Terrorism prevention: a mathematical model for assessing individuals with profiling

Oludare Isaac Abiodun[1†]

School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia
Nigerian Defence Academy, Kaduna, Nigeria

Aman Jantan[††], Abiodun Oludare Esther Omolara[†††], Manmeet Mahinderjit Singh [††††], Mohammed Anbar[†††††]

School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia
Correspondent Author: Aman Jantan

Kemi Victoria Dada[††††††]

Department of Statistics, Faculty of Science, Ahmadu Bello University Zaria, Nigeria

Summary

The act of terrorism in the last two decades has caused society of many damages and developmental setbacks in which the cost may be inestimable as trillions of United States Dollars have been lost globally. This study provides an empirical model technique for assessing individuals towards terrorism using people's profiling to mitigate frequency attacks. Though, there have been research efforts in the direction of terrorism prevention yet assessing individuals with profiling on a large scale through empirical model remains a gap in literature. This research used least square regression technique to generate a mathematical or empirical model that can assessed individual tendency towards crime such as terrorism. During data analysis and model evaluation, a profile of one hundred people was selected by random sampling. The experimental result shows a record of 97.34% assessing accuracy on the generalized test. Assessing rate shows the effectiveness and superiority of the model when compared with some state-of-the-art algorithms and models on terrorism prevention studies such as using data mining technique, machine learning algorithms, fuzzy logic, social media analysis models, knowledge-based framework, anomalies detection etc. Hence, this work proposes a simple but efficient method of the least square empirical model for assessing individuals' tendency towards terrorism.

Key words:

Security, people's profiling, integration, empirical model, assessing individual, and terrorism prevention.

1. Introduction

There has been research on terrorism prevention such as identifying dangerous materials like chemical, biological, radiological, nuclear [1,2,3,4] suicide bombing [5] and the use of air defense systems counter measures for attacks [6]. While, some study focused on the different attacks in terrorism by modeling their relationship, [7] rather than pattern of individual terrorists (as people) and applying empirical analysis to detect such individuals [7]. Some work concentrates on location of vulnerable safe places for terrorist hide-out using geographical information system [8].

Meanwhile, other researchers continued terrorist activity detection by investigating the individual incident in terrorism [9]. Other prevention measures include focused on the use of social network analysis, knowledge-based, software, encryption, scenario planning [10, 11], application of operation research models [12] analytical models [13,14,15,16], and game-theoretic models [17, 18] to explore uncertainty about terrorist activities. Other current approaches such as confronting, preventing violent extremism and deradicalization are having little effects [19]. Recently, the use of inference statistics was common among the researchers. Nevertheless, the continued used of explanatory and descriptive statistics will remain because of its usefulness in providing an evidence. However, for the current trend in the forensic study and future perspective, there is need to be more focus on empirical research not only for a better performance and accuracy but for more proving evidence in terrorism prevention [20,21,22,23]. Nowadays, digital forensic pieces of evidence are gathered from the medium such as e-mails, internet browser histories [24,25,26]. Although security agencies are actively working on the prevention, detection, investigation and prosecution of potential terrorists. However, preventing all attacks and assessing individual tendency toward terrorism is quite difficult that the most dangerous terrorist attack is caused by "individual actors [19]. A trained individual terrorist or criminal is capable of death and destruction using improvised weapons [28,29,30,31,32]. Just as an individual with a potentially lethal weapon who has peaceful intentions, does not pose a threat.Though the recent research approaches to terrorism has been encouraging.

Manuscript received July 5, 2018
Manuscript revised July 20, 2018

However, most terrorism research methods are fragmentary, as they lack validations and have few empirical analysesthat could provide evidence and, they are typically inconclusive [19].

Therefore, to addressed these problemsof fragmentary, validation and analysis,this research propose people's profiling method as a solution to terrorism in the society. The scope of the study is within crime prevention techniques through people's profiling. The motivation for this research originates from the past and present security challenge of terrorism in the society. Also, this research effort will be beneficiary to the government security organizations like police, army, intelligent agencies, immigration, custom, and prison unit. Furthermore, this work will be useful to communities, nations and global society effort to finding a solution to terrorism security challenge.

2. Security screening to counter-terrorism

Over the past decade, security screening to counter - terrorism has become a high-priority issue of national interest and concern especially at aviation sector and public places [33]. The motorist and passenger screening operation at highway, bus station and motor part, railway station, super-markets, hotels, schools, holidays centers, seaport and an airport terminal can be subdivided into multiple screening stages, with decisions made to assign each traveler to one of several available security groups at each such stage. An individual passenger's assessed attack threat or risk value may first have determined by an automated prescreening machine system is updated after the passenger proceeds through each screening stage.

Though, designing flexible screening policies that provide optimal security under imperfect individual risk information can be quite challenging. However, such some flexible screening policies are necessary for the adequate security of lives and properties. The screening rule must be strategic and not give the terrorist an advantage to attack for example behavioral detection must be introduced or integrated by government security agencies to detect anomalous or suspicious behavior by individuals or passengers in the major city and non-city terminals. Such character can be questioned or interrogated and possibly referred to police or immigration officers.

In a terrorism, prevalent society security screening is a critical component of road-networks, railway station, market and supermarket, public offices and buildings, seaport and airport systems. Thus, an improved security checkpoint separates certain individuals into a secure, enclosed wanding station for further security screening. Regrettably, the traditional testing system deployment by various security personnel was not only insufficient but ineffective and inefficient for assessing individual towards terrorism. Crime prevention through the traditional security multiple searches can be tedious, time wasting, inefficient and without significant success as illustrated in Figure 1.

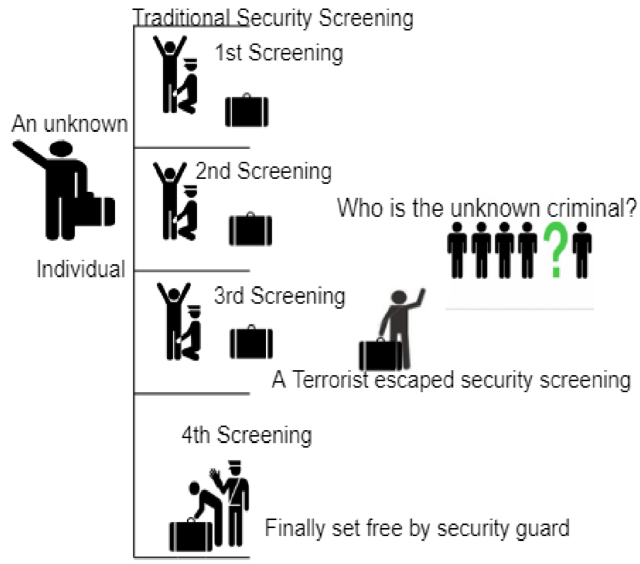

Fig. 1 Traditional crime prevention technique: assessing or screening of individuals towards crime.

3. Preliminaries

Case I- In a Bayesian network analysis and queueing theory:

Given that k = 1,2,...,K, i = 1,2,...,k, and m = 0,1,...,k, define random variables Zm,ik such that

(i) $$Z^{k}_{o,1} \equiv +\infty,\ for\ 1 \leq i \leq k \quad (1)$$

(ii) $$Z^{k}_{m,i} \equiv -\infty, for\ m > k - i + 1 \quad (2)$$

(iii) $$\left[AT_i^{(l)} v\ E\left[Z^{k}_{m,\ i+1} \middle| F_i\right]\right] \wedge E\left[Z^{k}_{m-1,\ i+1} \middle| F_i\right] \quad (3)$$

(iv) $$Z^{k}_{1,k} \equiv AT_i^{(l)} \quad (4)$$

(v) $$\left[AT_i^{(l)} v\ E\left[Z^{k}_{m,\ i+1} \middle| F_i\right]\right] \wedge E\left[Z^{k}_{m-1,\ i+1} \middle| F_i\right] \quad (5)$$

$$for\ 1 \leq m \leq k - i + 1, and\ for\ i \leq k - 1$$
$$for\ 1 \leq m \leq k - i + 1, and\ for\ i \leq k - 1$$

where, F_i , i= 1,2,...,kis a sigma field over all possible realizations of vector $\{AT_i^{(l)}\}_{m=1,}^{k}$ $k = 1, 2, 3, \dots K$, and the notations v and $\wedge$ imply maximum and minimum, respectively.
Then considering stage l >1, when there are k = 1,2,...,K remaining individuals to test at "k" security screening in "intervals." If for each individual i= 1, 2, . . . ,k, partition the line segment [0,1] ⊂ R into k−i+ 1 random intervals defined by the breakpoints 0, such as,

$$E\left[Z_{k-i,\ i+1}^{k}\middle|F_i\right], E\left[Z_{k-i,\ i+1}^{k}\middle|F_i\right], \dots, E\left[Z_{1,\ i+1}^{k}\middle|F_i\right], 1.$$

Then, the optimal assignment (OA) is to assign the ith individual to the mth most secure interval remaining if $at_i^{(l)}$ lies in the mth highest interval or, **alternatively**, if

$$Z_{m,i}^{k} = at_i^{(l)}.$$

Case II-Probability theory:
In a profiling approach on airport security screening, William Press proposes a mathematical method known as "square root biased sampling technique" [34]. The square-root-biased sampling is a mathematically optimal compromise between random sampling and strong profiling that can identify a criminal, given fixed screening resources [34]. In this technique if the probability of finding a criminal is z + 1st looks such as;
(1-tm*)*tm $(\mathbf{1 - t_m}*)^{\mathbf{x}}\mathbf{t_m}*$ and the probability of not finding the criminal is exactly z ≥ 0 looks,
where, a single criminal is expressed as K = m*.$\mathbf{k = m}*$
Then the average $\mu_{\mathbf{D}}$ "μ" "$\mu_{\mathbf{D}}$"of looks needed can be given as;

$$\mu_D = \sum_{z=0}^{\infty}(z+1)(1-t_m*)^{x}t_m* = 1/t_m* \quad (6)$$

Also, the expectation can be given over the remaining random variable, namely, that value m is $m*$. This expectation can minimize the subject to $\sum t_i = 1$, which can be stated as;

$$\mu_D = \sum_{z=1}^{N} p_m/t_m \quad (7)$$

Then minimizing with a Lagrange multiplier to the optimal choice for the *tm's* as;

$$p_m = \frac{t_{m^{\frac{1}{2}}}}{\sum_{i=1}^{N} t_{m^{\frac{1}{2}}}} \quad (8)$$

and the mean number "μ_D" of tests per discover criminal can be written as;

$$\mu_D = \left(\sum_{z=1}^{N} t_{m^{\frac{1}{2}}}\right)^2 \quad (9)$$

The equation (9) indicates that individuals should be selected for screening proportionally to the *square root* of prior probability. The use of "priors" for screening make the screening to be weak because it can result in secondary screening being distributed over a much larger segment of the population compare to "strong profiling". Therefore, equation (9) should be a known result, in a simple way, if there is only a single criminal [34].
The critiques of the square-root-biased sampling technique are that it is biased since the tests are not uniform among the people asbeing a citizen of a country does not make someone not to be a potential terrorist.
Assessing an individual's tendency towards crime is a vision-based empirical model for crime prevention that requires robust mathematical expression, i.e. an expression that can be applying to people's profiling. The output of people's profiling is the fundamental element in the subsequent process of detecting a criminal [31, 35]. The fundamental task of this process is to separate the criminal from the non-criminal [35]. According to Jonathan Rae, [35] "If people's profiling is possible, it would be an irresistibly attractive method for countering crimes such as cybercrime, network intrusion or terrorist attacks as it would maximize the efficiency of prophylactic resource allocation, increasing the likelihood of the interception of an attack".
Security measures allow the public to continue to live normal lives even in an increasingly dangerous world. As a result of the increasing dangers in the society, security precautions are becoming common parts of modern life. For instance, security checkpoints at public locations provide increased safety to the public through the screening, location, and collection of identified harmful materials, thereby helping to prevent the presence of these harmful materials in the public places. In exchange for this increased safety, the public are made to trades inconvenience and loss privacy.

4. Security Intelligence Service

People's profiling can help to discover behavioral frequencies (normal and abnormalities), and patterns that can lead to attributing in identifier a person involved in a crime. An example of profiling is a rapist profiling, theft profiling, robbery profiling, cybercriminal profiling, network intruders profiling and terrorist profiling. Which can be used to focus on a criminal at populations within a crowd of legal residence, foreigners, travelers for example at the airport terminal, seaport, rail station, bus station etc. In his study of security screen at the airport, a researcher named William Press at the University of Texas at Austin has found that secondary security screening at airports is mathematically flawed and has identified a way to select people for screenings more efficiently and fairly [34]. Basic criminal assessing, or suspicion indicators can be of the form in Figure 2.

Fig. 2 Basic crime assessment indicators and process

As highlighted in Figure 1, the basic crime assessment or indicators can begin from the situation at hand. The situation means in a security attempt to prevent terrorism, an individual can be assessed or suspected based on some indicators this include behavior, appearance, belongings, documents, and person's story.

5. Intelligence Cycle

In some country security intelligence service has a unique assessment process [36]. The process follows in conducting investigations, collecting intelligence, assessing it and reporting to the Government can be illustrated in what is known as the "security intelligence cycle". Identifying terrorism threats include the first stage of the cycle is the identification of a potential threat. Terrorism threats to security of lives and properties could arise from: long-term circumstances such as the presence of organization working under some form of cover, or short-term circumstances for example, a visit to ones' country by someone thought to be pursuing a terrorist objective. Before decision action to investigate a potential threat, there must be a clear understanding of what that threat comprises, so that any investigation is appropriate and effectively directed. This security intelligence cycle can be illustrated as in Figure 3.

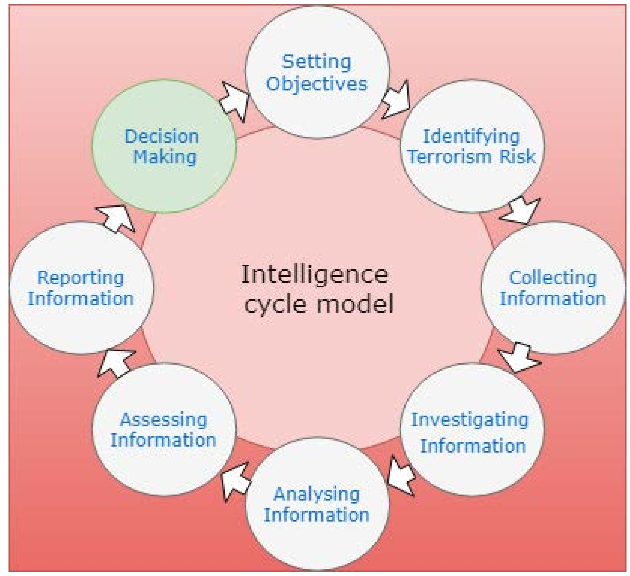

Fig. 3 An illustration in form of intelligence cycle

Collection of information: Once data has been collected, the next phase is to examine it, which involves assessing and Figure 4.

Fig. 4 Data collection and investigation processes

An investigation processes involves extracting the relevant pieces of information from the collected data. Then analysis involves extraction of relevant data to draw conclusions. Reporting is the process of preparing and presenting the outcome of the analysis. Therefore, intelligence model involves capturing, recording and analysis of network events to discover the source of attacks.

6. Proposed new method

Recent advances in mathematics, statistics and computer science provide a powerful tool for modeling complex probability distributions by automatically discovering intermediate abstractions from a huge number of basic features. This paper proposes least square regression model

to peoples profiling to mitigate terrorism attacks.The ordinary least square modeling involves the use of statistical techniques that allow the recognition of patterns in large quantities of data, aggregated in databases. When these patterns or relationships are used to identify or represent people, they can be called profiling.
The profiling information such as behavior, belongings, documents in possession, organization membership, email activities, website affiliation, social media profiles, phone records analysis, and banking activities. Other include travel records, nationality, occupation, marital status, office address, residential address, handwriting recognition etc.
All these profiles information was extracted and analyzed on a hundred individual and collectively, using least squares regression model. The aims at performing the analysis of one hundred people for assessing individuals using profiling is demonstrated in the proposed modeling Figure 5.

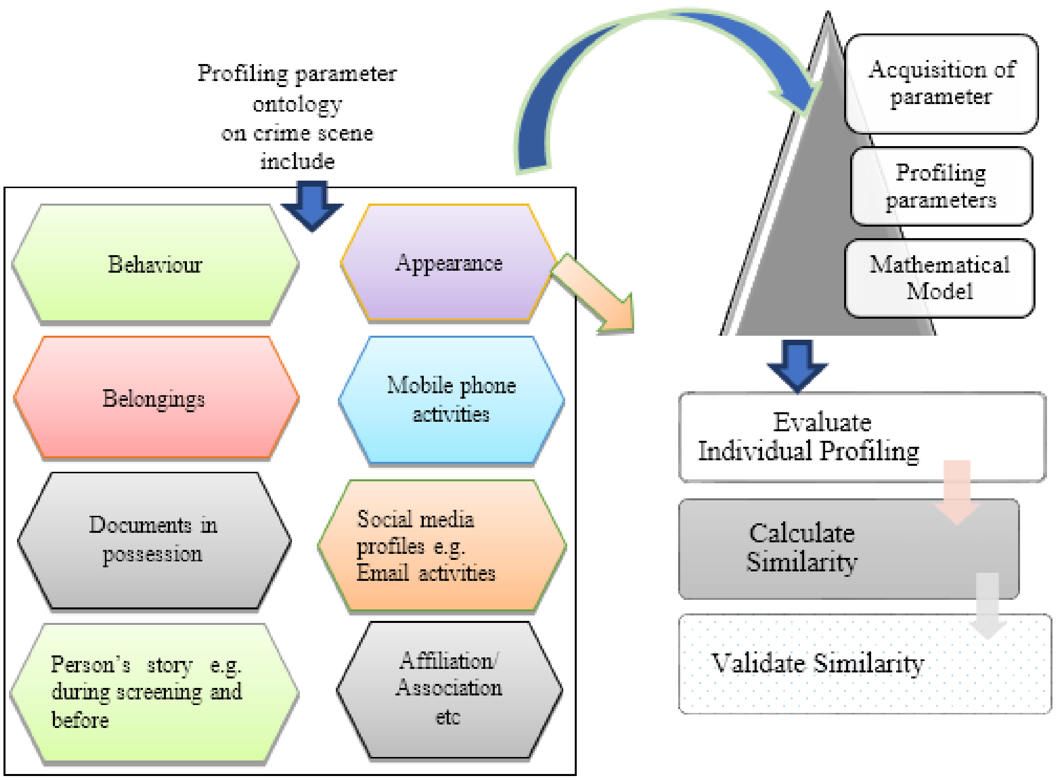

Fig. 5 Flow chart of the proposed model

Mathematical proof;
Let parameter "y"assume to be a linear combination of some independent input parameter plus some independent parameter referred to as disturbance or noise "ε". The way the independent parameters are combined is defined by a variable vector:$y = X\lambda + \epsilon$. Also, assuming that the disturbance term is drawn from a standard Normal distribution:$e \sim N(0,1)$. For some estimate of the model variables$\hat{\lambda}$, the model's prediction errors/residuals "e" are the difference between the model prediction and the observed output values and this can be express as;

$$e = y - X\hat{\lambda} \tag{10}$$

The ordinary least squares (OLS) solution to the problem (means determining an optimal solution for $\hat{\lambda}$) involves minimizing the sum of the squared errors with respect to the model variables, $\hat{\lambda}$. Then the sum of squared errors is equal to the inner product of the residuals vector with itself$\Sigma e_i^2 = e^T e$:
where,

$$e^T e = (y - X\hat{\lambda})^T (y - X\hat{\lambda})$$
$$= y^T y - y^T (X\hat{\lambda}) - (X\hat{\lambda})^T y + (X\hat{\lambda})^T (X\hat{\lambda})$$
$$= y^T y - (X\hat{\lambda})^T y - (X\hat{\lambda})^T y + (X\hat{\lambda})^T (X\hat{\lambda})$$
$$= y^T y - 2(X\hat{\lambda})^T y + (X\hat{\lambda})^T (X\hat{\lambda})$$
$$= y^T y - 2\hat{\lambda}^T X^T y + \hat{\lambda}^T X^T \hat{\lambda}$$

i.e,

$$e^T e = y^T y - 2\hat{\lambda}^T X^T y + \hat{\lambda}^T X^T \hat{\lambda} \tag{11}$$

Then, determining the estimator of the model variables, $\hat{\lambda}$, and minimizing the sum of squared residuals with respect to the variables, then let integrate as follow;

$$\frac{\partial}{\partial \lambda}[e^T e] = 0$$

$$= -2x^T y + 2x^T x\hat{\lambda}$$

$$\text{Hence,} \quad x^T y = x^T x\hat{\lambda} \qquad (12)$$

due to the identity $\frac{\partial a^T b}{\partial a} = b$, for vectors a and b. Thus, this relationship is matrix form of the Normal Equations. Therefore, solving for $\hat{\lambda}$ gives the analytical solution to the ordinary least squares problem as:

$$\hat{\lambda} = (aX^T X)^{-1} X^T y \qquad (13)$$

Ordinary least squares regression are parametric, in that the regression function is defined in terms of a finite number of unknown variables that are estimated from the dataset.
In the dataset approach to this research, values of numbers were assigned to each parameter to form a dataset because in dataset parameter design approach Sarah Bouslaugh and Paul Andrew Watters [48], stated that "Before you can use statistics to analyse a problem, you must convert information about the problem into data. That is, you must establish or adopt a system of assigning values, most often numbers, to the objects or concepts that are central to the problem in question. This is not an esoteric process but something people do every day" [37].
Therefore, to obtain a dataset from each variable of people's profile parameters, in each of the different design model of people's profiling, a regression analysis technique was applied with the aid of a statistical software. Francis Chin, and Gultekin Ozsoyoglu [38] stated maintained that the "design of a statistical database should use a statistical security management facility to enforce the security problems at the conceptual model level".
In the analysis of individual terrorist, linear and generalized regression modeling provide a set of tools apply to data in the form of cases (named groups) by variables (traits and behaviors of the groups).

7. Experimental results and discussion

The result of the test is a generalised empirical expression, Ỳ, for detecting individuals as a function of the stipulated input parameters, Xi: i = 1,2,3,…,100, was obtained as model equation from the given original equation;
Y = ao + a1x1+a2x2+a3x3+…+a100x100 + ∈k……as in (1)

I. The Mathematical model

$$\begin{aligned}
\grave{Y} = {} & 0.3159 -0.0236x_1+0.0171x_2+0.0004x_3+0.0002x_4-2.0757x_5-0.1133x_6+0.0209x_7-0.0018x_8+2.62284x_9+0.0454x_{10}+0.0075x_{11}+0.0455x_{12}+1.91172x_{13}-0.4660x_{14}-0.0003x_{15} \\
& +0.0083x_{16}+0.0003x_{17} -0.0554x_{18}+1.0857x_{19}-0.6780x_{20}-0.0471x_{21}+0.0070x_{22}+0.0012x_{23} \\
& +0.0003x_{24}-2.0257x_{25}-0.1134x_{26}+0.0106x_{27}-0.0019x_{28}+0.0319x_{29}+0.0461x_{30}-0.0472x_{31}+0.0071x_{32}+0.0001x_{33}+0.0002x_{34}-2.0757x_{35}-0.1133x_{36}+0.0208x_{37}-0.0018x_{38}+2.61173x_{39}+0.0454x_{40}+0.0075x_{41}+0.0455x_{42}+1.91172x_{43}-0.4660x_{44}-0.0001x_{45} \\
& +0.0083x_{46}+0.0003x_{47} -0.0554x_{48}+1.0857x_{49}-0.6780x_{50}-0.0471x_{51}+0.0070x_{52}+0.0012x_{53} \\
& +0.0003x_{54}-2.0257x_{55}-0.1134x_{56}+0.0106x_{57}-0.0019x_{58}+0.0319x_{59}+0.0461x_{60}-0.0472x_{61}+0.0071x_{62}+0.0001x_{63}+0.0002x_{64}-2.0757x_{65}-0.1133x_{66}+0.0105x_{67}-0.0018x_{68}+2.61173x_{69}+0.0454x_{70}+0.0075x_{71}+0.0455x_{72}+1.91172x_{73}-0.4660x_{74}-0.0001x_{75} \\
& +0.0083x_{76}+0.0003x_{77} -0.0554x_{78}+1.0857x_{79}-0.6780x_{80}-0.0471x_{81}+0.0070x_{82}+0.0012x_{83} \\
& +0.0003x_{84}-2.0257x_{85}-0.1134x_{86}+0.0106x_{87}-0.0019x_{88}+0.0319x_{89}+0.0461x_{90}-0.0472x_{91}+0.0071x_{92}+0.0189x_{93}-0.064x_{94}-0.0557x_{95}+0.1130x_{96}+0.0036x_{97}- 0.0016x_{98} \\
& +0.02164x_{99}+0.05922x_{10} \qquad (14)
\end{aligned}$$

$$\text{i.e. } \grave{Y} = 0.97342$$

Therefore, Ỳ = 0.97.342 ≅ 97% detection rates of crime, or a prediction of 97.34% accuracy, where Ỳ is acceptable at, Ỳ < 1 i.e. the summation of Ỳ is less than 1, and 0.3159 is constant, the Xi's represent parameters or independent variables of each person's profiling.
This is an interesting result of mathematical model used for crime detection using people's profiling. The mathematic formula have ability to capture large number of people such as in hundreds to billions for assessment on crime at once to generate an instant output if data are readily available. Equation (14), is referred to as the model equation of Ỳ. The equation (14) is an important design empirical equation which can be used to predict or determine the degree or value of the individual's in the generalized empirical expression, Ỳ, from given values of Xi, which are the independent variables. The sum of the calculated value of the model, Ỳ, from given values of Xi, is given as 0.97342 Therefore, Ỳ is predicted at; 0.97.342 or an approx., 97%, that means Ỳ, is significant and acceptable for generalized detecting prediction on the individual.

II. Summary of F-test statistical data and validations

The coefficient of determination, R2, of the model is presented in Table IV, which indicates goodness-of-fit of the regression and shows the percentage of the variation in Y that could be accounted for by the one hundred (100) X variables. In this work, it is observed that 97.34% of prediction, Ỳ, could be accounted for by these one hundred (100) Independent Variables, X; while, perhaps 2.67% could be explained by other factors. The errors are being minimized at 2.741936 x 10-3, while the absolute percentage error obtained is 0.412.

In making decisions involving validity, Andrew Siegel and other researchers have shown that R2 can be used in testing the validity of a model [20,39,40,41]. Since the model (equation (5)) produced R2 of 0.89625 or approximately 90% it means that R2 = 0.89625 is greater than the benchmark scale or threshold value of R2 = 0.673 or 67.3°% for n =15 and k = 1,2,3,…,15, this stand at the acceptable level of validity. Thus, this model equation is significant at the given significant level of 5%.The summary of the F-test statistics on people's profiling detecting prediction is presented in Table I.

Table 1: Summary of F-test statistics on people's profiling detection prediction

Parameter	**Value**
Dependent Variable	Y (100)
Ind Independent Variables	X(100,000)
Coefficient of Determination, (R2)	0.97342
Coefficient of Variation	0.0508
Mean Square Error, MSE	0.002741936
Square Root of MSE	0.052363499
Average Absolute % Error	0.412
Number of observations, n	20

Table II presents the result of t-test statistics on an individual profile.In Table II there are values of the regression coefficients, b(i), and the t-values for every independent variable X_i. This gives the validity or acceptability of each of the independent variables.

Table 2: Computational results for the model validation process

Independent variable	**Regression Coefficient**	**Standard Error Sb(i)**	**t-value to test Ho=B (i)= 1**	**Probability Level**	**Reject Ho at 5%**	**Power of test at 5%**
X2	0.0741	0.0398	4.021	0.1876	Yes	0.0119
X11	0.0081	0.0081	3.172	0.3493	Yes	0.1405
X17	0.0001	0.0002	3.222	0.4528	Yes	0.1062
X25	0.0000	0.0000	3.124	0.5443	Yes	0.0858
X29	-2.1867	2.3786	3.044	0.3886	Yes	0.1256
X31	-0.1143	0.0508	3.024	0.0593	Yes	0.4917
X34	0.0105	0.0261	3.016	0.698	Yes	0.0643
X36	-0.0018	0.0116	3.004	0.8743	Yes	0.0523
X38	2.7283	0.7913	3.012	0.0108	Yes	0.8392
X40	0.0564	0.0891	3.460	0.5463	Yes	0.0856
X42	0.0085	0.0132	2.440	0.5381	Yes	0.088
X44	0.0543	0.0274	2.480	0.0881	Yes	0.4015
X47	0.0418	0.0168	2.960	0.0419	Yes	0.572
X55	-0.576	0.3913	3.360	0.1838	Yes	0.2478
X65	0.0000	0.0000	2.840	0.5443	Yes	0.0858
X76	-2.1867	2.3786	2.180	0.3886	Yes	0.1256
X85	-0.1143	0.0508	3.860	0.0593	Yes	0.4917
X95	0.0105	0.0261	3.405	0.698	Yes	0.0643

In Table II the t-values of nineteen suspected peoples among the one hundred peoples sampled and tested on profiling in which their t-value are significantly higher than threshold t-value 2.365. As each X's, has a calculated t-values of 4.021, 3.172, 3.222, 3.124, 3.044, 3.024, 3.016, 3.004, 3.012, 3.460, 2.440, 2.480, 2.960,3.360, 2.840, 2.180, 3.860,3.405 and 3.575 respectively.

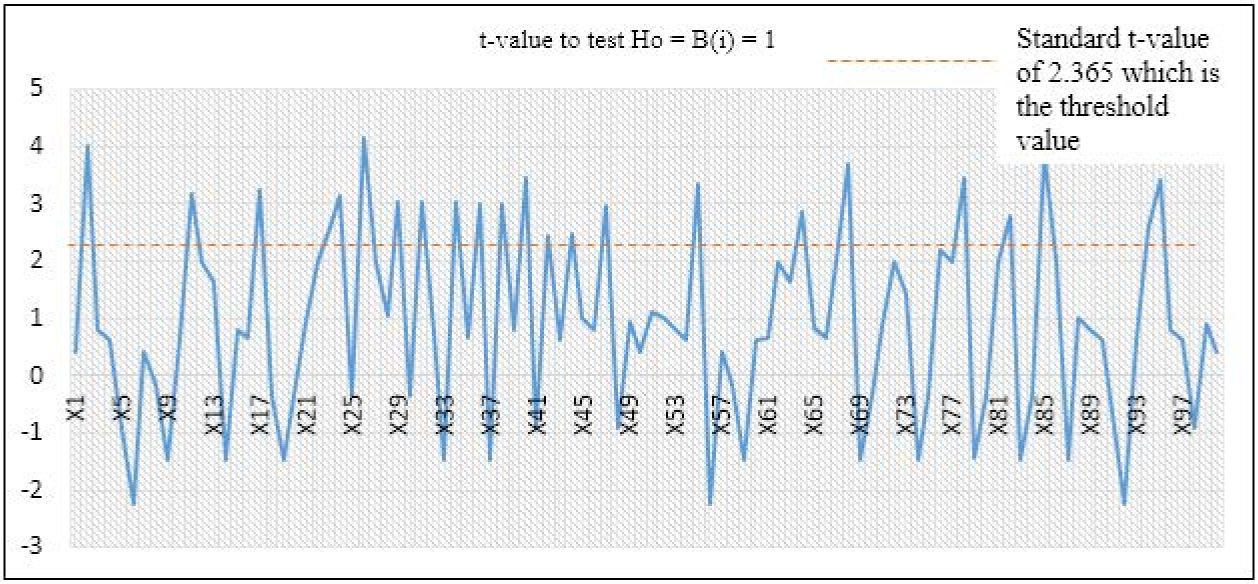

Fig. 6 Graphical representation of t-value as a function of the people's profiling

The dotted line in Fig. 6, demarcate the standard t-values of 2.365 from the resulting variables of people's profiling that are significantly higher than 2.365. Hence, the plot above the dotted line indicates the ten notable indicators for assessing an individual for a crime. Therefore, for acceptability, it is required that at least one of the t-values of the input parameters exceeds the threshold value, the developed model equation is acceptable by the t-test validation. Furthermore, the graph representation of the regression coefficient, bi, as a function of the input parameters, Xi: i = 1,2,3,…,100, is shown in Figure7.

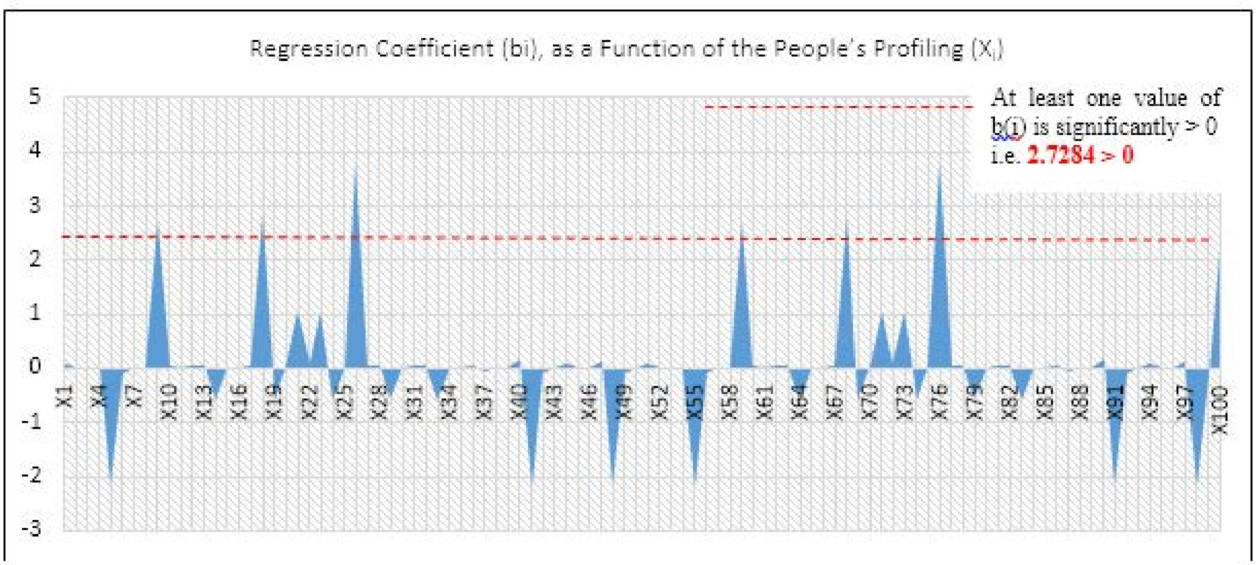

Fig. 7 Graphical representation of regression coefficient, bi, as a function of the people's profiling

Figure 7 clearly show the validation of the use of the empirical expression given in equation (14) for the calculation of prediction, Ỳ. To further validate the empirical model in equation (14), since at least one value of bi is not equal to zero (0) i.e. since the value of the regression coefficient, bi, for X9, X18, X21. X23, X26, X59, X68, X71, X73, X76, and X100 are significantly greater than zero, the design or model could be accepted as being valid. Moreover, it suggests that the variables (Xi's) are linearly related to, Ỳ.

8. Conclusion

With a simple mathematical model, we explored the antiterrorist effectiveness of society through individual profiling systems. The effectiveness and efficiency of the model are tested on one hundred benchmark functions with different characteristics. The results show that the proposed prevention method is efficient and effective in terms of data analysis factors such as performance, accuracy, detection speed and validations.

The research objective was achieved as there was a record of 0.97.342 or 97.34% an approximately 97% prediction on the overall testwhich signifies the level of performance. This means that people's profiling have asignificant effect toward optimizimation of security if been integrated into the system as a solution to terrorism management challenge as it will be more effective, efficient, reliable and productive.

9. Future Work

This study proposes an empirical model for assessing individual towards terrorism using people's profiling. In addition, the empirical data can aid forensic and security research [42-68] and complexity in the society like other methods currently in practice. Meanwhile, the future works will focus on combination of regression analysis and traditional spatial pattern analysis such as data clustering. Inaddition to other emerging approaches to terrorism research and integrate the developed mathematical formula into a software for assessing an individual for terrorism.

Acknowledgement

The work of the authors was supported in part by two organizations. The Center for Cyber Safety and Education, United States Internal Revenue segregated fund of (ISC)², Inc. Code. EIN: 45-2405127 through the (ISC)2 graduate cybersecurity scholarship award,311 Park Place Blvd. Suite 610 Clearwater, FL 33759 USA. Also, by Fundamental Research Grant Scheme (FRGS) for ''content-based analysis framework for better email forensic and cyber investigation" [203/PKOMP/6711426], SFRG Lab, School of Computer Sciences, Universiti Sains Malaysia, Penang, 11800, Malaysia.

References

[1] Yang, Y. T., Fishbain, B., Hochbaum, D. S., Norman, E. B., &Swanberg, E. (2013). The supervised normalized cut method for detecting, classifying, and identifying special nuclear materials. INFORMS Journal on Computing, 26(1), 45-58.

[2] Salama, S., & Hansell, L. (2005). Does intent equal capability? Al-Qaeda and weapons of mass destruction. Non-proliferation Review, 12(3), 615-653.

[3] Silke A., "A Review of the Impact of 9/11 and the Global War on Terrorism," Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security, 2008, New York, Springer.

[4] Schmid, A. P. (2016). Links between terrorism and migration. International Centre For Counter Terrorism (ICCT), ICCT Research Paper.

[5] Kaplan, E. H., Mintz, A., & Mishal, S. (2006). Tactical prevention of suicide bombings in Israel. Interfaces, 36(6), 553-561.

[6] Von Winterfeldt, D., & O'Sullivan, T. M. (2006). Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? Decision Analysis, 3(2), 63-75.

[7] Kolajo, T., & Daramola, O. (2017, March). Leveraging big data to combat terrorism in developing countries. In Information Communication Technology and Society (ICTAS), Conference on (pp. 1-6). IEEE.

[8] Eisman, E., Gebelein, J., & Breslin, T. A. (2017). Developing a geographically weighted complex systems model using open-source data to highlight locations vulnerable to becoming terrorist safe-havens. Annals of GIS, 23(4), 251-267.

[9] Schroeder, T. (2017). When security dominates the agenda: The influence of ongoing security threats on female representation. Journal of Conflict Resolution, 61(3), 564-589.

[10] Chasteen, L. (2016, May). Using scenario planning to predict/prevent future terror attacks. In Technologies for Homeland Security (HST), 2016 IEEE Symposium on (pp. 1-4). IEEE.

[11] Trope, R. L. (2004). Guarding against terrorism and liability. IEEE Spectrum, 41(1), 85-86.

[12] Wright, P. D., Liberatore, M. J., &Nydick, R. L. (2006). A survey of operations research models and applications in homeland security. Interfaces, 36(6), 514-529.

[13] Peterson, R. M., Bittel, R. H., Forgie, C. A., Lee, W. H., & Nestor, J. J. (2007). Using USCAP's analytical models, the transportation security administration balances the impacts of aviation security policies on passengers and airlines. Interfaces, 37(1), 52-67.

[14] Lee, E. K., Chen, C. H., Pietz, F., &Benecke, B. (2009). Modeling and optimizing the public-health infrastructure for emergency response. Interfaces, 39(5), 476-490.

[15] Gorman, M. F. (1998). Santa Fe Railway Uses Operating Plan Model to Improve its Service Design. Interfaces, 28(4), 1-12.

[16] Toure, I., &Gangopadhyay, A. (2016, May). Real time big data analytics for predicting terrorist incidents. In Technologies for Homeland Security (HST), 2016 IEEE Symposium on (pp. 1-6). IEEE.

[17] Wang, C., & Bier, V. M. (2011). Target-hardening decisions based on uncertain multiattribute terrorist utility. Decision Analysis, 8(4), 286-302.

[18] Gorman, M. F. (2012). Analytics, Pedagogy and the Pass the Pigs Game. INFORMS Transactions on Education, 13(1), 57-64.

[19] Quiggin, T. “On and Off the Radar: Tactical and Strategic Responses to Screening Known Potential Terrorist Attacker,”. Perspectives on Terrorism, 2017, 11, 5.

[20] Oludare, A. I., Jantan, A., Omolara, A. E., & Mahinderjit, M. M. (2018). Big Data: an approach for detecting terrorist activities with people’s profiling. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).

[21] Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 14(2).

[22] Omolara, A. E., Jantan, A., Abiodun, O. I., & Arshad, H. (2018). An enhanced practical difficulty of one- time pad algorithm resolving the key management and distribution problem. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).

[23] Stoeslein, M., Kanet, J., Gorman, M. F., Minner, S. (2013). Time-phased safety stocks planning and its financial impacts: empirical evidence based on european econometric data. International Journal of Production Economics, 149, 47-55.

[24] EviyantiSaari, Aman Jantan, (2011). F-IDS: A Technique for Simplifying Evidence Collection in Network Forensics, J.M. Zain et al. (Eds.): ICSECS 2011: Software Engineering and Computer Systems pp 693-701

[25] Mohd. Izham Ibrahim, Aman Jantan, (2011). A Secure Storage Model to Preserve Evidence in Network Forensics, J.M. Zain et al. (Eds.): ICSECS 2011, Part II, CCIS 180, pp. 391-402.

[26] Rasmi M. Aman Jantan, (2011). Attack Intention Analysis Model for Network Forensics, J.M. Zain et al. (Eds.): ICSECS 2011, Part II, CCIS 180, pp. 403-411.

[27] Popp, R., & Poindexter, J. (2006). Countering terrorism through information and privacy protection technologies. IEEE Security & Privacy, 4(6).

[28] Silke, A. “The devil you know: Continuing problems with research on terrorism,” Terrorism and political violence, 13, 4, 2001, pp. 1-14.

[29] Silke, A. (2004) “An introduction to terrorism research. Research on terrorism: trends, achievements, and failures,” 2004, pp, 1-29.

[30] Crenshaw Martha, (2004). “Current research on terrorism: The academic perspective. Studies in Conflict &Terrorism, 15,1, 1992, pp. 1-11 Schmid, A. (2004).

[31] Crawford, Kamillia (2016). To Catch a Terrorist: The Improper Use of Profiling in US Post-9/11 Counter-terrorism.

[32] Amani Mobarak AlMadahkah (2016) Big Data In computer Cyber Security Systems. International Journal of Computer Science And Network Security, Vol. 16 No. 4 pp. 56-65.

[33] Martonosi, S. E., & Barnett, A. (2006). How effective is security screening of airline passengers? Interfaces, 36(6), 545-552.

[34] Press, W. H. (2009). Strong profiling is not mathematically optimal for discovering rare malfeasors. Proceedings of the National Academy of Sciences, 106(6), 1716-1719.

[35] Rae, J. (2012). Will it ever be possible to profile the terrorist? Journal of Terrorism Research, 3(2).

[36] Hildebrandt, Mireille; Gutwirth, Serge (2008). Profiling the European Citizen. Cross Disciplinary Perspectives. Springer, Dordrecht. doi:10.1007/978-1-4020-6914-7.

[37] Bouslaugh S. and Watters,P.A. (2008) “Basic Concepts of Measurement,” Statistics in a Nutshell. 2008, 2nd Edition. Beijing, Cambridge, Farnham, Köln, Sebastopol, Taipei, Tokyo.

[38] Chin, F. Y., and Ozsoyoglu, G. (1981). Statistical database design. ACM Transactions on Database Systems (TODS), 6(1), 113-139.

[39] Browne, M. W., &Cudeck, R. (1993). Alternative ways of assessing model fit. Sage focus editions, 154, 136-136.

[40] A.F. Siegel, Practical Business Statistics. Elsevier Inc. 2012.

[41] G. Asghar, and Z. Saleh, “On normality assumption checked using plot of errors against the predicated values of the variables and on a probability scale. Testing for normality of the error distribution. Normality Tests for Statistical Analysis: A Guide for Non-Statisticians. Int J Endocrinol Metab, Springer; 10, 2, pp. 486 – 489, 2012.

[42] Mohammad Rasmi, Aman Jantan , Hani Al-Mimi. , 2013. A new approach for resolving cybercrime in network forensics based on generic process model. Jordan, ISBN: 978-9957-8583-1-5.

[43] AmirRizaan Rahman, Putra Sumari, 2009. Probability Based Page Data Allocation Scheme in Flash Memory. IEEE Pacific-Rim Conference on Multimedia (PCM 2009). Bangkok Thailand.

[44] Guetl, C., Ismail, L., & Lexar, C. (2013, July). Track A: foundations of digital ecosystems and complex environment engineering. In Digital Ecosystems and Technologies (DEST), 2013 7th IEEE International Conference on (pp. 1-1). IEEE.

[45] Shrivastava, A. K., Payal, N., Rastogi, A., & Tiwari, A. (2013, September). Digital forensic investigation development model. In Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on (pp. 532-535). IEEE.

[46] Simon Barthel, Sascha Tönnies, Benjamin Köhncke, Patrick Siehndel, Wolf-TiloBalke:
What does Twitter Measure?: Influence of Diverse User Groups in Altmetrics. JCDL 2015: 119-128

[47] Najmul Ikram Qazi, Muhammad Abdul Qadir, Muhammad Tanvir Afzal, (2018) Investigating Correlation between Protein Sequence Similarity and Semantic Similarity Using Gene Ontology Annotations. IEEE/ACM Trans. Comput. Biology Bioinform. 15(3): 905-912

[48] [48] Lytle, A., Stephens, N., Conner, J., Bashiri, S., & Jones, S. (2016). Digital Forensics and Enforcement of the Law. Newsletter, 2016.

[49] Mazurczyk, W., Caviglione, L., &Wendzel, S. (2017). Recent Advancements in Digital Forensics. IEEE Security & Privacy, 15(6), 10-11.

[50] Riaz Ahmad, Muhammad Tanvir Afzal, Muhammad Abdul Qadir: Pattern Analysis of Citation-Anchors in Citing Documents for Accurate Identification of In-Text Citations. IEEE Access 5: 5819-5828 (2017)

[51] Hana, R. O. A., de Almendra Freitas, C. O., Oliveira, L. S., & Bortolozzi, F. (2008). Crime Scene Representation (2D, 3D, Stereoscopic Projection) and Classification. J. UCS, 14(18), 2953-2966.

[52] Muhammad Tanvir Afzal: Applying Ontological Framework for Finding Links into the Future from Web. I-SEMANTICS 2009: 656-662

[53] Leong, K., Li, J., Chan, S. C. F., & Ng, V. T. (2009). An Application of the Dynamic Pattern Analysis Framework to the Analysis of Spatial-Temporal Crime Relationships. J. UCS, 15(9), 1852-1870.
[54] Moghaddam, A. S., Hosseinkhani, J., Chuprat, S., Birgani, A. M., & Keikhaee, S. (2017). Applying Social Network Analysis Techniques in Crawler Based Search Engine to Support Web Terrorism Mining. International Journal of Computer Science and Network Security, 17(8), 75-81.
[55] Omolara, A. E., Jantan, A., Abiodun, O. I., & Poston, H. E. (2018). A novel approach for the adaptation of honey encryption to support natural language message. In Proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).
[56] Faiza Anwer, Shabib Aftab, Muhammad Salman Bashir, Zahid Nawaz, Madiha Anwar (2018). Empirical comparison of XP & SXP. International Journal of Computer Science and Network Security, Vol. 18 No. 3 pp. 161-168
[57] Mohammad Rasmi, Aman Jantan, Hani Al-Mimi. , 2013. A new approach for resolving cybercrime in network forensics based on generic process model. Jordan, ISBN: 978-9957-8583-1-5.
[58] AlShehri, M. A. R. (2018). A review of mobile and sim forensics tools. International Journal of Computer Science and Network Security, 18(3), 150-154.
[59] Mohamed, N. A., Jantan, A., & Abiodun, O. I. (2018). An improved behaviour specification to stop advanced persistent threat on governments and organizations network. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).
[60] Fatemeh Halim, Salman Yussof and Mohd. Ezanee Rusli (2018), Cyber Security Issues in Smart Meter and Their Solutions. International Journal of Computer Science and Network Security, Vol. 18 No. 3 pp. 99-109.
[61] Mohd Taufik Abdullah, Ramlan Mahmod, Abdul Azim Ab. Ghani, Mohd Zain Abdullah, Abu Bakar Md Sultan (2008) Advances in Computer Forensics. International Journal of Computer Science and Network Security, Vol. 8 No. 2 pp. 215-219
[62] Mohammed Abdul Rahman AlShehri (2018). A Review of Mobile and SIM Forensics Tools. International Journal of Computer Science and Network Security, Vol. 18 No. 3 pp. 150-154.
[63] Alsolami, E. (2018). Security threats and legal issues related to Cloud based solutions. . International Journal of Computer Science and Network Security, 18(5), 156.
[64] Ahmed, A., Manzoor, A., Halepoto, I. A., Abbas, F., & Rajput, U. (2018). Security Threats and Countermeasures in Software Defined Networks. International Journal of Computer Science and Network Security, 18(4), 69-74.
[65] Ayaz Khan, Uffe Kock Wiil, Nasrullah Memon (2010). Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering.