International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 2, April 2024, pp. 1797~1808
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i2.pp1797-1808

Predictive analysis of terrorist activities in Thailand's Southern provinces: a deep learning approach

Thittaporn Ganokratanaa[1], Mahasak Ketcham[2]
[1]Applied Computer Science Program, Department of Mathematics, Faculty of Science, King Mongkut's University of Technology Thonburi, Bangkok, Thailand
[2]Department of Management Information Systems, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand

Article Info

Article history:

Received Aug 13, 2023
Revised Oct 12, 2023
Accepted Nov 29, 2023

Keywords:

Data-driven analysis framework
Deep neural networks
Event categorization and forecasting
Terrorist events prediction
Thailand's Southern border provinces

ABSTRACT

Terrorist activities have been on the rise globally, with Thailand experiencing significant challenges, particularly in its three southern border provinces. This study offers a comprehensive analysis aiming to predict forthcoming terrorist events in these provinces. We employed historical data, categorized into nine groups based on military expert recommendations, to train our prediction model. This research tested the prediction capabilities of various methodologies, including decision trees, naïve Bayesian learning techniques, and deep learning artificial neural networks. Notably, the deep neural network emerged as the superior predictive tool, achieving an impressive accuracy of 98.21% and a root mean square error (RMSE) of 0.59%. The primary anticipated events include bombings, shootings, assaults, and acts of vandalism. Our findings also revealed that Pattani Province was the most affected, accounting for 45% of incidents. Specific districts, such as Panare and Yarang, exhibited high crime rates of 40% and 36.84%, respectively. Yala Province, particularly Bannang Sata District, was identified as the hotspot for shooting incidents, with a rate of 34%.

Corresponding Author:

Mahasak Ketcham
Department of Management Information Systems, King Mongkut's University of Technology North Bangkok
1518 Pracharat 1 Rd., Wongsawang, Bangsue, Bangkok, 10800, Thailand
Email: mahasak.k@itd.kmutnb.ac.th

1. INTRODUCTION

The ongoing rise in terrorist events across various regions in many countries has inflicted a profound impact on people's lives, manifesting in various forms of violence, including the loss of loved ones, property damage, and numerous injuries, leading to a pervasive sense of insecurity in daily existence. The causative factors behind these acts of terrorism and unrest are multifaceted, ranging from suppressed grievances seldom openly discussed, provocative social environments, to the perpetuation of collective memory across generations. Bahgat and Medina's 2013 meta-analysis of counterterrorism studies [1] shed light on the influence of sociopolitical perspectives intertwined with geographic barriers, primarily due to the scarcity of high-quality geographical reference datasets and underutilized Geographic Information Systems (GIS). However, an additional dimension of territorial terrorism warrants attention. Terrorism often emerges as an endeavor to manipulate and contest political boundaries [2]. Consequently, regions lacking territorial security frequently serve as breeding grounds for terrorism [3]–[5], as the absence of effective government control fosters an environment conducive to the pursuit of autonomy by terrorist factions [6]. Highly populated and bureaucratic areas become attractive and cost-effective strategic targets, where cities with high global and regional prominence become increasingly appealing targets for acts of terrorism [7]. Furthermore, the specific motives driving acts of terrorism often exhibit geographic components. Examples include religious groups targeting individuals they perceive as immoral [8], right-wing terrorists targeting government officials [9], persecuted individuals launching attacks in everyday places like shopping malls [10], and territorial terrorists operating in familiar surroundings, creating self-reinforcing cycles in previously targeted areas that draw more attackers [11]. Additionally, there is a discernible link between the planning and preparation of attacks and the selection of target locations [12]–[15]. Thailand has been grappling with a persistent terrorist threat for over a decade, leaving a trail of trauma and psychological distress among the populace, especially in the three southern border provinces where the roots of these conflicts remain obscured. For instance, in April 2017, simultaneous explosions rocked four provinces: Pattani, Songkhla, Narathiwat, and Yala. Data from the Deep South Incident Database (DSID) revealed a staggering 19,279 incidents of terrorist events between January 2004 and April 2017, resulting in 6,544 deaths and 12,963 injuries during this period. In summary, over the past 13 years, from 2004 to 2016, a total of 19,507 individuals lost their lives or suffered injuries. These attacks often targeted police booths, police residences, and government properties, suggesting meticulous planning and target selection by local assailants who possessed knowledge of the terrain. Consequently, security forces were deployed to monitor key sites such as government offices and suspicious objects in the area to safeguard the public. However, the sporadic nature of these attacks, coupled with restrictions on surveillance in previously targeted areas, renders it challenging to predict whether similar incidents will occur in the vicinity or when the next attack might take place.

The technological response to these challenges has seen a rise in innovative solutions. Machine learning, especially tools based on Python due to its extensive library support and community-driven enhancements, has been at the forefront of these endeavors. In response to these challenges, Singh *et al.* [15] proposed a real-time terrorist threat prevention system based on hidden Markov chains for analyzing historical attacks. Dixon *et al.* [16] introduced a model for detecting suspicious behavior using a feed-forward neural network (NN), achieving an accuracy rate of 0.6 with a success rate of 0.68. Ensemble techniques were also employed to forecast attacks, resulting in accuracy ranging from 0.79 to 0.85 [17]. Mo *et al.* [18] applied various models, including logistic regression (LR), support vector machine (SVM), and naïve Bayes classifiers, with the highest accuracy reaching 0.78. Recently, Uddin *et al.* [19] proposed a prediction model for terrorist and weapon attacks using NNs, SVM, LR, and naïve Bayes classification, with deep NNs outperforming other techniques with an accuracy of 0.95, while others achieved a maximum accuracy of 0.83. Furthermore, these authors conducted analyses and predictions of future threats based on the previous ten attack events [20]. Historical analyses and the application of big data have profoundly informed our understanding of terrorism patterns. For instance, Krieg [21] developed a model for predicting terrorism, suggesting that such acts seem to occur as independent events rather than continuous processes. This notion underscores the challenges inherent in predicting such sporadic acts. Further, the emphasis on state-centric model translations by Krieg signifies the uniqueness of each region's terrorism dynamics. Similarly, Ozgul [22] delved into terrorist detection and prediction using crime prediction model (CPM) on a dataset encompassing various terrorist events in Turkey. His approach focused on unsolved crimes and clustered them based on event similarities for superior predictions.

The scope of research on detecting and predicting terrorist attacks is extensive. While some have focused on classifying tweets related to terrorism [23], our work primarily aims at predicting the actual terrorist events. This distinguishes our approach from other studies primarily geared towards the detection facet using attack features [24]–[27]. Further innovations, such as Ramya's hybrid deep learning, random forest, and naïve Bayes (DRN) models, which uniquely combines deep learning (DL), random forest (RF), and naïve Bayes algorithms, highlight the field's evolving nature, pushing the boundaries of prediction accuracy [28]. Further expanding the horizons of terrorism research, Buffa *et al.* [29] introduced a model for terrorism detection and prediction, which incorporated geospatial and population dynamics of European crime events. Their methodology captured a wide spectrum of terrorist activities, ranging from organizational progressions to escalations in attack lethality, within specific geographical and temporal parameters [30]–[35]. Python *et al.* [36] and Li *et al.* [37] also made significant strides in understanding the continuous nature of terrorism events and classifying terrorism within broader paradigms. In recent studies, data mining techniques have been instrumental in addressing various real-world challenges. Adekitan *et al.* [38] employed data mining approaches, including the naïve Bayes, decision tree (DT), and the probabilistic neural network (PNN) Predictors, to classify the operational performance of three-phase induction motors under balanced or unbalanced voltage supply conditions. With an accuracy exceeding 98%, these techniques demonstrated their capability in performance evaluations of these motors. Priyanto *et al.* [39] delved into earthquake predictions, using non-parametric methods like multivariate adaptive regression spline (MARS) and conic MARS. By analyzing the variable contributions, this study identified potential earthquake-prone areas in Lombok. Furthermore, Mamaril and Ballera [40] harnessed pattern discovery techniques in educational data mining to predict ideal college program selection and enrollment forecasting for incoming freshmen. This knowledge base proved essential for enhancing the services of admission departments in educational institutions.

One significant characteristic of this violence is its protracted and chronic nature, exhibiting cycles of high and low severity over 13 years. Notably, the peaks occurred in 2007 (2,409 events) and 2012 (1,851 events). One hypothesis posits that if this pattern continues in future cycles, it may result in seasonal violence, with peak intensities every four to five years, followed by cyclical declines and resurgences. Recognizing the significance of imminent events, we embarked on a comprehensive study and analysis of past events in the three southern border provinces. We collected data from reputable online sources, gathering event details such as date, time, location, and relevant environmental factors. Our objective was to forecast events in the upcoming period, employing a variety of forecasting techniques, including deep learning artificial neural networks, decision tree methods, and naïve Bayesian learning techniques. We then selected forecasting techniques with reliability values exceeding 80% for application to real data, culminating in the design and production of data visualizations derived from the model-generated insights. Our contribution can be concluded as follows.

a. We proposed a data-driven prediction model for Thailand, introducing a data analysis framework to predict upcoming terrorist events in the country's three southern border provinces. The events were categorized into nine groups based on expert recommendations.
b. We employed and compared a range of forecasting techniques, including deep learning artificial neural networks, decision tree methods, and naïve Bayesian learning techniques. Notably, our deep neural network achieved the highest prediction accuracy at 98.21%.
c. We pioneered localized event analysis by identifying and emphasizing the most probable terrorist events for specific regions within provinces, offering granular insights into potential hotspots.
d. We introduced practical application and visualization by selecting and applying the most efficacious forecasting techniques to real-world data, subsequently producing detailed data visualizations from the insights generated.

2. THE PROSED METHOD

In this section, we present our operational procedures for modeling and forecasting terrorist events with data mining techniques. The overview of the research process was illustrated as shown in Figure 1. According to Figure 1, the research process could be divided into five steps: data management, data partitioning, data training, data testing, and data visualization. Data management is to clean the data in a complete format. Once we obtained the completed data, we implemented data partitioning by dividing it into two parts: the training and the testing dataset. Then a label class was created as data classification to be used in the comparison process for three classification techniques in which the predictive accuracy of more than 80% is selected for modeling. After that, the forecasting models were applied to the data testing data to determine forecasting performance and forecasting data. Then, the information acquired into the Business Intelligence process to create a dashboard to present the information in a visual format.

2.1. Data management

Data management was divided into four stages: data collection, null elimination, duplicate data elimination, and data conversion to numerical values. We first collected events of the South Thailand insurgency data from January 2013 to September 2018, totaling 4,972 events as shown in Table 1. Then, we eliminate the null value since it is a significant process in forecasting modeling; if there were any lost data, it would not be able to perform the modeling. Therefore, the nonvalue data must be examined and eliminated. We then collaborated with the South Thailand insurgency experts to determine the new value of the null data instead.

Besides, duplicate data may lead to modeling distortion; thus, it was necessary to eliminate duplicated data by selecting the first seen recorded data or search results and then deleting the same following data. Finally, we convert the data into numerical values. Since forecasting was a probability calculation that relies on numerical data, textual or literal data were not much supported by the forecasting techniques. Therefore, it was necessary to convert literal data to numbers to create forecasting models from the classification techniques. There were three categories for the conversion described as:

a. Conversion of numerical data from consonant arrangements: the features, i.e., PlaceOccur and DescriptionOccurr, are converted to numbers by sorting Thai alphabets in ascending order.
b. Conversion of numerical data from the issue of interest: the features are converted to numbers regarding the issues of interest by sorting the most concerning problems with great interest in the first place, followed by the level of its importance, i.e., CauseType, Strategy, ViolentDegree, and Casualty. Example of conversion for replacing the CauseType feature.

c. Conversion of numerical data from a location database: the features are converted to numbers regarding the issue of interest by sorting the most concerning problems with great interest in the first place, followed by the level of its importance: subdistrict, district, province, and village. The numbers used for reference were from the LAT/LONG location data in the Subdistrict and DATA GO which published location data throughout Thailand. The Village feature represented the reference to the numbers of a combination of sub-districts, districts, and provinces, followed by numbers sorted alphabetically.
d. Group management of events before feeding the data into the learning and testing processes. There was a data file containing 18 sets divided into nine training and nine testing sets by segmenting the event type assisted by the experts to determine the grouping. The grouping was segmented considering the Cause Type and Strategy features. Any incidents that have the same or similar causes and patterns are grouped together. The examples of incident grouping are shown in Table 2.

However, the event will be classified into other groups if there is no group to which it belongs. These nine events include explosions, harassment, shooting, collisions, assaults, arson, fire, and stealth. We then added a label feature to predict whether it is true following the actual ones.

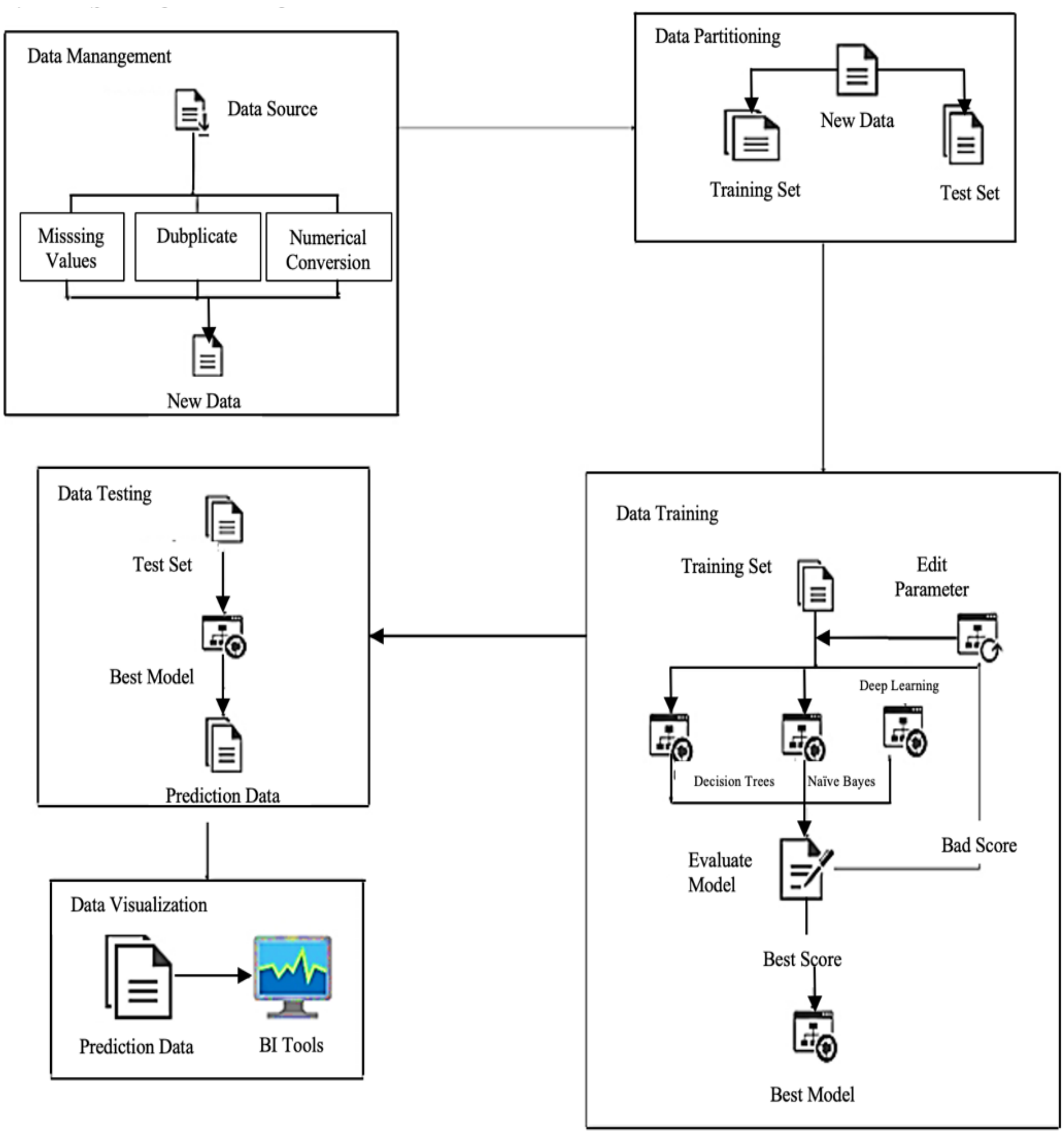

Figure 1. System conceptual framework

Table 1. Data name, type, and detail for modeling

Name	Desc.	Data type
DateOccur	Incident date	Datetime
Eventype	Type of incident	String
CauseType	Cause of the incident	String
Strategy	Tactics of the incident	String
Village	The village where the incident occurred	String
Subdistrict	Subdistrict where the incident occurred	String
District	District where the incident occurred	String
Province	Province where the incident occurred	String
ViolentDegree	The level of severity of the incident area	String
Casualty	Event damage	String
PlaceOccur	Incident place	String
DescriptionOcurr	Event details	String

Table 2. Event grouping

Event name	Description
Harassment	Create a disruptive situation
Explosion	Grenade/drop bomb
Shooting	Shoot, sniper, strafe, melee
Collision	Clash, hit, fighting crowd
Assault	Make a physical attack on, hit, strike
Stealth	Robbery
Arson	Caused by burning, stirring
Fire	Caused by natural disasters or short circuit
Others	Events other than vandalism, explosions, shootings, clashes, assault, robbery, arson, and fire

2.2. Data partitioning

Following the CRISP-DM modeling principles, the implementation of the model involved a comprehensive comparison between forecasted outcomes and actual historical data. The dataset was split into two distinct sets: a training set comprising 4,197 samples collected from 2013 to 2016, and a testing set consisting of 775 samples collected from 2017 to 2018. This approach aimed to evaluate the model's performance across different time periods.

2.3. Data training

After processing the output data into nine sets based on the event, all data sets were taken and tested with three benchmarks. This includes decision tree, naïve Bayesian learning, and deep learning neural network technique. The procedure of data training is shown as follows.

2.3.1. Decision tree

Decision tree modeling selects the feature with the most class affinity as the top node, i.e., the root node. The following feature is searched after this process. Information gain (IG) is used to determine the feature relationship as shown in (1), in which each feature is calculated. We select the feature with the highest IG as the root of the decision tree and then calculate the next node. If any node cannot branch out, then it is the last node on that branch.

$$IG = Entropy(parent) - \sum_{n=1}^{k}(Prob(C_n) \times Entropy(C_n)) \quad (1)$$

where

$$Entropy(Condition) = -\sum_{n=1}^{k}(Prob(C_n) \times log_2(Prob(C_n)))$$

From categorizing nine events, we would like to choose an event to show how to model the decision tree, that is, the explosion event consisting of 4,196 training samples with a total of 10 features including DateOccur, CauseType, Strategy, Village, Subdistrict, District, ViolentDegree, Casualty, PlaceOccur, and DescriptionOccur. Then we find the feature that is suitable to be the root of the tree by calculating the IG value of the training data set. There are a total of 4,196 items in which we are interested in the Actual class in predicting the data. The Actual class has two values: "Yes" and "No" with a total of 727 and 3,469, respectively. Since we know the number of classes, it can be formed in each feature and calculated with (2):

$$\mathrm{Entropy(parent)} = -\mathrm{p(yes)\ x\ log2(p(yes))} - \mathrm{p(no)\ x\ log2(p(no))} \quad (2)$$

where

$$P(yes) = \frac{Amount\ of\ Case\ Yes}{Total\ Class\ Actual}$$

$$P(no) = \frac{Amount\ of\ Case\ No}{Total\ Class\ Actual}$$

Then

$$\begin{aligned}
&Entropy(Parent)\\
&= -\,P(Yes) \times log2P(Yes) - P(No) \times log2P(No)\\
&= -\,\{(0.17326 \times log2(0.17326)) + (0.82674 \times log2(0.82674))\}\\
&= -\,\{(0.17326 \times (-2.53)) + (0.82674\ \times\ (-0.27))\}\\
&= -\,\{(-0.44) + (-0.22)\}\\
&= 0.66
\end{aligned}$$

We calculate the Entropy in various features divided by class. Once the Entropy has been reached, we find the IG value, which is calculated as shown in (3).

$$\mathrm{IG} = \ \mathrm{Entropy(parent)} - \textstyle\sum_{n=1}^{k}(\mathrm{Prob}(C_n) \times \mathrm{Entropy}(C_n)) \tag{3}$$

The decision modeling of the explosion event is shown in Figure 2.

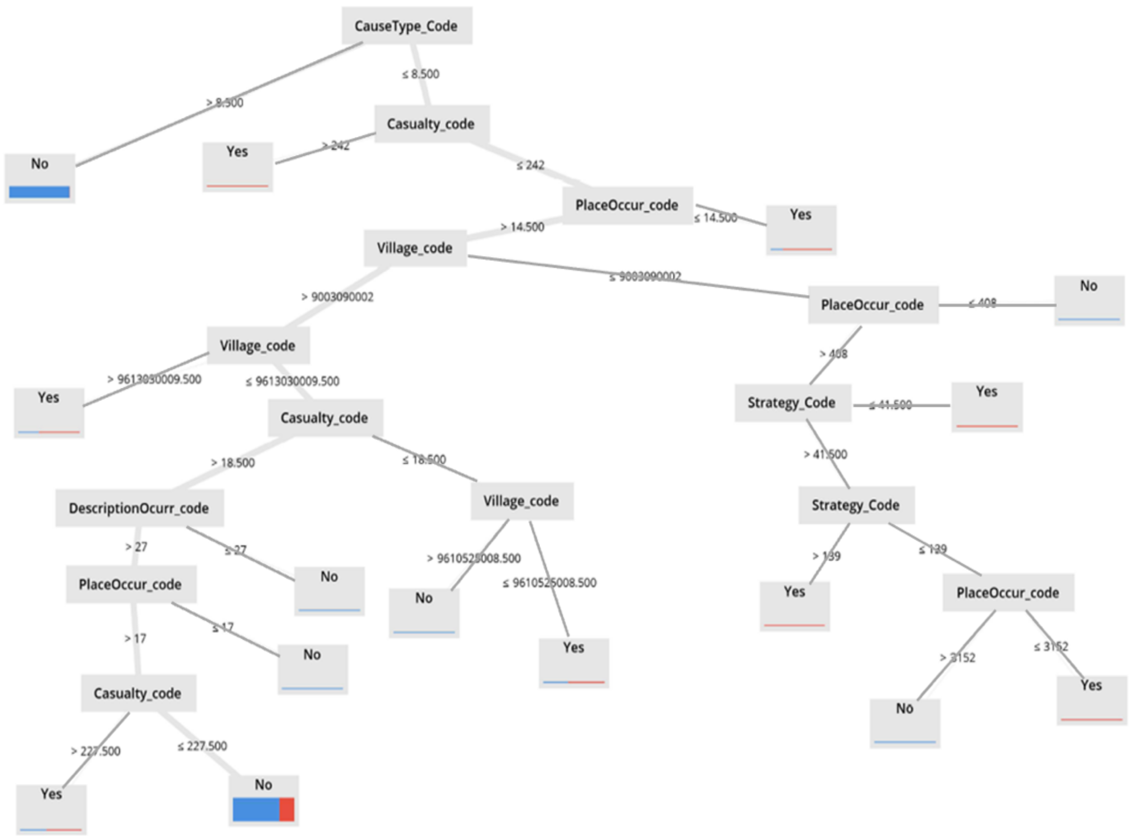

Figure 2. Decision modeling of the explosion event

2.3.2. Naïve Bayesian learning

To assess the performance of our dataset, we employed the naïve Bayesian learning technique. Initially, the process involved assigning new instances for classification. The subsequent implementation procedures of naïve Bayesian learning are detailed as follows.

Given $X =< personal\ matter\ (18), personal\ matter/drug\ (19), short\ circuit\ (15), incendiary\ (2), cause\ unknown\ (23) >$.

Then we predict the probability of whether the perpetrator will create an explosive situation in the case that x is qualified. The data can be divided as the Actual class consisting of "Yes" or "No". The Prior Probabilities can be calculated in (4) and (5).

$$\begin{aligned} P\ (Actual{:}\ Yes) &= Total\ of\ Case\ Yes\ /\ Total\ Case \\ &= 727/4196 \\ &= 0.17326 \end{aligned} \tag{4}$$

$$\begin{aligned} P\ (Actual{:}\ No) &= Total\ of\ Case\ No\ /\ Total\ Case \\ &= 3469/4196 \\ &= 0.82674 \end{aligned} \tag{5}$$

The probability of each property known as Likelihood probabilities can be calculated by substituting the values. We first determine what causes an explosion by considering the $Causetype$ value individually. The calculation of Likelihood probabilities can be described:
<$Causetype = 1$> predicts whether an explosion will occur or not. It can be calculated from the equation:

$$Pr(Y)Pr(Cauestype = 1|Y) = (0.17326)(0.00688) = 0.00119203$$
$$Pr(N)Pr(Cauestype = 1|N) = (0.82674)(0.3759) = 0.31077157$$

Thus, it can be concluded that $Causetype = 1$ would not be the cause of the explosion.
<$Causetype = 2$> predicts whether an explosion will occur or not. It can be calculated from the equation:

$$Pr(Y)Pr(Cauestype = 2|Y) = (0.17326)(0.99037) = 0.17159151$$
$$Pr(N)Pr(Cauestype = 2|N) = (0.82674)(0.60824) = 0.50285634$$

Therefore, it can be concluded that $Causetype = 2$ can be the cause of the explosion.
<$Causetype = 3$> predicts whether an explosion will occur or not. It can be calculated from the equation:

$$Pr(Y)Pr(Cauestype = 3|Y) = (0.17326)(0) = 0$$
$$Pr(N)Pr(Cauestype = 3|N) = (0.82674)(0.00721) = 0.0059608$$

Therefore, it can be concluded that $Causetype = 3$ can be the cause of the explosion.
<$Causetype = 4$> predicts whether an explosion can happen or not. It can be calculated from the equation:

$$Pr(Y)Pr(Cauestype = 4|Y) = (0.17326)(\ 0.00138) = 0.0002391$$
$$Pr(N)Pr(Cauestype = 4|N) = (0.82674)(\ 0.00865) = 0.0071513$$

Therefore, it was concluded that $Causetype = 4$ was not the cause of the explosion.
<$Causetype = 5$> will predict whether an explosion will occur or not. It can be calculated from the equation:

$$Pr(Y)Pr(Cauestype = 5|Y) = (0.17326)(\ 0.00138) = 0.0002391$$
$$Pr(N)Pr(Cauestype = 5|N) = (0.82674)(0) = 0$$

Therefore, it can be concluded that $Causetype = 5$ can be the cause of the explosion. However, these calculations are just part of the modeling because some features are quite large. Thus, the values have been substituted into the equations to understand the calculation principles and construction steps. When we put assumptions into the model, we found that a forecasting model constructed using a simple Bayesian learning technique result in an accuracy in forecasting at 98.80 percent. The experimental results show that class *No* achieves 0.827 with 12 distributions and class *Yes* achieves 0.173 with 12 distributions.

2.3.3. Deep learning neural network approach

In the deep learning neural network approach, we need to convert the value to the range of -1 to 1. After the conversion, the value was fed into the hidden layer and output layer, passing through the activation function. We use Sigmoid, $F(X) = \frac{1}{1-e^{-x}}$, as the activation function in this work. The min-max value of each attribute of training and test data. The model has learned based on the adjusted weight, which helps it to reach the lowest variance forecast. Specifically, the input data was multiplied by the weight (weight: W), which represents the significance of each input data, and combined with the bias value (bias: b). The results of the weighted sum and bias values were sent to the transfer function. Since W and b could be adjusted during the learning, the result will depend on the transfer function. The loss function had to be defined to find the errors between the predicted output with the value of the target y. We tried to obtain a lower loss value and optimize the model.

2.4. Data testing

We compared and assessed the forecasting methods' accuracy, including naive Bayesian learning, deep learning artificial neural networks, and decision tree methods. After that, we chose forecasting methods with an 80% or higher dependability value to use on actual data, including creating data visualizations from the model's output. The artificial neural network model cannot be calculated and must be converted within a range of -1 to 1. After the min-max value was successfully converted, the converted value was input into the hidden layer calculation equation, and the output layer was sent to the activate function that was selected using Sigmoid. The artificial neural network models and deep learning neural networks adjusted the weighting values and sent values to each node to obtain forecast values with the lowest variance, where the input data was processed by multiplying the weight (weight: W), which represented the significance of each input data combined with the bias (b). Then, the sum of the resulting data adjusted the weight value and the bias value and then sent it to the transfer function, which had an equation for calculating the resulting value.

We use root mean square error (RMSE) to measure of the differences between the values predicted by a model and the actual observed values. RMSE can be calculated by

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2},$$

where n = number of observations, y_i = actual values, $\hat{y}_i$ = predicted values. A lower RMSE indicates a better fit of the model to the data, meaning the predictions are closer to the actual values. Conversely, a higher RMSE indicates a poorer fit, suggesting the model predictions are less reliable.

2.5. Data visualization

The data obtained from training and testing were utilized to generate graphs. This helps enhancing accessibility and understanding through business intelligence machines. The data management procedures for testing are elaborated as follows:

a. The comparison results of data mining technologies show which technologies provided the most accurate forecasting, and the accuracy value must be higher than 80%.
b. The accuracy of the model shows the model's efficiency implementation with test data in which the outcome of the forecast was compared to the original data that has already been generated. The prediction of unrest in surveillance areas is shown by revealing the percentage of the incidence rate and identifying the provinces with the highest probability of incidents. This gave meaning to areas that required special attention; orange represented a moderate and high incident rate; green represented a moderate and low incident rate and green represented the least likely incident rate but remained vigilant. The result was shown as a point on the map to see what district, subdistrict, or village would occur by showing the name of the village, subdistrict, district, or province. A separate filter for events, which are divided by province, or by month and year, can be chosen.

3. RESULTS AND DISCUSSION

The application of deep learning neural network techniques for predicting terrorist events was undertaken through a systematic process: analysis, design, and development. We followed a structured approach to assess the effectiveness of the neural network models. The details are shown as follows.

3.1. Implementation detail

This project utilized a computational framework by deploying our model on a central processing unit (CPU), specifically the Intel Core i7-7700HQ with a clock speed of 2.81 GHz. The system is accompanied by 4 GB of RAM and solid-state drive (SSD) with a storage capacity of 250 GB. The entire system ran on the Windows 10 64-bit operating system.

3.2. Forecasting results of the terrorist events

We compare the results from the three benchmark methods, including decision tree techniques, Naïve Bayesian learning, and a deep learning artificial neural network. According to the experimental results, it was found that deep learning techniques achieved the best accuracy while the decision tree techniques had better accuracy values than naïve Bayesian learning techniques. The forecasting results for various events are as follows:

a. Fire events: 99% accuracy, 49.61% precision, 50% recall.
b. Disruptive events: 100% in all three metrics: accuracy, precision, and recall.
c. Stealth events: 98.32% accuracy, 53.57% precision, 99.16% recall.
d. Assault events: 66.71% accuracy, 56.03% precision, 78.90% recall.
e. Collision events: 98.32% accuracy, 49.16% precision, 50% recall.
f. Shooting events: 83.74% accuracy, 85.28% precision, 86.68% recall.
g. Explosion events: 100% in all three metrics: accuracy, precision, and recall.
h. Arson events: 98.58% accuracy, 99.28% precision, 76.09% recall.
i. Other events: 98.58% accuracy, 99.28% precision, 67.65% recall.

These results highlight the varied effectiveness of the forecasting model across different event types. The data underscores that deep learning techniques, especially artificial neural networks, tend to provide superior accuracy in forecasting compared to the other methods. This can be attributed to the ability of neural networks to detect intricate patterns within large datasets, making them particularly adept at forecasting events based on historical data. However, decision trees also showed commendable performance, outpacing Naïve Bayesian learning in most event types. Decision trees are known for their simplicity and interpretability, which can be beneficial in scenarios where understanding the model's decision logic is crucial. Interestingly, the results varied significantly across event types. While certain events like disruptive and explosion events achieved impeccable accuracy, precision, and recall with the deep learning method, other events like assault showcased a considerable drop in these metrics. This discrepancy could stem from the inherent complexities and variables involved in predicting different types of events. Therefore, while deep learning artificial neural networks emerge as the most potent technique for forecasting these events, the effectiveness can fluctuate based on the event type. Moving forward, these insights will be invaluable for agencies and organizations aiming to preemptively address or respond to such events. Adopting the most effective forecasting method tailored to the specific event type can significantly improve preparedness and response strategies.

3.3. The results of the simulation of the terrorist events

We show the results from the simulation of the terrorist events. The comparison of forecasting results includes decision tree techniques, naïve Bayesian learning, and a deep learning artificial neural network. The experimental results of our proposed model are revealed:

a. Deep learning techniques provided the highest forecast accuracy overall.
b. Decision tree technique showed better accuracy than the Bayesian learning technique.
c. Accuracy in forecasting varies by event type:
   - Fire incidents: Deep learning achieved the highest accuracy at 99.90%.
   - Disruptive event: Both deep learning and decision tree techniques had the highest forecast accuracy at 99.98%.
   - Stealth event: decision tree had the highest forecast accuracy at 99.95%.
   - Incident event: deep learning had the highest forecast accuracy at 99.93%.
   - Clash event: decision tree had the highest forecast accuracy at 100%.
   - Shooting event: deep learning achieved the highest forecasting accuracy of 99.98%.
   - Explosion event: deep learning had the highest forecast accuracy of 100%.
   - Arson event: naïve Bayes technique had the highest forecast accuracy of 99.98%.
   - Other events: deep learning had the highest forecast accuracy of 100%.

Based on this accuracy assessment, we applied the data obtained from these techniques to create data visualizations using business intelligence tools. These visualizations display the risk levels of events, along with information about their location down to the sub-district, district, and province levels. For instance, examples of data visualizations for explosion, assault, and disruptive events can be found in Figure 3, respectively. The map represents four provinces-Songkhla (depicted in dark green), Pattani (in red), Yala (in pink), and Narathiwat (in pale green).

Figure 3 shows explosion events occur in 15.74% of the total area across the four provinces. Pattani Province has the highest incidence, accounting for 45.90%. It is followed by Yala at 23.77%. The third highest is Narathiwat with 19.67%. The least affected is Songkhla, with an occurrence rate of 10.66%.

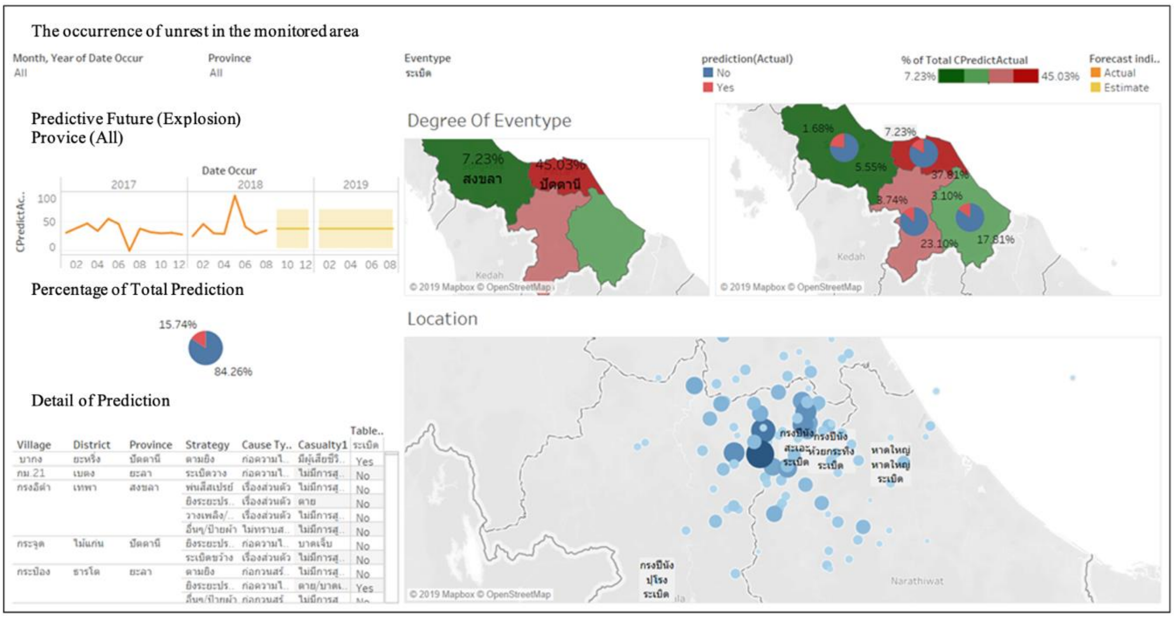

Figure 3. Simulation of the explosion events in the target provinces

3.4. Discussion and interpretation

The comparative analysis of three benchmark methods-decision tree techniques, naïve Bayesian learning, and deep learning artificial neural networks-provides valuable insights into their predictive capabilities. The consistent superior performance of deep learning artificial neural networks in terms of accuracy across most event types can be attributed to their complex architectures and ability to process extensive datasets. Deep learning excels in identifying intricate patterns and nonlinear relationships that might elude simpler models. However, while deep learning appears to be the preferred choice for most event types, our results also highlight scenarios where decision tree techniques outperform. For instance, decision trees achieve a remarkable 100% accuracy rate for clash events and 99.95% for stealth events. This suggests that, despite their simplicity, decision trees excel in specific contexts. Their hierarchical feature segregation makes them interpretable and less prone to overfitting under certain conditions. Interestingly, the Naïve Bayes technique delivers the highest forecast accuracy for arson events, underscoring the importance of aligning the choice of model with the underlying data distribution. Spatial simulation reveals a disproportionate distribution of events across the target provinces. Pattani Province emerges as a consistent hotspot for various event types, bearing the highest percentage of occurrences, closely followed by Yala and Narathiwat. Conversely, Songkhla consistently reports the lowest event rates, hinting at distinct underlying factors or varying levels of security measures across these provinces.

Moreover, our experiments demonstrate the superiority of the deep learning technique, achieving an impressive forecast accuracy of 98.21% with a minimal RMSE of 0.59%. To put this in perspective, the RMSE of 0.59% indicates that, on average, the model's predictions deviate by only 0.59% from the actual observed values. With a forecast accuracy of 98.21%, this RMSE value suggests that the model's predictions closely align with the ground truth, highlighting its reliability for predictive purposes. In summary, the comparison of these methods underscores the significance of selecting the right model for specific scenarios, acknowledging the complex interplay between model architecture, data distribution, and predictive performance. The spatial analysis sheds light on localized vulnerabilities and emphasizes the need for tailored security measures. Finally, the low RMSE value affirms the accuracy of our model, affirming its utility in forecasting and situational awareness applications.

3.5. Ramifications and future utility

Given these findings, a hybrid approach might be most beneficial for predictive modeling, wherein different models are employed based on the specific nature and intricacies of the event being predicted. Moreover, regions like Pattani Province, with consistently high event rates, need more focused counter-terrorism strategies and resources. The ability to visualize risk levels across sub-districts, districts, and provinces through business intelligence tools enhances proactive decision-making. By knowing areas of higher risk, security forces can strategize deployments, while policymakers can delve deeper into the root causes of such trends. Moving forward, the insights from this study can be crucial for policy formulation and resource allocation. By understanding the strengths and weaknesses of each predictive model, as well as the spatial distribution of terrorist events, authorities can employ a more nuanced, data-driven approach to counter-terrorism.

4. CONCLUSION

In this study, we developed a forecasting model for terrorist events in three southern provinces of Thailand, employing benchmark methods such as Naive Bayesian learning, deep learning artificial neural networks, and decision trees. Our experimental results demonstrated that the deep learning artificial neural network technique outperformed others, achieving an impressive forecast accuracy of 98.21% with an RMSE of 0.59%. This high accuracy validates the efficacy of deep learning artificial neural networks in predicting terrorist events. Our analysis identified the most likely types of terrorist events, including explosions, shootings, assaults, and disruptive events, with specific regions of concern within Pattani, Panare District, Yarang District, and Mayo District. This information enhances situational awareness and contributes to maintaining public safety. For future research, we recommend incorporating additional variables, such as city conditions, rebel organization activities, crime site characteristics, event nature, suspect group profiles, perpetrator behaviors, and suspect lists, to further improve the model's predictive capabilities. Additionally, integrating latitude and longitude data from the Google Maps API dashboard can enhance the effectiveness of troop deployment and surveillance in preventing terrorist attacks.

ACKNOWLEDGEMENTS

This work is supported by Department of Mathematics, Faculty of Science, King Mongkut's University of Technology Thonburi.

REFERENCES

[1] K. Bahgat and R. Medina, "An overview of geographical perspectives and approaches in terrorism research," *Perspectives on Terrorism*, vol. 7, pp. 38–72, 2013.
[2] C. Flint, *The geography of war and peace: From death camps to diplomats*, Oxford Uni. 2004.
[3] F. A. G. Jr, "A geographical analysis of un-governed spaces," *Pennsylvania Geographer*, vol. 44, no. 2, 2006.
[4] C. C. B. Kittner, "The role of safe havens in Islamist terrorism," *Terrorism and Political Violence*, vol. 19, no. 3, pp. 307–329, Jul. 2007, doi: 10.1080/09546550701246791.
[5] R. E. M. Korteweg, "Black holes: On terrorist sanctuaries and governmental weakness," *Civil Wars*, vol. 10, no. 1, pp. 60–71, Mar. 2008, doi: 10.1080/13698240701835482.
[6] J. C. Rock, "The geographic nature of terrorism," *Pennsylvania Geographer*, vol. 44, no. 2, 2006.
[7] H. V Savitch and G. Ardashev, "Does terror have an urban future?," *Urban Studies*, vol. 38, no. 13, pp. 2515–2533, Dec. 2001, doi: 10.1080/00420980120107529.
[8] J. J. Hobbs, "The geographical dimensions of Al-Qaeda rhetoric," *Geographical Review*, vol. 95, no. 3, pp. 301–327, 2005.
[9] S. Nunn, "Incidents of terrorism in the United States, 1997–2005," *Geographical Review*, vol. 97, no. 1, pp. 89–111, 2007.
[10] D. Mustafa, "The terrible geographicalness of terrorism: Reflections of a hazards geographer," *Antipode*, vol. 37, no. 1, pp. 72–92, Jan. 2005, doi: 10.1111/j.0066-4812.2005.00474.x.
[11] N. Kliot and I. Charney, "The geography of suicide terrorism in Israel," *GeoJournal*, vol. 66, no. 4, pp. 353–373, Aug. 2006, doi: 10.1007/s10708-006-9034-z.
[12] C. Berrebi and D. Lakdawalla, "How does terrorism risk vary across space and time? An analysis based on the Israeli experience," *Defence and Peace Economics*, vol. 18, no. 2, pp. 113–131, Apr. 2007, doi: 10.1080/10242690600863935.
[13] B. L. Smith, J. Cothren, P. Roberts, and K. R. Damphousse, "Geospatial analysis of terrorist activities: the identification of spatial and temporal patterns of preparatory behavior of international and environmental terrorists," *US Department of Justice*. 2008, Accessed: Nov. 08, 2020. [Online]. Available: https://www.ncjrs.gov/pdffiles1/nij/grants/222909.pdf
[14] D. K. Rossmo and K. Harries, "The geospatial structure of terrorist cells," *Justice Quarterly*, vol. 28, no. 2, pp. 221–248, Apr. 2011, doi: 10.1080/07418820903426197.
[15] S. Singh, J. Allanach, Haiying Tu, K. Pattipati, and P. Willett, "Stochastic modeling of a terrorist event via the ASAM system," in *2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No.04CH37583)*, vol. 6, pp. 5673–5678, doi: 10.1109/ICSMC.2004.1401098.
[16] S. J. Dixon, M. B. Dixon, J. Elliott, E. Guest, and D. J. Mullier, "A neural network for counter-terrorism," *International Conference on Innovative Techniques and Applications of Artificial Intelligence*, pp. 229–234, 2011, doi: https://doi.org/10.1007/978-1-4471-2318-7-18.
[17] S. Saha, H. Aladi, A. Kurian, and A. Basu, "Future terrorist attack prediction using machine learning techniques," *PESIT South Campus*, 2017.
[18] H. Mo, X. Meng, J. Li, and S. Zhao, "Terrorist event prediction based on revealing data," in *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, Mar. 2017, pp. 239–244, doi: 10.1109/ICBDA.2017.8078815.
[19] M. I. Uddin *et al.*, "Prediction of future terrorist activities using deep neural networks," *Complexity*, vol. 2020, pp. 1–16, Apr. 2020, doi: 10.1155/2020/1373087.
[20] F. Ding, Q. Ge, D. Jiang, J. Fu, and M. Hao, "Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach," *PLOS ONE*, vol. 12, no. 6, Jun. 2017, doi: 10.1371/journal.pone.0179057.
[21] S. J. Krieg, C. W. Smith, R. Chatterjee, and N. V Chawla, "Predicting terrorist attacks in the United States using localized news data," *PLOS ONE*, vol. 17, no. 6, Jun. 2022, doi: 10.1371/journal.pone.0270681.

[22] F. Ozgul, Z. Erdem, and C. Bowerman, "Prediction of unsolved terrorist attacks using group detection algorithms," in *Lecture Notes in Computer Science*, 2009, pp. 25–30.
[23] M. F. Abrar, M. S. Arefin, and M. S. Hossain, "A framework for analyzing real-time tweets to detect terrorist activities," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Feb. 2019, pp. 1–6, doi: 10.1109/ECACE.2019.8679430.
[24] G. M. Tolan and O. S. Soliman, "An experimental study of classification algorithms for terrorism prediction," *International Journal of Knowledge Engineering-IACSIT*, vol. 1, no. 2, pp. 107–112, 2015, doi: 10.7763/IJKE.2015.V1.18.
[25] D. Talreja, J. Nagaraj, N. J. Varsha, and K. Mahesh, "Terrorism analytics: learning to predict the perpetrator," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sep. 2017, pp. 1723–1726, doi: 10.1109/ICACCI.2017.8126092.
[26] P. Agarwal, M. Sharma, and S. Chandra, "Comparison of machine learning approaches in the prediction of terrorist attacks," in *2019 Twelfth International Conference on Contemporary Computing (IC3)*, Aug. 2019, pp. 1–7, doi: 10.1109/IC3.2019.8844904.
[27] S. Chaurasia, V. Warikoo, and S. Khan, "Global terrorism predictive—analysis," in *Advances in Computer Communication and Computational Sciences*, 2019, pp. 77–85.
[28] A. Python *et al.*, "Predicting non-state terrorism worldwide," *Science Advances*, vol. 7, no. 31, 2021, doi: 10.1126/sciadv.abg4778.
[29] C. Buffa, V. Sagan, G. Brunner, and Z. Phillips, "Predicting terrorism in Europe with remote sensing, spatial statistics, and machine learning," *ISPRS International Journal of Geo-Information*, vol. 11, no. 4, Mar. 2022, doi: 10.3390/ijgi11040211.
[30] N. Johnson *et al.*, "Pattern in escalations in insurgent and terrorist activity," *Science*, vol. 333, no. 6038, pp. 81–84, Jul. 2011, doi: 10.1126/science.1205068.
[31] N. F. Johnson, "From particles to people: social, cultural and behavioral dynamics in insurgency, terrorism and beyond," *Advances in design for cross-cultural activities, Part II*, pp. 398–407, 2013.
[32] N. F. Johnson, E. M. Restrepo, and D. E. Johnson, "Modeling human conflict and terrorism across geographic scales," *Social Phenomena*, pp. 209–233, 2015.
[33] A. B. Vanderzee, "Predicting the spread of terrorist organizations using graphs," *Diss. Monterey, CA; Naval Postgraduate School*, 2018.
[34] J. Bang, A. Basuchoudhary, J. David, and A. Mitra, "Predicting terrorism: a machine learning approach," *Peace Economics, Peace Science, & Public Policy*, vol. 24, no. 4, 2018.
[35] Y. Yang, A. R. Pah, and B. Uzzi, "Quantifying the future lethality of terror organizations," *Proceedings of the National Academy of Sciences*, vol. 116, no. 43, pp. 21463–21468, 2019.
[36] A. Python, J. B. Illian, C. M. Jones-Todd, and M. Blangiardo, "A Bayesian approach to modelling subnational spatial dynamics of worldwide non-state terrorism, 2010–2016," *Journal of the Royal Statistical Society Series A: Statistics in Society*, vol. 182, no. 1, pp. 323–344, Jan. 2019, doi: 10.1111/rssa.12384.
[37] T. Li, Y. Huang, J. Evans, and I. Chattopadhyay, "Long-range event-level prediction and response simulation for urban crime and global terrorism with granger networks," *arXiv preprint arXiv:1911.05647*, 2019.
[38] A. I. Adekitan, A. Adewale, and A. Olaitan, "Determining the operational status of a three phase induction motor using a predictive data mining model," *International Journal of Power Electronics and Drive Systems (IJPEDS)*, vol. 10, no. 1, pp. 93–103, Mar. 2019, doi: 10.11591/ijpeds.v10.i1.pp93-103.
[39] D. Priyanto, M. Zarlis, H. Mawengkang, and S. Efendi, "Analysis of earthquake hazards prediction with multivariate adaptive regression splines," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 2885–2893, Jun. 2022, doi: 10.11591/ijece.v12i3.pp2885-2893.
[40] J. C. O. Mamaril and M. A. Ballera, "Multiple educational data mining approaches to discover patterns in university admissions for program prediction," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 11, no. 1, pp. 45–56, Apr. 2022, doi: 10.11591/ijict.v11i1.pp45-56.

BIOGRAPHIES OF AUTHORS

Thittaporn Ganokratanaa received the B.Sc. degree (Hons.) in media technology from King Mongkut's University of Technology Thonburi, Thailand, in 2015 and the M.Eng. and Ph.D. degrees in electrical engineering from Chulalongkorn University, Bangkok, Thailand, in 2018 and 2021, respectively. Currently, she is a university lecturer at the Applied Computer Science Program, Department of Mathematics, King Mongkut's University of Technology Thonburi. Her research interests include video anomaly detection, human-computer interaction, machine learning, artificial intelligence, data science, image processing, computer vision, and internet of things. She serves as IEEE Region 10 student activities committee (SAC) and Member and Geographic Activities (MGA) SAC committee. She also is a reviewer for leading journals such as Pattern Recognition Letters, IEEE Access. She can be contacted at email: thittaporn.gan@kmutt.ac.th.

Mahasak Ketcham received Ph.D. in computer engineering, Chulalongkorn University, Thailand. He is an assistant professor in Department of Information Technology Management, King Mongkut's University of Technology North Bangkok, Thailand. He is the Chair of IEEE System, Man and Cybernetics Thailand Chapter. His research of interests are anomaly detection, image and video analysis, AI and human-computer interaction. He can be contacted at email: mahasak.k@itd.kmutnb.ac.th.