Cyber-attack method and perpetrator prediction using machine learning algorithms

Abdulkadir Bilen [Corresp., 1] , **Ahmet Bedri Özer** [2]

[1] Criminal Department, General Directorate of Security, Ankara, Turkey

[2] Department of Computer Engineering, Firat University, Elazığ, Turkey

Corresponding Author: Abdulkadir Bilen
Email address: abdulkadir.bilen@egm.gov.tr

Cyber-attacks have become one of the biggest problems of the world. They cause serious financial damages to countries and people every day. The increase in cyber-attacks also brings along cyber-crime. The key factors in the fight against crime and criminals are identifying the perpetrators of cyber-crime and understanding methods of attack. Detecting and avoiding cyber-attacks are difficult tasks. However, researchers have recently been solving these problems by developing security models and making predictions through artificial intelligence methods. A high number of methods of crime prediction are available in the literature. On the other hand, they suffer from deficiency to predict cyber-crime and cyber-attack methods. This problem is tackled to identify an attack and the perpetrator of such attack, using actual data. The data include the type of crime, gender of perpetrator, damage and methods of attack. The data were acquired from the applications of the persons who were exposed to cyber-attacks to the forensic units. In this paper, we analyze cyber-crimes in two different models with machine-learning methods and predict the effect of the defined features on the detection of cyber-attack method and the perpetrator. We used eight machine-learning methods in our approach and concluded that their accuracy ratios were close. The Support Vector Machine Linear was found out to be the most successful in the cyber-attack method with an accuracy rate of 95.02%. In the first model, we could predict the types of attacks that the victims were likely to be exposed to with a high accuracy. The Logistic Regression was the leading method in detecting attackers with an accuracy rate of 65.42%. In the second model, we predicted whether the perpetrators could be identified by comparing their characteristics. Our results have revealed that the probability of cyber-attack decreases as the education and income level of victim increases. We believe that cyber-crime units will use the proposed model. It will also facilitate the detection of cyber-attacks and make the fight against these attacks easier and more effective.

Cyber-Attack Method and Perpetrator Prediction Using Machine Learning Algorithms

5 Abdulkadir Bilen[1], Ahmet Bedri Özer[2]

7 [1]Criminal Department, General Directorate of Security, Ankara, Turkey
8 [2] Department of Computer Engineering, Fırat University, Elazığ, Turkey

10 Corresponding Author:
11 Abdulkadir Bilen[1]
12 Ankara, Turkey
13 Email address: abdulkadir.bilen@egm.gov.tr

15 *Abstract*— Cyber-attacks have become one of the biggest problems of the world. They cause
16 serious financial damages to countries and people every day. The increase in cyber-attacks also
17 brings along cyber-crime. The key factors in the fight against crime and criminals are identifying
18 the perpetrators of cyber-crime and understanding methods of attack. Detecting and avoiding
19 cyber-attacks are difficult tasks. However, researchers have recently been solving these problems
20 by developing security models and making predictions through artificial intelligence methods. A
21 high number of methods of crime prediction are available in the literature. On the other hand, they
22 suffer from deficiency to predict cyber-crime and cyber-attack methods. This problem is tackled
23 to identify an attack and the perpetrator of such attack, using actual data. The data include the type
24 of crime, gender of perpetrator, damage and methods of attack. The data were acquired from the
25 applications of the persons who were exposed to cyber-attacks to the forensic units. In this paper,
26 we analyze cyber-crimes in two different models with machine-learning methods and predict the
27 effect of the defined features on the detection of cyber-attack method and the perpetrator. We used
28 eight machine-learning methods in our approach and concluded that their accuracy ratios were
29 close. The Support Vector Machine Linear was found out to be the most successful in the cyber-
30 attack method with an accuracy rate of 95.02%. In the first model, we could predict the types of
31 attacks that the victims were likely to be exposed to with a high accuracy. The Logistic Regression
32 was the leading method in detecting attackers with an accuracy rate of 65.42%. In the second
33 model, we predicted whether the perpetrators could be identified by comparing their
34 characteristics. Our results have revealed that the probability of cyber-attack decreases as the
35 education and income level of victim increases. We believe that cyber-crime units will use the
36 proposed model. It will also facilitate the detection of cyber-attacks and make the fight against
37 these attacks easier and more effective.
38 **Keywords:** Machine-Learning, Cyber-Attacks, Cyber-Crimes, Crime Prediction, Data Analysis,
39 Artificial Intelligence

I. INTRODUCTION

40

41   Nowadays, it has become exceedingly difficult to ensure the security of our systems including
42 both corporate and personal data. Major countries, such as the United States and the United
43 Kingdom, struggle with cyber-attacks and crimes by producing various security strategies [1].
44 Countries are striving to ensure security in cyber space and adapt to this field [2]. Protecting the
45 critical infrastructures has a vital importance for countries. Chemical, financial, health, and energy
46 sectors, even nuclear power plants in some countries can be counted among these [3]. Due to
47 millions of cyber-attacks, financial losses significantly increase day by day [4]. In 2020, data stolen
48 from the information system of Airbus Company were put on the dark web market. Medical data
49 of millions of people have been stolen and even state of emergency has been declared due to attacks
50 on some cities [5]. The most important elements ensuring cyber security are integrity,
51 confidentiality, authentication, authorization, nonrepudiation, and availability [6].
52   With each passing day, work force becomes insufficient in fighting against cyber incidents and
53 new solutions are sought. Solutions such as autonomous cyber defense systems [7], smart cyber
54 security assistant architecture [8] and intrusion detection systems [9] are investigated in the fight
55 against cyber-attacks and crimes. Researchers use machine-learning methods to detect power
56 outages due to cyber-attacks [10] and to prevent vulnerabilities of the Internet of things [11]. Other
57 areas of use are to determine spam and network attacks [12], to detect the phishing attacks against
58 the banking sector [13] and to reduce sexual crimes on social media [14]. These methods have
59 been implemented in fields as stock prediction [15], risk mapping by crimes [16] and cyber
60 profiling [17]. Predicting crime trend and pattern [18], criminal identity detection [19] and crime
61 prevention [20] are also areas of implementation.
62   There are three main objectives in our study. First is to use actual cyber-crime data as input to
63 predict a cyber-crime method and compare the accuracy results. Second is to measure whether
64 cyber-crime perpetrators can be predicted based on the available data. The third objective is to
65 understand the effect of victim profiles on cyber-attacks.
66   In this paper, real cyber-crime data of 5-years in Elazığ / Turkey were used. By using machine-
67 learning methods, the method of attack was predicted, and the perpetrator was detected. The
68 detection was based on features like age, gender, income, education, marital status, occupation,
69 and the damage of the crime. By working on certain features such as age, gender, etc., we predicted
70 the kind of attack methods and the victims of these attacks. These results will be used in cyber-
71 crime modelling and attack detection by the police forces dealing with cyber-crimes. Major
72 contributions of the proposed approach are:
73   •   Providing advantages to cyber-crime department as it allows using actual data,
74   •   Enabling prediction of attacks that victims may be exposed to,
75   •   Allowing determination of the optimum performance by comparing machine-learning
76   algorithms.
77   In Section II, the literature is reviewed, and the current studies and the missing parts are revealed.
78 Section III explains the machine-learning methods to be used in research. Section IV presents the
79 predictions and accuracy rate from the dataset and a comparison with previous studies. Section V
80 includes results and future work.

II. RELATED WORKS

81

82   The importance of the fight against such cyber-attacks, cyber-crimes and cyber security is
83   highlighted in various studies. Cyber security is the protection of physical-digital data, networks,
84   and technological systems from cyber-attacks, unauthorized accesses, disruptions, modifications,
85   destructions, and damages through various processes, applications, and applied technologies [21].
86   Cyber-attacks such as distributed denial of service attacks by sending malicious packets [22],
87   phishing attacks to banking and shopping sites that deceive the user [23] have increased
88   significantly. In addition, attackers have been using malicious attack software (virus, worms,
89   trojans, spyware and ransomware) that is installed into the user's computer without any consent of
90   the user [24] increasingly. Again, the most common of these attacks and one of the attacks that are
91   most difficult to be prevented is the social engineering attacks. They are based on technical skill,
92   cunning and persuasion, made by taking advantage of the weakness of the victim. Kevin Mitnick,
93   one of the world's famous hackers in social engineering attacks, penetrated most systems he
94   attacked with this method [25]. In the work by Breda F et al., this attack is mentioned as one of
95   the biggest security vulnerabilities in the system no matter how secure a technical system is [26].
96   Likewise, attacks against IoT devices, which have increased rapidly in recent years, affect the
97   society considerably. Thus, attacks and threats to the IoT structure should be understood for
98   security purposes [27]. Studies conducted to understand and combat cyber-attacks reveal the
99   importance of crime prediction as discussed in this study.

100   The attacks described above are defined as prohibited criminal acts within the legal framework
101   of many governments. The duty of fighting against crime and criminals is given to law enforcement
102   departments. Researchers assist the institutions conducting the investigation with various analysis
103   and prediction methods. For example, big data [28] and machine-learning [20] methods have been
104   used to analyze crimes in many studies. They have contributed to crime and crime fighting
105   institutions with artificial intelligence models. Among these are determining the areas where the
106   crime can be committed and its story [29], predicting the crime using spatial, temporal and
107   demographic data [30], and analyzing crime with literacy, unemployment and development index
108   data [31].

109   Time series of crime data in San Francisco, Chicago and Philadelphia were used for predicting
110   crimes in the following years. Decision Tree classification model performed better than KNN and
111   Naive Bayes [32]. Crime data were passed through two different data processing procedures in
112   Canada. A crime prediction was made with an accuracy between 39% and 44% using the KNN
113   and Decision Trees [33]. Data such as location, type, date, time, latitude, and longitude of the
114   crimes taking place in the USA were used as input. The result of the crime predictions made with
115   KNN Classification, Logistic Regression, Decision Trees, Random Forest, Support Vector
116   Machine, and Bayesian methods was that the KNN classification was the most successful with an
117   accuracy of 78.9% [34].

118   Thirty-nine different categories of crime data happened in the city of San Francisco were used.
119   By using Gradient Boosted Trees and Support Vector Machines, a model dividing crimes into two
120   classes, blue/white collar crime and violent/non-violent crime, was created. High accuracy was
121   achieved in the classification of blue- & white-collar crimes. However, the study did not yield
122   significant results in the classification of violent & non-violent crimes [35]. Data from a 10-year
123   murder occurred in Brazil were used. Predictions with 97% accuracy were made using the random
124   forest method in order to measure the effect of non-Gaussian residuals and urban metrics on

125 murders. The results of this study revealed that unemployment and ignorance were important
126 variables in murder. Also, the order of importance in predicting the crime was determined [36]. In
127 another study, the type, time and location of the crime data were used to predict crime in certain
128 regions in India. The KNN prediction method was used. The method predicted when and where
129 robbery, gambling, accident, violence, murder, and kidnapping crimes would occur. It was found
130 to be more successful than a similar study conducted previously [37].
131 Big data and machine-learning framework were implemented by using crime data collected from
132 social media platforms. The data were gathered through Volunteered Geographic Information,
133 web, and mobile crime reporting applications. Crime predictions were produced from the collected
134 data using the Naive Bayes algorithm. The purpose of these predictions is to determine the location
135 of possible crimes and prevent them [38]. The demographic and geographical data of the events
136 that took place in the previous years were used to predict the terrorist incidents in India. This model
137 predicted terrorist incidents using artificial intelligence algorithms and achieved results with
138 relatively high accuracy [39].
139 The cyber-crime data analyzed were publicly available data from social media platforms,
140 including Facebook and Twitter. Researcher compared the algorithms according to the F-measure
141 value, which is the degree of accuracy and precision. With an accuracy of 80%, RF algorithm was
142 found the best fit in the scenario. Threats were automatically determined through the model
143 analyzing cyber-crimes [40]. Real-time crime data published in the internet news were used
144 through the screening program. SVM, Multinomial NB and RF classification methods were used.
145 The data were separated into two; crime and non-crime. The most important part is that it currently
146 provides analysis to the news [41]. Cyber-crime incident data occurring in India were classified
147 using machine-learning techniques. The model, which predicted crimes with 99% of accuracy,
148 reduced amount of time spent in analysis and manual reporting [42]. A universally compared
149 intrusion detection dataset obtained from Kaggle was used. DNN was used to develop an effective
150 and efficient intrusion detection system in the IoMT environment to classify and predict
151 unforeseen cyber-attacks. DNN outperformed machine-learning algorithms [43]. When the related
152 works are examined, a summary is presented in Table 1.
153
154
155 Based on the review of the literature, we can suggest that cyber-attacks and crimes are important
156 to study since they cause substantial damages to individuals and states. As we could observe the
157 fields where machine-learning methods were used and these methods were successful in
158 predictions, they were used in our study. Studies made significant contributions to the literature
159 and particularly to the criminal units conducting investigations. In these studies, general crimes,
160 cyber-crimes and attacks are generally used as a dataset. The actual dataset based on personal
161 attributes is studied to a lower extent and therefore a machine learning-based model using the
162 dataset of our study is proposed. Cyber-attack and perpetrator estimation method is tackled due to
163 the importance of fields that are studied.
164
165

166	# III. MATERIALS & METHODS

167   When people become a victim of a crime, they resort to cops dealing with that particular type of
168   crime. These data are recorded in detail in the database of this unit. Police units report these crimes
169   by their type, method, year, etc. They prepare statistics according to their characteristics, analyze,
170   and visualize them. When multiple cyber-attacks are made simultaneously against a victim, this is
171   recorded in police records as a single attack. Therefore, it is necessary to look at the details of the
172   event, rather than the statistical data, in order to understand whether multiple methods are used.
173   Although a large number of crimes exist in the database, the focus is cyber-crimes as in recent
174   years. Cyber-crimes have caused considerable material and moral damages and they have not been
175   prevented yet. Cyber-crime is chosen as the subject matter since most studies on this field do not
176   employ actual data. In the proposed model, the objective is to take preventive measures against
177   future crimes based on the characteristics of the victim. In addition, it will provide advantages to
178   the police department in predicting cyber-crimes, profiling these crimes, perpetrators and victims.
179   In addition, thanks to the model, consequential suffering will be prevented. The outcome of the
180   study will enable to take tailored measures and facilitate informing people of the crimes they may
181   be exposed to. Our dataset was real cyber-crime data that occurred in the province of Elazığ
182   between 2015 and 2019. Accessing to actual data and preparing these data for processing with
183   machine-learning methods was a challenging process. When the dataset was obtained, all cyber-
184   crime details were examined. The redundant areas were removed using various data science
185   methods. The number of crimes, damages, attacks and methods of attack in the dataset are shown
186   in Figure 1. In addition, the details of these four features are divided into color groups. With these
187   data, predictions were made using various libraries in the Python 3.7 program. Main libraries of
188   this program such as Numpy, Pandas, Matplotlib were used and the data were visualized through
189   this program. The key advantages of using machine-learning methods in the paper are; the
190   possibility to recognize multiple structured and unstructured data patterns, high-level success in
191   detecting crime tactics as they change, extraction of relationships between complex data and the
192   ability to produce results unpredictable by humans.
193
194

195   **A.   Features**

196   Feature selection is the process of selecting interrelated and useful features in the dataset. It saves
197   time and memory during data training in machine learning. If the features are improperly selected,
198   time required for training may increase. This makes interpretation of the model difficult and
199   increases the error rate in the model. The attributes of the features in our dataset were determined.
200   Each entry was related to a real crime shown in Table 2. These features were used as inputs in
201   training data. In Figure 2, the criteria of the features in our dataset are determined as median,
202   maximum, and minimum.
203
204

205   **B.   Preprocessing**

206   Standardization is the rescaling of features in a normal distribution. This needs to be completed
207   before using machine-learning methods. The data were made suitable, numbers from 1 to 10 were

208 given according to the variety of data in the columns. The StandardScaler () in the Python library
209 was used to optimize the data to be used in algorithms. The bidirectional relationship between type
210 of crime and damages, attack and method of attack is shown in Figure 3. The data were divided
211 into 80% training data and 20% test data.

212

213

214 In the first model, the method of attack was tried to be predicted by giving the features of crime,
215 gender, age, job, income, marital status, education, attack, harm, and perpetrator.
216 In the second model, the perpetrator of crime was tried to be predicted by giving the features of
217 crime, gender, age, income, job, marital status, education, attack, harm, and attack method.

C. Logistic Regression (LR)

219 It is an equation allowing one to predict the value of one from the other, based on the relationship
220 between two or more variables. Assuming that the variance of y is constant, the coefficients can
221 be solved using the least squares method. This minimizes the error between the actual data point
222 and the regression line. The equation for the Logistic Regression line is given as:

$$y' = b + w_1 x_1 + w_1 x_1 + .. + w_n x_n \tag{1}$$

224 Where,
225 y' is the desired output,
226 b is bias value,
227 x is the property of the input,
228 w is the weight of the features.

D. K-Nearest Neighbors (K-NN)

230 The KNN classifier is based on the distance function that measures the difference and similarity
231 between two or more samples. The Euclidean distance d (x, y) between two samples is defined as:

$$d(x,y) = \sum_{k=1}^{n}(x_k + y_k)^2 \tag{2}$$

233 Where,
234 x_k and y_k are the nth element.
235 n is the nth property of the dataset.
236 First, the k parameter is determined and the distance of the new data to be included in the dataset
237 is calculated one by one according to the existing data. The closest neighbour is found and assigned
238 to the neighbour class k.

E. Support Vector Machine (SVM)

240 This method includes support vector classification and support vector regression. SVM is based
241 on the concept of decision limits, supporting both binary and more classifications. Considering
242 the training data D:

$$D = \{(x_i, y_i) \mid x_i \in R p, y_i \in \{-1, 1\}\}_{i=1}^{n} \tag{3}$$

244   Here y_i is 1 or -1 and determines the class to which the x_i point belongs. Every x_i is a p-
245   dimensional real vector. The support vector is at the closest point to the hyperplane of optimum
246   separation. In the classification process, mapping input vectors on the separation hyperplane side
247   of the feature space fall into one class, and locations fall into the class on the other side of the
248   plane.

249   **F. Naive Bayes (NB)**

250   The naive bayes classifier is a simple probability classifier based on applying Bayes' theorem
251   with strong independence assumptions between properties. A naive bayes based on the multi-label
252   classification model can be applied. Given a dataset $\{a_1, a_2,..., a_j\}$ labelled $\{v_1, v_2,..., v_j\}$, the
253   results are predicted using the following equation:

254    $$v_{NB} = \underset{v_j \in V}{\arg max} \; P(v_j)\prod_i Pa_i|v_j \tag{4}$$

255   **G. Decision Tree (DT)**

256   Decision tree is a classification method that creates a tree-like model consisting of decision nodes
257   and leaf nodes by classification, feature, and target. A decision tree or classification tree is a tree
258   where each internal node is labelled with an input property. Arcs from this tagged node are tagged
259   with each of the possible values of the target attribute or lead to a sub-decision node in a different
260   input attribute. A tree can learn by dividing the set of resources into subsets according to an
261   attribute value test. This process is repeated in a recursive manner, called recursive partitioning,
262   on each derived subset. The iteration is complete when the subset in a node has the full value of
263   the target variable or the division no longer adds value to the predictions.

264    $$(x, Y) = (x_1, \; x_2, \; x_3, \; ..., \; x_k, Y) \tag{5}$$

265   The dependent variable Y is the target variable that we are trying to understand, classify or
266   generalize. The vector x consists of input variables such as $x_1, \; x_2, \; x_3$ used for this task.

267   **H. Random Forest (RF)**

268   Random forest is an algorithm that creates classifier on training data and combines outputs to
269   make the best predictions on test data. Randomness minimizes variance to avoid over-learning
270   according to training data.

271    $$y = \underset{p \, \in \{h(x_1)..h(x_k)\}}{\arg max} \; \{\sum_{j=1}^{k}(I(h(x|\theta_j) = p\,))\} \tag{6}$$

272   Where,
273    $h(x|\theta)$ is a classification tree,
274   k is the number of the tree selected from a pattern random vector.
275   If $D(x, y)$ represents the training data, each classification tree in the ensemble is constructed using
276   a different subset $D_{\theta_k}(x, y) \subset D(x,y)$) of the training data. Each tree then works like normal

277   decision trees. Data is segmented by randomly selected value until it is fully partitioned, or the
278   maximum allowed depth is reached.

279   **I.   eXtreme Gradient Boosting (XGBoost)**

280   The first step in XGBoost is to make the first prediction (base score). This prediction can be any
281   number, as the correct result will be reached by converging with the operations to be done in the
282   next steps. This number is 0.5 by default.
283   First, the loss function $L(y_i, F(x))$ is created. y_i is the observed value, $F(x)$ is the predicted value:

284
$$F_0(x) = \underset{\gamma}{\text{argmin}} \sum_{i=1}^{n} (L(y_i, \gamma) \qquad\qquad (7)$$

285   Here, the constant variable is determined. It is the value loss function in sigma in the formula. γ
286   (gamma) is the predicted value.

287
$$r_{im} = -\left[\frac{\partial L(y_i, F(x_i))}{\partial F(x_i)}\right]_{F(x) = F_{m-1}(x)} \quad i = 1, \dots, n \qquad (8)$$

288   Where,
289   r means residual,
290   i is observation number,
291   m denotes the number of the established tree.
292   The basic learning terminal node in tree growth is the regression tree. It is formulated below:

293
$$\gamma_{im} = \underset{\gamma}{\text{argmin}} \sum_{x_i \in R_{ij}} L(y_i, F_{m-1}(x_i) + \gamma) \qquad j = 1 \dots J_m \qquad (9)$$

294
$$F_m(x) = F_{m-1}(x) + \sum_{j=1}^{j_m} \gamma_{jm} I(x \in R_{jm}) \qquad (10)$$

295   **J.   Accuracy, Precision, Recall, F1-Score**

296   Accuracy (Acc) score is a method used to evaluate the performance of the model made by
297   comparing the predictions made after running the algorithm with the test data. A value between 0
298   and 1 is produced according to the ratio of the entire predicted value for a prediction to match with
299   the real values. To determine the accuracy of the forecast:
300   •   TP = Prediction is positive(normal) and actual is positive(normal).
301   •   FP = Prediction is positive(normal) and actual is negative(abnormal).
302   •   FN = Prediction is negative(abnormal) and actual is positive(normal).
303   •   TN = Prediction is negative(abnormal) and actual is negative(abnormal)
304   The other evaluation metrics for the proposed model are precision, recall and F1-score. Precision
305   (P) is the rate of correctly classified positive instances to the total number of positive instances.
306   Recall (R) shows how successfully positive instances are predicted. F1-Score (F1) is the weighted
307   average of the Precision and Recall values.
308

309
$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \qquad (11)$$

310

311
$$P = \frac{TP}{TP + FP} \qquad (12)$$

312

313
$$R = \frac{TP}{TP + FN} \qquad (13)$$

314

315
$$F1 = \frac{2TP}{2TP + FN + FP} \qquad (14)$$

IV. RESULTS & DISCUSSION

316

317   The study aims to analyze the data collected about incidents correctly, to avoid crimes and to
318 catch the perpetrators. The main subject of this paper is to draw conclusions from the analyzed
319 data and combat crimes based on the outcome. These results will reveal and shed light on the
320 investigations carried out by law enforcement officers and any concealed facts. Based on the
321 information on the victim and the method of the cyber-crime, and whether the perpetrator is
322 identified or not, machine-learning methods may be used to determine if the same perpetrator
323 carried out the cyber-attack. The damages suffered by the victims in cyber incidents in Elazığ
324 province have been discovered over the years through various methods. The sum of monetary
325 damages suffered by each victim in the dataset was obtained by summing over the years. It is
326 thought that the decrease in such incidents, observed especially after 2017, results from deterrence
327 secured by the laws and awareness activities. The amount of economic losses due to cyber-attacks
328 is profoundly serious in Elazığ, as shown in Figure 4. The damage mentioned above is enough to
329 show the importance of dealing with cyber security and attack methods.
330

331   In this section, results obtained by use of Support Vector Machine (Linear), Random Forest,
332 Logistic Regression, eXtreme Gradient Boosting, Support Vector Machine (Kernel), Decision
333 Tree, K-Nearest Neighbors, Naive Bayes algorithms are presented. We can evaluate the Pearson
334 correlation coefficient between these data as shown in Figure 5. This correlation matrix shows that
335 there are substantial correlations between practically all pairs of variables.
336

337   During the experiment, the dataset was first trained and tested in all algorithms. Accuracy and
338 evaluation criteria were also adopted. Accuracy, precision, recall and F1 score values were
339 obtained by comparing the predicted values with the test data.
340

341

342   The prediction accuracy, precision, recall and F1-score data among the algorithms of the first
343 model predicting the method of attack are shown in Table 3. The comparison of accuracy is shown
344 in Figure 6. When the results were compared, SVML showed the best performance with an
345 accuracy rate of 95.02% in terms of prediction accuracy. SVML algorithm outperformed RF, LR,
346 XGBoost, SVMK, DT, KNN, and NB algorithms by 0.54%, 1.1%, 1.66%, 2.2%, 2.76%, 5.52%
347 and 13.25% margin, respectively. NB showed the poorest performance with a rate of 81.7%. The
348 performances of algorithms other than NB were close to each other. The distribution graph of the
349 actual values and the predicted values obtained by the SVML algorithm are shown in Figure 7a
350 and the error matrix is shown in Figure 7b.
351

352

353   Comparing the model in terms of precision, recall and F1-scores, the best result was also obtained
354 with SVML algorithm, albeit a small margin. While LR, SVMK, DT, RF and XGBoost gave
355 results above 92%, their performances were close to each other. Out of these three scores, a
356 difference of approximately 10% was found between the underperforming KNN and NB. In
357 general, all algorithms produced sufficient results. These results showed that the machine-learning
358 approach could be successfully applied to predict the cyber-attack method. In the model to be

359 created, when the features of a person (Table 2) are entered, it can be predicted which crime such
360 person will be exposed to. Also, warning systems can be created for groups of persons.
361

362   The prediction accuracy, precision, recall and F1-scores data among the algorithms of the second
363 model that predicts the attacker are given in Table 4. The comparison of accuracy is shown in
364 Figure 8. LR showed the best performance in this model with 65.42% and SVML, KNN, SVMK,
365 XGBoost, RF, DT and NB algorithms achieved accuracy with a margin of 0.78%, 0.85%, 1.33%,
366 1.39%, 1.88%, 2.44% and 3.34%, respectively. Even though NB showed the poorest performance,
367 the performances of algorithms were very close to each other. The distribution graph of the actual
368 values and the predicted values obtained by the SVML algorithm are shown in Figure 9a and the
369 error matrix is shown in Figure 9b.
370

371

372   In terms of precision, recall, and F1-scores, the results of the algorithms varied between 55% and
373 65%. The results were not satisfactory. Based on the known/unknown feature of the perpetrator,
374 we aimed to find out whether the same perpetrator committed the crime after comparing the
375 features of the attacker who carried out the incident. However, the results of the model indicated
376 that a new model should be created by adding new attributes.
377   When the papers shown in the table in section II are compared with our model, eight of the
378 datasets of these works include general street-crimes. One of them works with terrorist crimes, and
379 two of them work with cyber-crimes. Cyber-crime data is one of the less studied crime types in
380 the literature so that we use these data for our proposed study.
381   In the other predictions, it is seen that the data such as the type, time, place, region, attacker,
382 demographic and regional factors of the crime are mostly used as features. In our study, predictions
383 are made according to the features of age, gender, income, occupation, harm, and attack methods
384 because there are very few studies using these features.
385   When the studies conducted by Arora et al. and Ch et al. were compared with our study, it was
386 found out that some features were similar. All studies focused on cyber-crime, the datasets and
387 parameters were different from each other, though. The accuracy rate was found to be 80% in the
388 study conducted by Arora et al. and 99.3% in the study carried out by Ch et al.
389   The limitation of our study is the quantity of data set since our data set consists of actual data.
390 The temporal data enables estimation of time series; however, these data are not available in our
391 dataset. Likewise, if the technical details of the attacks were available in the police records, detailed
392 estimates could make it easier to catch the perpetrator.
393   Many studies have predicted where and when crimes will occur in the future. However, many of
394 them have not touched upon the method by which crimes occur, how they can be prevented, and
395 what the features of the perpetrator are. One of the key advantages of this study is using actual
396 data and it is a preliminary step towards profiling for people having similar features with the
397 attacked victims. Another advantage of the proposed study is predicting what the cyber-attack
398 method will be and whether its perpetrator can be detected. Our results show that any exposure to
399 cyber-crimes reduces as the level of education and income increases.

V. CONCLUSIONS & FUTURE WORK

This paper suggests a method that predicts and detects cyber-attacks by using both machine-learning algorithms and the data from previous cyber-crime cases. In the model, the characteristics of the people who may be attacked and which methods of attack they may be exposed to are predicted. It has been observed that machine-learning methods are successful enough. The Support Vector Machines linear method is the most successful of these methods. The success rate of predicting the attacker who will make a cyber-attack in the model is around 60%. Other artificial intelligence methods may be able to try to increase this ratio. In our approach, it is concluded that it is necessary to draw attention to especially malware and social engineering attacks. It is found that the higher the levels of the victim's education and income are, the less the probability of cyber-attack is. The primary focus of this study is to lead law enforcement agencies in the fight against cyber-crime and provide faster and more effective solutions in detecting crime and criminals. New training and warning systems can be created for people with similar characteristics by the evaluation of the characteristics of the attack victims emerged in our analysis study.

For future works; crime, criminal, victim profiling, and cyber-attacks can be predicted using deep learning algorithms and the results can be compared. Based on the talks with other authorized units having crime databases, cyber-crime data of other provinces may also be obtained to use for comparison with this study. The data of other provinces can be compared to similar studies. Intelligent criminal-victim detection systems that can be useful to law enforcement agencies in the fight against crime and criminals can be created to reduce crime rates.

REFERENCES

[1]   Reid R, Van Niekerk J. 2014. From information security to cyber security cultures. Information Security for South Africa. IEEE, p. 1-7

[2]   Goel S. 2020. National Cyber Security Strategy and the Emergence of Strong Digital Borders. Connections: The Quarterly Journal, 19(1), 73-86 https://doi.org/10.11610/Connections.19.1.07

[3]   Critical Infrastructure, https://www.cisa.gov/critical-infrastructure-sectors, Accessed 28 September 2020

[4]   Jang-Jaccard J, Nepal S. 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993 doi.org/10.1016/j.jcss.2014.02.005

[5]   Check Point Security Report. 2020. https://research.checkpoint.com/

[6]   Bayuk JL, Healey J, Rohmeyer P, Sachs MH, Schmidt J, Weiss J. 2012. Cyber security policy guidebook (pp. 3-4). Hoboken: Wiley

[7]   Crawford J. 2017. The Impact of Artificial Intelligence on Autonomous Cyber Defense. PhD Thesis. Utica College.

[8]   Sayan CM. 2017. An intelligent security assistant for cyber security operations. IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W). p. 375-376.

441 [9] Ben-Asher N, Gonzalez C. 2015. Effects of cyber security knowledge on attack detection.
442   Computers in Human Behavior, 48: 51-61. doi.org/10.1016/j.chb.2015.01.039

443 [10] Wang D, Wang X, Zhang Y, & Jin L. 2019. Detection of power grid disturbances and cyber-
444   attacks based on machine learning. Journal of Information Security and Applications, 46,
445   42-52. doi.org/10.1016/j.jisa.2019.02.008

446 [11] Zolanvari M, Teixeira MA, Gupta L, Khan KM, & Jain R. 2019. Machine learning-based
447   network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things
448   Journal, 6(4), 6822-6834. doi.org/10.1109/JIOT.2019.2912022

449 [12] Canbek G, Sagiroglu Ş, Temizel TT. 2018. New techniques in profiling big datasets for
450   machine learning with a concise review of android mobile malware datasets. IBIGDELFT
451   IEEE, p. 117-121.

452 [13] Moorthy RS, Pabitha P. 2020. Optimal Detection of Phishing Attack using SCA based K-
453   NN. Procedia Computer Science, 171: 1716-1725 doi.org/10.1016/j.procs.2020.04.184

454 [14] Ngejane CH, Mabuza-Hocquet G, Eloff JH, & Lefophane S. 2018. Mitigating online sexual
455   grooming cybercrime on social media using machine learning: A desktop survey. In 2018
456   International Conference on Advances in Big Data, Computing and Data Communication
457   Systems (icABCD) pp. 1-6. IEEE.

458 [15] Gurjar M, Naik P, Mujumdar G, & Vaidya T. 2018. Stock market prediction using ANN.
459   Int. Res. J. Eng. Technol.(IRJET), 5, 2758-2761.

460 [16] Wheeler AP, Steenbeek W. 2020. Mapping the risk terrain for crime using machine learning.
461   Journal of Quantitative Criminology, 1-36 doi.org/10.1007/s10940-020-09457-7

462 [17] Zulfadhilah M, Prayudi Y, Riadi I. 2016. Cyber profiling using log analysis and k-means
463   clustering. International Journal of Advanced Computer Science and Applications, 7.7: 430-
464   435

465 [18] Biswas AA, Basak S. 2019. Forecasting the Trends and Patterns of Crime in Bangladesh
466   using Machine Learning Model. 2nd International Conference on Intelligent Communication
467   and Computational Techniques (ICCT). IEEE, p. 114-118

468 [19] Bharathi ST, Indrani B, Prabakar MA. 2017. A supervised learning approach for criminal
469   identification using similarity measures and K-Medoids clustering. ICICICT. IEEE, p. 646-
470   653

471 [20] Lin YL, Chen TY, Yu LC. 2017. Using machine learning to assist crime prevention. 6th IIAI
472   International Congress on Advanced Applied Informatics (IIAI-AAI). IEEE, p. 1029-1030

473 [21] Fischer EA. 2009. Creating a National Framework for Cybersecurity: an Analysis of Issues
474   and Options. Library of congress Washington DC congressional research service

475 [22] Kaur Chahal J, Bhandari A, Behal S. 2019. Distributed Denial of Service Attacks: A Threat
476   or Challenge. New Review of Information Networking, 24.1: 31-103
477   doi.org/10.1080/13614576.2019.1611468

478 [23] Sahingoz OK, Buber E, Demir O, & Diri B. (2019). Machine learning based phishing
479   detection from URLs. Expert Systems with Applications, 117, 345-357.
480   doi.org/10.1016/j.eswa.2018.09.029

481 [24] Biju JM, Gopal N, Prakash AJ. 2019. Cyber Attacks and Its Different Types.
482   doi.org/10.6633/IJNS.201309.15%285%29.09

483 [25] Mitnick KD, & Simon WL. 2009. The art of intrusion: the real stories behind the exploits of
484   hackers, intruders and deceivers. John Wiley & Sons

485 [26] Breda F, Barbosa H, Morais T. 2017. Social engineering and cyber security. International
486   Technology, Education and Development Conference

487 [27] Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR, & Singh S. 2020. A Review
488   on Cyber Crimes on the Internet of Things. arXiv preprint arXiv:2009.05708.)

489 [28] Rewari S, Singh W. 2017. Systematic review of crime data analytics. International
490   Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). IEEE,
491   p. 3042-3045 doi.org/10.1109/ICPCSI.2017.8392284

492 [29] Hassan M, Rahman MZ. 2017. Crime news analysis: Location and story detection. 20th
493   International Conference of Computer and Information Technology (ICCIT). IEEE, p. 1-6
494   doi.org/10.1109/ICCITECHN.2017.8281798

495 [30] Zhao X, Tang J. 2017. Exploring transfer learning for crime prediction. IEEE International
496   Conference on Data Mining Workshops (ICDMW). IEEE, p. 1158-1159
497   doi.org/10.1109/ICDMW.2017.165

498 [31] Vineeth KRS, Pandey A, Pradhan T. 2016. A novel approach for intelligent crime pattern
499   discovery and prediction. International conference on advanced communication control and
500   computing technologies (ICACCCT). IEEE, p. 531-538
501   doi.org/10.1109/ICACCCT.2016.7831697

502 [32] Feng M, Zheng J, Han Y, Ren J, & Liu Q. 2018. Big data analytics and mining for crime
503   data analysis, visualization and prediction. In International Conference on Brain Inspired
504   Cognitive Systems (pp. 605-614). Springer, Cham. doi.org/10.1007/978-3-030-00563-4_59

505 [33] Kim S, Joshi P, Kalsi PS, & Taheri P. 2018. Crime analysis through machine learning. In
506   2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication
507   Conference (IEMCON) (pp. 415-420). IEEE. doi.org/10.1109/IEMCON.2018.8614828

508 [34] Bharati A, RA Dr S. 2018. Crime Prediction and Analysis Using Machine Learning.
509   International Research Journal of Engineering and Technology (IRJET), 5.09

510 [35] Chandrasekar A, RAJ AS, Kumar P. 2015. Crime prediction and classification in San
511   Francisco City. URL http://cs229.Stanford.Edu/proj2015/228{_}report.Pdf

512 [36] Alves LGA, Ribeiro HV, Rodrigues FA. 2018. Crime prediction through urban metrics and
513   statistical learning. Physica A: Statistical Mechanics and its Applications, 505: 435-443
514   doi.org/10.1016/j.physa.2018.03.084

515 [37] Kumar A, Verma A, Shinde G, Sukhdeve Y, & Lal N. 2020. Crime Prediction Using K-
516   Nearest Neighboring Algorithm. In 2020 International Conference on Emerging Trends in
517   Information Technology and Engineering (ic-ETITE) pp. 1-4. IEEE. doi.org/10.1109/ic-
518   ETITE47903.2020.155

519 [38] Jha P, Jha R, & Sharma A, 2019. Behavior Analysis and Crime Prediction using,
520   International Journal of Recent Technology and Engineering (IJRTE), p. 1

521 [39] Verma D, Yarlagadda R, Gartner SS, & Felmlee D. 2019. Understanding patterns of
522   terrorism in india (2007-2017) using artificial intelligence machine learning. The
523   International Journal of Technology, Knowledge, and Society, 15(4), 23-39.
524 [40] Arora T, Sharma M, Khatri SK. 2019. Detection of Cyber Crime on Social Media using
525   Random Forest Algorithm. 2nd International Conference on Power Energy, Environment
526   and Intelligent Control (PEEIC). IEEE, p. 47-51
527 [41] Ghankutkar S, Sarkar N, Gajbhiye P, Yadav S, Kalbande D, & Bakereywala N. 2019.
528   Modelling Machine Learning For Analysing Crime News. In 2019 International Conference
529   on Advances in Computing, Communication and Control (ICAC3) pp. 1-5. IEEE.
530   doi.org/10.1109/ICAC347590.2019.9036769
531 [42] Ch R, Gadekallu TR, Abidi MH, & Al-Ahmari A. 2020. Computational system to classify
532   cybercrime offenses using machine learning. Sustainability, 12(10), 4087.
533   doi.org/10.3390/su12104087
534 [43] RM SP, Maddikunta PKR, Parimala M, Koppu S, Gadekallu TR, Chowdhary CL, & Alazab
535   M. 2020. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion
536   detection in IoMT architecture. Computer Communications, 160, 139-149.
537   https://doi.org/10.1016/j.comcom.2020.05.048
538

Table 1. Related work summary comparison

Author	Year	Country	Dataset	Features	Method	Accuracy	Advantage
Chandrasekar at al	2015	USA	General Crime in San Francisco	Date, Day of the week, Name of the Police Department District, Address, Latitude, Longitude, Category, Description, Resolution	RF, SVM, Gboost	Md1 SVM 96% Md1 Gboosted 75.02%	Including time series modeling to understand temporal correlations of blue / white collar and Violent / Nonviolent crime classification data and predicting fluctuations in different crime categories
Feng at al	2018	USA	General Crime in San Francisco, Chicago, Philadelphia	Date, Category, Descript, Dayof Week, P. D. District, Resolution, Address, x, y, Dome, Arrest	NB, KNN, RF, XGBoost	XGboost 70%	Predicting overall crime in the coming years using time series
Kim at al	2018	Canada	General Crime in Vancouver	Crime Type, Month, Day, Hour, Weekday, Address, Neighborhood, x, y	KNN, XGBoost	Md1 Gboost 41.9% Md2 Gboost 43.2%	Predicting crime location
Bharati at al	2018	USA	General Crime in Chicago	Block, Location, District, Community Area, Latitude, X, Y, Longitude, Hour, Month,	KNN, LR, DT, RF, SVM, NB	KNN 78.9%	Detecting, predicting, and solving crimes much faster, thereby lowering the crime rate
Alves at al	2018	Brazil	Murder Crimes	Child labor, Elderly - Female- Male Population, GDP, Homicides, Income, Literacy, Sanitation, Suicides, Traffic Accidents, Unemployment	RF	RF 97%	The prediction revealed that unemployment and ignorance were the most important variables in defining murders in Brazilian cities, and the order of importance of urban indicators in predicting crimes was determined.
Verma at al	2019	India	Terrorist Incidents	Incident Location, Time, Type, Weapon, Intensity of Attack, Capital, Perpetrator	DT, RF, IG	RF 84%	Predicting the occurrence of terrorist incidents on demographic and geographic data
Jha at al	2019	India	Murder Crimes on the Internet	Crime Type, Year, Address, Place, Territory	NB	NB 51.2%	Analyzing crimes in minimum time and predicting the location and type of future crimes
Arora at al	2019	Public	Cybercrime Data Publicly Available on Social Media	Synonyms, Age, Location, Gender, Hashtags, and Sarcasm	RF	RF 80%	Detecting cyber threats automatically
Ghankutkar at al	2019	Public	Real-time Crime Data from HuffPost News Site	Category, Headline, Authors, Link, Short Description, Date	SVM, MNB, RF	RF 85.83%	Providing analysis to current news after being classified as crime and non-crime data
Kumar at al	2020	India	Murder, Kidnapping, Violence, Robbery, Gambling, Accident, Indore, Crimes	Hour, Longitude, Latitude, Day of the Week, Week, Month	KNN	Prev 93.23% Proposed 99.51%	Predicting the type of crime, and where and when it may occur
Ch at al	2020	India	Cybercrime	Incident, Harm, Access, Year, Violation, Victim, Offender	SVML, LR MNB, RF	LR 99.3%	Finding and analyzing cyber-attacks that exploit vulnerabilities.

Table 2. The attributes used for feature selection

Crime	• Misuse of Debit Cards or Credit Cards • Through Informatics Theft • Hacking into the Information System and Capturing Data
Gender	M – F
Age	27 and under / Between 28-37 / Between 38-50 / 51 and above
Income	Low – Middle – High
Job	Other – Student – Retired – Justice and Security – Health Sector Manager – Housewife – Education – Technical – Finance Sector
Marital status	Single – Married
Education	Primary Education – High School – Undergraduate – Graduate
Harm	• Internet Shopping by Introducing Himself as a Bank Clerk • Internet Shopping out of Knowledge • Withdrawals without Knowledge • Withdrawing Money by Introducing Himself as a Bank Clerk • Fraud • Do Moral Harm • Threating / Blackmailing
Attack	• Obtaining Electronic Bank Accounts • Copying Bank / ATM Cards • Hacking Social Media Accounts • Obtaining and Using Data in Digital Environment • Selling Counterfeit Products
Attack Method	• Social Engineering • Hacking Tools or Malware • Card Copying / Generating Devices • Phishing Attack • Receiving Public Data on Social Media • Creating a Fake Shopping Site
Perpetrator	Known – Unknown

Table 3. Performance of machine learning algorithms for model 1

	Accuracy %	Precision %	Recall %	F1-score %
LR	93.92	94.41	93.92	94.1
KNN	89.5	71.73	76.24	72.69
SVML	95.02	95.43	95.03	95.16
SVMK	92.82	92.99	92.82	92.88
NB	81.77	81.79	81.77	81.23
DT	92.26	92.3	92.27	92.28
RF	94.48	94.48	94.48	94.48
XGBOOST	93.36	92.75	92.82	92.76

Table 4. Performance of machine learning algorithms for model 2

	Accuracy %	Precision %	Recall %	F1-score %
LR	65.42	60.67	60.22	59.14
KNN	64.57	56.85	56.91	56.85
SVML	64.64	65.75	64.64	63.54
SVMK	64.09	65.24	64.09	62.90
NB	62.08	57.93	57.46	55.66
DT	62.98	63.50	62.98	62.18
RF	63.54	63.91	63.54	62.92
XGBOOST	64.03	65.74	65.19	64.55

Figure 1

Figure 1.The number of crimes, damages, attacks and methods of attack in the dataset
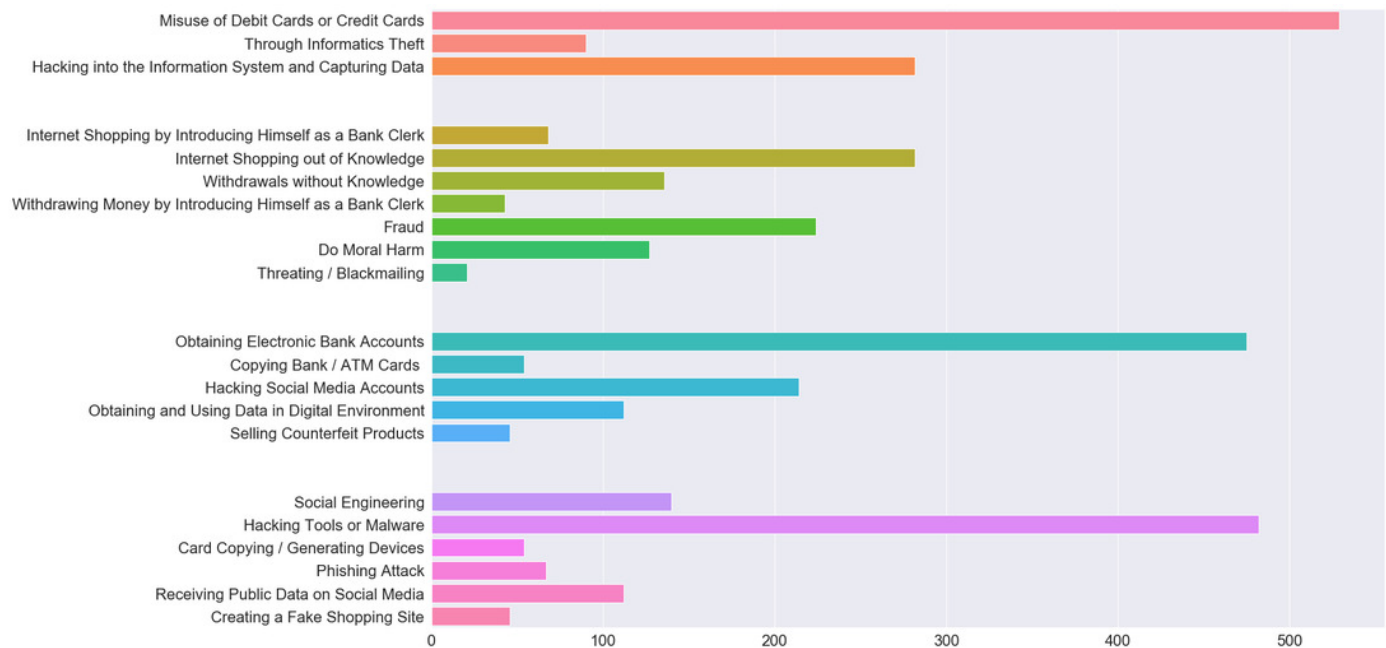
Figure 2

Figure 2. Measure of features
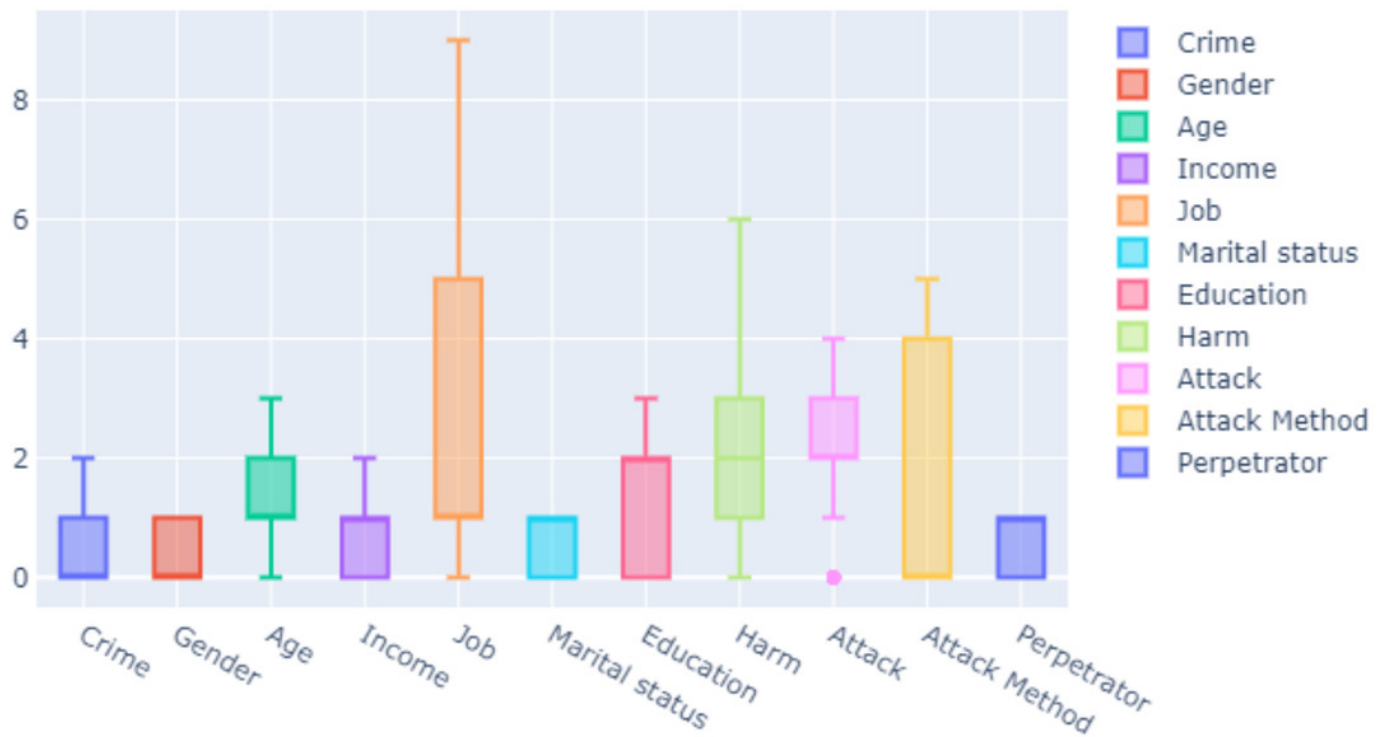
Figure 3

Figure 3. Pairwise relationship between crime, harm, attack, and attack method
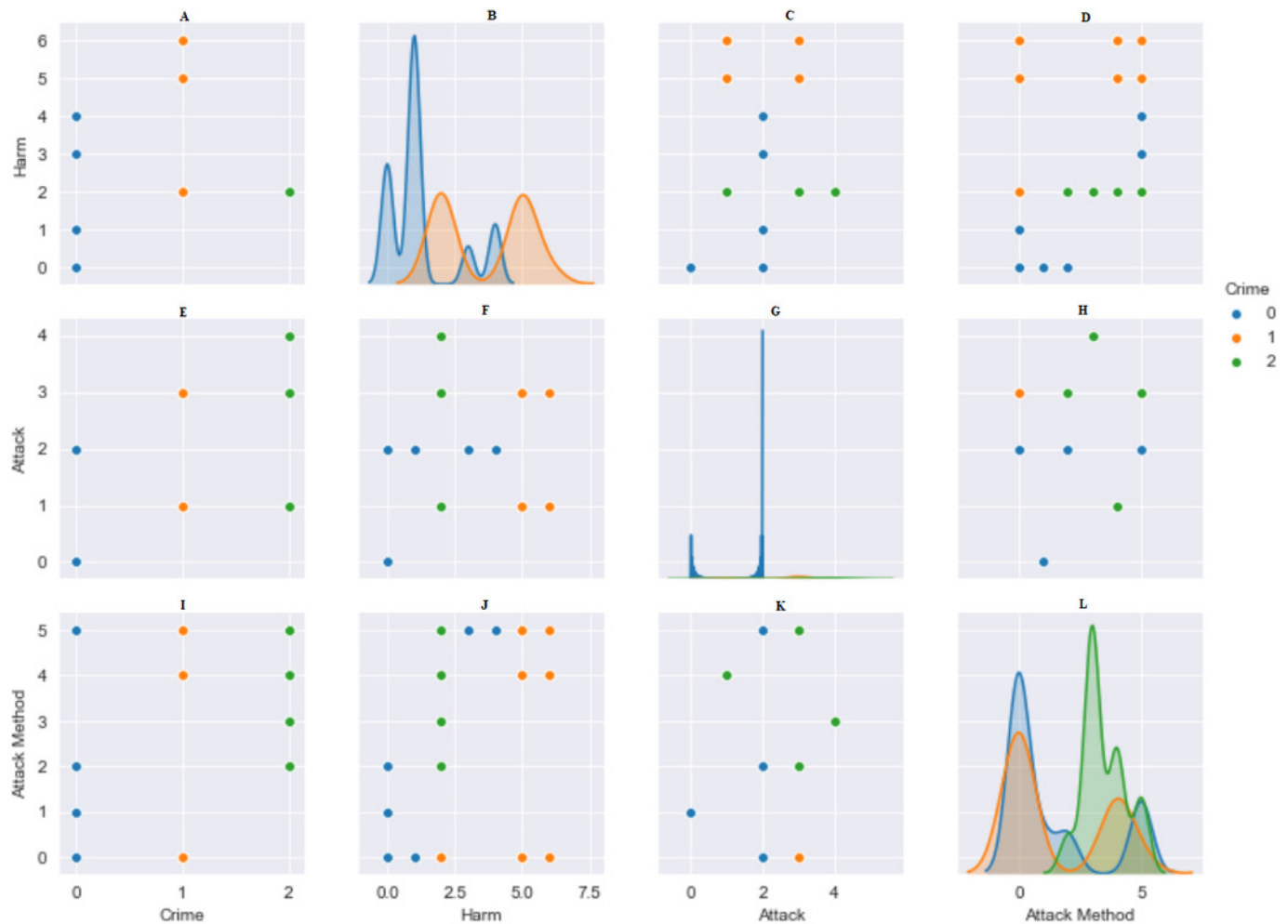
Figure 4

Figure 4. Damage caused by cyber-attacks in Elazığ province
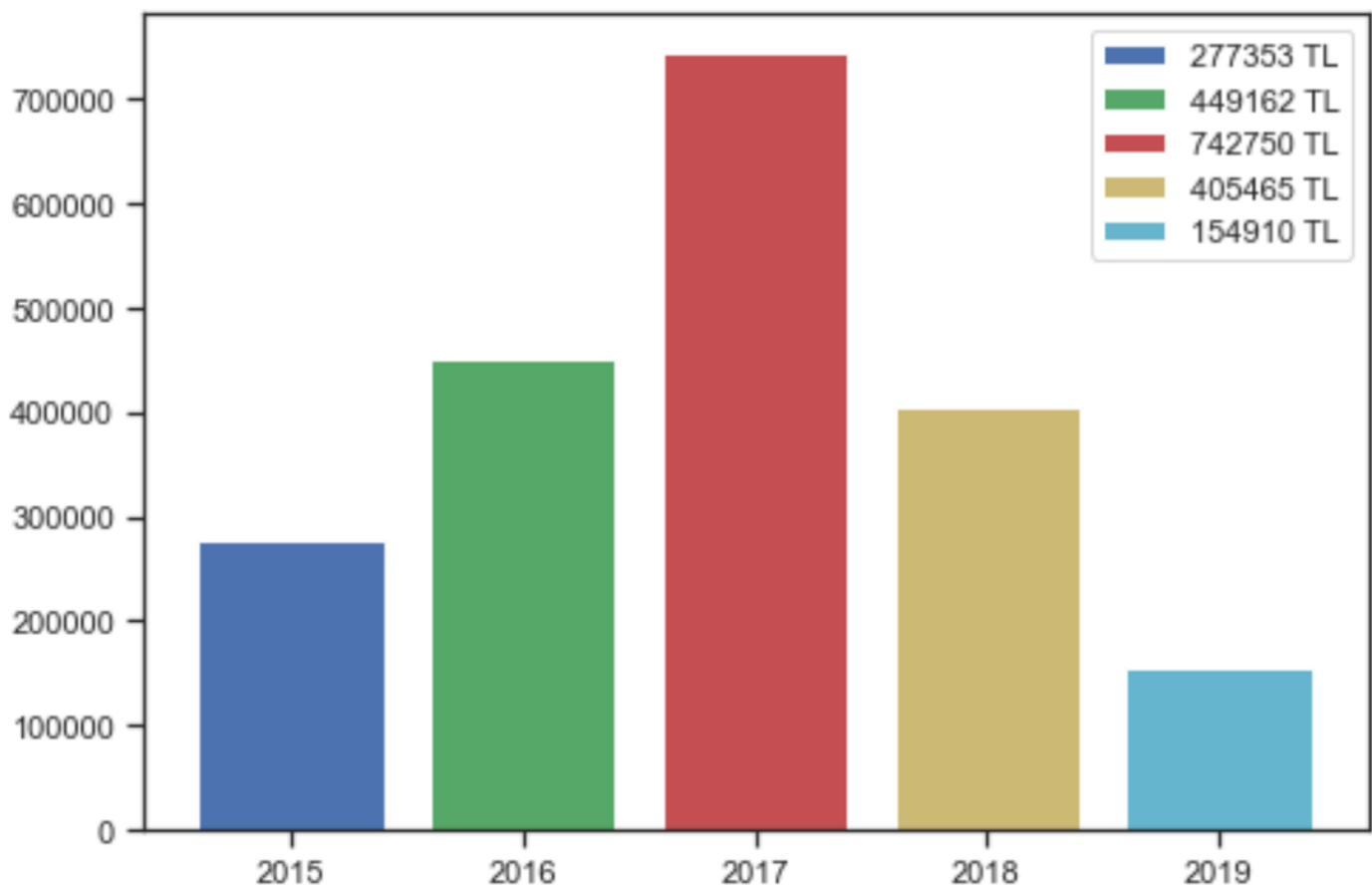
Figure 5

Figure 5. Pearson's linear correlations matrix
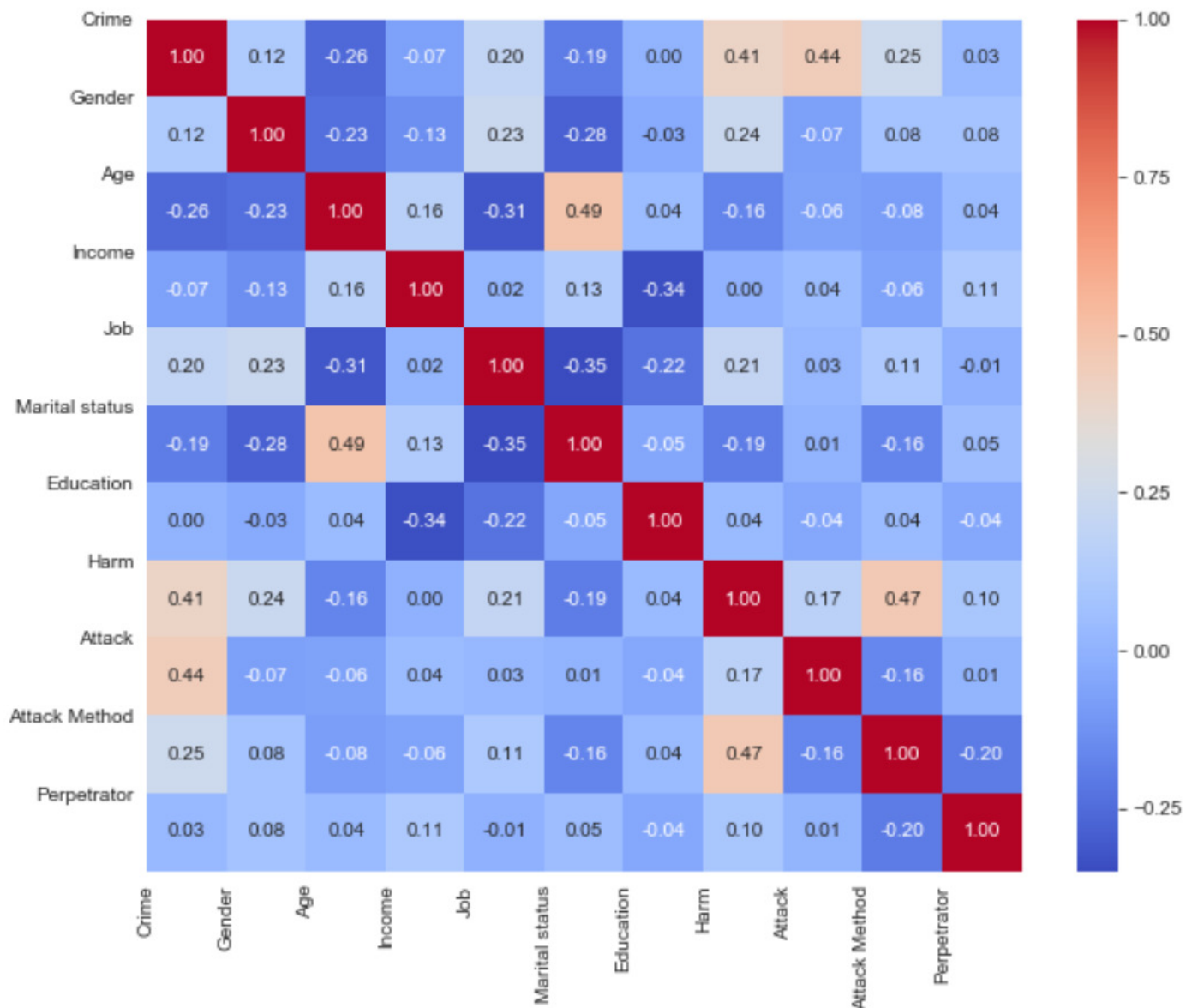
Figure 6

Figure 6. Accuracy rate of algorithms applied in attack method prediction
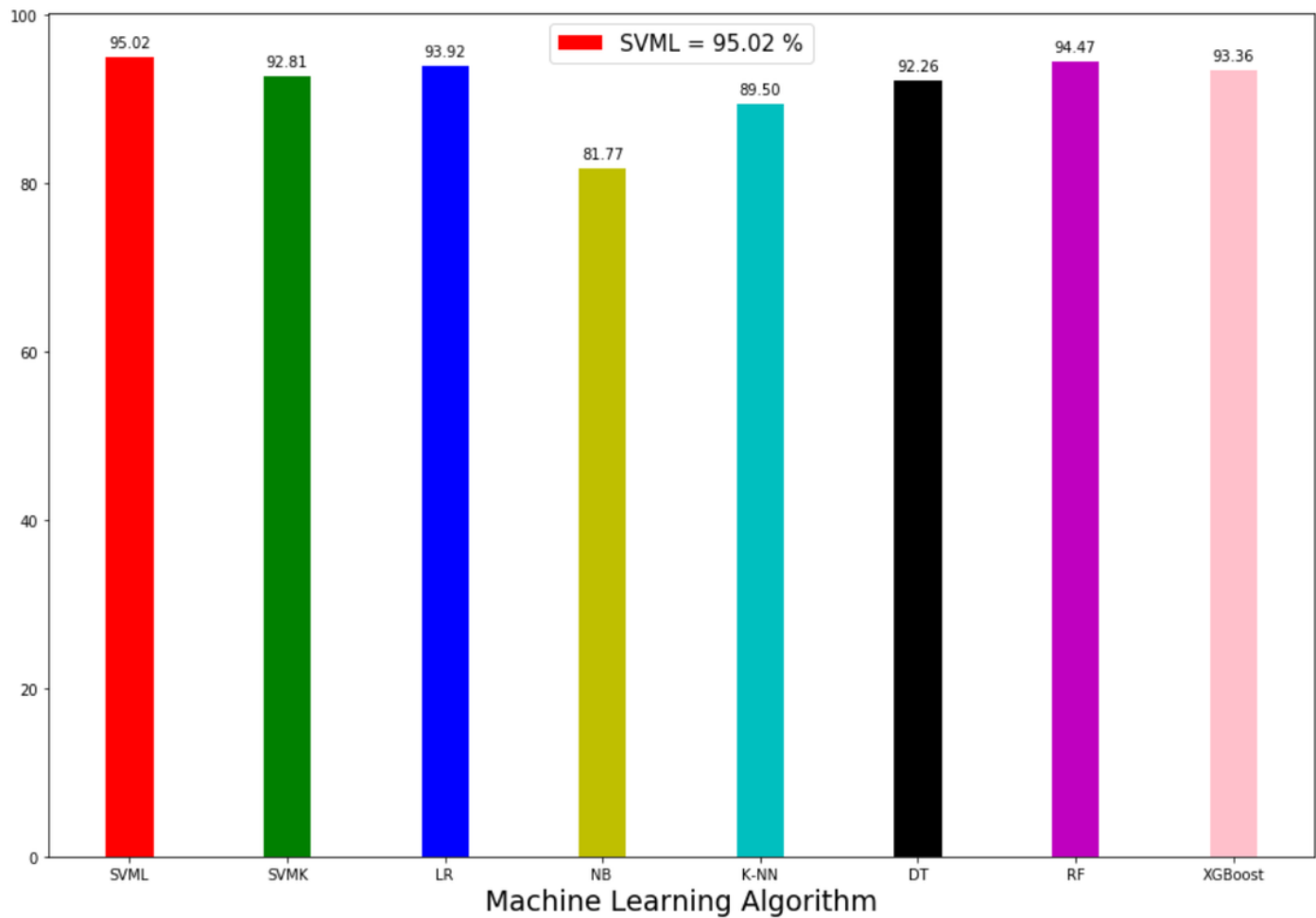
Figure 7

Figure 7. A) Model 1 comparison values (Results are colored redder as they approach the actual values and more purple as they move away). B) Confusion matrix of predicted values

Where 0 is "Hacking Tools or Malware", 1 is "Card Copying / Generating Devices", 2 is "Phishing Attack", 3 is "Creating a Fake Shopping Site", 4 is "Receiving Public Data on Social Media", 5 is "Social Engineering".
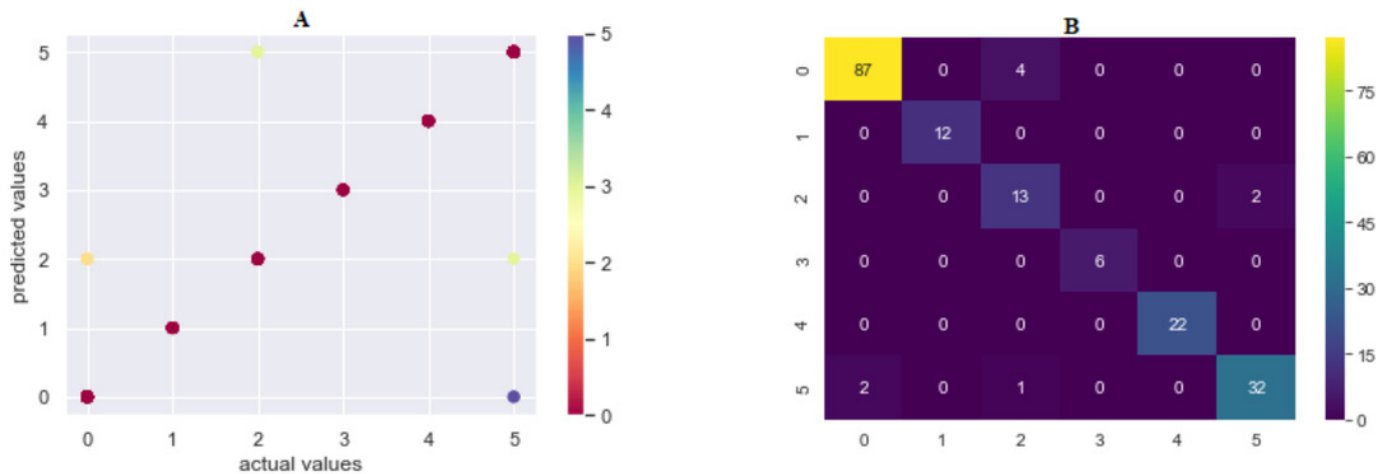
Figure 8

Figure 8. Accuracy rate of algorithms applied in perpetrator prediction method
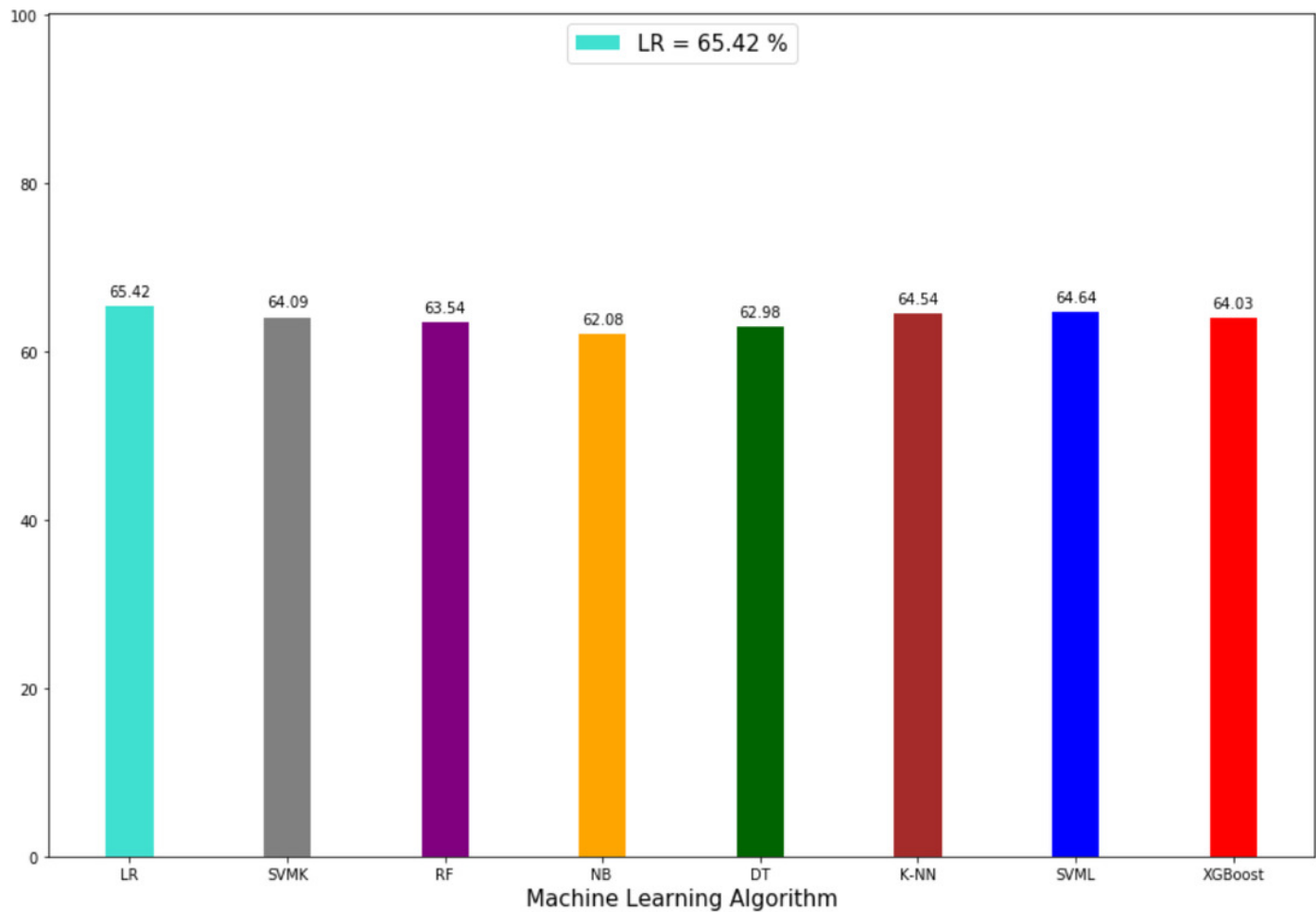
Figure 9

Figure 9. A) Model 2 comparison values (Results are colored redder as they approach the actual values and more purple as they move away). B) Confusion matrix of predicted values

Where 0 is "Perpetrator Known", 1 is "Perpetrator Unknown".