



Predictive Policing Using Deep Learning: A Community Policing Practical Case Study

Omowunmi Isafiade^(✉), Brian Ndingindwayo, and Antoine Bagula

Department of Computer Science, University of the Western Cape, Cape Town,
South Africa
oisafiade@uwc.ac.za

Abstract. There is relentless effort in combating the issue of crime in South Africa and many parts of the world. This challenge is heightened in under-resourced settings, where there is limited knowledge support, thus resulting in increasing negative perceptions of public safety. This work presents a predictive policing model as an addition to a burglar alarm system deployed in a community policing project to improve crime prevention performance. The proposed model uses feature-oriented data fusion method based on a deep learning crime prediction mechanism. Feed-Forward Neural Network (FFNN) and Recurrent Neural Network (RNN) models are employed to predict the amount of calls made to police stations on a monthly basis. Device installation and census data are used in the feature selection process to predict monthly calls to a police station. Coefficient of correlation function is used to isolate the relevant features for the analysis. To provide a viable way of achieving crime reduction targets, the models are implemented and tested on a real-life community policing network system called MeMeZa, which is currently deployed in low-income areas of South Africa. Furthermore, the model is evaluated using coefficient of determination function and the accuracy of the predictions assessed using an independent dataset that was not used in the models' development. The proposed solution falls under the Machine Learning and AI applications in networks paradigm, and promises to promote smart policing in under-resourced settings.

Keywords: Public safety · Resource-constrained settings · Deep learning · Memeza · Predictive policing

1 Introduction

There is evidence that South Africa(SA) has a high rate of crime [1], as seen in the ten-year trend presented in Fig. 1. Hence, combating crime is still a top priority for stakeholders [2]. Moreover, high crime and violence levels not only

place a heavy burden on the criminal justice system, but also on health care and state expenditure, amongst others. Notably, preventing crime has been a priority for the government since 1994 [3]. Many aspirations to curb crime and achieve crime reduction goals are embodied in several national laws and international agreements, including several provincial and national community outreach campaigns [4]. Community safety receives particular attention in South Africa’s primary strategic framework for development, according to the National Development Plan (NDP) 2030 [6]. The program sets out recommendations aimed at improving the functioning of the criminal justice system and at protecting vulnerable women and children.

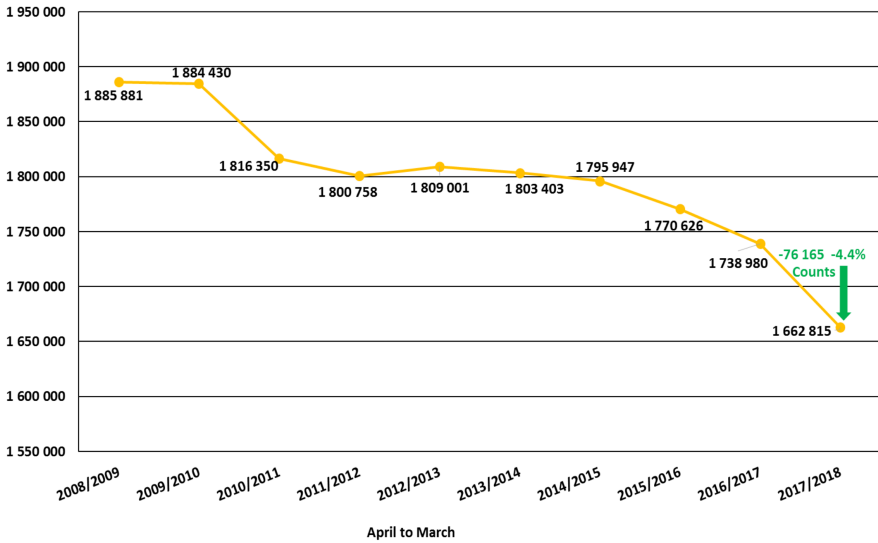


Fig. 1. Trend of crime in South Africa over a ten year period [1]

Despite the efforts by the government, crime trends still remain high in South Africa with only a small portion detected as a result of police action. In general, random patrol activities have not been very effective [7]. Furthermore, police to citizen ratio in South Africa is at 1:450, and that means one police officer is expected to protect 450 people, which is a near impossible task [4]. Hence, the need for efficient systems that can assist the police [5]. Currently, there is limited or no real-time analysis on crime at source and this hampers service delivery [1,2]. Moreover, residents have not always been predisposed to being policed by the state due to the inherent socio-political terrain of high crime spaces in South Africa, and the poor response time and intervention perceived from the police. Clearly, efficient service delivery has been hampered by massive shortage of resources, which include real-time analysis and knowledge support. There is obviously a need for the government to devise more strategies to combat

crime, and encourage more community policing initiatives. One of such initiatives is the MeMeza community policing network, which provides community safety solution to the most vulnerable people of the society.

1.1 MeMeZa Community Policing Platform

MeMeza is a South African initiative that offers innovative solutions to combat crime in vulnerable communities, ensuring that the poor can lead a safe and fulfilling life [8]. The aim of the organization is to provide community-based approaches to crime eradication by running campaigns and providing tools that offer easy access to the police and citizens. The organization provides an alarm system and also tries to fight crime by offering counselling services, addressing topics such as gender-based violence, bullying and crime prevention. This work focuses on the alarm system component of MeMeZa as depicted in Fig. 2.

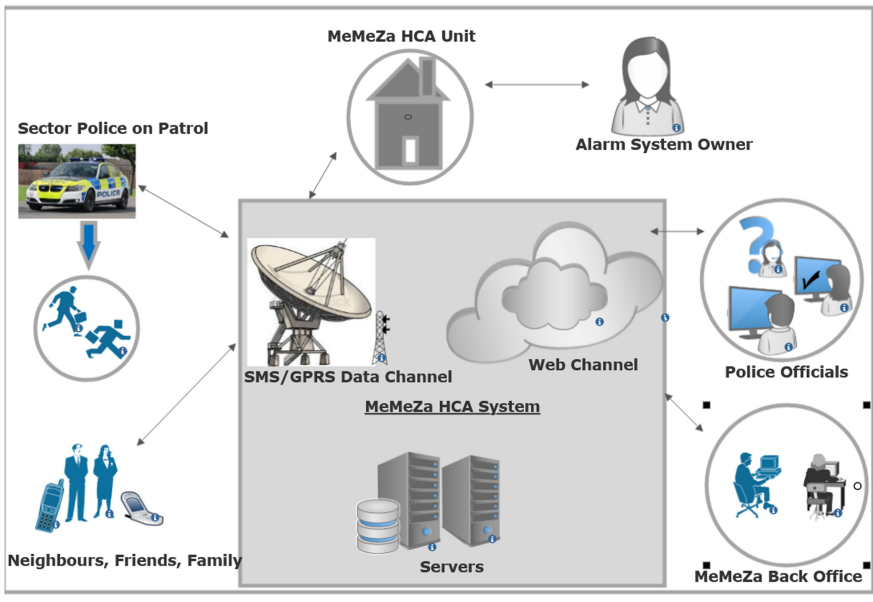


Fig. 2. A depiction of the Memeza community policing project deployed in low-income areas in SA.

The Memeza alarm system is used to mobilize established communities with low-income to fight crime [8]. The system consists of (i) the home community alarm (HCA) unit, which is installed at a subscriber’s home, and (ii) the HCA system, which consists of the server that manages all communications within the system. The HCA unit communicates with the system, and vice versa, using a client-server handshake. The subscriber sends a panic message to the police

through the system by activating, for example, a “*silent police panic*”, among others, which alerts the police on the need to respond to the location where such panic alert is initiated. A user initiates a panic mode on the alarm system by pressing a red button. The call is then immediately logged to a database in the back-end, to alert the police of the need for intervention. Figure 2 summarises the structure and functionality of the Memeza crime prevention and community mobilisation system.

1.2 Summary of Gaps and Opportunities

According to a report by Memeza and SAPS [8], the following have been achieved as a result of the Memeza pilot project:

1. SAPS response time measured within the pilot area was relatively faster, as opposed to the previous longer (almost 24 h) response time.
2. A migration in the crime hotspots, with a high prevention rate in houses that have the alarm system installed.
3. A reduction in serious crime within the region.

However, while acknowledging this success, it also points out that there are still challenges and that more could be done to address certain problems that still exist. For example, the preliminary analysis we conducted on the MeMeZa data confirms that some incident calls were not responded to by the police as seen in Fig. 3, which shows the top 5 police stations identified with missed incident calls. This means that even when the subscribers initiated a “police panic” call, there was no police presence or reaction as expected or anticipated. This is rather wanting as such experience tends to further reduce public (victim’s) confidence in the police, and consequently defeats the intended goal of suspects’ apprehension and crime deterrence. Notably, the under-utilised plethora of data archived by the MeMeZa back-end system could be analysed and used for knowledge support. Hence, this research aims to fill the gap.

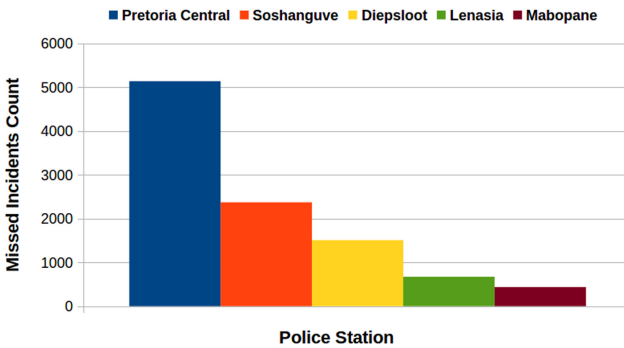


Fig. 3. Top 5 police stations with missed incident calls

Concretely, the unanswered (missed or “distressed”) calls could be attributed to a number of factors, such as: (i) insufficient police resources (for example, man power); (ii) repeated calls, perhaps induced by continuous or uncontrollable panic attack by the victim; and (iii) technological constraint such as network infrastructure issues, amongst others. The first factor (i.e. limited police resources) identified is a more general concern [9] that requires some strategic intervention. Moreover, we note that an earlier investigation and research has highlighted limitations that hamper effective policing in resource-constrained environments such as in South Africa [2]. The highlighted limitations have elicited limited policing resources as a major challenge in these under-resourced communities. Hence, any research effort that promotes the effective and strategic use of these limited resources will greatly alleviate the problem.

1.3 Research Problem and Focus

The MeMeza alarm system is rather reactive than proactive and there is not enough evidence of calls decreasing over time. Whilst efforts have been made to increase the number of police stations in the country in the past year [1], it is important to note that this may not be sufficient. There is a need to understand the trend of crime per precinct (or municipality) and leverage technological solutions to improve policing in such areas. Concretely, the plethora of data archived by the MeMeZa system can be explored and analysed so as to alleviate some of the current challenges faced by the police. Hence, this research uses machine learning (deep learning) to predict crime calls in order to inform the police on trend of crime across precincts at different periods of time. This work presents a crime prediction system that is anchored on the well-established correlation between offenders and their target environment [10]. Historical datasets from MeMeZa are used to train two machine learning algorithms and the best performing one identified based on prediction accuracy and computation performance. With a prediction accuracy of up to 90%, this solution serves as an advancement on MeMeZa and has great potential in contributing to the fight against crime in resource-constrained environments.

The rest of the paper is organised as follows: Sects. 2 and 3 present the related work and models, while the implementation and experimental results are documented in Sect. 4 and 5. Section 6 summarises and concludes the research.

2 Related Work

In recent years, there have been various studies on the prediction and control of crime occurrences [10–15, 17]. Crime prediction techniques have shifted from simply extrapolating historical data or trend using basic statistical techniques [19] to more advanced techniques that are scalable [20, 21] and incorporate intelligence such as machine learning techniques, which thrives in the big data spectrum [14, 16, 18]. Previous approaches were limited in their computational power. However, current trends involving machine learning techniques have paved the

way for the development of proactive measures that can make the police more efficient in combating crime [10]. Such trend lies at the intersection of predictive policing, data mining and information dissemination [13, 15, 18]. Wang *et al.* [14] addressed a foundational problem of crime rate inference using large-scale crowd-generated point-of-interest and taxi flow data, in order to provide new insight into causal and social factors on crime rate inference relating to the city of Chicago. Mookiah *et al.* [12] conducted a review on crime prediction techniques, while noting lack of cohesion in some previous research. Authors noted lack of extraction of patterns using multiple heterogeneous data attributes, such as crime news stories, user profiles, and social media. McClendon *et al.* [22] analysed crime with various machine learning techniques such as, Linear Regression, Additive Regression, and Decision Stump algorithms using the same finite set of features on crime dataset. In another research [23], the authors use 2010 California burglaries data to find the relationship between week, time of the day, repeat victimization, connector and barriers by plotting the occurrence of a crime on a map. Whereas Lin *et al.* [24] incorporate the concept of a criminal environment in grid-based crime prediction modelling and establishes a range of spatial-temporal features based on different types of geographic information by applying Google API to theft data for Taoyuan City, Taiwan.

Furthermore, Nurul *et al.* [13] reviewed current implementations of crime prediction methods with the aim of highlighting their strengths and possible areas for improvement. Fuzzy theory, support vector machine (SVM), multivariate time series and artificial neural network (ANN) were methods considered as those, among others, that can assist crime intelligence in fighting crime. In recent times, the deep learning approach, which is based on artificial neural network (ANN), has become a trendy technique in crime prediction [11, 25, 26]. A feature level-data fusion based deep learning model was used by Kang *et al.* [11] to predict crime for the city of Chicago, being the largest city with a high crime density. Stec *et al.* [26] also used a deep learning approach for making future crime occurrence predictions within city partitions, using Chicago and Portland crime data. Hence, this research also explores this trendy technique, using appropriate feature tuning and enhancement with census data as a means to introduce some intelligence into the MeMeZa network system. Two architectures of the deep learning model were explored, which are Feed-Forward Neural Network (FFNN) and Recurrent Neural Network (RNN). While Stec *et al.* [26] used joint recurrent and convolutional neural network for the purpose of predicting crime, our approach differs as it considers FFNN and RNN, and is implemented on a real-life community policing network.

3 Deep Learning Models

Tapping into the potential and success of deep learning in data-driven decision support, this work explores two models based on a deep learning crime prediction mechanism. These are Feed-Forward Neural Network (FFNN) and Recurrent Neural Network (RNN) approaches [27].

3.1 Feed-Forward Neural Network (FFNN)

The feed-forward model is a simple neural network model as depicted in Fig. 4, wherein connections between the nodes are not cyclic [26]. The size of the input layer corresponds to the size of the features in the data and the output layer consists of the possible predictions. The hidden layers are called hidden because they are not directly connected to the data and usually determined experimentally. When the hidden layer in a neural network is greater than one, then it is referred to as deep neural network (deep learning). Hence, the more the number of hidden layers, the more the complexity of the network and its ability to learn. However, too many hidden units could result in a complicated model with high variance and low bias, thus causing over-fitting [27]. In the network, each unit is connected to the previous and the next layer by a weight ($w^{(i)}$), where i denotes each corresponding layer as shown in Fig. 4. Each record is fed into the input layer, and then the values are fed forward using some weight (w) through the network. This sequence continues, where the values are fed forward from one layer to the next through intermediate computations, using an activation function. In this research, the number of input layers is four. Also, rectified linear units (ReLU) is used as the activation function in the hidden layer, while the softmax activation is used for the output layer. The ReLU function overcomes the vanishing gradient problem and often achieves better performance. ReLU is a piecewise linear function that outputs the input if it is positive and zero otherwise.

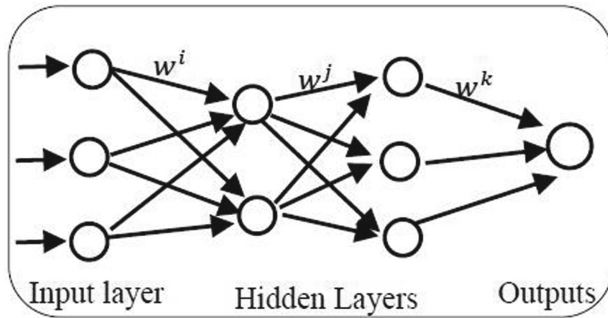


Fig. 4. Feed forward neural network

3.2 Recurrent Neural Network (RNN)

Recurrent neural network(RNN) differs from FFNN by a feedback loop which is connected to their past decisions. RNN usually have two sources of input, which is the current and past recent input [27]. These two sources of input combine to influence how they respond to produce output for the new data. Hence, the decision reached at time step t influences the decision it will reach at time step

$t + 1$ as depicted in Fig. 5. Long Short Term Memory (LSTM) is a special and the most common type of RNN as it solves the vanishing gradient problem that is inherent in RNN. The LSTM have the ability to remove or add information to the cell state, which is carefully regulated by structures called gates. Gates are a way to optionally let information through [25]. They are composed out of sigmoid neural layer and pointwise multiplication operation. A sigmoid layer outputs numbers between zero and one, describing how much of each component should be let through. A value of zero means let nothing through while a value of one means let everything through. An LSTM has three of these gates, to protect and control the cell state.

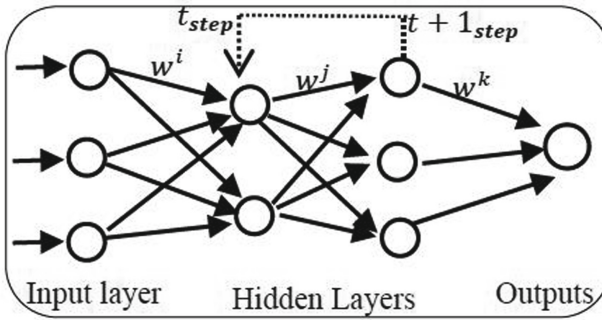


Fig. 5. Recurrent neural network

4 Model Implementation

4.1 Data Used: MeMeZa Data

The data used for the experiment consists of 44,043 records derived from the MeMeZa community policing project in 2017. The original data is stored in two separate (Excel) main files, which are referred to as “People” and “Incidents” files. Table 1 presents a description of some features and subjects associated with the files. The table shows a high level summary of the different categories of data features archived on the MeMeZa system. The Incidents file stores or reports on the amount of calls made by a device to a particular police station at a specific time from a particular location, while the “people” file consists of information regarding the alarm system and corresponding subscriber.

The end goal of the experiment is to predict with high level of certainty that the police can rely on the amount of burglaries per unit area so that the police can focus on the area and plan accordingly. Table 1 depicts the nature of the data sets used in this analysis and Fig. 6 depicts the data cleaning and preparation process. The selected attributes are the relevant ones or the key attributes for our analysis purpose.

Table 1. Different categories of data features considered

Features	Category
Victim (“people”) information (subscriber)	device_id, installation date, gender, device_status, subscription_bill
“Incidents” information	location, time, device_id, device_descr, suburb

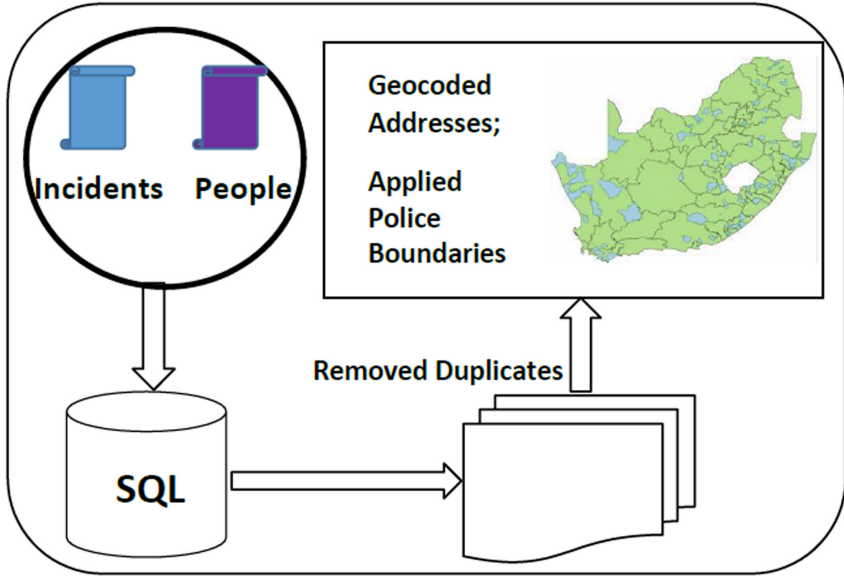


Fig. 6. Data cleaning process

The two data sets are combined by a unique identification (device_id and person_id) for further processing. This combination helps to identify the address of each device. The MeMeZa data contains loosely typed addresses, and for further processing it became necessary to locate the point at which the crime occurred. To achieve this, the Google API which is an online tool for mapping addresses is used to search the address and compute the longitude and latitude at which the event occurred. Police station boundaries are then applied to determine the associated records for corresponding police stations. However, it is noted that 5,698 records have no addresses and cannot be used for analysis, hence, these were ignored in the experiment. Furthermore, we identified duplicate records (see Fig. 6). 18,074 records are marked as duplicates from the database using these two conditions: (i) if the previous record had the same address as the current one; and (ii) if the time frame between the calls is less than 5 minutes. These duplicate records were assumed to be distressed calls from the users when police

were probably not responding to their calls. Eventually, the data set with sample depicted in Table 2 is used, by performing a “join” on the people and incidents table.

Table 2. MeMeza incidents data set sample

Id	Date	Longitude	Latitude	Police.Station
5497	2017-10-07 12:54	28.268015	-25.748704	BROOKLYN
5498	2017-10-07 12:54	28.268015	-25.748704	BROOKLYN
5500	2017-10-07 13:49	28.268015	-25.748704	BROOKLYN
5507	2017-10-07 14:20	28.268015	-25.748704	BROOKLYN
5501	2017-10-07 14:46	28.268015	-25.748704	BROOKLYN

4.2 Feature Selection and Data Fusion

The number of calls made from a certain location is the target and this is computed by summing the calls made in a period of every one month - this gives a fairly randomly distributed data to work with. For further processing and to strengthen the analysis, we combined demographic features from the South African Census data in the features selection process as used in previous research [26]. Certain features in the census data such as unemployment rate, literacy level and age demographics have been found to be very useful in crime prediction. Hence, this data fusion (crime and census dataset) assists our analysis to improve prediction performance.

In order to coordinate and select the best features that will assist the model, the correlation coefficient function was used. The correlation coefficient expresses the statistical measure of the mutual relationship between quantities. Hence, the function helps to filter features that are highly correlated and those that are not correlated in order to remove non-informative or redundant predictors from the model. The formula for computing the correlation, often referred as Pearson r is presented in Eq. 1:

$$r = \frac{1}{n - 1} \sum \frac{(x_i - \bar{X})(y_i - \bar{Y})}{s_x s_y} \tag{1}$$

- n is the sample size
- x_i, y_i are the individual sample points indexed with i
- $\bar{X} = \frac{1}{n} \sum_{i=1}^n x_i$ (the sample mean for features)
- s_x is the standard deviation of x feature

Features with the Pearson whose magnitude is greater than 0.02 are selected in the experiment (Fig. 7). The features used in the analysis are:

- number of installations in that month
- month of the year
- tertiary value from the census data for that location cell
- uneducated value from the census data for that location cell

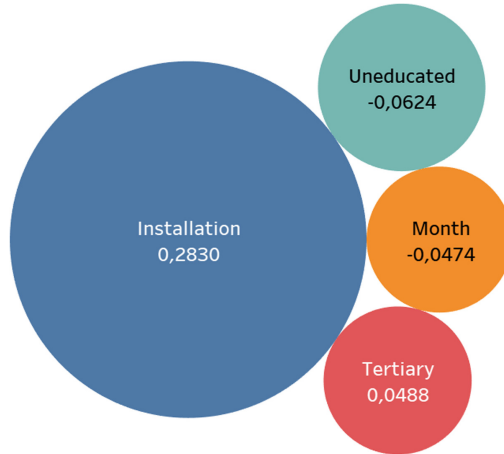


Fig. 7. Pearson values between call count and features

For the experiment, the data was randomised and then split into *80%* training set and *20%* test set. This helps to avoid over-fitting the model and improve its performance. The analysis was conducted on the rest of the police stations. It is noted though that some of the police stations have very few entries, so a filter was applied to get only those police stations with incidents that are more than *350* in a year. The filtering process resulted in twenty police stations for the analysis. The two models are used in predicting crime per unit month across police stations in the precincts by iterating through them and saving the results of the predictions in a database table in SQL. The number of nodes in the input layer is four. The number of hidden layers for FFNN is sixty-four, while that of LSTM is fifty. ReLU, Softmax and linear activation functions were used in the models.

4.3 Evaluation Metric

The R^2 function, depicted in Eq. 2, is used to evaluate the model. The function finds the relationship between the predicted outputs and the actual crime counts. The R^2 function, which is also referred to as Coefficient of determination, gives an indication of the goodness of fit. It gives a visual output of how the predicted crime count compares with the actual values. R^2 is a proportion, hence it ranges between 0 and 1. If $R^2 = 1$, this means that all of the predicted outputs correspond to the actual crime counts (i.e. perfect fit), while $R^2 = 0$ indicates that

none of the predicted outputs is anywhere close to the actual values. Hence, an R^2 value closer to one (1) is more desirable.

$$R^2 = 1 - \frac{\sum_{i=1}^n (x - y)^2}{\sum_{i=1}^n |x - y|^2} \tag{2}$$

5 Experimental Results and Discussion

To provide a viable way of achieving crime reduction targets, the model is implemented and tested on MeMeZa dataset. The research used the tensor-flow open source-libraries for deep learning, based on the keras high level neural network API, since it allows for convenient and fast prototyping. The rectified linear unit (ReLU) and softmax activation functions from the Keras framework were considered for the experiment. We present prediction results for three stations having relatively high incident calls. Figures 8 and 9 show prediction results for Diepsloot station using FFNN and LSTM respectively, while Fig. 10 presents FFNN result for Pretoria Central station.

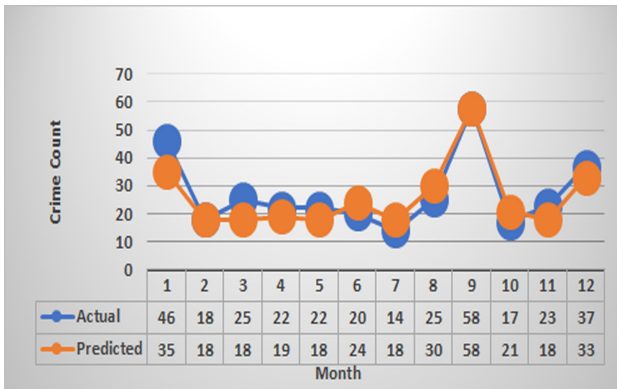


Fig. 8. FFFF diepsloot prediction results.

Figures 11 and 12 present prediction results for Tembisa station, while Fig. 13 presents the result for Roodepoort station. From the visualisation, it is clear that the algorithm predicts the crime for the particular period examined (on a monthly basis) with a high level of accuracy with respect to the actual crime observation. It is observed that there are lots of calls at the beginning of the year for both Diepsloot and Tembisa stations. This is partly due to the fact that many installations of the MeMeZa alarm system were observed to have been implemented at the beginning of the year, until the month of May or thereabout. The number of installed alarm units were noted to be one of the

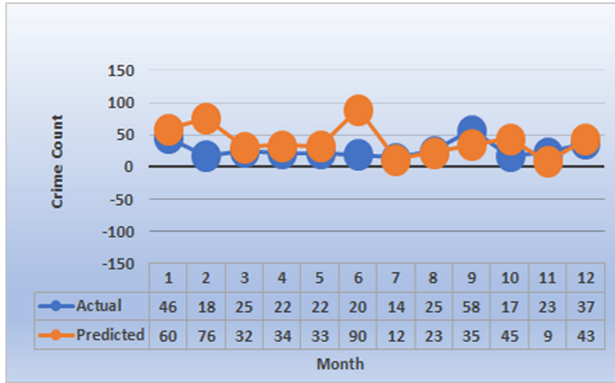


Fig. 9. LSTM diepsloot prediction results.

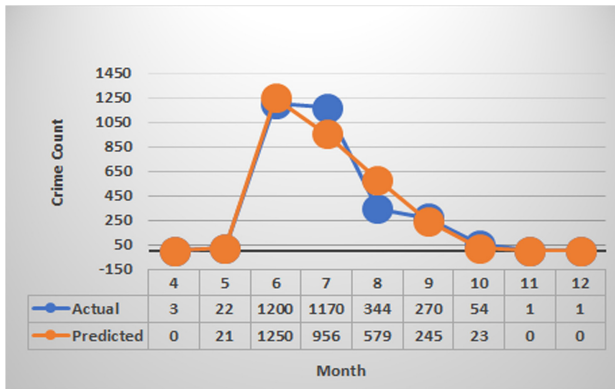


Fig. 10. FFNN pretoria central prediction results.

factors responsible for raising the number of calls made to specific police stations, which relatively makes sense. DiepSloot achieves R^2 of 0.8368 with the FFNN, which is fairly good since it is close to 1. LSTM has an R^2 of 0.0014 which is very poor. Calls were generally on the decline in 2017 except for the month of September. It is noted that three(3) of the calls were from the new installations, and four of the calls in the month of September were from a particular device with device_id 9066, which was activated in March 2016.

There were no calls until the month of April since no installations were done in Pretorial Central until the 3rd of May 2017. The R^2 is at 0.9464 for the FFNN, indicating a very good fit of the model, and that for the LSTM is 0.6418 which is good. As the number of installations increases, so did the calls. It can also be noted that in the month of June alone, 135 calls went unanswered by the police. This shows that installations were done, but probably no co-ordination was made with the police to manage the expected calls. Hence, a reality of

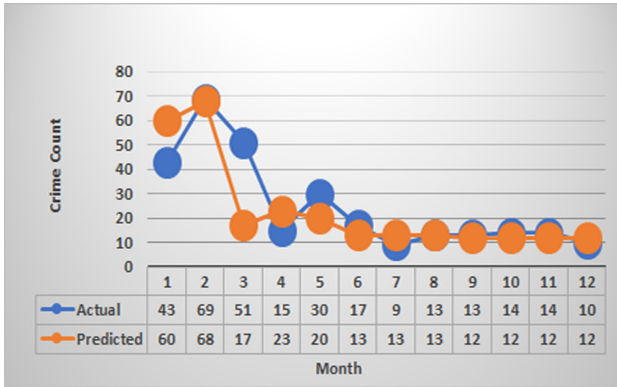


Fig. 11. FFNN tembisa prediction results.

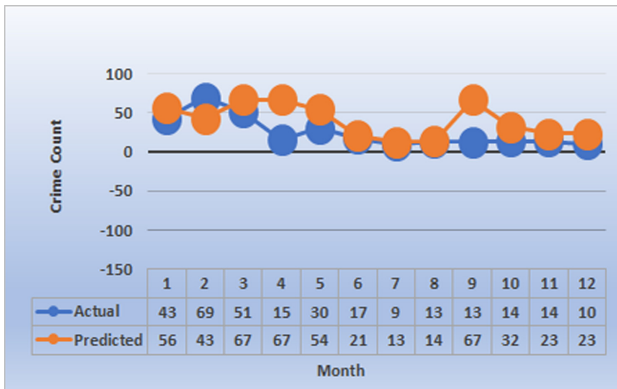


Fig. 12. LSTM tembisa prediction results.

resource shortage. However, in June, there is relatively an increase in the number of calls that the police responded to.

Tembisa has an R^2 of 0.5998 for FFNN which is fairly good, but not perfect. The LSTM has an R^2 of 0.4426 . There are many calls at the beginning of the year dropping to about 10 calls a month for the subsequent months. Most of the installations are done at the beginning of the year until the fifth month, that is why there is a higher number of calls in the first quarter of the year. The number of installed units is noted to be a major factor that is increasing the calls made to the police for the stations.

R^2 for the FFNN is 0.9808 for Roodepoort police station which is almost a perfect fit for the model. The LSTM R^2 is 0.9475 . There are many calls at the beginning of the year, dropping to about 10 calls a month for the subsequent months. Most of the installations are in the second month, about 1337 of them, the number of actual calls remain low throughout the year.

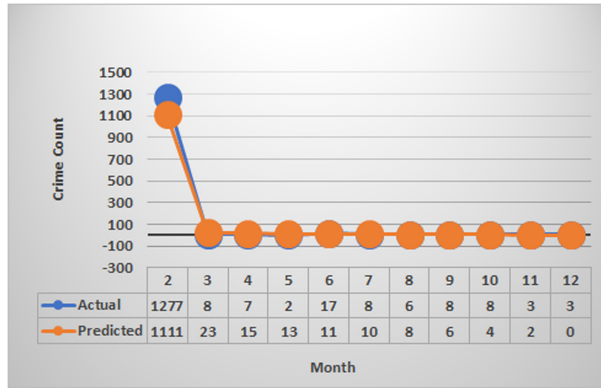


Fig. 13. FFNN roodepoort prediction results.

FFNN is noted to have higher values of R^2 for most of the police stations considered, this means the model gives a better fit for the stations. Figure 14 shows the performance evaluation of the models on the respective police stations. This work shows potential in advancing the MeMeZa system to improve performance on fighting crime.

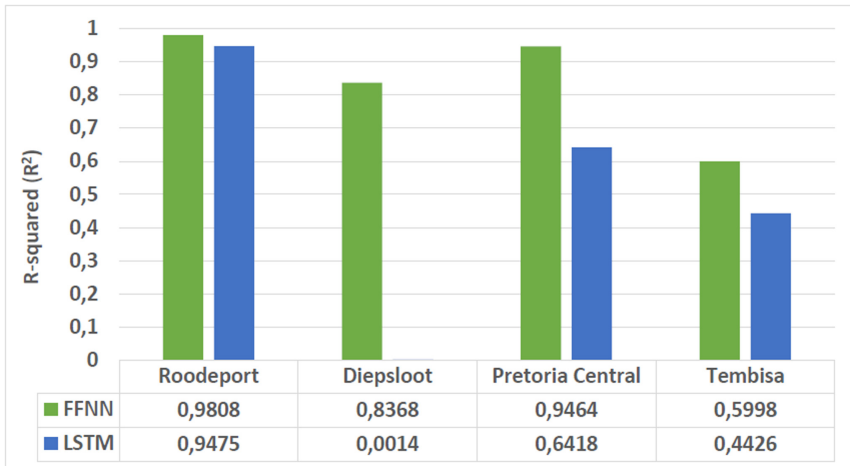


Fig. 14. FFNN vs LSTM results with R^2 across different stations.

6 Conclusion and Future Work

Combating crime in South Africa is an ongoing effort. This culminated in the launch and implementation of the MeMeZa community policing platform, which

provides safety solution to the most vulnerable people of the society in low-resource communities. The MeMeZa system allows a victim to initiate a “police panic” call to alert the police to a crime scene. The system is noted to have helped in achieving some level of crime reduction in certain low-income areas of South Africa. However, an analysis conducted on the data reveals that some calls remained unanswered even when a panic call was initiated. High level of unanswered calls defeats crime reduction efforts as it gives the criminal an opportunity to escape. Moreover, this may cause more negative public perceptions of public safety and MeMeza could lose credibility. This work unlocked the value of incorporating intelligence in the form of predictive policing into the existing MeMeZa public safety system, to improve crime prevention. The study used two deep learning models (feed forward and recurrent neural network) to predict crime across different police stations in various regions in South Africa. The paper examined the two models and combined census (demographic) information in the feature selection process to identify the model that gives the prediction with the best accuracy. Coefficient of correlation function was used to isolate the relevant features for the analysis. The main projected benefits of this newly proposed solution is in strategic resource management and predictive policing in the MeMeZa network system.

As a future extension of this work, there is more that can be explored in terms of building an efficient cloud storage capacity using object oriented database that will facilitate efficient operational support, as well as mining streaming crime data from the current MeMeZa system for real time knowledge support, among others. Furthermore, applying more classification models to increase crime prediction accuracy, identifying hotspots and enhancing the overall performance of the system are aspects that could be considered.

Acknowledgment. Authors gratefully appreciate resources made available by the MeMeZa foundation, South Africa.

References

1. South African Government: Crime report. In South African police service annual crime report 2017/2018. https://www.gov.za/sites/default/files/gcis_document/201809/crime-stats201718.pdf. Accessed June 2020
2. Isafiade, O., Bagula, A.: Fostering smart city development in developing nations: a crime series data analytics approach. In: Proceedings of the ITU-Kaleidoscope: Challenges for a Data-Driven Society, pp. 89–95. IEEE, Nanjing, China (2017)
3. Du Plessis, A., Louw, A.: Crime prevention in South Africa: 10 Years After. *Can. J. Criminol. Crim. Justice/La Revue canadienne de criminologie et de justice pénale* **47**(2), 1–20 (2005). <https://doi.org/10.3138/cjccj.47.2.427>
4. South African Police Service: Together squeezing crime to zero. *J. Strateg. Plan* **3**(1), 3–21 (2014)
5. Isafiade, O., Bagula, A.: CitiSafe: adaptive spatial pattern knowledge using Fp-growth algorithm for crime situation recognition. In: Proceedings of the IEEE International Conference on Ubiquitous Intelligence and Computing (UIC-ATC), pp. 551–556, December 2013

6. National Development Plan 2030: Our Future - make it work, pp. 1–70. <https://www.gov.za/sites/default/files/Executive%20Summary-NDP%202030%20-%20Our%20future%20-%20make%20it%20work.pdf>. Accessed June 2020
7. Mohler, G.O., et al.: Randomized controlled field trials of predictive policing. *J. Am. Stat. Assoc.* **110**(512) (2015)
8. MeMeZa crime prevention and community mobilisation project: Memeza shout crime prevention Diepsloot pilot results summary. <http://memeza.co.za/wp-content/uploads/2016/05/Memeza-Diepsloot-Pilot-Report-2015.pdf>. Accessed September 2018
9. Wilson, J.M., Weis, A.: Police staffing allocation and managing workload demand: a critical assessment of existing practices. *J. Policing* **8**, 1–13 (2014). <https://doi.org/10.1093/police/pau00>. Advance Access-Oxford University Press
10. Isafiade, O., Bagula, A.: Data mining trends and applications in criminal science and investigations, pp. 1–386. IGI Global, USA (2016)
11. Kang, H.W., Kang, H.B.: Prediction of crime occurrence from multi-modal data using deep learning. *J. PLOS-ONE* **12**(4), 1–19 (2017)
12. Mookiah, L., Eberle, W., Siraj, A.: Survey of crime analysis and prediction. In: *The Twenty-Eighth International Flairs Conference*, pp. 440–443 (2015)
13. Mohd Shamsuddin, N.H., Ali, N.A., Alwee, R.: An overview on crime prediction methods. In: *Proceedings of the 6th ICT International Student Project Conference (ICT-ISPC)*, pp. 1–5, Malaysia (2017)
14. Wang, H., Kifer, D., Graif, C., Li, Z.: Crime rate inference with big data. In: *Proceedings of the International Conference on Knowledge Discovery in Database*, pp. 635–644. ACM (2016)
15. Isafiade, O., Bagula, A.: Series mining for public safety advancement in emerging smart cities. *Future Gener. Comput. Syst.* **108**, 777–802 (2020)
16. Almanie, T., Mirza, R., Lor, E.: Crime prediction based on crime types and using spatial and temporal criminal hotspots. *Int. J. Data Min. Knowl. Manage. Process (IJDKP)* **54**, 1–19 (2015)
17. Isafiade, O., Bagula, A., Berman, S.: A revised frequent pattern model for crime situation recognition based on floor-ceil quartile function. *Procedia Comput. Sci.* **15**, 251–260 (2015)
18. Isafiade, O., Bagula, A., Berman, S.: On the use of Bayesian network in crime suspect modelling and legal decision support. In: *Data Mining Trends and Applications in Criminal Science and Investigations*, pp. 143–168, USA (2016)
19. Greenberg, D.: Time series analysis of crime rates. *J. Quant. Criminol.* **17**(4), 291–327 (2001)
20. Flaxman, S., Chirico, M., Pereira, P., Loeffler, C.: Scalable high-resolution forecasting of sparse spatiotemporal events with kernel methods: a winning solution to the NIJ Real-Time Crime Forecasting Challenge. *Mach. Learn.* **13**, 1–30 (2018). <https://arxiv.org/abs/1801.02858>
21. Isafiade, O., Bagula A: Efficient frequent pattern knowledge for crime situation recognition in developing countries. In: *Proceedings of the 4th Annual Symposium on Computing for Development*, pp. 1–2, ACM (2013)
22. Mclendon, L., Meghanathan, N.: Using machine learning algorithms to analyze crime data. *Mach. Learn. Appl. Int. J. (MLAIJ)* **2**(1), 1–12 (2015)
23. Almanie, T., Mirza, R., Lor, E.: Crime prediction based on crime types and using spatial and temporal criminal hotspots. *Int. J. Data Min. Knowl. Manage. Process* **5**(4), 1–9 (2015)

24. Lin, Y.-L., Yen, M.-F., Yu, L.-C.: Grid-based crime prediction using geographical features. *ISPRS Int. J. Geo Inf.* **7**(8), 298 (2018). <https://doi.org/10.3390/ijgi7080298>
25. Azeez, J., Aravindhar, D.J.: Hybrid approach to crime prediction using deep learning. In: *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1701–1710. IEEE, Kochi (2015)
26. Stec, A., Klabjan, D.: Forecasting crime with deep learning. arXiv preprint [arXiv:1806.01486](https://arxiv.org/abs/1806.01486), pp. 1–20 (2018)
27. Zhang, Q., Yang, L.T., Chen, Z., Li, P.: A survey on deep learning for big data. *J. Inf. Fusion* **42**, 146–157 (2018)