Journal of Research Administration
Society of Research Administrators International

UTILIZING SENSOR DATA FROM MOBILE PHONES IN CRIME SCENE INVESTIGATION: A NOVEL APPROACH

Sukhada Aloni*
Research Scholar, Pacific University, Udaipur, Rajasthan, India Email: sukhada.aloni@gmail.com

Dr. Divya Shekhawat
Assistant Professor Faculty of Computer Science,Pacific University, Udaipur,Rajasthan, India
Email: divya.shekhawat23@gmail.com
*Corresponding author:- Sukhada Aloni

Abstract—
In contemporary times, mobile phones have become ubiquitous tools serving various beneficial purposes. Among these, they play pivotal role in capturing real-time crime scenes, promptly reporting incidents, and swiftly alerting law enforcement. Our innovative approach introduces a method of scrutinizing crime scenes through the utilization of sensor data obtained from mobile phones. This pioneering technique employs classification algorithms like Gaussian SVM and KNN to detect potential criminal events. Impressively, our methodology yielded an 81% accuracy rate with KNN and a 78% accuracy rate with Gaussian SVM. This breakthrough technique holds promise for future forensic endeavors, offering a valuable tool in unraveling enigmatic cases.

I. INTRODUCTION

In our surroundings, we see people visiting the malls, parks or any other public places. Criminal instances are common in such places. Public spaces, such as malls, parks, and other frequented areas, are unfortunately not immune to criminal activity. In our daily environment, we often witness people frequenting malls, parks, and other public spaces where instances of criminal activity are not uncommon. These activities encompass a wide range, including robbery, theft, assault, extortion, pickpocketing, abduction, and even murder. Changes in an individual's physical state before and after committing a crime vary over time. Monitoring and recording vital body metrics such as heartbeat rate, oxygen levels, and body posture could significantly aid law enforcement in identifying perpetrators. This proactive approach could ultimately enhance public safety.

In an era of rising crime rates, the need for real-time crime reporting and swift intervention has become increasingly paramount. The escalating frequency of criminal incidents demands that law enforcement agencies remain abreast of ongoing events to ensure public safety. The Internet of Things (IoT) presents a promising solution, offering a collaborative platform for civilians and law enforcement to combat crime effectively. By implementing a robust IoT system, the public can seamlessly capture and report crimes in real-time through a user-friendly interface. This real-time data transmission directly to law enforcement agencies enables prompt and informed responses to reported incidents. A dedicated mobile application can serve as the primary communication channel, alerting officers to the nature, location, and time of the crime, empowering them to make informed decisions and deploy resources effectively. The transformative potential of IoT lies in its ability to bridge the gap between human observation and sensor-driven data collection. This enhanced connectivity facilitates continuous monitoring and real-time situational awareness, ensuring that law enforcement remains one step ahead of potential threats. By leveraging IoT technology, we can establish a proactive public safety infrastructure that empowers both citizens and law enforcement to combat crime collectively.

The development of a user-centric mobile application stands at the heart of this proposed model. This application will serve as a critical tool for real-time crime reporting, enabling citizens to actively contribute to their safety and the safety of their communities. By fostering a culture of collaboration and timely response, we can transform public safety systems, creating a safer and more secure environment for all. These criminal activities may include robbery, theft, extortion, assault, abduction, murder and many more. The difference in body structure before and after the crime varies with time. If the body vitals such as rate of heartbeat, oxygen levels, body posture were monitored and recorded, it would prove to be useful for the police officials to get hold of the attacker. This would in turn ensure the safety of the common man. Real-time crime reporting and swift actions on these crimes is the major challenge in this world. With the increasing number of crimes, to ensure the safety of public, the police officials need to be aware of the crimes happening in real-time so that they can take actions accordingly.

Figure 1 shows the proposed work flow diagram. We used multiple videos for the creation of normal and fight sequence datasets. This data is uploaded to the server for training. Ma- chine learning is being used to analyze these datasets. Finally, the dataset collected in real-time is accurately classified into a normal and abnormal sequence.

II. LITERATURE REVIEW

In 2019, Tundis and his teammates proposed a technique to detect and track criminals using IoT sensors. With the help of these IoT devices, communication was initiated amongst the officials and common man using a mobile application. The mobile application consists of various layers that perform different tasks. The first layer namely, IoT layer comprise of the devices that the user owns. The second layer is an intermediate layer called the edge layer which enables the collection of data and storage of data to the cloud. Lastly, the analysis layer uses the data collected, performs analysis and presents a detailed result of the crime executed [1] .

Lewis studied the effects of crimes on a community in 2012. The study included research on the the crime investigation and its mitigation techniques [2]. The study conducted by Lewis had three main goals, namely role of existing tech- nology in prevention of crimes, development that can done in terms of technology for prevention of crimes and crime prevention techniques. The aim was to reduce the amount of crimes taking place in urban communities by making the common man aware of their surroundings. This was done with the help of technology easily availaible to the common man. In 2013, Agangiba and Agangiba designed a device that was deployed in order to detect the crimes in the surroundings. The mobile device could also be used in reporting the crime. The user was allowed to upload any criminal evidences and contact the police officials through the mobile application. This information was transferred to a remote server using the Internet. The mobile application enabled the police to be aware of any criminal happenings in the surroundings as well as

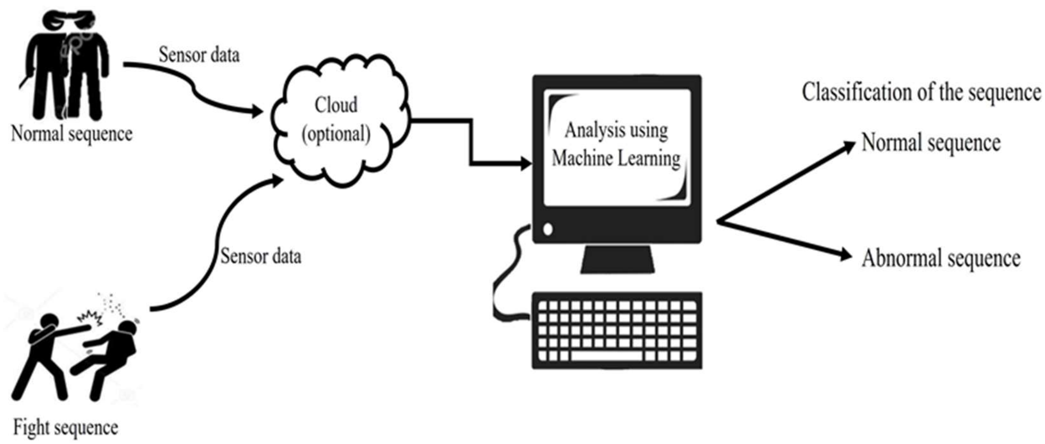


Fig. 1. The flow of the proposed work. The datasets of normal and fight sequences are created by accessing multiple videos. The datasets are uploded to the cloud. Analysis of these datasets is done with the help of machine learning. Lastly, the sensor data collected is classified into a normal and abnormal sequence with maximum accuracy.

take actions on those. If the remote server detected a regular offender, the police was informed accordingly [3] .

A mobile application that monitored the streets was de- veloped and deployed by Fernando. It was named as "Street Watch". This mobile application enabled its user to upload information of the crimes and alert the police officials for immediate action. Similarly, other users would also be aware of the crimes taking place in the close surroundings. It also stores the data of the past crimes. Thus incase a user enters a crime-prone area, the application notifies him or her about it [4] .

In 2016, Jeon and Jeong, developed a system to prevent crime. Their system collected the database of crimes from publicly availaible sources and made the people aware. The proposed system deployed a system which included big data and Internet of Things. Collection of data was done using the a recording device. This recording was then compared to a reference to estimate and determine the severity of the crime. On the basis of the degree of crime, the user was notified through the phone or a wearable sensor device [5] .

Recently, AlDahoul, Karim, Datta, Gupta, Agrawal, and Albunni (2021) designed a violence detectiom system using an LSTM based IoT node. The algorithm of Long Short Term Memory was executed on the Raspberry Pi. Videos of different types were captured and information was extracted. The training and validation datasets were RWF-2000 and RLVS-2000 respectively. The model displayed an acccuray of approximately 73%. On the basis of this model, the officials were alerted [6].

III. METHODOLOGY

To collect mobile data, sensors need to be connected to the device and an object named MobileDEV needs to be created to store the data.

The sensor data was collected even when the device does not have a network connection using the sensor data log, which was stored locally. Periodic access to the camera and acquisition of the images was obtained at a set resolution,autofocus and flash mode. Other than images from the camera, acceleration, angular velocity, magnetic field, orientation and position were also logged.

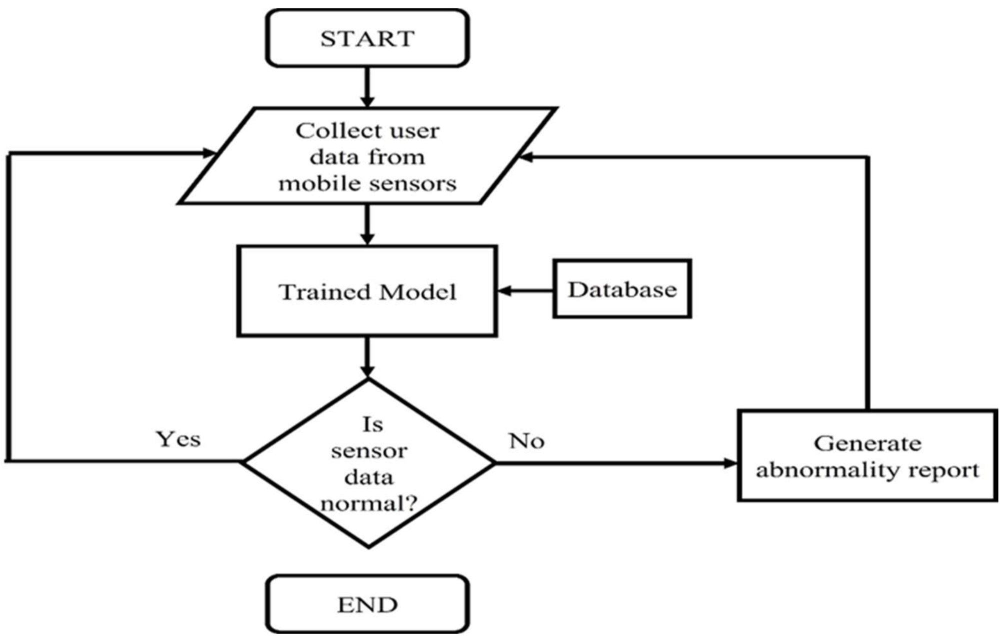


Fig. 2. Proposed system flowchart. Data is collected using various mobile sensors, and the data is stored in an object called MobileDev.

KNN and Gaussian SVM machine learning models are used during model training for classification. Features such as principle component analysis are used on time series data. The results are saved in a database and sent to be analyzed further. Once trained the system goes through real-time sequence classification based on the trained model. If the data sequence is classified as "normal," then the sensors are instructed to continue collecting data. In the other case, i.e. the "abnormal" case, an abnormality report is generated.

Acceleration was measured in meter per second square whereas angular velocity was measured in radian per second, and magnetic field was measured in microtesla. Orientation is measured assuming elevation, XYZ coordinates and yaw roll, and pitch. Positions of the mobile recorded were latitude, longitude, speed, altitude, and course.

Latitude was measured in degrees with respect to the equator where positive degrees indicate north and negative degrees indicate south. Longitude in degrees was with respect to meridian where positive indicates east and negative indicates west. Speed is measured in meters per second, altitude is measured in meters from sea level and course is measured in degrees with respect to true north.

To enable data transmission user needs to select "stream to cloud or log." Also, the user needs to select "send position data" in the background, "auto-upload". For the proof of concept, we collected the data manually and this data was classified as normal and as a fight scenario. To collect the data, the data logger app was installed into the user's mobile app.
Three similar fight sequences with a time interval of approxi- mately 15 to 20 seconds were recorded. These fight sequences were recorded using the data logger app. The sampling rate was set to 300 milliseconds.
Parameters such as acceleration, angular velocity, magnetic field, orientation and position were extracted from the fight sequences. This technique was followed for all three se- quences. A dataset containing all these findings was created for further processing. The normal and fight sequence dataset were compared.

In order to train a model which will be able to classify the normal and abnormal sequence, the k-nearest neighbors (KNN) and the Gaussian SVM algorithms were used. Here, a training dataset is generated through a mobile application. It is connected to various sensors which are deployed in various locations to record real-time data. The dataset is stored in an object called MobileDEV. The KNN algorithm is a classification technique that forms a group or cluster of similar looking data. The group or cluster is treated as a class. On the other hand, gaussian SVM is a classification technique that differentiates the dataset on the basis of features that are extracted from the data.

The figure 2 displays the flowchart of the proposed system. Data is collected with the help of various mobile sensors and an object named MobileDev is used to store the data. A machine learning model is trained using KNN and Gaussian SVM. The results are stored in a database and sent for further analysis. The system undergoes classification of sequence. In case the sequence is termed as "normal", the sensors are instructed to continue with collecting data. However, in the reverse case, that is the "abnormal" case, an abnormality report is generated.

IV. RESULTS AND DISCUSSIONS

Figure 3 depicts various fight sequence data that were collected through the Matlab app. The latitude and longitude was recorded as 41.29 and 72.35 degrees respectively. The speed was 25 meters per second. The XYZ coordinates of the acceleration were recorded as 0.27, 0.23 and -10.19 meters per second square. Also, coordinates of angular velocity are -0.22, 0.07 and 0.06 radians per second respectively. The altitude was

200.1 meters while the horizontal accuracy was 9 meters.

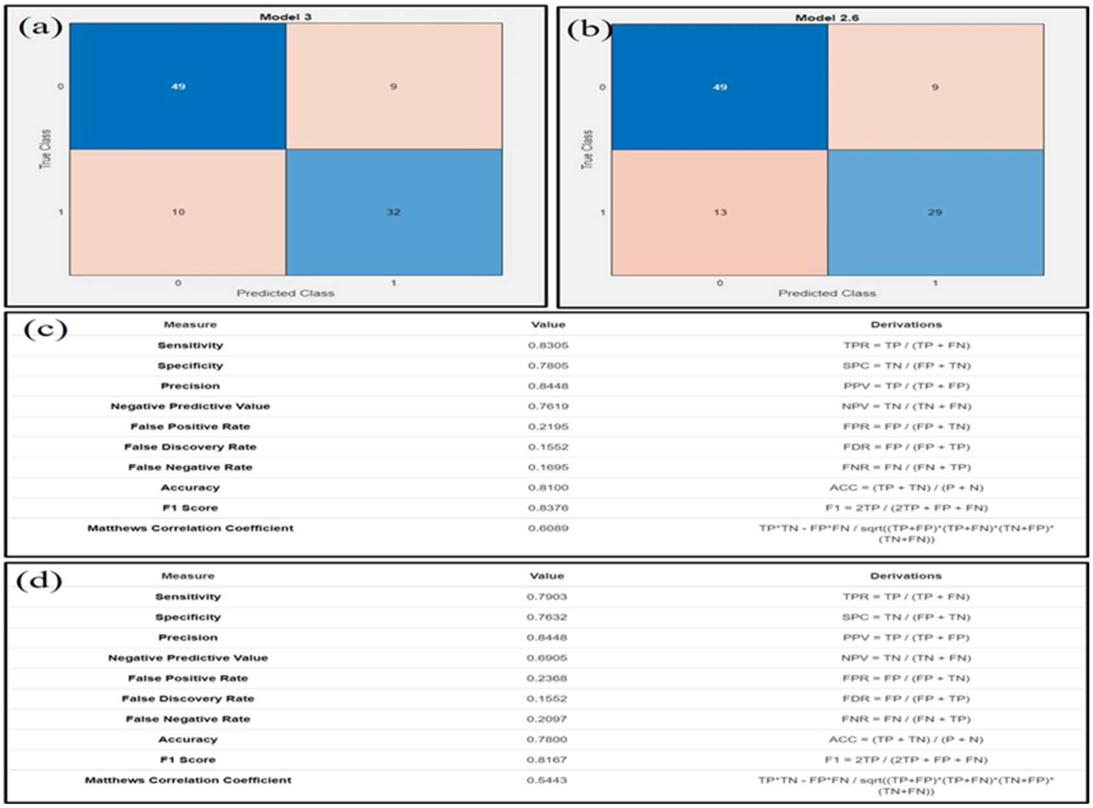
```
mobiledev with properties:

                   Connected: 1
           Available Cameras: {'back' 'front'}
                     Logging: 1
   AccelerationSensorEnabled: 1
AngularVelocitySensorEnabled: 1
       MagneticSensorEnabled: 1
    OrientationSensorEnabled: 1
       PositionSensorEnabled: 1

Current Sensor Values:
                Acceleration: [0.27 0.23 -10.19]  (m/s^2)
             AngularVelocity: [-0.22 0.07 0.06]   (rad/s)
               MagneticField: [3.56 1.56 -48.19]  (microtesla)
                 Orientation: [85.91 -27.1 0.35]  (degrees)

       Position Data:
                    Latitude: 41.29  (degrees)
                   Longitude: -72.35  (degrees)
                       Speed: 25  (m/s)
                      Course: 83.6  (degrees)
                    Altitude: 200.1  (m)
          HorizontalAccuracy: 9.0  (m)
```

Fig. 3. The sample of various data points that were determined for the fight sequence from different sensors.

The Figure 4 displays the varied outcomes obtained post the implementation of KNN and Gaussian SVM. The result metrics encompass sensitivity, specificity, precision, negative predictive value, false positive rate, false discovery rate, false negative rate, accuracy, F1 score, and Matthews correlation coefficient as observed in figures 4c and 4d. In terms of KNN, the accuracy, F1 score, and precision were noted at 81, 83.76, and 84.48, respectively. Conversely, the Gaussian SVM exhibited an accuracy of 78, an F1 score of 81.67, and a precision of 84.48. Sensitivity values for KNN and Gaussian SVM stood at 0.8305 and 0.7903, respectively. KNN showed a specificity of 0.7805, while Gaussian SVM exhibited 0.7632. Further metrics for KNN include a negative predictive value of 0.7619, false positive rate of 0.2195, false discovery rate of 0.1552, and false negative rate of 0.1695. Meanwhile, for Gaussian SVM, these metrics were observed at a negative predictive value of 0.6905, false positive rate of 0.2368, false discovery rate of 0.1552, and false negative rate of 0.2097. Finally, the Matthews correlation coefficient recorded for KNN and Gaussian SVM were 0.6089 and 0.5443, respectively.

V. CONCLUSIONS

The mobile phone has become an exceedingly common device utilized for various practical purposes. Its functionalities extend to capturing real-time data at crime scenes, promptly reporting incidents, and swiftly alerting law enforcement. Introducing an innovative approach to investigating crime scenes, we harness sensor data obtained from mobile phones present at the crime scene. Employing classification methods like Gaussian SVM and KNN, our methodology effectively identifies various criminal events, distinguishing between normal occurrences and abnormalities such as assaults. Notably, we achieved an accuracy rate of 81% with KNN and 78% with Gaussian SVM. This pioneering technique holds promise for future forensic applications, offering a valuable tool in solving perplexing cases.



(c)

Measure	Value	Derivations
Sensitivity	0.8305	TPR = TP / (TP + FN)
Specificity	0.7805	SPC = TN / (FP + TN)
Precision	0.8448	PPV = TP / (TP + FP)
Negative Predictive Value	0.7619	NPV = TN / (TN + FN)
False Positive Rate	0.2195	FPR = FP / (FP + TN)
False Discovery Rate	0.1552	FDR = FP / (FP + TP)
False Negative Rate	0.1695	FNR = FN / (FN + TP)
Accuracy	0.8100	ACC = (TP + TN) / (P + N)
F1 Score	0.8376	F1 = 2TP / (2TP + FP + FN)
Matthews Correlation Coefficient	0.6089	TP*TN - FP*FN / sqrt((TP+FP)*(TP+FN)*(TN+FP)*(TN+FN))

(d)

Measure	Value	Derivations
Sensitivity	0.7903	TPR = TP / (TP + FN)
Specificity	0.7632	SPC = TN / (FP + TN)
Precision	0.8448	PPV = TP / (TP + FP)
Negative Predictive Value	0.6905	NPV = TN / (TN + FN)
False Positive Rate	0.2368	FPR = FP / (FP + TN)
False Discovery Rate	0.1552	FDR = FP / (FP + TP)
False Negative Rate	0.2097	FNR = FN / (FN + TP)
Accuracy	0.7800	ACC = (TP + TN) / (P + N)
F1 Score	0.8167	F1 = 2TP / (2TP + FP + FN)
Matthews Correlation Coefficient	0.5443	TP*TN - FP*FN / sqrt((TP+FP)*(TP+FN)*(TN+FP)*(TN+FN))

Fig. 4. Results with two classification methods (a) Confusion matrix using KNN (b) Confusion matrix using Gaussian SVM. (c) Results obtained, after the KNN classification was implemented. (d) Results obtained, after the Gaussian SVM classification was implemented. TP: True positive, FP: False positive, TN: True negative and FP: False positive were used for analysis purpose.

APPENDIX A DECLERATIONS

A. Authors' contributions:

Conceptualization was done by Divya Shekhawat (DS). All the experiments/code executions were performed by Sukhada Aloni (SA) and DS. The formal analysis was performed by SA and DS. Manuscript writing- original draft preparation was done by SA. Review and editing were done by DS. Visualization work was carried out by SA and DS.

Funding information:

No funding was involved in the present work.

B. Ethics approval:

All authors consciously assure that the manuscript fulfills the following statements:

1) This material is the authors' own original work, which has not been previously published elsewhere.
2) The paper is not currently being considered for publication elsewhere.
3) The paper reflects the authors'own research and analysis in a truthful and complete manner.
4) The paper properly credits the meaningful contributions of co-authors and co-researchers.
5) The results are appropriately placed in the context of prior and existing research.

C. Conflicts of interest:

Authors S. Aloni and D. Shekhawat declare that there has been no conflict of interest.

D. Consent to participate:

This article does not contain any studies with animals per- formed by any of the authors. Informed consent was aquired from all human participants. All the necessary permissions were obtained from Institute Ethical committee and concerned authorities.

E. Consent for publication:

Authors have taken all the necessary consents for publica- tion from participants wherever required.

F. Code availability:

Codes can be made available on reasonable request to the corresponding author.

REFERENCES

1. Tundis, H. Kaleem, and M. Mühlhäuser, "Detecting and tracking criminals in the real world through an IoT-based system," Sensors, vol. 20, no. 13, pp. 3795–3795, 2020.
2. S. Lewis, "Examining and designing community crime prevention tech- nology," CHI'12 Extended Abstracts on Human Factors in Computing Systems, pp. 939–942, 2012.
3. W. Agangiba, M. A. Akotam, and Agangiba, "Mobile solution for metropolitan crime detection and reporting," Journal of Emerging Trends in Computing and Information Sciences, vol. 4, no. 12, pp. 916–921, 2013.
4. M. Fernando and G. Corazon, "STREETWATCH: A mobile application for street crime incident avoidance and safety solution," TENCON 2015- 2015 IEEE Region 10 Conference, pp. 1–5, 2015.
5. Jin-Ho Jeon and Seung-Ryul Jeong, "Designing a crime-prevention sys- tem by converging big data and IoT," Journal of Internet Computing and Services, vol. 17, no. 3, pp. 115–128, 2016.
6. N. Aldahoul, A. Karim, R. Datta, S. Gupta, K. Agrawal, and A. Albunni, "Convolutional Neural Network-Long Short Term Memory based IOT Node for Violence Detection," 2021 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), pp. 1–6, 2021.