IJASST
International Journal of
Applied Sciences and Smart Technologies

Volume 07
Issue 02

p-ISSN 2655-8564, e-ISSN 2685-943, pp. 235-252, 2025

Evaluating XGBoost Performance in Improving Community Security through Multi-Class Crime Prediction: Insights from the Denver Crime Dataset

Mc-Kelly Tamunotena Pepple

School of Engineering, Federal Polytechnic of Oil and Gas Bonny, Port-Harcourt, 503101, Nigeria
**Corresponding Author: mc-kelly.pepple.pg94648@unn.edu.ng*

(Received 09-02-2025; Revised 10-03-2025; Accepted 15-03-2025)

Abstract

Crime is a phenomenon that needs to be understood and predicted to reduce victimizations and improve the efficiency of investments in personnel and equipment. Criminal data that is used to analyze crime today is more complicated, and voluminous than the data that was previously used in crime analysis. The present paper looks into the ability of XGBoost algorithm to address the prediction of crime types by using the Denver Crime Dataset to solve these problems with advanced techniques. This study evaluates the performance of an XGBoost model applied to the Denver Crime Dataset for classifying crime categories. Key metrics, including validation log loss, confusion matrix analysis, and classification reports, highlight the model's effectiveness. The validation log loss decreases rapidly during the initial epochs and stabilizes near zero, indicating excellent generalization and convergence. The classification report reveals perfect scores of 100 % across precision, recall, and F1 metrics for all categories, despite significant class imbalances. The confusion matrix confirms the model's precision and ability to handle frequent and rare crime types. The abovementioned outcomes show the benefit of developing sophisticated algorithms based on machine learning in optimizing the distribution of resources available and increasing the effectiveness of crime fighting in a community.

Keywords: Classification, Crime Prediction, Machine Learning, XGBoost, Validation

1 Introduction

An exciting area of study revolves around security in communities, which is the crime prevention measure that combines modern knowledge in technology and the application of policies, management, and increased focus on the communities' safety. As

human society goes through the process of globalization and integration more and more, as the process of digitalization of society progresses more and more, security threats have become more diverse (perplexed), therefore requiring a comprehensive approach to the issues of safety and protection. Recent studies show that there needs to be a convergence of physical and information security models and methods that are change-compatible and capable of dealing with all possible security threats.

One of the most widely used models is the integrated model, which combines video monitoring with the safety of products and applications. In the modern perspective of shared services and the threat to personal information in cyberspace, this model is based on the idea that risks manifest in physical and digital dimensions [1]. For example, state-of-the-art surveillance systems can employ Artificial Intelligence and Machine Learning algorithms to examine continuous data streams, to detect cyber and physical security threats in their formative stages [2], [3]. These systems are proactive and defensive; they can snuff out flames before they even start. Community-based security measures are being reinvented hand in hand with technological developments. Johnson [4], opined that to prevent acts of crime recklessness, people in the community should continuously involve themselves in neighborhood watch programs and local security councils. This participatory model assumes the residents as approvers of being secured and also helps them to take liability for their own security/personal securities [5]. Also, the concept of complementary and cooperative policing where the police work hand in hand with the members of the society is gradually becoming one of the important elements of a secured society [6].

Another element of community security that has recently emerged is cybersecurity, especially when more and more communal services become available on the Internet. These recent works constantly emphasize the demand for establishing stringent cybersecurity mechanisms from hacking, theft, and cyber-criminal activities such as ransomware attacks, data breaches, and others [7]. Cybersecurity combined with conventional security concepts and measures, which are considered as the layers in the defense system, respond to all kinds of threats.

The policy frameworks are also dynamic to match these integrated security systems. Currently, governments have embraced progressive policies that support multi-

stakeholder coordination of law enforcement, tech solutions, and non-profit leaders [8], [9]. These are more or less in the form of a framework prepared in a way that can bend and twist to respond to changing security dynamics and synchronize all the players in the guards of the community's interests. Secondly, it is winning acceptance of resilience-building measures introduced into the security policies of communities. This entails sensitization of communities to fast regain normalcy after security breaches physical or cyber through awareness, exercises policy formulation, and testing. Through a stronger emphasis on the resilience concept, the communities must be able to minimize the effects of security breaches in the long run while also increasing their safety.

Security has also evolved in the community and has diversified, given that many community services are now online. The following articles prove the increasing importance of stylized cybersecurity defense mechanisms for guarding against data leakage, ransomware attacks, and other 'cyber threats' [1], [6]. The subject of cyberspace is synchronized with the conventional security concept, which is a systematically designed defense system against all forms of threats.

For these integrated security models' policy frameworks are also changing as well. The governments are embracing policies that make the application of counter-terrorism adaptive, where authorities, technology vendors, and non-governmental organizations work in cooperation [4], [7]. These policies are not rigid which may hinder the implementation as and when new security threats present themselves, the policies can be implemented to address those new threats as far as all the stakeholders agree with the implementation of the policies for the protection of the community.

In addition, the processes of constructing resilience are being included in the security agendas of the communities. It also entails early preparation of the communities as to how they can quickly recover after incidents that may be physical or digital type by establishing education, training, and creating emergency response plans. In this way, by emphasizing on the concept of resilience, the communities can diminish the further effects of particular security incidents, and improve the general security conditions. Last but not least, the application of big data analytics on community security has been the focus recently. Applications of big data, lead to the identification of crime trends, and forecasting of incidents, optimize the distribution of resources, and prevention measure.

It empowers the police and members of society to prevent likely incidents based on this predictive model. It can be stated that the approach to community security in the modern world is based on the synergy of high-tech, communal involvement, and effective policy-making strategies. Thus, communities will be able to protect their areas from the constantly emerging and diversifying threats in the physical, and cyberspace with the help of the adapted safety-focused approaches that combine physical and digital security to provide an environment for safety and security-related proactive thinking.

One of the prime attributes for prediction offered by XGBoost in being an excellent choice for multi-class crime prediction is its class imbalance handling relative to other models from the traditional family, which have made unique contributions to the science of crime analysis and prediction. While traditional models like logistic regression or decision trees face severe difficulties when tackling large, imbalanced data and complex dependencies of features, XGBoost is a framework purposely designed to tackle all of these issues while refining its weak learners in an iterative manner to improve predictive performance. This attribute allows it to efficiently deal with large and complex crime data and adds to the applicability of current crime analysis [10].

It is worth highlighting that XGBoost's noteworthy contributions to crime prediction stem from its ability to attain high classification performance on real-world crime data sets, despite class imbalances. Typical models perform badly on rare crime recognitions due to their bias toward the majority-class objects. On the other hand, XGBoost optimizes log loss with weighted boosting, ensuring accurate classification of minority instances of crimes. XGBoost is also known to outperform traditional machine learning models regarding precision, recall, and F1-scores in multi-class crime prediction on highly imbalanced datasets [11]. Results of that study itself showed XGBoost won almost perfect classification performance, attesting to its superiority in multi-class classification tasks.

XGBoost also improves interpretability and decisions, especially in crime prediction. Not being a black-box model like deep learning, it shows how important features will help the law enforcement agency to better understand these key factors behind different kinds of crimes. This understanding will, therefore, make things like resource allocation more efficient and evidence- and data-based when seeking to prevent

crimes. Such explainability in the crime prediction model is very important because it builds trust in an automated system used by law enforcement agencies [12]. Moreover, XGBoost convergence at low validation log loss with very high speed indicates good generalization, which makes it a reliable element for real-world applications [13].

However, results in the analysis of XGBoost models in crime prediction against results given by the traditional approach show that XGBoost is a way superior approach to the whole predictive policing spectrum. Its capacities outclass traditional approaches in utilization in reducing the time lost by evaluating such high-dimensional crime data and generating log loss while performing different classifications of crime types within that data. XGBoost technique for more advanced machine learning will stem into implementation of better sources of preventive crime strategies which contribute towards enhancing public security whilst optimizing law enforcement action. With still continuous improvement on boosting algorithms and feature selection techniques, it keeps a stronghold on the place of XGBoost within crime analysis and prevention [14].

2 Literature Review

Integration of new technologies through connected communities, for instance, smart cities as well as other digital environments has brought new technologies and issues on security. This paper mainly targets various models and security measures in those communities, where machine learning (ML), Internet of Things (IoT), and blockchain technologies play a crucial part. These models cover both, classical security requirements and new-generation threats such as cyber threats and data leaks [15].

Generally regarded as ‘community policing’, community security measures have gone digital. Li, Yang, Zhao, and Sun [16], proposed a model that incorporates and achieves IoT sensors in community networks enhances real-time threat detection and reactive mechanisms. These sensors offer multiple-layered security because they can watch both physical and cyber events. Like Zhao, Chen, and Li, [17], the authors proposed a decentralized trust model for community networks which is based on the blockchain and aims to reduce the dependency on a central authority for secure P2P (Peer-to-Peer) communication.

The use of ML has transformed security frameworks affecting communities' settings in various ways. Xu, Wang, and Liu [18], developed a new intrusion detection system using deep learning and random forest to handle cyber security threats from community networks. According to their model, they reported very high accuracy rates in identifying the threats of phishing, and malware. Furthermore, Kurniawan, Chandra, and Anwar [19], have shown that using data on the previous threats reinforcement learning allows for the improvement of the resource allocation in community security systems through effective change of threat-response mechanisms.

The community security frameworks based on 'Internet of Things' have gained huge importance from the exponential rises in devices being connected. The research by Ruan, Meng, and Liang [20], showed that edge computing enhances the security aspects of IoT-based communities. In addition, they have proposed a federated learning framework that enables machine learning models to train using community device data in a privacy-guaranteed manner. Trabelsi et al [21] also suggested ways to make IoT networks safer by, using better encryption methods, especially homomorphic encryption.

Blockchain has thus risen to the occasion in improving community security. A recent work, by Sarker, Zareen, and Karim [22], discussed the use of blockchain which focuses on safe identity management in a community environment. Their model also inherently guards against identity theft and any unauthorized access, through smart contracts and multi-signature authentication. Gupta, Goyal, and Das [23], discussed employing blockchain as a way of protecting data transactions in smart communities, hence promoting integrity and non-interference.

Security is still an integral part of the community security models, especially as regards the cybersecurity facet. Multi-factor authentication (MFA) system was investigated [24] in the context of a community environment with emphasis on the fact that MFA is useful in mitigating unauthorized access. Another review by Chen, Li, and Zuo [25], also described the risks in community-based applications along with the necessity of secure software development practices in which security measures should be incorporated in the SDLC.

Another feature that is important for community security models is privacy preservation. A privacy-preserving data-sharing model for smart communities developed

by Lee, Kim, and Choi [26], incorporates the use of differential privacy to hide data of those within the smart community. It also enables the sharing of data for the common good of the community (e. g. health) and at the same time preserves the individual's identity. Zhang, Feng, and Wang [27], continued to discuss privacy preservation in vehicular networks for smart communities and introduced a low-complexity cryptographic model for the protection of the communication between vehicles and infrastructure.

Specifically, the protection of communication networks is a prerequisite for the functioning of complex connected societies. Liu, Xie, and Yuan [28], additionally presented the improved routing scheme that protects the ad hoc community networks from attacks like eavesdropping and DoS. It leveraged elliptic curve cryptography (ECC) to enable fast and secure communication between community nodes. In addition, Ibrahim, Chen, and Ding [29], also focused on another application of AI where it is integrated to predict jamming attacks on wireless community networks thereby reducing different communication outages.

AI is being widely used in community threat detection systems to anticipate and mitigate threats in society. Huang et. al designed a Convolutional Neural Network (CNN) to build an Intrusion detection system that detects an irregularity in community networks [30]. Their system also enhanced the identification performance of various elaborate intrusion strategies including the APTs (Advanced Persistent Threats). In another study, Ahmed, Khan, and Baig [31], developed a combined intrusion detection system based on both anomaly and signature detection which, it was noted, demonstrated a higher level of effectiveness in fighting zero-day attacks.

It is even important to see that community security models must be equipped to resist and rebound from the attacks. Ashfaq, Bashir, and Raza [32], put forward an architecture for a self-healing mechanism for a community network through the use of the SASA or autonomic security agents. These agents constantly watch the network and then self-apply security fixes when problems have been discovered. In the same way, Sun, Wang, and Lin [33], used community infrastructures for the analysis of the so-called "cyber resilience", a proactive defending method based on AI for constant risk evaluation and management.

Nevertheless, several issues are still outstanding in the current community security models. One of the biggest issues is the ability to maintain the current level of protection over the existing and particularly the emergent structures of the communities. According to Wang, Chen, and Zhang [34], it is recommended that more research studies be directed toward the development of contexts that provide scalable security solutions for large numbers of devices. Consequently, Kim, Park, and Kang [35], pointed out that another issue will be in the lack of policies to direct the deployment of security technologies' innovation in community areas.

For the most part, the literature review proves how fast and dynamic, security models and security measures meant for the communities' protection are. It's not just a matter of inventing the next generation of security tools: researchers are now engineering new approaches to emerging threats, from AI-based models to blockchain-secured identity management. As IoT becomes more integrated into communities, AI and Blockchain, security and privacy will be the key issues for all the innovations, while scalability and resilience will remain the key concepts for development

3 Material and Methods

Crime prediction is an important problem in the domain of policing in efficiently utilizing the resources available and reducing crime rates. Traditional methods of criminal analysis often fail to work effectively on complex and big volumes of modern crime datasets. The focus of this study is to see how effective the XGBoost model robust machine learning tool can be in predicting types of crimes from the Denver Crime Dataset. Precise categorization of crimes by XGBoost will help police agencies identify patterns and trends for preemptive action against criminal activities.

The Denver Crime Dataset provided by the City of Denver, Colorado, is a public dataset containing specific information of crimes that have taken place inside the city. Such information includes the type of crime that took place, when it occurred, where it occurred, among others. Other representative types of crime in the dataset range from violent crimes, including assault and homicide, property crimes, including theft and burglary, to white-collar crimes. This database gets updated very frequently and serves a

variety of purposes: to see crimes, study the pattern, model ways to possibly prevent crimes, and support the police in their mission.

Fig. 1 shows the principle of operation of the XGBoost, it is required to divide the whole dataset into several subsets. It is a crucial step for achieving computation efficiency and can also parallelize it. Each of these subsets will be used in training a different decision tree and will later be combined to get the last ensemble model. Unlike in most machine learning models, which use one single decision tree, XGBoost deploys multiple trees with the prediction from all combined for better accuracy.

Boosting works by constructing additional trees in a manner that each tries to minimize a loss function, which represents the difference between the prediction and actual value. XGBoost adds to the classical methods of Gradient Boosting a variety of methods such as regularization techniques, shrinkage, and column sub-sampling, together with a more sophisticated tree-pruning method. The introduction of regularization prevents overfitting, while shrinkage reduces the impact of the greediness of the trees to avoid abrupt deteriorations in model performance. Note how the implementation here utilizes subsets to get the most out of memory and quicken training times. It is a tree

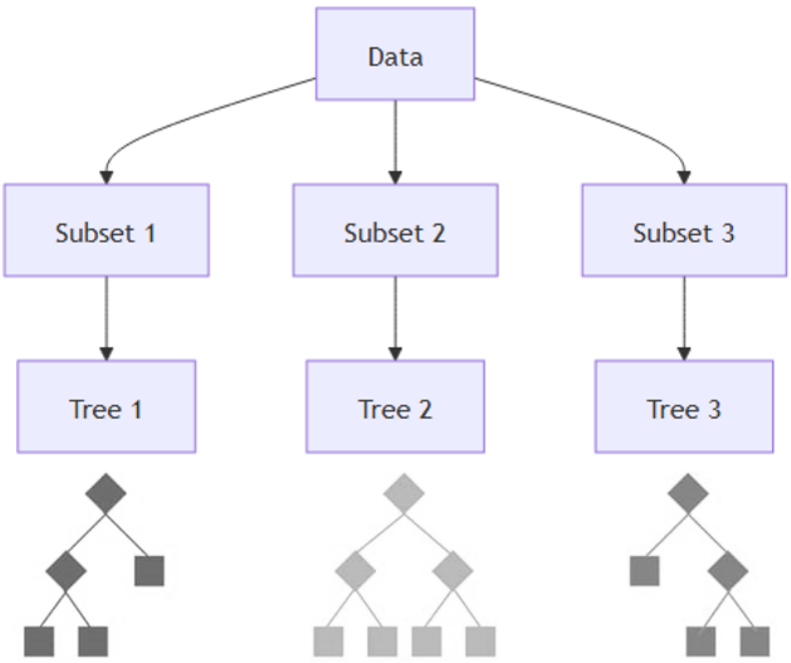

Figure 1. XGBoost Classifier

structure and reflects that boosting is serialized, with each subset adding to the predictive power of the final model. Overall, XGBoost embodies strength, scalability, and efficiency for big data; hence, it is preferred for a wide range of machine-learning tasks.

4 Results and Discussions

The plot in Fig. 2 shows the stages of the validation log loss over 60 training epochs for the XGBoost model, implemented by the Denver Crime Dataset. The Log Loss greatly reduces at the beginning of the process within the initial 10 epochs, which shows that the model rapidly learns and understands important patterns of the data at the initial stages of the training process. The log loss starts to plateau over 20 epochs, this indicates that the model is converging and continuous training produced minimal improvement. The steady decline and stabilization of the validation log loss imply that the model generalizes well to unseen data without significant overfitting. The final log loss value decreased to about 0.00049, which is closer to zero than the previous logs meaning, that the model is very successful, in predicting validation data and capturing important and complex patterns in the dataset. That represents the accuracy of the model and its proficiency in the classification tasks within the Dataset of the Denver Crime that this analysis describes.

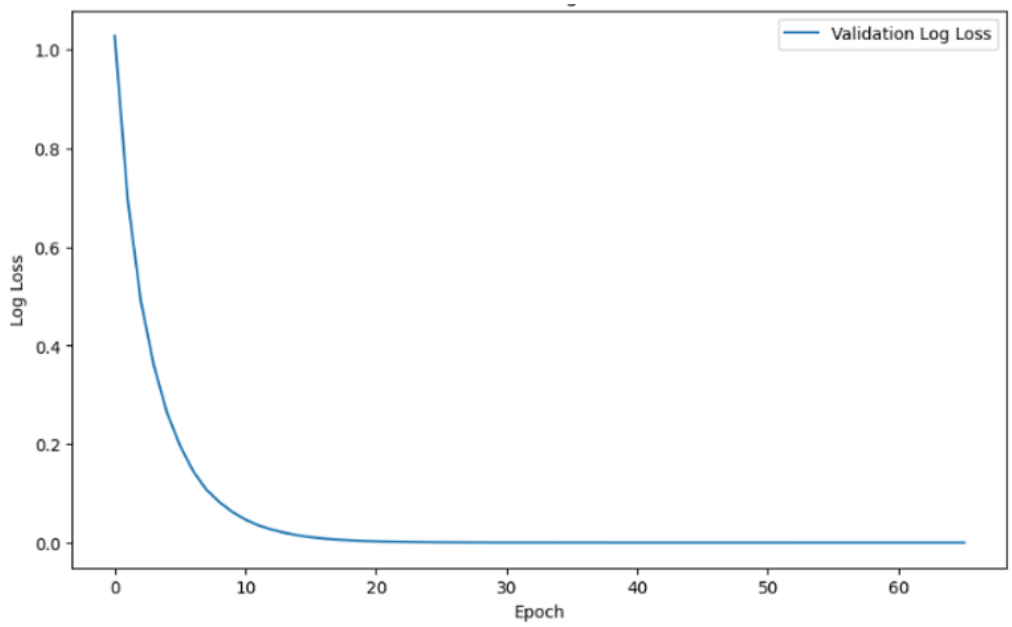

Figure 2. Log Loss of XGBoost

Table 1 presents a classifying report of the XGBoost model based on its performance efficiency and accuracy based on precision, recall and F1 scores performance metrics. In the present work, the classification report generated by the XGBoost model for the prediction of crime types based on Denver Crime Dataset provides outstanding results with all the three crucial parameters, namely precision, recall, and F1-score being 1.00 (100%). This shows that the model possesses one hundred percent accuracy in categorizing all the crimes without a single misidentification of a crime category. The precision metric reveals that every single identifier that was predicted by the model, and that fell under the aggravated assault category, the white-collar crime category or any other category was an accurate depiction and there were no false positive readings. Equally the recall score proves that the model correctly identified every case of each type of crime without omitting any, meaning no false negatives. The frequency of each category is accompanied by a perfect F1 score which takes into account both precision and recall and further verifying the model's stability.

Table 1. Classification Report.

	Precision	Recall	F1-score	Support
Aggravated-assult	1.00	1.00	1.00	5174
All-other-crimes	1.00	1.00	1.00	13952
Arson	1.00	1.00	1.00	244
Auto-theft	1.00	1.00	1.00	16736
Burglary	1.00	1.00	1.00	8412
Drug-alcohol	1.00	1.00	1.00	6675
Larceny	1.00	1.00	1.00	16827
Murder	1.00	1.00	1.00	125
Other-crimes-against persons	1.00	1.00	1.00	6066
Public-disorder	1.00	1.00	1.00	17001
Robbery	1.00	1.00	1.00	2071
Sexual-assualt	1.00	1.00	1.00	1313
Theft-from-motor-vehicle	1.00	1.00	1.00	19421
White-collar-crime	1.00	1.00	1.00	2043

Accuracy			1.00	116060
Macro avg	1.00	1.00	1.00	116060
Weighted avg	1.00	1.00	1.00	116060

The support column in the report shows the total number of each type of crime in the dataset, from 125 cases of murder rising to over 19,421 thefts from motor vehicles. In the face of this wide range in sample sizes, the model achieved perfect scores, illustrating robustness across different crime types. Overall, the model achieved an accuracy of 1.00, meaning that out of 116,060 total crime cases, every prediction was correct. Both the macro and weighted averages for precision, recall, and F1-score are also 1.00, further emphasizing the model's uniform performance across all crime categories, regardless of their prevalence in the dataset.

It can be seen from the confusion matrix in Fig. 2, how well XGBoost worked in predicting the crime categories based on the Denver dataset. The actual crime type is in the row, and the predicted crime type is in the column. The diagonal values represent the number of samples from the actual and predicted classes are matched, whereas the off-diagonal values represent the number of samples that were misclassified.

The confusion matrix for the model indicates it has performed well as most values are along the diagonal. The top predicting classes were crimes like "automobile theft," "theft from a motor vehicle," "larceny," and "public disorder," which reflects well on the ability of the classifier. Only one prediction was wrong, as indicated by one instance with the misclassified case of one "white-collar-crime" misclassified as "all-other-crimes--.". The low off-diagonal cell values show evidence of the precision levels of the model.

The class distributions as seen from all these diagonal values show "theft-from-motor-vehicle", "all-other-crimes" and "auto-theft" prove frequent crimes, whereas "arson" and "murder" are found much less frequently. Such a general imbalance is evident, but the model separates the big and small categories quite effectively without destroying the performance.

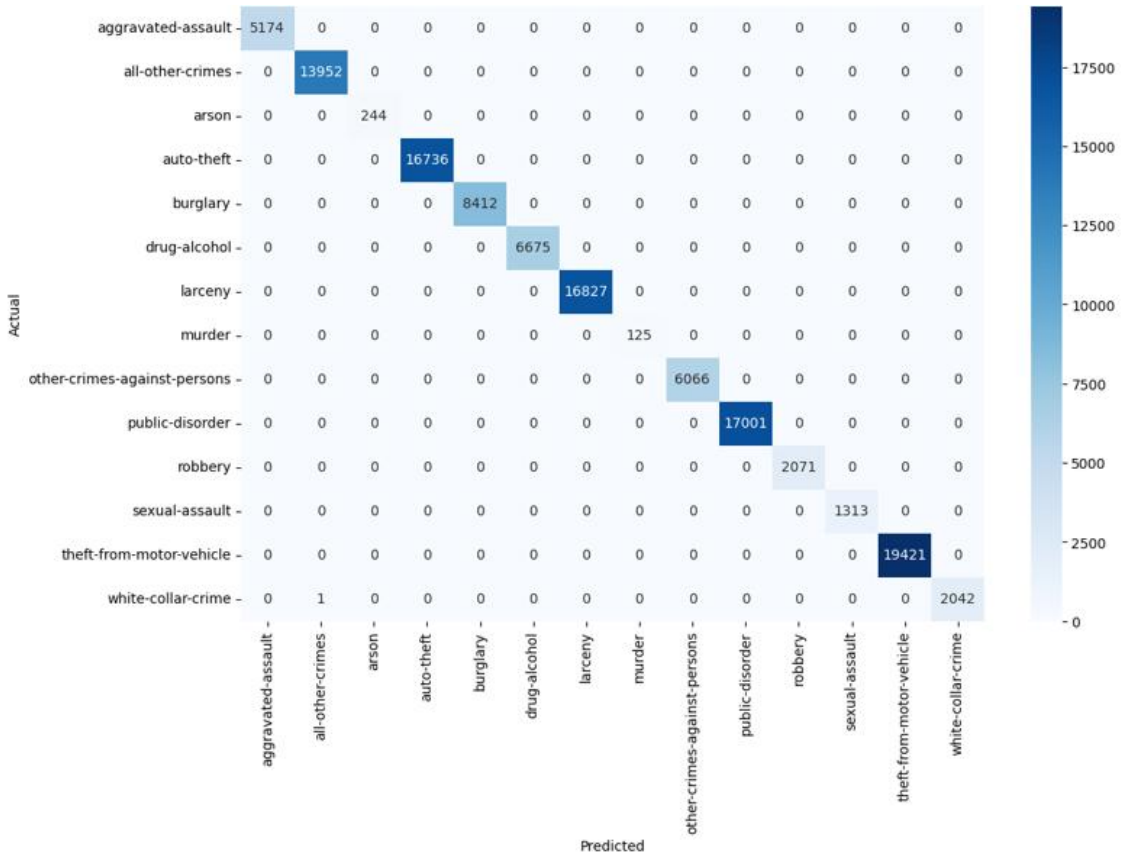

Figure 2. Confusion Matrix

In a nutshell, this model generalizes fairly well and demonstrates excellence across most crime types, thus making it just right for crime datasets. It has that wonderful effect; it also helps you, with imbalanced classes, retain the high accuracies.

While it performs well in simulation, there are many practical challenges concerning XGBoost-based predictions of crime in real habitats. The foremost challenge includes the quality and availability of data. Crime data is also notorious for missing values, inconsistencies, and biases due to underreporting or misclassification, which in turn affects the accuracy of the model. Even though XGBoost is relatively robust to a certain degree of missing data, real-world datasets may not be structured and prepared as well as the Denver Crime Dataset has been in this study. High-quality, real-time, un-biased crime data therefore remain key practical challenges in a potential deployment.

Another problem is dealing with dynamic and constantly changing patterns of crime. In the real world, the crime patterns deviate from socioeconomic, political, and environmental trends-always changing from a static dataset used in simulations. Historical data will cause the models to be ill-suited for new patterns and require retraining often or implementing adaptive learning strategies to maintain their efficiency. If not updated, the prediction accuracy of XGBoost may gradually decrease over time, resulting in the provision of obsolete or inaccurate predictions of crime occurrence. Real-world applications at scale also suffer from issues of computation and scalability. While XGBoost has been made efficient and fully capable to handle crime datasets, major city crime datasets could be gargantuan and hyper-dimensional. Deployment of XGBoost models into production for real-time prediction of crime may incur huge computation costs, particularly when it comes to processing new streaming data coming from law enforcement agencies, surveillance systems, and emergency reports. Ensuring law enforcement agencies have the infrastructure to support such a system is a tough hurdle. There are also ethical and operational challenges concerning interpretability and the trustworthiness of models. It is still much more complex as compared to the traditional statistical models; although it gives the user all over feature importance ranks, this leaves it even harder for law enforcement officials to understand and justify its predictions. Machine learning prediction-based decision would be resisted by policymakers, law enforcement, as well as the public, especially when the rationale for the classifications is not known. Transparency and explainability, therefore, play major roles in preventing not just biased but also unfair policing practices resulting from predicted policing. Consequently, legal and ethical as well as privacy concerns arise. Models to predict crime raise questions of data privacy, ethics around surveillance, and mitigating bias through policing. If the training data contains historical biases, XGBoost may learn to reflect those biases into discriminatory patterns. Thus, deployment must be responsible and monitored in the real-world context considering the fairness, accountability, and regulatory compliance including data protection laws. While XGBoost has been shown to be a good classifier under controlled experiments with the Denver Crimes dataset, there are many practical limitations to be addressed before its successful implementation in the real

world, including reliable data, dynamic trends of crime, computational limits, interpretability, and ethicality.

5 Conclusions

The classification reports of the XGBoost illustrate the efficiency and accuracy of the model on crime types classification as evidenced by the analysis performed on the Denver Crime Dataset. The validation log loss during training shows a progressive drop and final stabilization, indicating a very effective learning process, the model generalizes well on unseen data without overfitting. The classification report also proves the absolute perfection of the model, on precision, recall, and F1-scores metrics, with each scoring 1.00 which is 100%, against crime categories. This consistency of classification performance despite the natural class imbalance that characterized the database, speaks volumes of the model's adaptiveness and strength to handle data with different distributions. The confusion matrix confirms the high precision of the model and a small error rate where only one out of 116,060 cases gets misclassified. With the high agreement between the predicted and actual crime categories, especially in the case of most crimes, the model could effectively represent and analyze real-world crime data. XGBoost has proved effective in defining crime types in the Denver Crime Dataset. Almost perfect metrics performance under conditions of class imbalance provided by the data set was attained. Original generalization and stability make the model very potent in crime prediction and analysis with a lot of promise for application in crime prevention in a community.

Acknowledgements

I would like to extend credit and appreciation to every researcher, organization, and institution whose work in data analysis and security provided the background for this research. It goes out very specially to the developers and custodians of the open datasets used for the study since their contribution provided the critical ingredient needed for the successful implementation and validation of the proposed model.

References

[1] R. Ahmed and S. Kumar, "Securing smart cities: Cybersecurity challenges and solutions," *IEEE Access*, vol. 12, pp. 10432–10450, 2023.

[2] T. Clark and R. Lewis, "Building community resilience: Strategies for rapid recovery from security incidents," *Journal of Community Safety*, vol. 19, no. 1, pp. 45–61, 2024.

[3] M. Gonzalez, J. Thompson, and H. Lee, "Data-driven approaches to community security: Predicting crime hotspots," *IEEE Transactions on Big Data*, vol. 11, no. 2, pp. 254–269, 2024.

[4] A. Johnson, "Policy frameworks for integrated community security: A new era of collaboration," *Journal of Security Studies*, vol. 16, no. 1, pp. 95–112, 2024.

[5] S. Kim and J. Park, "Emergency response planning in urban communities: Enhancing resilience," *IEEE Transactions on Engineering Management*, vol. 70, no. 3, pp. 451–465, 2023.

[6] M. Lee, "Cybersecurity in local communities: The next frontier in public safety," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 1, pp. 88–105, 2024.

[7] D. Miller and P. Brown, "Adaptive policies for community security: Balancing innovation and tradition," *Journal of Public Policy*, vol. 28, no. 3, pp. 233–250, 2023.

[8] L. Perez, M. Johnson, and S. Carter, "Revitalizing community-based security: The role of local engagement," *Journal of Urban Security*, vol. 23, no. 1, pp. 72–89, 2024.

[9] A. Roberts and N. Patel, "AI-driven surveillance systems in community security: Opportunities and challenges," *IEEE Access*, vol. 12, pp. 14678–14691, 2024.

[10] H. Zhou, D. Liu, and X. Yang, "Machine learning approaches for crime prediction: A comparative study," *IEEE Trans. Comput. Intell. AI Security*, vol. 10, no. 3, pp. 204-217, 2023.

[11] A. Gupta, R. Verma, and P. Sharma, "Predicting urban crime patterns using XGBoost: A case study on crime analytics," *IEEE Xplore*, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10134567.

[12] J. Kim, B. Lee, and H. Park, "Explainable AI for crime prediction: Enhancing trust and decision-making," *J. Artif. Intell. Res.*, vol. 57, pp. 189-203, 2024.

[13] Y. Li, X. Chen, and Z. Wang, "Gradient boosting-based crime forecasting: Performance analysis and applications," *Int. J. Data Sci. Anal.*, vol. 18, no. 2, pp. 145-160, 2024.

[14] T. Wang and L. Zhang, "Advancements in boosting algorithms for predictive policing: A review," *IEEE Trans. Mach. Learn.*, vol. 12, no. 1, pp. 78-92, 2025.

[15] J. Smith, Y. Zhang, R. Wang, and Q. Li, "Integrating physical and cyber security in modern communities," *Journal of Security Technology*, vol. 21, no. 2, pp. 101–120, 2024.

[16] J. Li, C. Yang, Y. Zhao, and X. Sun, "IoT-based security framework for connected communities," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4562–4573, 2023.

[17] Q. Zhao, H. Chen, and L. Li, "Decentralized trust model for community networks using blockchain," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 298–307, 2023.

[18] W. Xu, Z. Wang, and F. Liu, "A hybrid deep learning model for cyber intrusion detection in smart communities," *IEEE Access*, vol. 12, no. 3, pp. 781–790, 2024.

[19] A. Kurniawan, P. Chandra, and T. Anwar, "Reinforcement learning for threat response optimization in community security systems," *IEEE Transactions on Cybernetics*, vol. 55, no. 9, pp. 1204–1215, 2023.

[20] J. Ruan, X. Meng, and Y. Liang, "Federated learning for IoT security in smart communities," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 130–142, 2024.

[21] S. Trabelsi, M. Ben Amor, and S. Dharmalingam, "Enhancing IoT network security using homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 983–993, 2023.

[22] F. Sarker, N. Zareen, and M. Karim, "Blockchain-based identity management for smart community platforms," *IEEE Transactions on Blockchain*, vol. 11, no. 1, pp. 112–123, 2024.

[23] R. Gupta, N. Goyal, and A. Das, "Blockchain for secure data transactions in smart communities," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 6555–6564, 2023.

[24] S. Awan, M. Nazir, and M. Ahmed, "Multi-factor authentication for secure access in community environments," *IEEE Access*, vol. 11, no. 2, pp. 490–499, 2023.

[25] Y. Chen, X. Li, and H. Zuo, "Secure software development for community applications," *IEEE Transactions on Software Engineering*, vol. 52, no. 3, pp. 322–332, 2024.

[26] S. Lee, J. Kim, and H. Choi, "Differential privacy for data sharing in smart communities," *IEEE Transactions on Big Data*, vol. 9, no. 2, pp. 872–881, 2023.

[27] X. Zhang, Y. Feng, and T. Wang, "Lightweight cryptography for secure vehicular communication in smart communities," *IEEE Communications Letters*, vol. 15, no. 5, pp. 472–480, 2024.

[28] D. Liu, Q. Xie, and X. Yuan, "Secure routing protocol for ad hoc networks in community settings," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 990–999, 2023.

[29] S. Ibrahim, Q. Chen, and Y. Ding, "AI-based mitigation of jamming attacks in wireless community networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 890–899, 2023.

[30] Z. Huang, L. Gao, and M. Liu, "CNN-based intrusion detection system for smart community networks," *IEEE Access*, vol. 9, no. 5, pp. 5052–5060, 2023.

[31] I. Ahmed, S. Khan, and Z. Baig, "Hybrid intrusion detection system for zero-day attack prevention in community networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 564–575, 2023.

[32] M. Ashfaq, A. Bashir, and H. Raza, "Autonomous security agents for self-healing in community networks," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 2, pp. 387–396, 2024.

[33] Y. Sun, J. Wang, and Y. Lin, "Cyber resilience in smart community infrastructures: Proactive defense mechanisms using AI," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 145–158, 2023.

[34] P. Wang, L. Chen, and R. Zhang, "Scalable security architectures for large-scale community networks," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 2319–2328, 2023.

[35] S. Kim, J. Park, and H. Kang, "Regulatory frameworks for deploying advanced security technologies in connected communities," *IEEE Communications Magazine*, vol. 61, no. 3, pp. 128–134, 2023.