International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 7(E); July 2018; Page No. 14200-14208
DOI: http://dx.doi.org/10.24327/ijcar.2018.14208.2567

Research Article

CONCEPTUALIZATION OF INTELLIGENT CLUSTERING METHODOLOGY FOR TERRORISTS ACTS CLASSIFICATION IN NIGERIA

George Uduak D[1]*., Inyang Udoinyang G[1] and Akinyokun Oluwole C[2]

[1]Department of Computer Science, University of Uyo, Uyo, Nigeria
[2]Department of Software Engineering, Federal University of Technology, Akure, Nigeria

A R T I C L E I N F O

Article History:

Received 11th April, 2018
Received in revised form 4th May, 2018 Accepted 23rd June, 2018
Published online 28th July, 2018

Key words:

Terrorist, Conceptualisation, Neuro-Fuzzy, Clustering, Snowflake, Fuzzification, Congnitive, Fault- Tolerance, Generalization, Sigmoid, Propagation, Threshold, Adaptive

A B S T R A C T

This paper aims at conceptualizing a platform for classifying terrorist acts using neuro-fuzzy and clustering techniques. The main objective is to design a knowledge base (comprising of knowledge warehouse, neural network (NN), fuzzy logic) and a neuro-fuzzy clustering system for Terrorists acts classification and also to propose a model for assigning numerical weights to qualitative Terrorists attributes. The conceptualization of neuro-fuzzy and clustering technique for classification of terrorists' acts is presented. The conceptualization involves the design of Knowledge Base which is an integration of Knowledge Warehouse, Fuzzy Logic and Neural Network (NN). The Knowledge Warehouse is an abstraction of intelligent information which provides the decision maker with an intelligent analysis platform that improves all phases of the knowledge management process. The star and the snowflake schemas are used as the building blocks. The star schema consists of a large central table known as fact table and a set of smaller attendant tables known as dimension tables displayed in a radial pattern around the fact table. The snowflake schema consists of a central fact table and a set of constituent dimension tables which can be further broken down into sub-dimension tables. The fuzzy logic component of the system consists of fuzzification, fuzzy inference engine and defuzzification. The fuzzy logic component provides the inference under cognitive uncertainty while the neural network (NN) component offers adaptation, parallelism, fault tolerance and generalization in the system. The Neural Network (NN) is a three layer feed forward Neural Network (NN) architecture with nine nodes at the input layer, six nodes at the hidden layer, one node at the output layer representing the fatality measure of the terrorists acts generated through the connection weights of the hidden layer using sigmoid transfer function. The computed output is compared with the desired output and the difference, which is the error term, is used to adjust the connection weights by means of a back-propagation algorithm. The process is repeated until the error term is within the acceptable threshold. The inference engine comprises the Fuzzy C-Means (FCM) Clustering and Adaptive Neuro-Fuzzy Inference System (ANFIS)

INTRODUCTION

Terrorism is an act of violence, which instills fear, causes serious injuries, destroys lives and properties of the citizens. It aims at compelling the government or organizations to follow a particular line of action. In recent times, incidents of terrorism and insurgency are reported almost on daily basis. Churches, mosques, schools, markets, viewing centers, motor parks, military/paramilitary formations, government agencies and diplomatic institutions are soft spots frequently affected terrorists. Terrorists, unlike traditional criminals, are much less spontaneous in their action, engage in substantial planning activities as well as commit ancillary and preparatory crimes in advance of a major terrorist incident. Terrorism think globally but act locally, there is need for security agencies to follow terrorists' patterns to tackle them. It has been noticed that adequate knowledge through scientific approaches is yet to be fully gained concerning the various attributes of terrorism .The lack of comprehensive database of various terrorism and other crime-related incidents accounts for the dearth in knowledge. It is also observed that the prevention of acts of terrorism is arduous and the use of force to fight them has proved to be of little value because terrorists are ready to die for their course. Furthermore, investigation, analysis, and classification of terrorism acts yield little or no success because of the vagueness of its attributes in addition to uncertainty, confusion, and varying tactics that often characterize the acts.

In response to the threats of terrorism, governments at various levels have employed several measures to curb it. Some of the

Corresponding author:* **Akinyokun Oluwole C.
Department of Software Engineering, Federal University of Technology, Akure, Nigeria

measures are preemptive, offensive and defensive in nature. Attempts to stop the operations of terrorists have not yielded the expected results since they also evolve to outwit the current tactics employed to fight them. The pursuit of adequate solutions to this nuisance is on-going through national, regional and international co-operations. New approaches are currently been adopted by law enforcement agencies at all levels in the fight against terrorists. Some of these methodologies include Science and Technology, intelligence gathering using Information Technology (IT) as well as other general scientific and technological equipment (Perry, 2003; Chakraborty, 2009). Science and Technology offer a considerable effectiveness and efficiency over the traditional military prowess since it uses various combating hardware devices such as ultra wide band (UWB), electromagnetic pulse (EMP), active denial system, tear gas, sleep gas, psycho-chemicals and directed energy weapon have been developed and deployed (Saeed *et al.*, 2012). However, these technological tools are very effective when the physical location of the terrorists and government operatives at not different. The introduction of computational intelligent electronic systems is capable of reading audit trails and carry out forensic analysis of log files of human activities. The versatility of computers offers in counter-terrorism fight.

The classification of terrorist acts is based on a number of techniques including Data Mining (DM) and Knowledge Discovery in Databases (KDD) (Thuraisingham, 2002; Han *et al.*, 2012; Elovici *et al.*, 2004). DM generates patterns, some of which are useful information, that was previously hidden to the owner or to the general public. KDD extracts useful patterns from a pool of data using different techniques including DM. The generated patterns drive decision support systems to assist humans to in effective decision-making (George, 2010).

Artificial Neural Network (ANN) and Fuzzy Logic (FL) are machine learning tools that rely on numeric data type to function and can learn from historical and operational data. ANNs are fault-tolerant and are basically used situations where known information is used to infer some unknown information. FL on the other hand is very good at handling vague, ambiguous or imprecise information as well as being a powerful modeling tool for complex systems with high level of uncertainties and partial truths, which are characteristics of terrorist behaviors and activities (Akinyokun, 2002). The application of machine learning (ML) techniques in prediction, classification and clustering patterns amongst others have been widely reported. Inyaem *et al.* (2010a) used fuzzy ontology to extract terrorism events, while classification of terrorism events using fuzzy inference system (FIS) and adaptive neuro-fuzzy inference system (ANFIS) was carried out in Inyaem *et al.* (2010b). In order to evaluate supply chain management, Thipparat (2012) made use of ANFIS. Inyang and Akinyokun (2014) proposed a hybrid knowledge discovery system for oil spillage risks pattern classification using ANFIS. Adnan and Rafi (2015) used co-clustering approach to extract patterns from the global terrorism dataset. Dwivedi *et al.* (2014) identified clustering as a potent tool in counter-terrorism and therefore developed an enhanced clustering algorithm for use in the fight against terrorism in the society. Stoffel (2010) used Fuzzy CMean clustering to analyze forensic data. In Marapan *et al.* (2008) an approach for countering terrorism using soft computing model known as Competitive Neural Tree (CNeT) was adopted. In (Akinyokun *et al.*, 2015), fuzzy logic-driven expert system for the diagnosis and classification of heart failures was presented.

This paper aims at conceptualizing an intelligent platform for classifying terrorists' acts using neuro-fuzzy and clustering-based techniques. The specific objective is to design a knowledge base (comprising of knowledge warehouse, neural network, fuzzy logic) and a neuro-fuzzy clustering system for terrorists acts classification and to propose a model for assigning numerical weights to qualitative terrorists attributes. Section 2.0 carries out a review of related works while the conceptualization of neuro-fuzzy and clustering technique for classification of terrorists' acts is presented in Section 3.0. Conclusion of the research and the references are presented in Section 4.0 and Section 5.0 respectively.

Related Works

In Motaz *et al*. (2015), hybrid classification algorithms for terrorism prediction in Middle East and North Africa is presented. The research is conducted in three major steps namely data reduction, data removal and experimentation using Waikato Environment for Knowledge Analysis (WEKA) software for the prediction and classification of terrorist groups. The reaserch yileded unstisfactory predictive accuracy and are not suited for uncertain, inaccurate, incomplete and complex situations like terrorism. Ghada and Omar (2015) presents an experimental study of classification algorithms for prediction of terrorism. Although the work offered approaches for handling missing data, compared and evaluated different classification algorithms implemented in WEKA-Naïve Bayes, K-Nearest Neighbour, Tree Induction, Iterative Dichotomiser and Support Vector Machine, it was limited by its inability to incorporate current methods that can enhance classification of terrorist groups as terrorist groups. Inyaem *et al*. (2010b) adopted Fuzzy Inference Systems (FISs) to classify terrorism events in four major steps; feature selection, information extraction, transformation of text data to list of vectors and construction of classification model. The research indicated that ANFIS is efficient in the prediction of terrorism events but could not provide accurate grouping of tactics of terrorists. Othman and Yau (2007) formulated a classification technique for bioinformatics problems using ANFIS and FCM clustering in an attempt to memorize the data pattern supplied as input to the developed system. Inyang and Akinyokun (2014) developed and applied a hybrid knowledge discovery system for classification of oil spillage risks pattern, by adopting NN, FL and GA to develop an intelligent hybrid system that assisted in identification, extraction and classification of oil spillage risk patterns. Its inability to perform a comparative analysis of ANFIS performance with GA as the learning algorithm was a major limitation.

In AL-Himyari (2014), an adaptive neuro-fuzzy model with fuzzy clustering is proposed for nonlinear prediction and control where the FCM clustering is used to initialize the ANFIS. The research contributed an ANFIS model for non-linear prediction and control but was unable to model the uncertainties and ambiguity inherent in engine operations and could not learn and recall the initial states of the system. Javiad *et al*. (2016) proposes segmentation and classification of calcification and hemorrhage in the brain using FCM and ANFIS. The research developed a method that segments and classifies brain hemorrhage using contrast, correlations, energy and homogeneity as input features. Although it provided a means of significantly classifying brain abnormalities, it lacked the ability to deal with the uncertainty and vague measurements of brain abnormalities inputs. In Ziasabounchi and Askerzade (2014), a classification model for adaptive neuro-fuzzy inference system for prediction of heart diseases is presented. A model for classifying the degree of heart diseases using ANFIS is developed. The research is limited by the inadequate input parameters that can be used for different databases and inability to initially partition the dataset in order to present a preliminary pattern for the classifier. A subjective weighting method based on group decision making for ranking and measuring criteria values is presented in Abbas *et al.* (2011). It contributed a subjective weighting method used to generate relative weights to different criteria. The research suffers from the fact that the number of decision makers that respond in the ranking and scoring of the criteria is inadequate to present a reasonable and dependable judgment. It also lacks standardized values for the weights of the criteria as it used group total which is not a good representation of a set of data. Reby *et al.* (1997) presents NN as a classification method in the behavioral sciences. Data for the research was gathered from the groans of four fallow deer bucks which were tape-recorded during the rut. It contributes a classification method for behavioral sciences using NN but lacks the facility to deal with the problem of imprecision in the vocalization patterns of the animal under study.

Conceptualization of Intelligent Clustering Methodology

The architecture of the conceptualized FCM-ANFIS model for classification of Terrorists Acts is shown in Figure 1. The major components in the architecture are knowledge base, inference engine, knowledge mining engine and decision support engine.

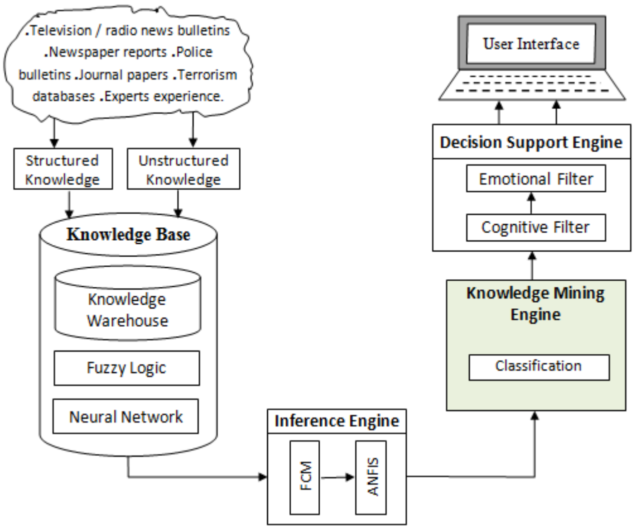

Figure 1 Architecture of FCM-ANFIS System for Terrorists Acts Classification

Knowledge Base

The Knowledge Base (KB) is a repository for semantically related and well organised facts, rules, events and attributes of terrorists acts modelled in a relational form. The unstructured knowledge is the knowledge acquired by domain experts through experience, guesses and informed judgements. The KB comprises, Knowledge Warehouse (KW), FL and NN. KW holds of heterogeneous knowledge obtained from multiple information sources containing historical, subjective and aggregate knowledge on terrorist activities. It is modeled as the star schema (Figure 2) and snowflake schema (Figure 3) are used as the building blocks for the KW. The star schema consists of a large central table known as fact table and a set of smaller dimension tables displayed in a radial pattern around the fact table (Han *et al.*, 2012). The snowflake schema consists of a central fact table and a set of constituent dimension tables which can be further broken down into sub-dimension tables (Levene and Loizou, 2003). The star schema of the Terrorist Acts facts table is shown in Figure 2. The star schema for the Terrorist Groups facts table is presented in Figure 3. The star schema for Casualty facts table is presented in Figure 4. The snowflake schema of the Terrorist Acts facts table is shown in Figure 5.

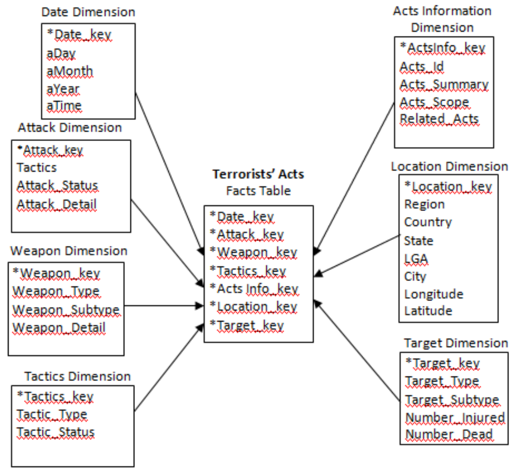

Figure 2: Star Schema for the Terrorist Acts Facts Table

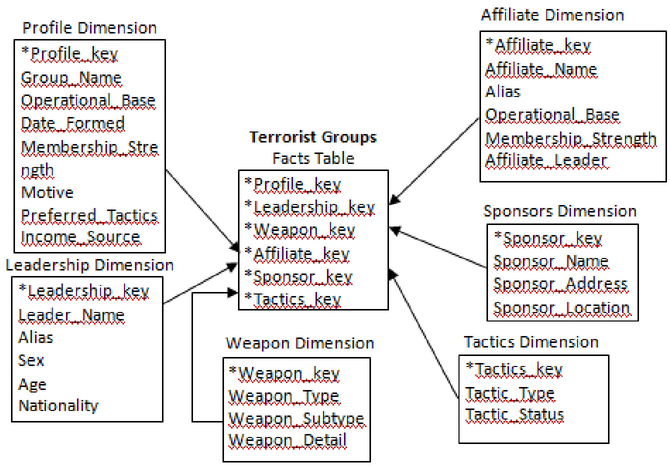

Figure 3: Star Schema for the Terrorist Groups Facts Table

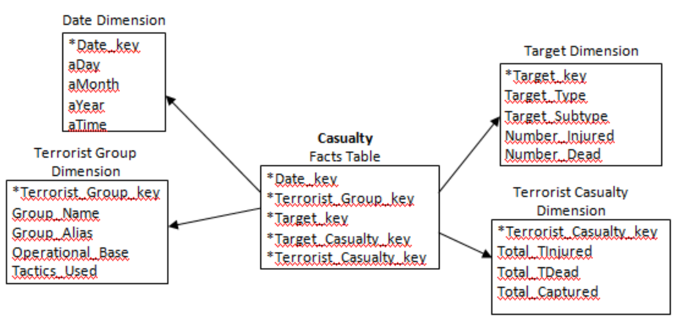

Figure 4: Star Schema for Casualty Facts Table

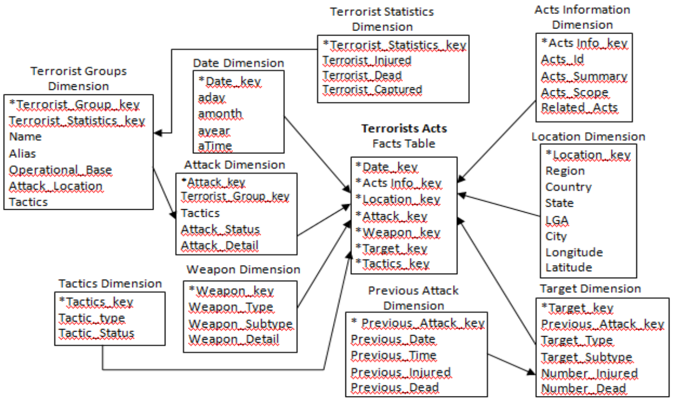

Figure 5: Snowflake Schema of the Terrorist Acts Facts Table

The snowflake schema of the Terrorist Groups facts table is shown in Figure 6. Its dimensions are as described in Figure 3. In this schema, the Leadership Dimension gives rise to the Training Dimension represented by the Training key and it contains Training_Place, Trainer, Trainer_Sex and Trainer_Origin. The Affiliate Dimension gives rise to the Sub_Affiliate Dimension represented by sAffiliate_key and contains sAffiliate_Name, sAffiliate_Alias, sOperational_Base, sMembership_Strength and sAffiliate_Leader.

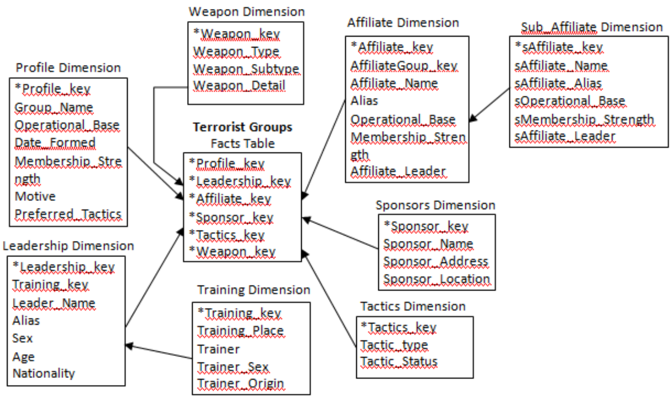

Figure 6: Snowflake Schema of the Terrorist Groups Facts Table

The KW is obtained by integrating all the facts tables into the facts constellation schema. Therefore, the KW integrates the Terrorist Acts facts table, Terrorist Groups facts table and the Casualty facts table shown in Figure 7.

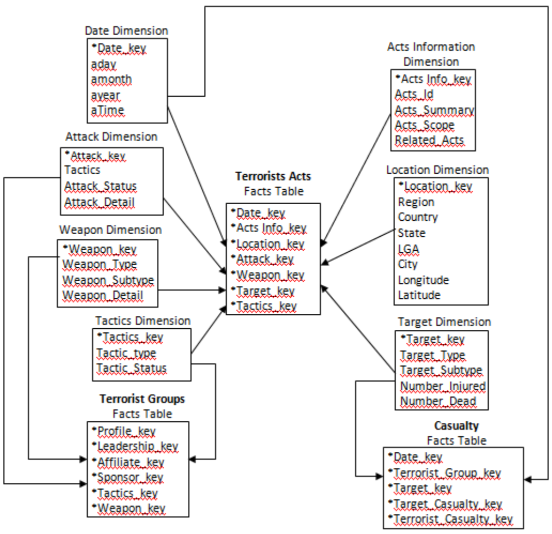

Figure 7: Facts Constellation Schema of Knowledge Warehouse

The Terrorist Acts facts table and Terrorist Groups facts table share the Attack Dimension (Attack_key and containing Tactics, Attack_Status and Attack_Detail) and Weapon Dimension (weapon_key and containing Weapon_Type, Weapon_Subtype and Weapon_Detail) while the Terrorist Acts and Casualty facts tables share the Target Dimension represented by Target_key and containing Target_Type, Target_Subtype, Number_Injured and Number_Dead.

Weight Assignment Model for Qualitative Data Attributes

In the terrorism domain, several qualitative data such as tactics used by terrorists, weapons used for attacks, the type of victims/target of attacks characterize the data set in addition to a few other quantitative data. Therefore, numerical representation of such qualitative data, taking into consideration their relative significance in the overall system, poses some challenges. A case that needs attention involves taking decisions in terms of prioritization and assignment of weights to several qualitative criteria and sub-criteria. There is the need to advance the application of neuro-fuzzy models to operate on qualitative data by applying some transformation techniques.

Suppose m decision experts are given the assignment to rank each criterion in order of priority (importance) by giving scores based on a given scale, a model for assigning numerical weights to the different criteria is is given in Equation 1 (Abbas *et al*., 2011)

$$V_i = \sum_{r=1}^{R} f_r \bar{x}_r \qquad , i = 1,2, \dots , n \tag{1}$$

V_i is the value of the ith criterion, r is the assigned rank, R is the number of ranks, f_r is the frequency of rank r and $\bar{x}_r$ is the mean of scores under rank r. Hence, the weight of the ith criteria (W_i) is the normalized value given as follows:

$$W_i = \frac{V_i}{\sum_{i=1}^{n} V_i} \tag{2}$$

Fuzzy Logic Design

The design of the FL subsystem is shown in Figure 8. It consists of fuzzification, fuzzy inference engine and defuzzification. The fuzzy logic component provides the inference under cognitive uncertainty (Inyang, 2012). At the fuzzification stage input data in the real world domain are transformed to linguistic terms in the fuzzy domain. The general form of the generated fuzzy set is shown in Equation 3.

$$S = \{\mu_S(x_i) : x_i \in X\}, \; i = 1, 2, \dots, n \tag{3}$$

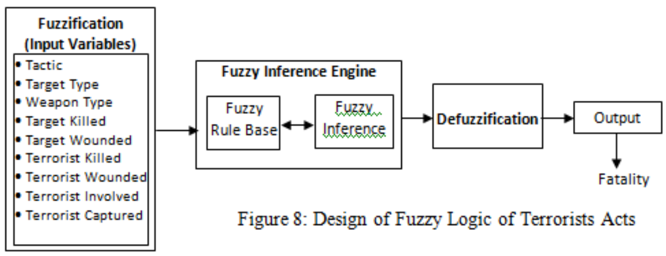

Figure 8: Design of Fuzzy Logic of Terrorists Acts

x_i is the terrorists act attribute in the universe of discourse X and $\mu_S(x_i)$ is the degree of membership of x_i in the fuzzy set *S*. The Triangular Membership Function (TMF) given in Equation 4 is adopted for the fuzzification of terrorists acts attributes.

$$\mu_S(x_i) = \begin{cases} 0 & \text{if } x_i < a \\ \dfrac{x_i - a}{b - a} & \text{if } a \le x_i < b \\ \dfrac{c - x_i}{c - b} & \text{if } b \le x_i < c \\ 0 & \text{if } c \le x_i \end{cases} \quad (4)$$

a, *b*, *c* are the parameters that govern the shape of the TMF. TMF has been shown to perform better than several other membership functions such as trapezoidal, bell-shaped, Gaussian and pi-shaped (Inyang and Akinyokun, 2014; Udoh, 2016). The terrorists acts attributes with their corresponding codes for use in the system are presented in Table 1.

Table 1 Terrorists Acts Input Parameters

SN	Parameter	Code
1	Tactics at *i*th incident	T_i
2	Weapon Type at *i*th incident	W_i
3	Victim/Target at *i*th incident	V_i
4	Number of Victim/Target Killed at *i*th incident	G_i
5	Number of Victim/Target Wounded at *i*th incident	D_i
6	Number of Terrorists Killed at *i*th incident	R_i
7	Number of Terrorists Wounded at *i*th incident	S_i
8	Number of Terrorists Involved at *i*th incident	P_i
9	Number of Terrorists Captured at *i*th incident	Q_i
10	Severity (Class Label) at *i*th incident	F_i

In this research, Sugeno inference mechanism is used to form production rules with the general format:

R_1: IF W_i is low AND V_i is low AND G_i is low AND D_i is low AND R_i is low AND S_i is low AND P_i is low AND Q_i is low THEN F_i= mild

R_2: IF W_i is low AND V_i is low AND G_i is low AND D_i is low AND R_i is low AND S_i is low AND P_i is low AND Q_i is high THEN F_i = mild

....

R_k: IF W_i is high AND V_i is high AND G_i is high AND D_i is low AND R_i is low AND S_i is low AND P_i is low AND Q_i is low THEN F_i = moderate

R_{k+1} IF W_i is high AND V_i is high AND G_i is high AND D_i is high AND R_i is low AND S_i is low AND P_i is low AND Q_i is high THEN F_i= severe

....

R_{n-1} IF W_i is high AND V_i is high AND G_i is high AND D_i is high AND R_i is high AND S_i is high AND P_i is high AND Q_i is high THEN F_i = very severe

R_n IF W_i is medium AND V_i is medium AND G_i is high AND D_i is high AND R_i is low AND S_i is low AND P_i is low AND Q_i is high THEN F_i= very severe

The centroid method used for defuzzification of terrorists acts is given in Equation 5 (Udoh, 2016):

$$Y = \frac{\sum_{i=1}^{n} \mu_A(x_i) z_i}{\sum_{i=1}^{n} \mu_A(x_i)} \quad (5)$$

where *Y* is the crisp value representing the fatality measure of a terrorist act, $\mu_A(x_i)$ is the membership function of terrorist acts parameters and z_i is the MAXMIN parameter of the membership functions.

Neural Network Design

A three layered feed forward NN with terrorists acts input parameter layer $x_i: i = 1,2,\dots,n$, hidden processing layer $h_j: j = 1,2,\dots m$, Fatality output layer $o_k: k = 1$; where *n* is the number of nodes in the input layer and *m* is the number of nodes in the hidden layer. The NN design has nine (9) nodes at the input layer, six (6) nodes at the hidden layer. The hidden layer receives and processes the signals from the input layer using the connection weights and hyperbolic transfer function. The output node represents the fatality measure of the terrorists acts generated through the connection weights of the hidden layer using sigmoid transfer function. The computed output is compared with the desired output and the difference, which is the error term, is used to adjust the connection weights by means of a back-propagation algorithm. The process is repeated until the error term is within the acceptable threshold. Figure 9 shows the proposed NN model for terrorists acts classification.

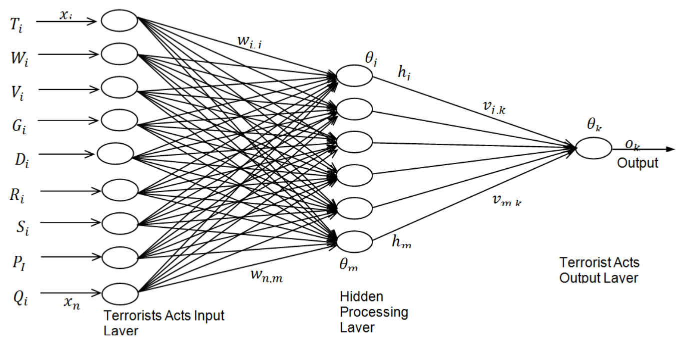

Figure 9 NN model of Terrorists Acts classification

The outputs of the hidden layer (h_j) and output layer (o_k) are as follows:

$$h_j = f\left(\sum_{i=1}^{n} w_{i,j}\, x_i - \theta_j\right), \quad j = 1,2,\dots,m \quad (6)$$

$$o_k = f\left(\sum_{j=1}^{m} v_{j,k}\, h_j - \theta_k\right), \quad k = 1,2,\dots,p \quad (7)$$

f is the neuron activation function, $w_{i,j}$ is the connection weight between the input layer *i* and the hidden layer *j*, x_i is the input vector from the *i*th input layer nodes, $v_{j,k}$ is the connection weight between the hidden layer *j* and the output layer *k*, h_j is the hidden layer output while θ_j and θ_k are the bias terms of the hidden and the output layers respectively.

The error vectors of output layer (e_k) and hidden layer (e_j) are computed as follows:

$$e_k = o_k(1 - o_k)(d_k - o_k) \quad (8)$$

d_k is the desired output.

$$e_j = h_j(1 - h_j) \sum_{j=1}^{m} w_{k,j}\, e_k \quad (9)$$

Weight updating between output and hidden layer nodes is based on Equation 10 while that between hidden and input layer nodes is based on Equation 11.

$$v_{j,k} = v_{j,k} + \eta h_j e_k \quad (10)$$

where η is the learnng rate.

$$w_{i,j} = w_{i,j} + \eta x_i e_j \quad (11)$$

The updating of the bias at output layer and hidden layer is shown in Equations 12 and 13 respectively.

$$\theta_k = \theta_k + \eta e_k \quad (12)$$

$$\theta_j = \theta_j + \eta e_j \quad (13)$$

A system of equations formulated for the input and hidden layers is given in Equation 14.

The system of Equations can be represented as: $W_{i,j}x_i = h_i$ where $W_{i,j}$ is the matrix of weights on the connection from the jth node in the hidden layer to the ith node in the input layer, x_i is the terrorists acts input vector and h_j^* is the hidden layer pre-output (output to be acted on by transfer function). It can also be represented as in Equation 15.

$$\begin{pmatrix} w_{1,1}x_1 + w_{1,2}x_2 + \cdots + w_{1,m}x_n \\ w_{2,1}x_1 + w_{2,2}x_2 + \cdots + w_{2,m}x_n \\ \vdots \\ w_{n,1}x_1 + w_{n,2}x_2 + \cdots + w_{n,m}x_n \end{pmatrix} = \begin{pmatrix} h_1^* \\ h_2^* \\ \vdots \\ h_m^* \end{pmatrix} \quad (14)$$

$$\sum_{j=1}^{m}\sum_{i=1}^{n} W_{i,j}x_i = h_j^* \quad (15)$$

The actual output at the hidden layer node h_j is obtained by subjecting the pre-output in Equation 14 to the hyperbolic transfer function shown in Equation 16.

$$h_j = \frac{e^{h_j^*} - e^{-(h_j^*)}}{e^{h_j^*} + e^{-(h_j^*)}} \quad (16)$$

Similarly, the computation in the output layer node is performed. Let $W_{j,k}$ be a matrix of weights that connects the k^{th} output layer node to the j^{th} hidden layer node and o_k^* is the pre-output value at the output layer. Output Equation is formulated as shown in Equation 17 and compressed in equations 18.

$$w_{1,1}h_1 + w_{1,2}h_2 + \cdots + w_{1,m}h_m = o_k^* \quad (17)$$

$$\sum_{i=1}^{p}\sum_{j=1}^{m} v_{j,k}h_j = o_k^* \quad (18)$$

The actual value of the output layer node, O_k, is obtained by subjecting the pre-output in Equation 19 to the sigmoid transfer function presented as follows:

$$o_k = \frac{1}{1 + e^{-(o_k^*)}} \quad (19)$$

Inference Engine

The FCM is used to assign membership values to every data point in the dataset which then serve as input to ANFIS. The inference engine comprises FCM Clustering and ANFIS

Fuzzy C-Means (FCM) Clustering

The Fuzzy C-Mean technique presented in (Chittineni and Bhogapathi, 2011; Hegde *et al*., 2015; Othman and Yau, 2007) is adapted for this research. FCM clustering is based on iterative optimization of objective function given as follows:

$$J_m = \sum_{k=1}^{n}\sum_{i=1}^{c} \mu_{i,k}^m \|x_k - c_i\|^2 \quad (20)$$

$\|x_k - c_i\|^2$ is the Euclidean distance between the feature vector, x_k, and the cluster centre, c_i. The choice of Euclidean distance is premised on its higher performance for FCM clustering over other distance-measuring techniques. The optimization takes place under the following constraints:

$$\sum_{i=1}^{c} \mu_i(x_k) = 1, \qquad for\ each\ k = 1,2,\ldots,n \quad (21)$$

$$0 \le \sum_{k=1}^{n} \mu_i(x_k) \le n, \qquad for\ each\ i = 1,2,\ldots,c \quad (22)$$

where $\mu_i(x_k)$ is the membership degree of feature vector (data points) x_k in cluster i, c is the total number of clusters and n is the total number of feature vector. The algorithm needs a fuzzification parameter m in the range [1, n] which determines the degree of fuzziness in the clusters. FCM algorithm behaves like a crisp clustering algorithm if m = 1 whereas for larger values of m the overlapping of clusters increases.

ANFIS Model

A five-layer ANFIS is used for the research as presented in Figure 10. The first and fourth layers are adaptive nodes with learning parameters while the second, third and fifth layers are fixed nodes without learning parameters. The input vector x_i, which is the output of the FCM process, is supplied to the ANFIS. The FCM contributes to the performance of ANFIS as the cluster centres generated and used in initializing the weights of back-propagation networks such as used in ANFIS help to yield reduction in training time (Jiang and Kam Siew Wah, 2003). The input is selected from several variables such as tactics (T_i), weapon type (W_i), victim type (V_i), number of victims killed (G_i), number of victims wounded (D_i), number of terrorists killed (R_i), number of terrorists wounded (S_i), number of terrorists involved in the operation (P_i) and number of terrorists captured (Q_i).

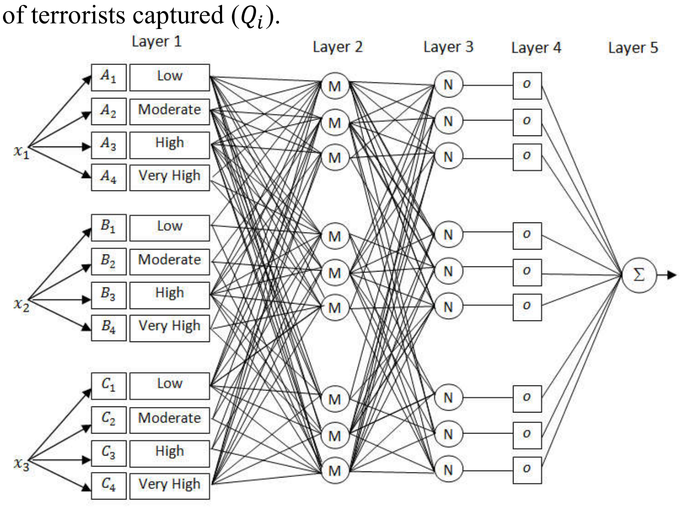

Figure 10 Architecture of ANFIS

The operations at each layer of the ANFIS are given as follows:

Layer 1 is the input fuzzification layer where each node, i, has a node function given as follows:

$$o_i^1 = \mu_{A_i}(x_i) \tag{23}$$

where x_i is the external input data of terrorists acts to node i: $i = 1, 2, \ldots, n$ and A_i is the linguistic label, determined as follows:

$$A_i = \begin{cases} Low & if\ x_i < 0.1 \\ Medium & if\ 0.1 \le x_i < 0.3 \\ High & if\ 0.3 \le x_i < 0.6 \\ Very\ \text{High} & if\ 0.6 \le x_i \le 1.0 \end{cases} \tag{24}$$

In other words, O_i^1, which is supplied by the FCM, is the membership function of x_i in A_i which specifies the degree of membership of x_i in the universe of discourse, A_i.

Layer 2, labelled *M*, is the rule node where each node multiplies the incoming signals as shown in Equation 3.80, in order to generate the firing strength of a rule.

$$w_i = \mu_{A_i}(x_1) * \mu_{B_i}(x_2) * \mu_{C_i}(x_3) \tag{25}$$

Layer 3 is the normalization node, labelled *N* and it computes the ratio of the *i*th rule's firing strength to the sum of all rules' firing strengths shown in Equation 26. The layer produces the normalized firing strengths.

$$o_i^3 = \overline{w}_i = \frac{w_i}{\sum_{i=1}^{n} w_i} \tag{26}$$

Layer 4 is the defuzzification node. It contains the consequent nodes which compute the contribution of each rule to the overall output as follows:

$$o_i^4 = \overline{w}_i f_i = \overline{w}_i (p_i x_1 + q_i x_2 + r_i x_3 + s_i) \quad i = 1,2,3 \tag{27}$$

$\overline{w}_i$ is the output of Layer 3 which is the normalized firing strength (or weight) of rules governing terrorist activities, f_i is the output of the fuzzy set of signals; x_1, x_2, x_3 represent the input (antecedent) parameters and p_i, q_i, r_i, s_i are the consequent parameters.

Layer 5 contains only a single node with a simple summing function for all incoming terrorist signals. It is the output node given as follows:

$$o_i^5 = Y = \sum_i \overline{w}_i f_i = \frac{\sum_{i=1}^{n} w_i f_i}{\sum_{i=1}^{n} w_i} \tag{28}$$

The hybrid learning algorithm is used in this research due to its effectiveness. In the forward pass of the hybrid learning algorithm, the node output traverses forward up to layer 4 and update the consequent parameters by least square method (Inyang and Akinyokun, 2014; Udoh, 2016; Inyaem *et al.*, 2010b). In the backward pass, the error signal propagates backwards and updates the premise parameters by gradient descent (back-propagation) method (Udoh, 2016; Inyaem, 2010b). For example, in the hybrid learning algorithm, the overall output in the forward pass can be expressed as linear combinations of consequent parameters set $\{p_i, q_i, r_i, s_i\}$. If there are three input variables $x_1 = x$, $x_2 = y$ and $x_3 = z$, the output can be represented as follows:

$$\begin{aligned} Y &= \sum_{i=1}^{n} \overline{w}_i f_i = \overline{w}_1 f_1 + \overline{w}_2 f_2 + \overline{w}_3 f_3 \\ &= (\overline{w}_1 x_1)p_1 + (\overline{w}_1 y_1)q_1 + (\overline{w}_1 z_1)r_1 + \overline{w}_1 s_1 + (\overline{w}_2 x_2)p_2 + (\overline{w}_2 y_2)q_2 + \\ &\quad (\overline{w}_2 z_2)r_2 + \overline{w}_2 s_2 + (\overline{w}_3 x_3)p_3 + (\overline{w}_3 y_3)q_3 + (\overline{w}_3 z_3)r_3 + \overline{w}_3 s_3 \end{aligned} \tag{29}$$

Suppose there are k entries for terrorist acts training data set, let *U*, *B* and *V* be the matrix of premise parameters, consequent parameters and desired output representing the fatality of terrorist acts respectively. They are presented as follows:

The interaction of *U*, *B* and *V* can be compressed as shown in Equation 30.

$$UB = V$$

where, *B* is an unknown vector whose elements are from the consequent parameters set. This is a standard linear least square problem and the best solution for *B* is the least square estimator (LSE), $B*$, which minimizes the squared error $\|UB - V\|^2$ between the computed and the desired output and is given as follows:

$$B^* = (U^T U)^{-1} U^T V$$

U^T is the transpose of *U* and U^{-1} is the inverse of *U*.

Knowledge Mining Engine

The knowledge mining engine carries out classification of the fatality of a terrorist's act using the data obtained from the inference engine. The classification of a terrorist's act is given as follows:

$$C = f(A\{\delta\}) \tag{32}$$

where $f(A\{\delta\})$ is a function of $A(\delta)$, $A(\delta)$ is the FCM-ANFIS inference engine output, *A* is the ANFIS function and δ is a set of terrorists act attributes membership values generated by FCM.

The fatality class C_F is determined as follows:

$$C_F = \begin{cases} Mild & if\ \ A\{\delta\} < 0.1 \\ Moderate & if\ \ 01 \le A\{\delta\} < 0.3 \\ Severe & if\ \ 0.3 \le A\{\delta\} < 0.6 \\ Very\ Severe & if\ \ 0.6 \le A\{\delta\} \le 1.0 \end{cases} \tag{33}$$

The fatality class serves as input to the Decision Support Engine where decision concerning the particular terrorist act is taken and appropriate response is carried out to mitigate or control the effects and re-occurrence of the act. The knowledge mining engine also classifies terrorists acts based on aggregate components of a location such as States and Local Government Areas of a country.

Decision Support Engine Design

The Decision Support Engine (DSE) helps the user of the system to make informed decision on the next course of action. DSE uses the unstructured knowledge of terrorism domain experts in making judgments on the outcome of the FCM-ANFIS platform. The components of the DSE are as follows:

1. Cognitive filter
2. Emotional filter

Cognitive Filter

The cognitive filter analyzes the output of the FCM-ANFIS platform and recommends a course of action based on the objective judgment of terrorism domain experts. In a typical act for illustration, a large truck loaded with explosive devices runs into a major motor park and started releasing series of explosions where survivors scamper for safety. At the motor park nearby surrounding, automatic gun shots attacking people were heard. The FCM-ANFIS system output can be any of the classes of terrorists acts such as “Very Severe”, “Severe”, “Moderate” and “Mild”. The classes of terrorists acts that serve as input to the cognitive filter and the possible course of action to take are described as follows:

Very Severe Terrorists Acts

In a very severe terrorists acts classification, the decision to address the incident may include the following:

1. Mobilize counter-terrorism and other security agents to the scene of incident.
2. Barricade the surrounding location and deploy bomb disposal squad to comb the area for hidden explosives.
3. Deploy anti chemical, biological, radiological and nuclear (CBRN) attack experts to the scene and its environs.
4. Urgently engage the services of fire fighters at the scene.
5. Engage the urgent services of a national or state emergency response team.
6. Intensify air surveillance of the environment.
7. Engage the services of emergency medical personnel.

Severe Terrorists Acts

In a terrorist attack classified to be severe, the following decisions may be taken:

1. Mobilize counter-terrorism experts and other security agents to the scene of incident.
2. Barricade the surrounding location and deploy bomb disposal squad to comb the area for hidden explosives.
3. Deploy anti chemical, biological, radiological and nuclear (CBRN) attack experts to the scene and its environs.
4. Urgently engage the services of fire fighters to the scene.
5. Engage the urgent services of a national or state emergency response team.
6. Intensify air surveillance of the environment.
7. Engage the services of emergency medical personnel.

Moderate Terrorists Acts

In a moderate terrorists act, the decision taken may include but not limited to the following:

1. Mobilize counter-terrorism experts and other security agents to the scene.
2. Barricade the surrounding location and deploy bomb disposal squad to comb the area for hidden explosives.
3. Intensify security at vulnerable targets.
4. Engage the urgent services of a national or state emergency response team.
5. Engage the services of emergency medical personnel.

Mild Terrorists Acts

For a mild terrorist’s act, the following decisions and other ones may be taken:

1. Mobilize counter-terrorism experts and other security agents to the scene.
2. Barricade the surrounding location and deploy bomb disposal squad to comb the area for hidden explosives.
3. Intensify security at vulnerable targets.
4. Engage the urgent services of a national or state emergency response team.
5. Engage the services of emergency medical personnel.

Emotional Filter

The emotional filter of the DSE analyses the output of the system and recommends a course of action based on the subjective feelings of terrorism domain experts. For example, a group of terrorists invaded an airport departure hall, started shooting sporadically in the air and hold the occupants hostage. Anybody who tries to escape is shot dead. Among the passengers are major government officials. At the expiration of a deadline of two hours given to the government to respond to their demands, one sampled individual is killed after every thirty minutes. The actions that may be taken based on the subjective feelings of experts and government are the following:

1. A decision to enlist the assistance of the military in enforcing security at a scene of terrorism and the environs.
2. A decision to follow up on a previous intelligence on an impending terrorist’s act which was not beforehand considered serious.
3. The use of high-ranking anti-terrorism officers at the scene of an attack to boost the morale of junior officers.
4. A decision to organize post-terrorism act preparedness awareness campaigns for the citizens.
5. A decision to solicit foreign assistance on tracking of suspected terrorists sponsors’ bank accounts.
6. The use of new or old post-attack response tactics based on the experience from similar acts that took place in the past.
7. A decision to consider a terrorist act as a preamble to an impending major attack.
8. A decision to limit the use of certain weapons against the terrorists in an attempt to rescue defenseless citizens.
9. A decision whether to follow a link or not, left at the scene of attack by the terrorists.

CONCLUSION

Terrorism has been one of the most worrisome violence in the world that threatens the peace of the citizens. Several approaches have been adopted to tackle the menace but it seems to be on the increase. This research has proposed a conceptualized approach using a neuro-fuzzy and clustering based technique that can predict and classify the acts of terrorism in order to assist in preventing its occurrence or mitigate its effect if it takes place. This work serves as a veritable analytic and decision support tool in the terrorism domain. The implementation of the design and evaluation of its performance with data on terrorist activities is a topic for further research.

References

Abbas, T., Mahdi, H., Masoumeh, A. & Pouneh, A. (2011). A Subjective Weighting Method Based on Group Decision Making For Ranking and Measuring Criteria

Values. *Australian Journal of Basic and Applied Sciences*, *5*(12), 2034-2040.

Adnan, M. & Rafi, M. (2015). Extracting patterns from Global Terrorist Dataset (GTD) using Co-Clustering approach. *Journal of Independent Studies and Research* - Computing *13*(1), 7-13.

Al-Himyari, B. A., Yasin, A. & Gitano, H. (2014). Adaptive neuro-fuzzy model with fuzzy clustering for nonlinear prediction and control. *Asian Journal of Applied Sciences* (ISSN: 2321 – 0893) *02*(03), 343-348.

Dwivedi, S., Pandey, P., Tiwari, M. S., & Kalam, M. A. (2014). Comparative study of clustering algorithms used in counter terrorism. *Journal of Computer Engineering* (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, *16*(6), Ver. VIII, 13-17.

Elovici, Y., Kandel, A., Last, M., Shapira, B., & Zaafrany, O. (2004). Using data mining techniques for detecting terror-related activities on the Web. *Journal of Information Warfare 3*, 1-13.

Ghada. M. T. & Omar. S. S. (2015). An experimental study of classification algorithms for terrorism prediction. *International Journal of Knowledge Engineering*. *1*(2), 107-112.

Inyaem, U., Horuechaiyasak, C., Meesad, P., & Tran, D. (2010b). Terrorism event classification using fuzzy inference systems. *International Journal of Computer Science and Information Security 7*(3), 247-256.

Inyang, U. G. & Akinyokun, O. C. (2014). A hybrid knowledge discovery system for oil spillage risks pattern classification. *Journal of Artificial Intelligence Research*, *3*(4), 77-86.

Javiad, Q., Arif, M. & Talpur, S. (2016). Segmentation and classification of calcification and hemorrhage in the brain using fuzzy c-mean and adaptive neuro- fuzzy inference system. *QUAID-E-AWAM University Research Journal of Engineering, Science & Technology*. *15* (1), 50-63.

Marappan, K, Nallaperumal, K, Kannan, K. S. & Bensujin, B. (2008). A soft computing model to counter terrorism. *International Journal of Computer Science and Network Security*. *8*(5), 141-147.

Motaz, M. H. Khorshid, Tarek, H. M. Abou-El-Enien & Ghada, M. A. Soliman (2015). Hybrid classification algorithms for terrorism prediction in Middle East and North Africa. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *4*(3), 23-29. ISSN 2278-6856.

Othman, M. F & Yau, T. M. S. (2007). Neuro-fuzzy classification and detection technique for bioinformatics problems. *Proceedings of the First Asia International Conference on Modelling & Simulation*. IEEE Computer Society. 1-6.

Reby, D., Lek, S., Dimopoulos, I., Joachim, J., Lauga, J. & Aulagnier, S. (1997). Artificial neural networks as a classification method in the behavioural sciences. *International Journal of Behavioural Processes. Elsevier Sciences. 40* (1997), 35-43.

Stoffel, K., Cotofrei, P., & Han, D. (2010). Fuzzy methods for forensic data analysis. Proceedings of the International Conference on Integration Techniques in Computational Forensics,1-6.

Thipparat, T. (2012). Application of adaptive neuro fuzzy inference system in supply chain management evaluation. Faculty of Management Sciences, Prince of Songkla Universit, Kohong Hatyai, Songkhla, Thailand.

Ziasabounchi, N. & Askerzade, I. (2014). ANFIS-Based classification model for heart disease prediction. *International Journal of Electrical & Computer Sciences*, *14* (02), 7-12.

How to cite this article:

George Uduak D *et al* (2018) 'Conceptualization of Intelligent Clustering Methodology For Terrorists Acts Classification In Nigeria', *International Journal of Current Advanced Research,* 07(7), pp. 14200-14208.
DOI: http://dx.doi.org/10.24327/ijcar.2018.14208.2567

****