International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced Crime Detection in Smart Cities through Hybrid Machine Learning and Advanced Feature Extraction Techniques

Ayush Singhal [1], Niraj Singhal [2], Pradeep Kumar [3]

Submitted: 05/05/2024 **Revised**: 18/06/2024 **Accepted**: 25/06/2024

Abstract Urban population growth has made it harder to police and monitor high-crime areas, increasing crime and insecurity. Smart cities use video surveillance for crime detection to improve security. The backlog of video data that supervisors must watch might raise mistake rates. This problem can be solved utilizing meta-heuristic optimization and Hybrid Machine Learning. This system rapidly and correctly analyzes video stream data to identify illegal behavior. This strategy should boost surveillance system efficiency and effectiveness. After pre-processing the video data using Video-to-Frame Normalization, Resizing, and Conversion, an efficient Semantic Segmentation-efficient FCN algorithm segments the frames. SIFT and the Improved Histogram of Oriented Gradients method retrieve features from segmented areas. The enhanced Relief Algorithm refines retrieved features for feature selection. Finally, a hybrid machine learning strategy for criminal anomaly detection combines transformer model, ANN, andSVM. Python is used to implement the technique.

Keywords: *Artificial Neural Network,Support Vector Machine, SIFT, FCN,Crime detection.*

1. Introduction

Smart city technologies have the capability to provide the appropriate services that cater to the requirements of the population. An essential factor in the development of SChasIoT technology is its ability to facilitate the connection of a vast multitude of devices [1]. Nevertheless, due to the diverse structure and intricate nature of anomalous occurrences, the task of automatically identifying them in a real-life scenario is very difficult. This research study introduces a very efficient and resilient method for detecting irregularities in extensive video data from surveillance systems by using Artificial Intelligence of Things[2]. Anomaly detection in IoT systems is a challenging and crucial issue due to the complex architectures and high-dimensional data they produce [3]. Anomalies are data structures that deviate from the well-defined properties of regular data patterns. "An anomaly is defined as an observation that differs significantly from previous observations, to the extent that it raises issues about whether it was produced by a separate process [4, 5]. In order to identify unusual activity [6], it is important to create a computer vision system that can accurately differentiate between normal and abnormal occurrences without human intervention. Furthermore, this automated solution not only serves the purpose of monitoring but also reduces the need for human labor to maintain continuous manual observation [7].

The rapid expansion of the Internet of Things (IoT) has led to the widespread deployment of IoT devices in smart cities [8]. The operations of a smart city, which aim to improve the efficiency and quality of life in urban areas, are based on real-world time. The rapid growth of the smart city network traffic via the IoT system, which is coupled to sensors directly linked to large cloud servers, is presenting new cyber-security issues [9]. The primary forms of assaults against smart cities are physical and cyber-attacks. During a physical assault, the assailant is in close proximity to the IoT sensors, enabling them to effortlessly manipulate or interfere with the communication-related IoT devices and sensors. This attack encompasses three different techniques: fake node injection,malicious code injection, andpersistent denial of service. The adversary in cyber assaults attempts to gain unauthorized access to smart city network components in order to implant malware or other dangerous software [10]. IoT devices often engage in communication with one other to provide high-quality service in an IoT ecosystem designed for smart cities. The ongoing connection among different IoT devices in the IoT ecosystem poses significant security vulnerabilities, such aserroneous data, surveillance,data probing, malicious operations, malicious controls, malicious scans, andDoS attacks. These abnormalities possess the capacity to generate significant hazards at any given moment and interrupt communication as per usual. Due to these inherent hazards, communication in IoT stays in an insecure condition. In order to maintain high quality of service (QoS) in smart cities, it is essential

[1] *Research Scholar, Department of Computer Science & Engineering, Shobhit Institute of Engineering & Technology, (NAAC Accredited Grade "A", Deemed to- be-University), Meerut (250110), India*
Assistant Professor, Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut
[2] *Director, Sir Chotu Ram Institute of Engineering & Technology, C.C.S. University, Meerut, India*
[3] *Assistant Professor, JSS Academy of Technical Education, Noida, Uttar Pradesh, India*

to actively monitor and detect any abnormalities or irregularities [11, 12]. The latest breakthroughs in deep reinforcement learning (DRL), machine learning (ML), and artificial intelligence (AI), for smart city applications. The study examined the role and impact of past efforts on the key elements of smart cities [13]. In order to tackle these problems, researchers propose a standardized approach for developing and deploying Fog Flow, an innovative framework for IoT smart city platforms that is based on fog computing [14]. The government is building smart cities using IoT devices to monitor and reduce criminal activity in the surrounding areas.

2. Review of Existing Literature

In 2021, Ahmad and Zhang et al. [15] suggested that integrating IoT technology into energy business models may enhanceconnection, intelligence, andefficiency. It has the capability to provide integrated solutions for reducing environmental impact and controlling energy consumption. The Internet of Things (IoT) is also enhancing operational efficiency and automating processes in sectors including logistics,power, manufacturing, andretail. Implementing IoT in the Energy Sector was a promising initiative aimed at constructing sustainable and efficient energy systems.

In 2015, Serrano et al. [16] introduced a novel approach using the LOF density-based clustering technique to identify and analyze assaults. The researchers discovered that the technique was successful in identifying threats while reducing the occurrence of false positives. Additionally, they observed that not all counters were valuable in detecting malware. The paper emphasizes the possibility of using clustering algorithms in intrusion detection systems, enhancing their efficacy in detecting and thwarting cyber-attacks.

In 2020, Alahakoon and Nawaratne et al. [17] introduced Self-building AI, a promising approach to address significant limitations in theanalysis, processing, and integrationof extensive data from several sources. The immense size, diverse nature, and unpredictable changes,of Big Data need technology that can automatically adjust, since human intervention becomes impossible. This technology has the capacity to transform data analysis and enhance its efficiency and effectiveness.

In 2018, Mohammadi and Al-Fuqaha et al. [18] proposed a hierarchical design that utilizes machine learning methods to effectively handle large volumes of data in smart cities. A semi-supervised framework for deep reinforcement learning was created to tackle these difficulties, and its potential was shown in several smart city applications. This study offers valuable insights into the efficient use of machine learning methods for effectively handling the vast amount of data in Smart cities.

In 2020, Sarker et al. [19] conducted a study on the notion of "Smart City Data Science," which entails extracting valuable information and identifying relationships by analyzing data collected from city sensors and related devices. This allows for the implementation of more advanced decision-making processes that are more suited for inhabitants. In order to do this, various machine learning models may be used to get a more profound understanding of municipal data, hence enhancing the computational process in real-world services provided by cities, making them more effective and intelligent.

In 2022, Qarafi and Alrowais et al. [20] introduced the OMLIDS-PB IoT system, which use machine learning to enhance the security of smart cities by identifying and thwarting unauthorized access. It is especially beneficial for safeguarding privacy in BIoT applications, such as disaster management,air quality monitoring, waste management, healthcare, emergency response, and traffic management. This concept might have a significant impact on preserving the integrity and ensuring the safety of smart city systems.

In 2019, Yang and Elisa et al. [21] presented a strategy to protect the confidentiality and integrity of e-government systems in smart city settings, addressing the obstacles associated with their implementation. An analysis was conducted to find technical answers for these problems, and the framework incorporates blockchain and AI advancements to provide a decentralized and safe e-government system. This study offers valuable insights for policymakers and stakeholders to enhance the security and privacy of e-government systems. Measures like as encryption and access limits may be effectively used in smart cities.

In 2021, Palanivinayagam and Gopal et al. [22] used four attribute-generation techniques to identify crime. Using K-means clustering, we were able to identify crime hotspots in a particular area by analyzing the distribution of criminal occurrences. Subsequently, a crime ratio matrix was generated, enabling the anticipation of crime likelihood when inputted into a machine-learning algorithm. The dataset was subjected to analysis using these approaches in order to discern prospective criminal tendencies and proactively deter future instances.

In 2021, Sharma and Dhankhar et al. [23] created a model for detecting anomalies in fog-enabled networks. This approach enables the identification of local anomalies utilizing nodes. This facilitated the identification of renegade nodes and further investigation. The succeeding sections of the study examined the use of statistical methods for identifying abnormalities, specifically focusing on DDoS assaults. The methods were used to evaluate time-series datasets that displayed patterns in incoming packets.

In 2022, Srihith and Kumar et al. [24] emphasized the significance of AI, ICT, and ML in attaining smart city objectives pertaining to policymaking, decision-making, plan implementation, and service provision. Utilizing educational technologies such as ML (Machine Learning) and DRL (Deep Reinforcement Learning) may aid in the creation of efficient and sustainable laws for smart city operations.

3. Proposed Methodology

In this proposed methodology for criminal anomaly detection, our objective is to create a novel hybrid deep learning strategy that synergistically utilizes the advantages of Convolutional Neural Networks and Long Short-Term Memory networks to enhance performance. The first stage of this strategy is data pre-processing, whereby the video data is transformed into separate frames via OpenCV video-to-frame conversion algorithms. Next, the frames are scaled using bicubic interpolation to decrease the complexity of the input data. The frames are normalized using standard deviation normalization in order to enhance the accuracy of the model. Subsequently, the frames undergo identification of Regions of Interest (ROI) via the use of an improved technique based on Semantic segmentation-optimised Fully Convolutional Network (FCN). The improved Fully Convolutional Network (FCN) method partitions the frames into coherent sections, facilitating the extraction of pertinent characteristics. Subsequently, the segmented areas are subjected to feature extraction utilizing two distinct methodologies: Enhanced Histogram of Oriented Gradients and Scale-Invariant Feature Transform. The SIFT method retrieves features such as blobs,corners,andedges, from the region of interest (ROI), while the HOG algorithm retrieves characteristics such as the form and orientation of objects. In order to eliminate any superfluous or redundant characteristics, the retrieved features are refined via the use of an enhanced Relief Algorithm. The last stage is the

This technique proposes a hybrid deep learning strategy that combines Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks to enhance the identification of anomalies. Convolutional Neural Networks (CNNs) are used to extract spatial characteristics from Regions of Interest (ROIs), whilst Long Short-Term Memory (LSTM) networks are used to capture temporal relationships in the data. The hybrid model suggested demonstrates superior performance compared to current models by using the synergistic characteristics of CNNs and LSTM networks, leading to enhanced accuracy and heightened anomaly detection capabilities. The model exhibits a high level of accuracy in detecting and categorizing several forms of assault,theft, including robbery, and criminal activities. As a result, it serves as a highly useful instrument for both crime prevention and surveillance purposes. Figure 1 illustrates the comprehensive flow diagram of the suggested concept.

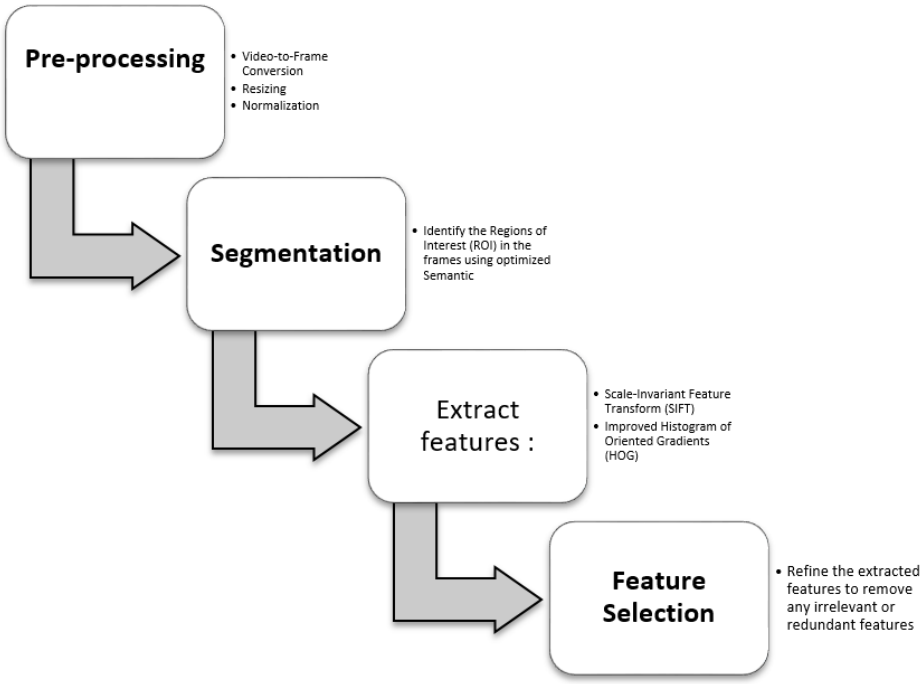

Fig. 1: Flow Diagram of the Proposed Model.

3.1. Crime Anomaly Detection

The suggested method introduces a unique hybrid deep-learning methodology for detecting criminal anomalies. It combines a transformer model with hybrid machine learning approaches, including support vector machine and artificial neural network. The suggested technique seeks to boost the precision of criminal anomaly detection and has the potential to bolster law enforcement endeavors.

3.1.1 "Support Vector Machine"

The Support Vector Machine is a widely used supervised learning model that is effective for evaluating data in the fields of outlier classification,regression, andidentification. Its ability to effectively process non-linear data makes it an invaluable tool for many practical applications. In SVM, the weight vector is determined by solving a mathematical equation that aims to discover the best hyperplane for separating data points into distinct classes, while simultaneously reducing classification errors. The LaGrange multipliers α are manipulated to regulate the balance between increasing the distance between the hyperplane and the data points and reducing mistakes in classification.

4. Findings and Analysis

The suggested model has been executed using the PYTHON programming language. The suggested model has undergone analysis in terms of MCC,FNR,FPR,NPV,specificity,sensitivity, f-measure,precision,and accuracy.

The table below displays the outcomes of assessing five distinct models namely SVM,ANN,Bi-LSTM,CNN, and the suggested model, with a learning rate of 0. The performance of the models was assessed using a range of indicators. The proposed model obtained the maximum accuracy score of 0.912516, indicating its ability to accurately categorize a significant amount of the data. In the same way, the Proposed model had the highest Precision score of 0.810237, which means it had the greatest percentage of accurate positive predictions compared to all other models. The Sensitivity score, representing the ratio of properly recognized real positives, reached its peak at 0.810237 for the Proposed model. Furthermore, the suggested model achieved the best specificity score of 0.946609, indicating its ability to accurately identify genuine negatives. The F-Measure, calculated as the harmonic mean of Precision and Sensitivity, had its greatest value of 0.810237 for the Proposed model. The Matthews Correlation Coefficient (MCC), a metric used to evaluate the performance of binary classification models, had its greatest value of 0.742051 for the Proposed model. The Negative Predictive Value (NPV), representing the ratio of true negatives to the anticipated negative values, reached its peak at 0.946609 for the Proposed model. The Proposed model achieved the lowest False Positive Rate (FPR) of 0.068186, indicating the smallest percentage of genuine negatives that were mistakenly recognized. The Proposed model achieved the lowest False Negative Rate (FNR) of 0.204558, indicating the smallest percentage of genuine positives that were mistakenly recognized. In general, the Proposed model had superior performance compared to the other models across most of the tested parameters, suggesting its efficacy in appropriately categorizing the data.

Table 1: TestingMetrics-Learn Rate--0

	SVM	ANN	Bi-LSTM	CNN	Proposed
FNR	0.287847	0.261195	0.307170	0.311168	0.204558
FPR	0.095949	0.087065	0.102390	0.103723	0.068186
NPV	0.918846	0.927730	0.912405	0.911072	0.946609
MCC	0.630998	0.666535	0.605234	0.599904	0.742051
F-Measure	0.726947	0.753600	0.707624	0.703627	0.810237
Specificity	0.918846	0.927730	0.912405	0.911072	0.946609
Sensitivity	0.726947	0.753600	0.707624	0.703627	0.810237
Precision	0.726947	0.753600	0.707624	0.703627	0.810237
Accuracy	0.870871	0.884197	0.861210	0.859211	0.912516

Table 3 displays the evaluation metrics for several machine learning models with a learning rate of 1. The models that were evaluated consist of SVM, ANN, Bi-LSTM, CNN, and the suggested model. The models exhibit varying levels of accuracy, with SVM achieving a score of 0.771590 and Proposed achieving a score of 0.940501. The precision scores range from 0.528386 for SVM to 0.866207 for Proposed. The SVM model has a sensitivity score of 0.528386, while the Proposed model has a sensitivity score of 0.866207. In terms of specificity, the SVM model has a score of 0.852659, while the Proposed model has a score of 0.965265. The F-measure for all models is comparable, with values ranging from 0.707624 to 0.866207. The Matthews Correlation Coefficient (MCC) varies between 0.366250 for SVM to 0.816678 for the Proposed method. The range of negative predictive value (NPV) values for all models is between 0.912405 and 0.965265. The FPR scores vary from 0.049529 (Proposed)

to 0.162136 (SVM), while the FNR values range from 0.148588 (Proposed) to 0.486408 (SVM). In summary, the Proposed model has superior accuracy and precision scores, as well as the highest MCC score and the lowest FPR and FNR scores among the evaluated models, suggesting its superior performance.

Table 2: Testing Metrics-Learn Rate—1

	SVM	ANN	Bi-LSTM	CNN	Proposed
FNR	0.486408	0.286515	0.307170	0.302506	0.148588
FPR	0.162136	0.095505	0.102390	0.100835	0.049529
NPV	0.852659	0.919290	0.912405	0.913959	0.965265
MCC	0.366250	0.632775	0.605234	0.611453	0.816678
F-Measure	0.528386	0.728280	0.707624	0.712289	0.866207
Specificity	0.852659	0.919290	0.912405	0.913959	0.965265
Sensitivity	0.528386	0.728280	0.707624	0.712289	0.866207
Precision	0.528386	0.728280	0.707624	0.712289	0.866207
Accuracy	0.771590	0.871537	0.861210	0.863542	0.940501

The testing metrics for several machine learning models with a learning rate of 2 are shown in Table 4. The models include of SVM, ANN, Bi-LSTM, CNN, and Proposed. The models' accuracy varies from 0.882198 for CNN to 0.964155 for Proposed. The Bi-LSTM model achieved the best accuracy of 0.923176 compared to all other models. The models exhibit a variety of accuracy values, with CNN achieving a precision of 0.749602 and Proposed achieving a precision of 0.913515. The accuracy of the Bi-LSTM model is 0.831558, which is the greatest among all the models. The sensitivity and F-measure of the models are equivalent to their precision values. The models have a variety of specificity, with the CNN model having a specificity of 0.926397 and the Proposed model having a specificity of 0.981035. The suggested model has the best level of specificity compared to all other models. The Matthews correlation coefficient (MCC) of the models varies between 0.661204 for CNN and 0.879755 for the suggested model. The Bi-LSTM model had the greatest Matthews Correlation Coefficient (MCC) of 0.770480 compared to all other models. The models' negative predictive value (NPV) varies from 0.926397 for CNN to 0.981035 for Proposed. The models exhibit a range of false positive rates (FPR), with the Proposed model having a rate of 0.033760 and the CNN model having a rate of 0.088398. Similarly, the models also show a range of false negative rates (FNR), with the Proposed model having a rate of 0.101280 and the CNN model having a rate of 0.265193. Overall, the Proposed model outperforms all other models in terms of false negative rate (FNR),false positive rate (FPR), negative predictive value (NPV), Matthews correlation coefficient (MCC), specificity, precision, andaccuracy.

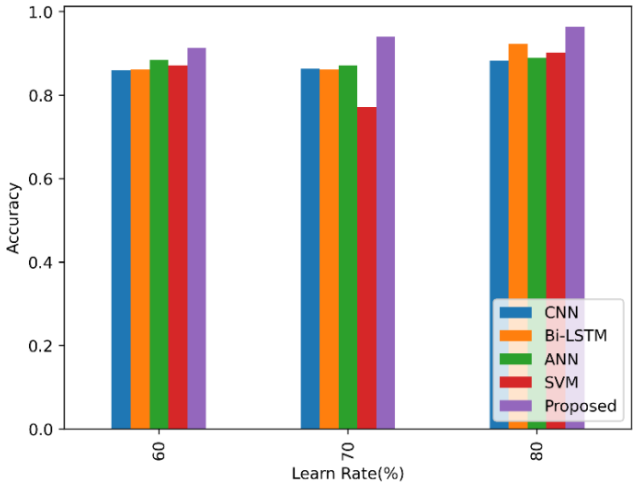

Fig 2: Graphical depiction of performance indicators - Accuracy

Accuracy is graphically shown as a performance measure in Figure 2. It quantifies the model's accuracy in predicting the result, shown as a percentage. This visual depiction aids in assessing the efficacy of the model's forecasts.

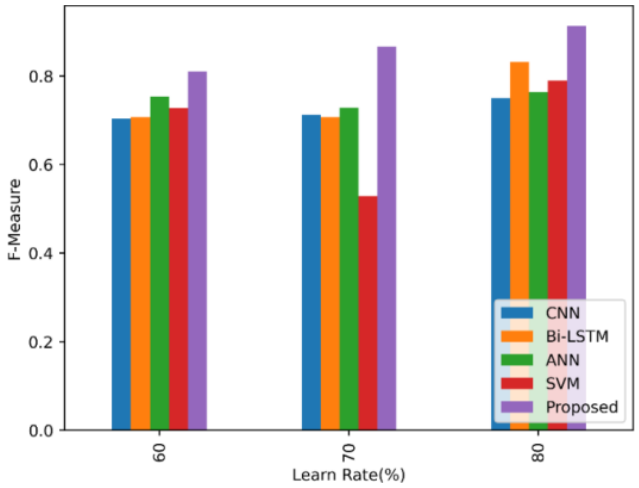

Fig 3: Visual depiction of the performance measures, namely the F-Measure.

Figure 3 illustrates the F-Measure as a performance statistic. The F-Measure is a quantitative evaluation of the model's accuracy and recall. A higher F-Measure indicates a superior capacity of the model to properly anticipate favorable outcomes. This visual depiction may aid in assessing the efficacy of the model's forecasts and in enhancing the model.

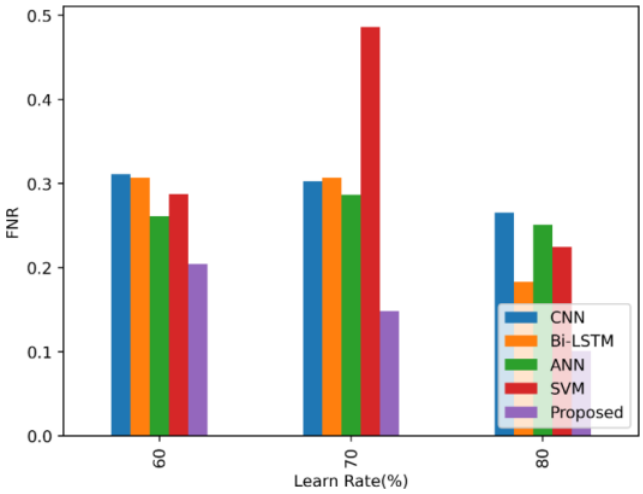

Fig 4: Graphical depiction of the performance statistic known as False Negative Rate (FNR).

Figure 4 depicts the False Negative Rate (FNR) as a performance parameter. The metric quantifies the proportion of true positive instances that were incorrectly classified as negative by the model. A lower false negative rate (FNR) implies superior performance of the model in accurately detecting positive situations. This visual depiction may aid in assessing and enhancing the efficacy of the model in identifying affirmative instances.

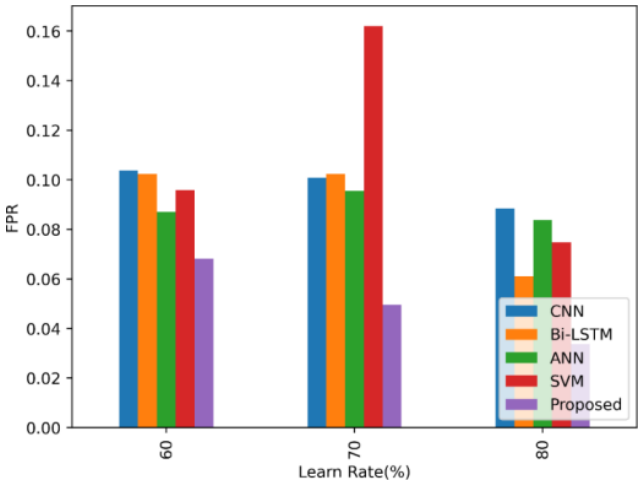

Fig 5: Visual depiction of performance indicators, namely the False Positive Rate (FPR).

Figure 5 displays the False Positive Rate (FPR) as a performance statistic. The metric quantifies the proportion of true negative instances that the model incorrectly classified as positive. A lower false positive rate (FPR) shows superior performance of the model in accurately avoiding false positive predictions.

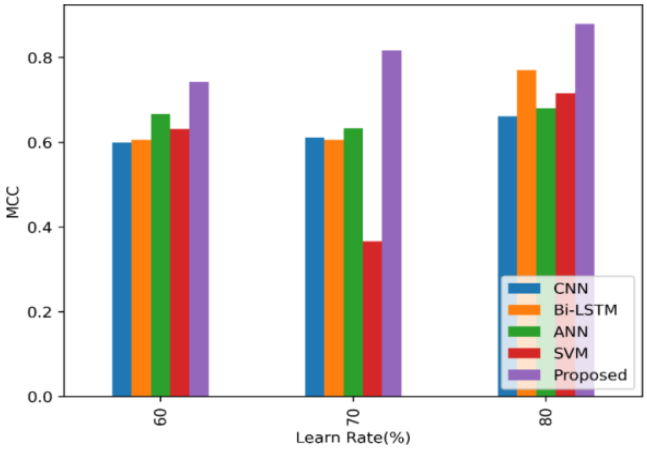

Fig 6: Graphical depiction of the performance measurements, namely the Matthews Correlation Coefficient (MCC).

Figure 6 depicts the Matthews Correlation Coefficient (MCC) as a measure of performance. The metric quantifies the degree of correlation between the expected and actual values, with a scale ranging from -1 to 1. Higher values indicate superior performance. The Matthews correlation coefficient (MCC) is a statistic that considers true positive, true negative, false positive, and false negative predictions, giving it a more complete and accurate measure compared to other metrics. This visual depiction might aid in assessing and enhancing the overall efficacy of the model.

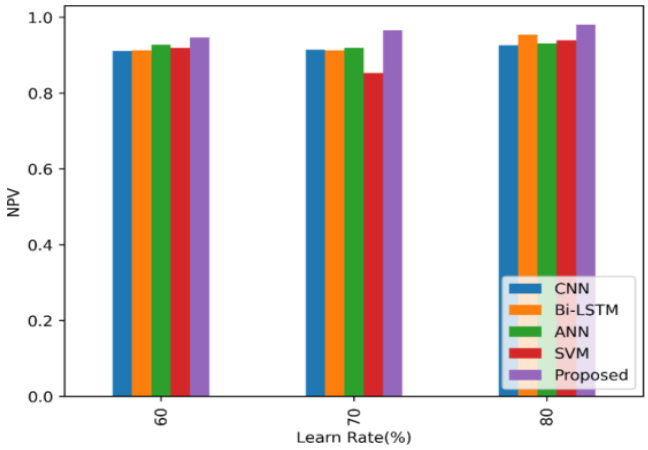

Fig 7: Visual depiction of the performance measurements, including the Net Present Value (NPV).

Figure 7 presents the Negative Predictive Value (NPV) as a performance statistic. The metric quantifies the accuracy of the model in properly identifying and predicting negative instances. A larger Net Present Value (NPV) signifies superior performance of the model in accurately recognizing negative scenarios. This visual depiction may aid in assessing and enhancing the efficacy of the model in minimizing incorrect negative predictions. The Net Present Value (NPV) is of utmost significance in medical contexts, since an erroneous negative forecast might result in grave repercussions.

5. Conclusion

To summarize, the proposed system examines video stream data to promptly and precisely detect criminal activity, hence enhancing urban security. The system performs pre-processing on video data by using Normalization techniques,Resizing, and Video-to-Frame Conversion. It then segments the frames using an efficient Semantic Segmentation-efficient FCN method to effectively monitor a large amount of video data. The SIFT and Improved Histogram of Oriented Gradients techniques extracted features from segmented regions. The updated relief approach for feature selection enhances the extracted features by lowering their amount and enhancing accuracy. A predictive approach was proposed to improve criminal anomaly detection by combining the support vector machine (SVM), transformer model, and artificial neural network (ANN) in a hybrid machine learning technique. The proposed solution's Python implementation may assist law enforcement agencies in using it for the purposes of crime prevention and detection. The proposed approach seems to have great potential for enhancing urban security and mitigating crime.

References:

[1] Guo,K.,Lu,Y.,Gao,H.,and Cao,R.,2018. Artificial intelligence-based semantic Internet of things in a user-centric smart city. Sensors,18(5),p. 1341.

[2] Islam,M.,Dukyil,A. S.,Alyahya,S. and Habib,S.,2023. An IoT Enable Anomaly Detection System for Smart City Surveillance. Sensors,23(4),p. 2358.

[3] Guo,Y.,Ji,T.,Wang,Q.,Yu,L.,Min,G. and Li,P.,2020.Unsupervised anomaly detection in IoT systems for smart cities. IEEE Transactions on Network Science and Engineering,7(4),pp. 2231-2242

[4] Cauteruccio,F., Cinelli,L., Corradini,E., Terracina,G., Ursino,D., Virgili,L., Savaglio,C., Liotta,A. and Fortino,G., 2021. A framework for anomaly detection and classification in Multiple IoT scenarios. Future Generation Computer Systems,114,pp. 322-335.

[5] Tukur,Y. M.,Thakker,D. and Awan,I. U.,2021. Edge-based blockchain-enabled anomaly detection for insider attack prevention in the Internet of Things. Transactions on Emerging Telecommunications Technologies,32(6),p. e4158.

[6] Rahman,M. A.,Asyhari,A. T.,Leong,L. S.,Satrya,G. B.,Tao,M. H. andZolkipli,M. F.,2020.Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society,61,p. 102324.

[7] Ullah,W.,Ullah,A.,Haq,I. U.,Muhammad,K.,Sajjad,M. andBaik,S. W.,2021. CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks. Multimedia tools and applications,80,pp. 16979-16995.

[8] Singh,S.,Sharma,P. K.,Yoon,B.,Shojafar,M.,Cho,G. H. and Ra,I. H.,2020.Convergenceofblockchainandartificialintelligenceinthesustainable smart city. Sustainable Cities and Society, 63,p. 102364.

[9] Manimurugan,S.,2021. IoT-Fog-Cloud model for anomaly detection using improved Naïve Bayes and principal component analysis. Journal of Ambient Intelligence and Humanized Computing,pp. 1-10.

[10] Kumar,P.,Kumar,R.,Srivastava,G.,Gupta,G. P.,Tripathi,R.,Gadekallu,T. R. and Xiong,N. N.,2021. PPSF: A privacy-preserving and secure framework using blockchain-based machinelearning for IoT-driven smart cities. IEEE Transactions on Network Science and Engineering,8(3),pp. 2326-2341.

[11] Xu,R.,Cheng,Y.,Liu,Z.,Xie,Y. and Yang,Y.,2020.Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services. Future Generation Computer Systems,112,pp. 228-242.

[12] Hasan,M.,Islam,M. M.,Zarif,M. I. I. and Hashem,M.

M. A.,2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things,7,p. 100059.

[13] Ullah,Z.,Al-Turjman,F.,Mostarda,L. andGagliardi,R.,2020.Applicationsof artificial intelligence and machine learning in smart cities. Computer Communications, 154,pp. 313-323.

[14] Cheng,B.,Solmaz,G.,Cirillo,F.,Kovacs,E.,Terasawa,K. and Kitazawa,A.,2017. FogFlow: Easy programming of IoT services over cloud and edges for smart cities. IEEE Internet of Things Journal,5(2),pp. 696-707.

[15] Ahmad,T. and Zhang,D.,2021. Using the Internet of Things in smart energy systems and networks. Sustainable Cities and Society,68,p. 102783.

[16] Garcia-Serrano,A.,2015. Anomaly detection for malware identification using hardware performance counters. arXiv preprintarXiv:1508. 07482.

[17] Alahakoon,D.,Nawaratne,R.,Xu,Y.,De Silva,D.,Sivarajah,U. and Gupta,B.,2020.Self-buildingartificialintelligenceandmachine learning toempowerbigdata analytics in smart cities. Information Systems Frontiers,pp. 1-20.

[18] Mohammadi,M. andAl-Fuqaha,A.,2018. Enabling cognitives martcitiesusing big data and machine learning: Approaches and challenges. IEEE Communications Magazine,56(2),pp. 94-101.

[19] Sarker,I. H.,2022. Smart City Data Science: Towards data-driven smart cities with open research issues. Internet of Things,19,p. 100528.

[20] Al-Qarafi,A.,Alrowais,F.,S. Alotaibi,S.,Nemri,N.,Al-Wesabi,F. N.,Al Duhayyim,M.,Marzouk,R.,Othman,M. and Al-Shabi,M.,2022. Optimal machine learning-based privacy-preserving blockchain assisted Internet of things with smart cities environment. Applied Sciences,12(12),p. 5893.

[21] Yang,L.,Elisa,N. and Eliot,N.,2019. Privacy and security aspects of E-government in smart cities. In Smart cities cybersecurity and privacy (pp. 89-102). Elsevier.

[22] Palanivinayagam,A.,Gopal,S. S.,Bhattacharya,S.,Anumbe,N.,Ibeke,E. and Biamba,C.,2021. An optimized machine learning and big data approach to crime detection. Wireless Communications and Mobile Computing, 2021,pp. 1-10.

[23] Sharma,D. K.,Dhankhar,T.,Agrawal,G.,Singh,S. K.,Gupta,D., Nebhen,J. and Razzak,I.,2021. Anomaly detection framework to prevent DDoS attacks in fog-empowered IoT networks. Ad Hoc Networks,121,p. 102603.

[24] Srihith,I. V. D.,Kumar,I. V. S.,Varaprasad, R.,Mohan, Y. R., Srinivas, T. A. S. and Sravanthi,Y.,2022. Future of Smart Cities: The Role of Machine Learning and Artificial Intelligence. South Asian Res J Eng Tech,4(5),pp. 110-119.