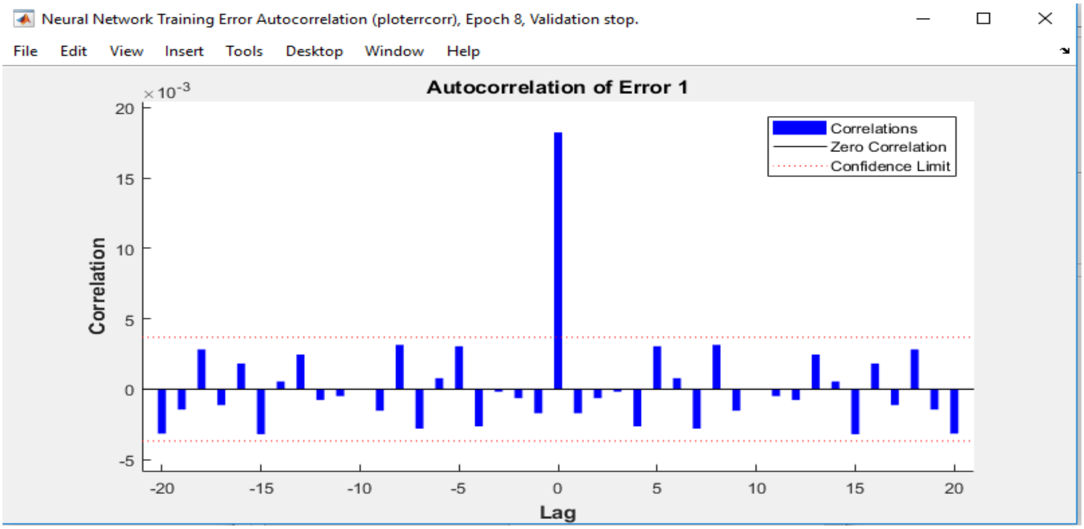

Neural Network Training Error Autocorrelation (ploterrcorr), Epoch 8, Validation stop.

Figure 5: Result for neural network training with autocorrelation.

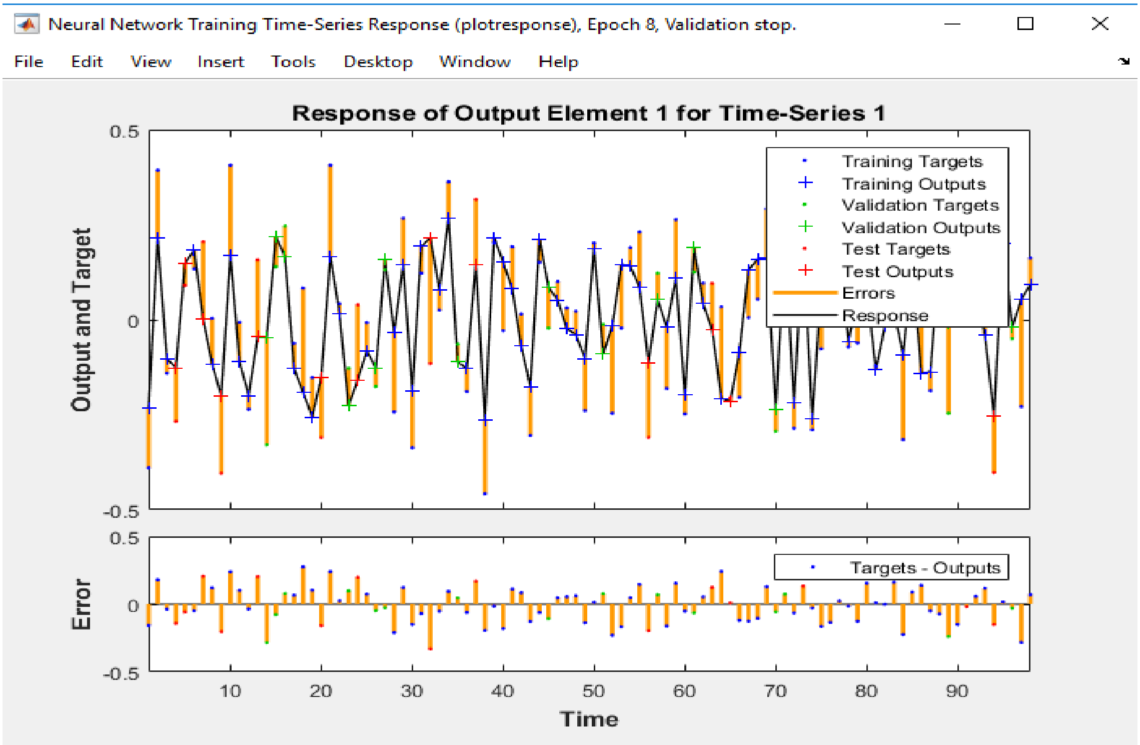

Neural Network Training Time-Series Response (plotresponse), Epoch 8, Validation stop.

Figure 6: Interface for neural network training with time series network.

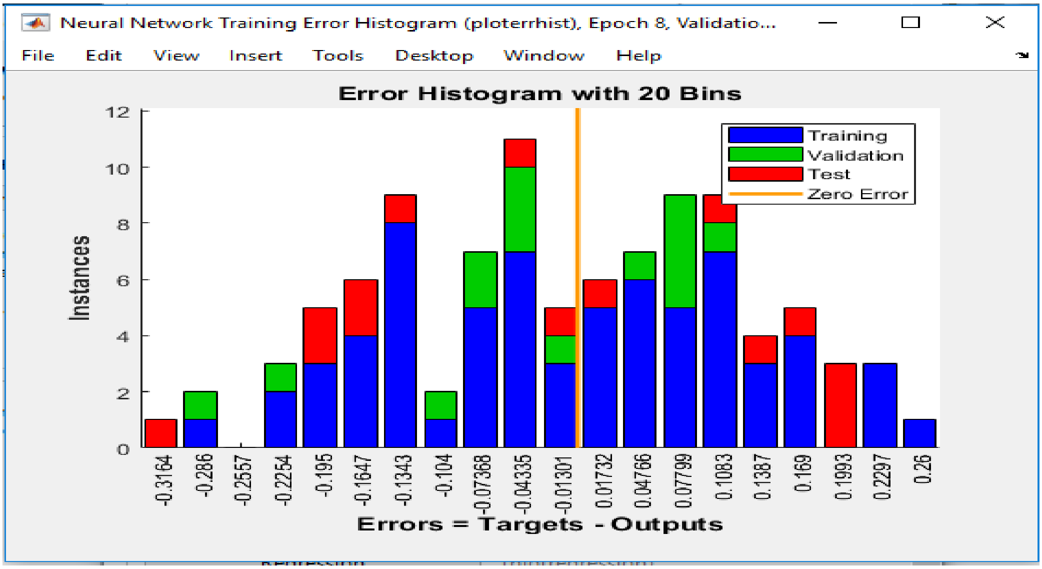


Figure 7: Interface for neural network training showing error histogram

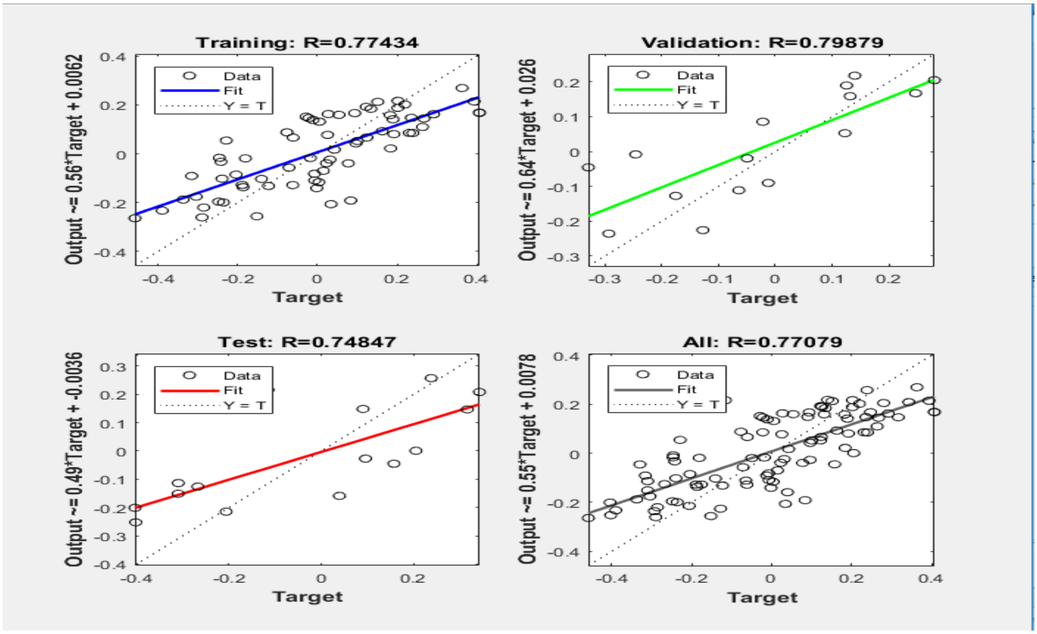


Figure 8: Result for neural network training showing the validation and test

The gradient, Mu and the validation checks is 0.0115, 0.00005 and 6 respectively, which shows that the epoch at 8 is best for the training with R=0.7743 and 0.7709. The average testing result is 0.7767 for the training.

5. Conclusion

In this study, an empirical investigation on the critical factors affecting the efficiency of information security management is conducted. The research adopts the use of questionnaires to gather user's responses (dataset). The designed questionnaire is hierarchical which allows the factors to be selected as critical factors. The hierarchy of the factor is designed starting from the perceived information technology organizational factors such as the organizational size, organizational security philosophy, organizational structure and external influence to the intermediate factors , such as the cost of project implementation, the consistency in the information technology sector, the validity of the product sold to the users in the society, the usability of these products and the agreement established within and without the information technology organization. The user factor such as adaptability of the products, the complexity in their usage, the risk involved in the used of this products, the feasibility of the product before and after being sold to the user, the credibility of these product and how useful they are, and the automation which suggest the primary usability of the product by users. To take advantage of these factors, a questionnaire was setup to acquire responses from affected persons, the information was extracted from questionnaire and pre-analysed with excel file. A method called Neuro-Fuzzy, which uses a machine learning algorithm, deduced from Neural Network theory to create the fuzzy sets and fuzzy rules for information risk management. Fuzzy sets sieve uncertainties in a logical statement, while neural network predicts the outcome from the set of given occurrence(s). Therefore, based on the rules generated by the Neuro-Fuzzy model, and the correlation statistics it was concluded that the gradient, Mu and the validation checks are 0.0115, 0.00005 and 6 respectively. The epoch at 8 is best for the training with R=0.7743 and the average testing result was 0.7767 after the training.

The fuzzy model implemented in this work makes it possible to carrying out continual analysis of the critical factors affecting information security risk management, and the information got as a result of modelling fuzzy makes it possible for risk managers to know these critical factors and reduce their impact.

References

Azeez NA, Salaudeen BB, Misra S, Damaševičius R, Maskeliūnas R et al (2020). Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electronic Security and Digital Forensics, Vol. 12, No. 2, pp 200-213.

Alcaraz C, Zeadally S. 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. International journal of critical infrastructure protection. 8:53-66.

ArogundadeO. ,Abayomi-Alli A. ,
Misra S. 2020. An Ontology-Based Security Risk Management Model for Information Systems. Arab J SciEng 45, 6183–6198.

Abioye, T.E., Arogundade, O.T., Misra,
S., Akinwale, A.T. and Adeniran, O.J., 2020. Toward ontology-based risk management framework for software projects: An empirical study. Journal of Software: Evolution and Process, 32(12), p.e2269.

Arogundade, O. T., Abioye, T. E., & Sanjay, M. (2020). An ontological approach to threats pattern collection and classification: a preliminary study to security management. International Journal of Electronic Security and DigitalForensics(Inderscience), 12(3), 323-335.

Cavusgil, S.T., Deligonul, S., Ghauri, P.N., Bamiatzi, V., Park, B.I. and Mellahi, K., 2020. Risk in international business and its mitigation. Journal of World Business, 55(2), p.101078.

Chai S, Kim M, Rao HR. 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. Decision Support Systems. 50(4):651-61.

Culnan MJ, Foxman ER, Ray AW. 2008. Why IT executives should help employees secure their home computers. MIS Quarterly Executive.7(1):6.

Datta SP, Banerjee P. 2011. Guidelines for performance measures of information security of it network and systems. International Journal of Research and Reviews in Next Generation Networks.1(1): 39-43.

Dubois, É., Heymans, P., Mayer, N. and Matulevičius, R., 2010. A systematic approach to define the domain of information system security risk management. In Intentional Perspectives on Information Systems Engineering (pp. 289-306). Springer, Berlin, Heidelberg.

Eweoya, I., Misra, S. 2014, Enhancing Security in the Software Development Lifecycle (SDLC). *In 9th Annual Symposiu on Information Assurance (Asia '14).* Albany, NY, 2014

Fan, K., Wang, S., Ren, Y., Li, H. and Yang, Y., 2018.Medblock: Efficient and secure medical data sharing via blockchain. Journal of medical systems, 42(8), p.136.

Glushenko SA. 2017. An adaptive neuro-fuzzy inference system for assessment of risks to an organization's information security.Бизнес-информатика. 1(39).

Hong KS, Chi YP, Chao LR, Tang JH.2003.An integrated system theory of information security management.Information Management & Computer Security. 11(5):243-8.

Jambhekar, N. D., Misra, S., &Dhawale, C. A. (2016). Mobile computing security threats and solution, International Journal of Pharmacy and Technology 8(4): 23075-23086

Jang JS. 1993. ANFIS: adaptive-network-based fuzzy inference system. IEEE transactions on systems, man, and cybernetics. 23(3):665-85.

Jambhekar N.D., Misra, S., Dhawale, C.A.. Cloud Computing Security with collaborating encryption Indian Journal pf Science and Technology, 9 (21), 95293, 2016.

Lowry PB, Moody GD. 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal. 25(5):433-63.

Martin N, Rice J. 2011. Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security. 30(8):803-814.

Odun-Ayo I., Misra S., Omoregbe N., Onibere E., Bulama Y., Damaševičius R., 2017. Cloud-Based Security Driven Human Resource Management System, Frontiers in Artificial Intelligence and Applications, Volume : Advances in Digital Technologies, 295: 96-106.

Osho O., Musa F.A., Misra S., Uduimoh A.A., Adewunmi A., Ahuja R. 2019. AbsoluteSecure: A Tri-Layered Data Security System. In: Damaševičius R., Vasiljevienė G. (eds) Information and Software Technologies. ICIST 2019. Communications in Computer and Information Science, vol 1078. Springer, Cham.

Safa NS, Von Solms R, Furnell S. 2016. Information security policy compliance model in organizations.Computers& Security. 56:70-82.

Sivarajah, U., Kamal, M.M., Irani, Z. and Weerakkody, V., 2017.Critical analysis of Big Data challenges and analytical methods. Journal of Business Research, 70, pp.263-286.

Uneojo A. V. and S. Misra 2012. Computer Worm Attack Using Ids and Traceback Approaches' Proceedings of 15th Annual New York State Cyber Security Conference and 7th Annual Symposium on Information Assurance, Empire State Plaza, Albany, NY.

Werlinger R, Hawkey K, Beznosov K. 2009. An integrated view of human, organizational, and technological challenges of IT security management.Information Management & Computer Security. 17(1):4-19.

Yildirim EY, Akalp G, Aytac S, Bayram N. 2011. Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management. 31(4):360-365.