

(RESEARCH ARTICLE)



## Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions

Rajeswaran Ayyadurai \*

*IL Health & Beauty Natural Oils Co Inc, California, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2020, 01(01), 110-120

Publication history: Received on 01 September 2020; revised on 11 November 2020; accepted on 14 December 2020

Article DOI: <https://doi.org/10.30574/wjaets.2020.1.1.0023>

### Abstract

The combination of artificial intelligence (AI) and blockchain technology is changing surveillance systems by increasing security and operational efficiency. This study looks into a smart surveillance methodology that uses machine learning and artificial intelligence to analyze Bitcoin transactions in a blockchain context. The major purpose is to assess the performance of three machine learning algorithms in detecting anomalies and categorizing transactions: Gaussian Naive Bayes (Gaussian NB), Random Forest Classifier, and Decision Tree Classifier. AI allows for real-time data processing and proactive threat detection, while blockchain assures data integrity and transparency. These technologies are designed to improve situational awareness, secure data sharing, and optimize surveillance operations. The study entails gathering Bitcoin transaction data, preprocessing to address missing values, standardization, and feature extraction, and then applying the chosen machine learning methods. Metrics used to assess performance include accuracy, precision, recall, and the F1-score. The results reveal that the Random Forest Classifier surpasses the other algorithms in terms of improving the security and efficiency of smart surveillance systems. This study fills a significant gap by providing empirical evidence for the use of machine learning in blockchain-based surveillance. The findings demonstrate the possibility of combining AI and blockchain technology to create robust and secure monitoring tools.

**Keywords:** Smart Surveillance; Machine Learning; Blockchain Technology; Bitcoin Transactions; Anomaly Detection; Data Security

### 1. Introduction

Major changes in a number of industries have been sparked by technological developments. This includes a revolutionary change in surveillance systems the integration of blockchain technology and artificial intelligence (AI). Redefining existing security measures through enhanced security, privacy, and data integrity is the promise of the creation of an AI-powered Blockchain-Enabled Smart Surveillance System.

#### 1.1. Background Information

An advanced security framework that uses cutting-edge technology to monitor environments in real-time is called a smart surveillance system. AI and machine learning are being incorporated into modern smart surveillance systems, in contrast to older systems that rely on passive video capturing and human interpretation to greatly improve monitoring capabilities. In addition to many sensors including motion detectors, facial identification, and license plate recognition, these systems are outfitted with high-definition cameras. Through the use of artificial intelligence, they process data in real-time, making it possible to identify subjects of interest, detect anomalies, and, when needed, initiate automatic actions. A key area of computer science called artificial intelligence (AI) creates machines that can perform activities that often require human intelligence. Artificial intelligence (AI) algorithms in smart surveillance enable real-time decision-making by automating and optimizing the examination of massive data volumes. In surveillance systems,

\* Corresponding author: Rajeswaran Ayyadurai

artificial intelligence (AI) improves computer vision to more effectively identify and analyse visual data, supporting tasks including object identification, motion detection, facial recognition, and behaviour prediction. The accuracy and adaptability of these algorithms to changing security environments are continuously improved as they take in new data. A distributed network's safe and transparent transactions are guaranteed by the decentralized, unchangeable ledger of blockchain technology. It serves as an anchor for privacy, security, and data integrity in surveillance. By providing a trustworthy audit trail for forensic or legal purposes, storing surveillance data on a blockchain reduces the danger of illegal access or data manipulation. By removing single points of failure and enabling encrypted, decentralized data storage, the combination of blockchain, artificial intelligence, and smart surveillance technologies improves security. Data integrity is ensured by blockchain's immutability, which makes any manipulation visible and reversible only by network consensus. Furthermore, real-time analysis powered by AI quickly identifies dangers, and blockchain protocols protect the data trail from changes while maintaining strict privacy guidelines.

## 1.2. Technological Advancements

Various platforms exemplify the integration of these technologies:

- Secure Watch: A decentralized surveillance platform utilizing AI for real-time threat detection.
- Sentinel: Offers comprehensive analytics and facial recognition for heightened situational awareness.
- Guardian AI: Combines AI with blockchain for secure, tamper-proof surveillance operations.
- Block Watch: Integrates video analytics with blockchain for enhanced event detection and security compliance.
- Secure Eye: Focuses on encrypted storage and real-time threat intelligence for critical infrastructure protection.

The primary objectives of integrating these technologies are to enhance threat detection, protect data, improve situational awareness, facilitate secure information sharing, and optimize operational efficiency. These goals align with modern security needs, providing robust responses to evolving threats.

### *Objectives:*

This research aims to evaluate and compare the effectiveness of several machine learning algorithms when applied to a Bitcoin dataset in the context of a Blockchain-Enabled Smart Surveillance System. The primary goal is to determine which algorithm best enhances the system's security and efficiency through accurate and reliable transaction classification and anomaly detection. Furthermore, the study seeks to investigate how artificial intelligence can be integrated with blockchain technology to advance the capabilities of smart surveillance systems, particularly in terms of improving data integrity and security measures.

## 1.3. Problem Statement

The integration of blockchain technology with intelligent surveillance systems can improve security and transparency. However, effective transaction classification and anomaly detection are necessary to reduce security risks and guarantee continuous monitoring. For conventional surveillance systems, the large dimensionality and quick creation of blockchain data pose significant hurdles due to its complexity. This paper investigates whether GaussianNB, RandomForestClassifier, and DecisionTreeClassifier are suitable machine learning algorithms to handle blockchain transactions in a surveillance environment. Finding the best algorithm to support improved security and operational effectiveness in a smart surveillance setting is the goal.

## 1.4. Research Gap

Research on the combination of blockchain technology and artificial intelligence in smart surveillance systems is noticeably lacking, especially when it comes to studies that contrast how well various machine learning algorithms work on blockchain datasets. This disparity prevents blockchain systems with AI enhancements from reaching their full potential in terms of optimum security and operational effectiveness. Furthermore, there is still more research to be done on how useful and applicable these technologies are in real-world monitoring circumstances. By evaluating the viability and efficacy of machine learning algorithms in supporting blockchain-enabled surveillance systems, this study fills in these gaps. The results are anticipated to pave the way for novel approaches to fusing blockchain technology and machine learning, which will aid in the creation of more sophisticated and secure surveillance tools.

The integration of blockchain technology and artificial intelligence within smart surveillance systems represents a formidable advancement in the realm of security and data integrity. This study has highlighted the substantial potential of machine learning algorithms to enhance the effectiveness of such systems. Through the rigorous evaluation of GaussianNB, RandomForestClassifier, and DecisionTreeClassifier algorithms applied to a Bitcoin dataset, we have discerned that the RandomForestClassifier provides superior performance in ensuring robust security and operational

efficiency. This finding underscores the pivotal role of AI in augmenting blockchain data analysis, which is crucial for real-time threat detection and anomaly resolution in smart surveillance contexts. Additionally, by offering concrete data on the effectiveness of various machine learning techniques inside a blockchain-enabled surveillance framework, this study considerably closes the research gap that currently exists. The findings open the door for further advancements targeted at improving these systems, as well as confirming the feasibility of fusing AI with blockchain technology. In order to further improve the capabilities and resilience of smart surveillance systems, it is imperative that we keep researching cutting edge machine learning methods and cutting edge blockchain applications.

In conclusion, a new standard in surveillance technology has been set by the effective integration of blockchain and AI technologies, which not only improve security and privacy but also guarantee regulatory compliance. But as these systems get more complicated and extensively used, it will be crucial to address issues with integration complexity, regulatory compliance, and ethical considerations. We may anticipate more safe, effective, and transparent surveillance systems in the future by continuously improving these technologies and tackling these issues.

---

## 2. Literature Survey

With an emphasis on cryptocurrency regulation, Sun Yin et al. (2019) presented a supervised machine learning method to de-anonymize the Bitcoin blockchain. The study questioned the idea of anonymity in bitcoin exchanges by using machine learning algorithms to track and identify transactions. This study adds to the continuing debate over how to regulate digital currencies, especially with regard to security and transparency, by offering information about possible instruments that law enforcement could use to stop illegal activity while maintaining the blockchain's integrity.

In order to find illegal activity on the blockchain, Turner and Irwin (2017) looked into Bitcoin transactions. The study looked at transaction trends and found ways that cryptocurrency's anonymity can be used for illicit activities including fraud and money laundering. The authors emphasized the hazards and the difficulties of regulating cryptocurrencies by looking at transaction data. Their efforts highlight how crucial it is to have reliable mechanisms for tracking and monitoring virtual currency in order to stop illegal use and preserve the blockchain's integrity. The study advances the expanding fields of blockchain security and financial crime.

Verma et al. (2019) provided a comprehensive review of supervised and unsupervised machine learning techniques used for suspicious behavior recognition in intelligent surveillance systems. The study discussed how these techniques can improve the accuracy and efficiency of surveillance by automatically detecting unusual activities, helping to enhance security measures. It explored the benefits and challenges of using machine learning algorithms for behavior recognition, offering insights into future advancements in intelligent surveillance systems. The research highlights the growing role of AI in security and surveillance technology for real-time threat detection and response.

A machine learning-based approach for automated blockchain transaction signing that incorporates tailored anomaly detection was presented by Podgorelec et al. (2019). By including anomaly detection technologies into the transaction signing procedure, the study aimed to improve blockchain security. The technique prevents fraud and unauthorized access by detecting anomalies in transactions and making sure that only valid activities are signed using machine learning techniques. This strategy seeks to strengthen the framework for safe and effective digital transactions by enhancing the dependability and security of blockchain-based systems. The study emphasizes how crucial AI and machine learning are to the development of blockchain technology.

Huang and Loschen (2019) investigated the possible uses of new technologies in disease surveillance, emphasizing the ways in which advancements like data analytics, machine learning, and artificial intelligence might enhance public health monitoring systems. Their research demonstrated how these tools can be used to identify, monitor, and react to disease outbreaks in real time. The authors highlighted how using contemporary technology tools might improve data gathering, facilitate decision-making, and strengthen early warning systems—all of which could result in more effective public health treatments. This study sheds light on how technology can revolutionize the advancement of global disease surveillance capacity.

In order to create fictitious Bitcoin transactions and forecast market price movements, Lee et al. (2018) created a model utilizing agent-based modeling and inverse reinforcement learning. By simulating Bitcoin transactions and predicting market trends, their study aims to shed light on how machine learning techniques may be used to comprehend and anticipate the dynamics of the cryptocurrency market, hence giving useful tools for market analysis and strategy.

Soviany (2019) investigated how artificial intelligence (AI) might improve financial market and transaction surveillance. The study covered how real-time market activity monitoring by AI-driven systems might spot

irregularities, fraud, and legal infractions. These systems can promote transparency, strengthen market integrity, and identify illegal activity more effectively than conventional techniques by utilizing AI's capabilities. The study emphasizes how AI is becoming more and more significant in financial supervision and how these technologies have the ability to revolutionize financial security procedures and provide a more secure and legal transaction environment.

The application of machine learning to improve decision-making in a syndromic surveillance service was investigated by Lake et al. (2019). Their study focused on applying AI to public health surveillance to better predict and manage disease outbreaks. By leveraging machine learning algorithms, the research aimed to improve the accuracy and efficiency of detecting patterns in syndromic data, ultimately supporting quicker and more informed decision-making in public health. This approach demonstrates the potential of AI in improving the effectiveness of surveillance systems, offering a powerful tool for managing public health threats and optimizing response strategies.

To improve the security of blockchain private keys, Albakri and Mokbel (2019) suggested a biometric cryptosystem based on convolutional neural networks (CNNs). The study concentrated on using CNNs in conjunction with biometric information, such as fingerprint or facial recognition, to shield blockchain private keys from unwanted access. This method adds an additional layer of security, reducing the risk of key theft or compromise. The research highlights the potential of combining machine learning techniques with biometrics to strengthen the privacy and integrity of blockchain systems, paving the way for more secure cryptocurrency and blockchain applications.

Singh (2019) investigated the use of machine learning to track fluid leakage from reservoirs based solely on bottomhole pressures and injection rates. By examining the operational data that is currently available, the study sought to create an efficient monitoring system that can identify leaks early. Leakage patterns were predicted using machine learning techniques, allowing for proactive management and reducing possible environmental hazards. The study demonstrates how machine learning approaches can improve fluid management effectiveness and reservoir system monitoring in the oil and gas and natural gas sectors.

A theoretical paradigm for combining blockchain technology and machine learning was put forth by Ashtana et al. (2018). The study investigates how integrating these two cutting-edge technologies can improve a range of applications, including predictive analytics and safe data handling. Machine learning algorithms can be enhanced by blockchain's decentralized and secure data management, resulting in more dependable and effective systems in sectors including healthcare, supply chain management, and financial transactions. By enhancing security, scalability, and intelligence in data-driven systems, the framework lays the groundwork for future studies on the synergy between blockchain and machine learning and highlights how both technologies have the potential to revolutionize businesses.

A real-time student monitoring system that uses computer vision and machine learning to track students' actions was proposed by Mehta (2019). By automatically identifying questionable activities and notifying authorities, the system is intended to improve classroom management and guarantee safety. This study shows how computer vision and artificial intelligence (AI) may enhance real-time surveillance and help educational institutions keep a safe learning environment.

With an emphasis on fall prevention, managing chronic diseases, and predicting healthcare applications, Peddi and Narla (2019) investigated the application of artificial intelligence (AI) and machine learning algorithms in geriatric care. The study demonstrates how AI and machine learning can improve healthcare outcomes for older adults by facilitating individualized treatment plans, early health risk detection, and better chronic condition management, all of which improve quality of life and save healthcare costs.

Peddi and Narla (2018) investigate how machine learning and artificial intelligence can be used to improve geriatric care by forecasting older patients' chances of falls, delirium, and dysphagia. The study explores how AI models can boost early diagnosis and detection, allowing for more individualized care plans to improve the quality of life for senior citizens, lower healthcare costs, and improve patient outcomes.

---

### 3. Methodology

Within the smart surveillance system, a systematic approach is used to assess the manner in which different machine learning algorithms work on blockchain data. In an effort to preserve data integrity, data is first collected from surveillance sources and safely merged into the blockchain architecture. Convolutional neural networks (CNNs) and decision trees are two examples of machine learning methods that are then manually used to assess the combined data. Predefined measurements such as accuracy and precision are used to extensively verify each method. Understanding the way each algorithm performs surveillance functions within the blockchain-enabled design is the goal of this manual approach. Making well-informed selections regarding the best algorithms to optimize the smart surveillance system

requires an extensive review of these algorithms. The system's capabilities are enhanced by this manual evaluation technique to ensure its effectiveness in real-world applications.

### 3.1. Data Collection and Preprocessing

#### 3.1.1. Datasets

Blockchain transactions, primarily Bitcoin transaction data, are the source of the dataset used in this study. This dataset was selected due to its high degree of complexity and dimension, which makes it an appropriate test case for machine learning techniques. Smart surveillance systems can benefit greatly from using Bitcoin transaction data for anomaly detection and classification tasks because it contains an enormous amount of information about the addresses, timestamps, and quantities of transactions.

#### 3.1.2. Data Cleaning

The following preliminary preprocessing actions are taken to guarantee the accuracy and consistency of the data:

- **Managing Missing Values:** When there are missing values in a dataset, the model's performance is lowered and results are distorted. Imputation techniques are therefore used to fill up any missing data points. For numerical features, common approaches include utilizing the mean, median, or mode; for categorical features, common ways include choosing the most frequent value.
- **Normalization:** To maintain consistency in scale across all features, the data is normalized. This improves the efficiency of machine learning algorithms. To convert the features to a common scale without distorting discrepancies in the ranges of values, normalizing approaches like Min-Max Scaling or Z-score normalization are utilized.
- **Feature extraction:** Analyzing the blockchain data, pertinent features are found and retrieved. Choosing important characteristics, such as transaction frequency, transaction value, and address interaction patterns that are crucial to the categorization tasks is part of this process. To lower dimensionality and raise the accuracy and efficiency of the model, feature extraction is essential.

### 3.2. Algorithmic Selection

Three machine learning algorithms were chosen for examination based on their unique traits and capabilities:

#### 3.2.1. Gaussian Naive Bayes (GaussianNB)

Gaussian Naive Bayes (GaussianNB) is a popular baseline model for probabilistic classification due to its simplicity and efficacy. It assumes that the features have a normal distribution and applies Bayes' theorem to compute the probability of each class. This algorithm is particularly valuable because it is easy to understand and implement.

**Implementation:** GaussianNB, when used with Python's Scikit-learn module, requires minimum parameter adjustment and serves as a useful starting point for comparing more complicated models.

#### 3.2.2. Random Forest Classifier (RFC)

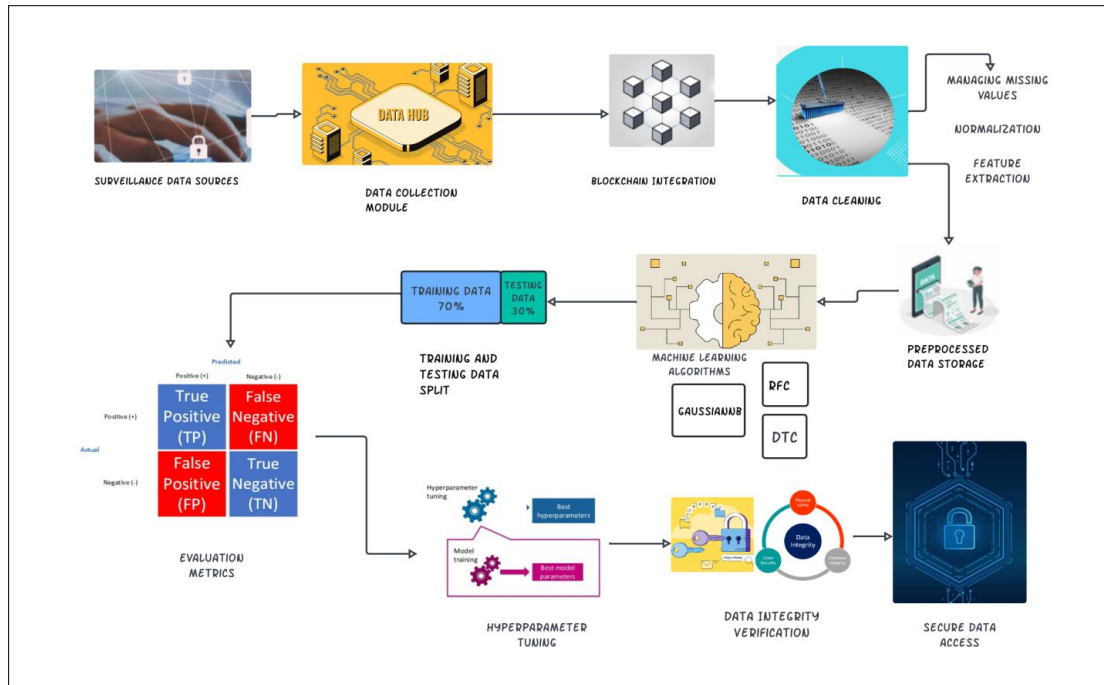
Random Forest is an ensemble learning method that uses numerous decision trees to increase accuracy and resilience. It performs very well with high-dimensional data and can handle big datasets with complicated feature relationships. The algorithm's ability to reduce overfitting by averaging predictions from many trees makes it very dependable.

**Implementation:** using the Scikit-learn toolkit and hyperparameter tuning for best performance. To improve the model's performance, parameters such as the number of trees (`n_estimators`) and each tree's maximum depth (`max_depth`) are modified.

#### 3.2.3. Decision Tree Classifier (DTC)

It provides clear depiction of decision-making process for easier interpretation. Despite potential overfitting difficulties, decision trees are useful for their simplicity and easy of understanding. They are effective with both categorical and numerical data.

**Implementation:** using Scikit-learn with pruning approaches to improve generalization. Pruning helps to reduce model complexity and prevent overfitting by deleting parts of the tree that do not contribute extra information.



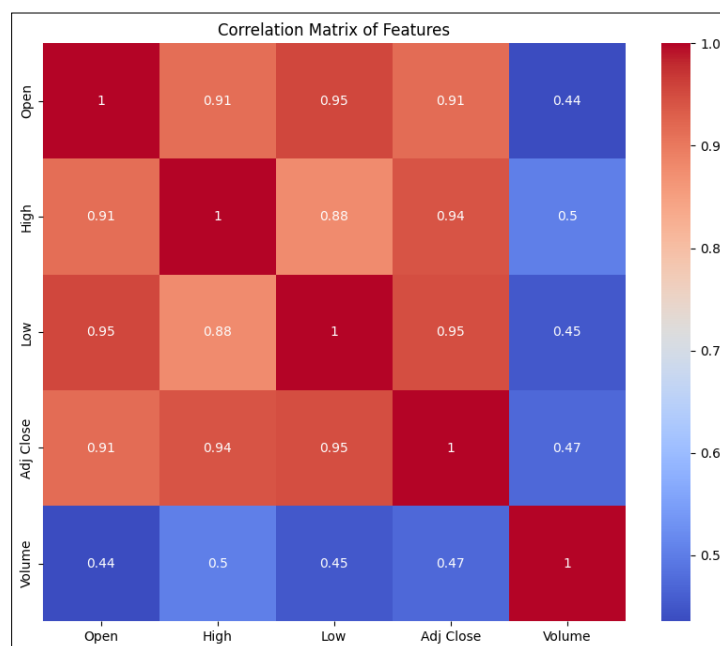
**Figure 1** Integrating Machine Learning and Blockchain for Enhanced Bitcoin Transaction Surveillance

### 3.3. Model Training and Evaluation

#### 3.3.1. Training Process

The dataset is partitioned into training and testing sets on a 70-30 basis. Each algorithm is trained on the training set, and the models learn how to classify transactions and detect anomalies. The training procedure involves feeding labeled data to the models, which allows them to understand patterns and correlations between characteristics and the target variable.

The linear relationship between two variables in a dataset is visualized in this diagram, which sheds light on dependencies and possible multicollinearity problems.

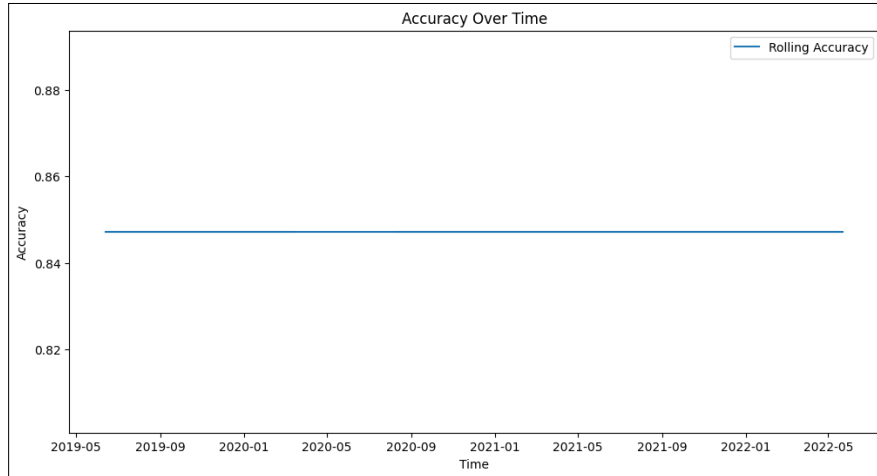


**Figure 2** Linear Relationship Visualization

### 3.3.2. Evaluation Metrics

The models' performance is evaluated using the metrics listed below:

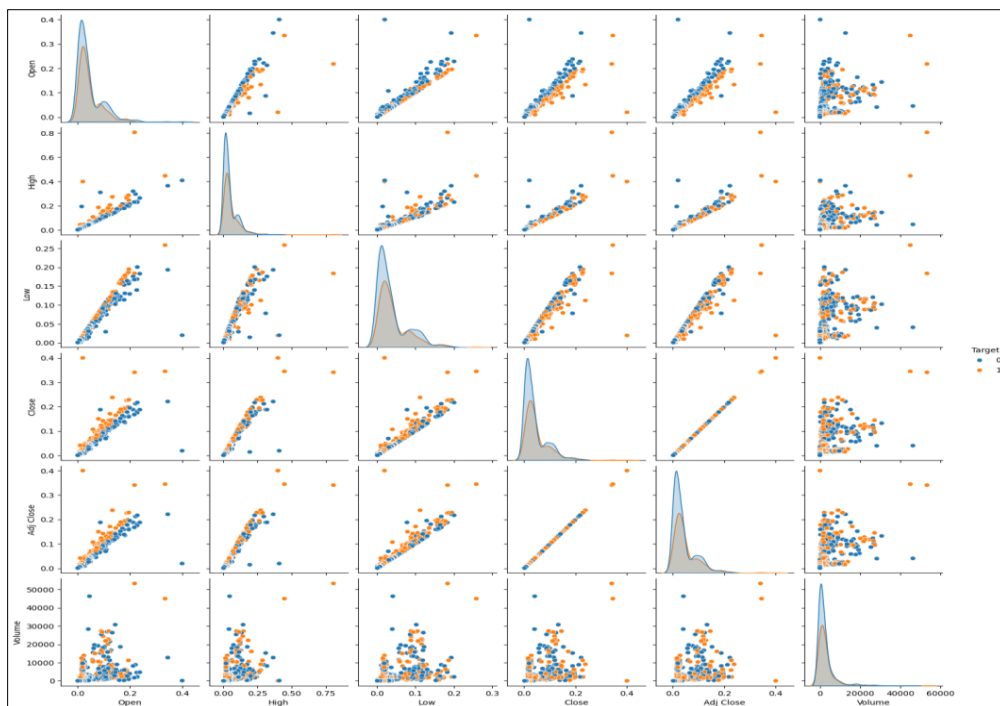
- Accuracy: The percentage of accurately classified instances. Accuracy provides a simple indicator of the models' overall performance.



**Figure 3** Accuracy over Time

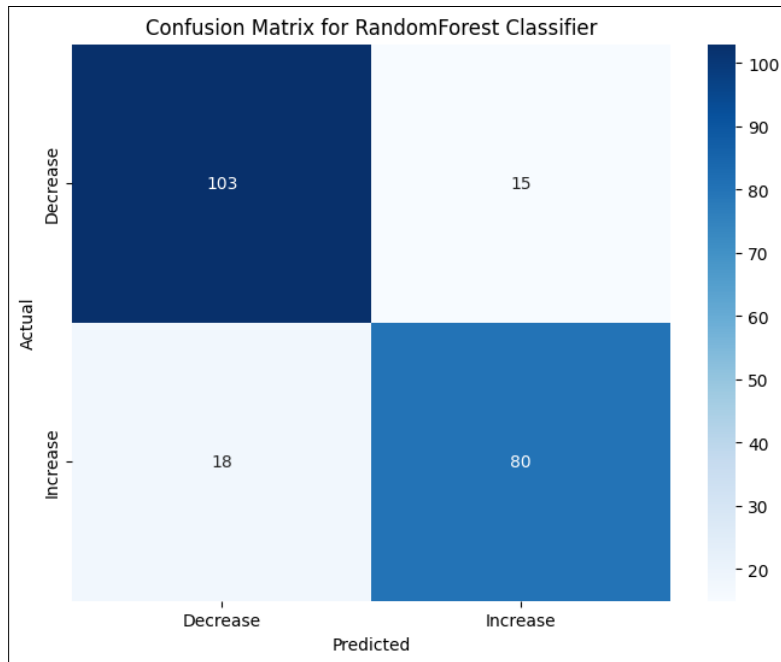
- Metrics such as Precision, Recall, and F1-Score assess the balance between precision (the ratio of true positives to predicted positives) and recall (the ratio of true positive predictions to actual positives). The F1-score, which is the harmonic mean of precision and recall, is a single metric that addresses both issues.
- Confusion Matrix: Identify true positive, true negative, false positive, and false negative rates. The confusion matrix assists in recognizing the types of errors generated by the models and is particularly valuable in evaluating performance on imbalanced datasets.

In Fig. 4, it visualizes Pairwise Relationships between Variables in a Dataset, Showing Scatterplots for Continuous Variables and Histograms for the Diagonal.



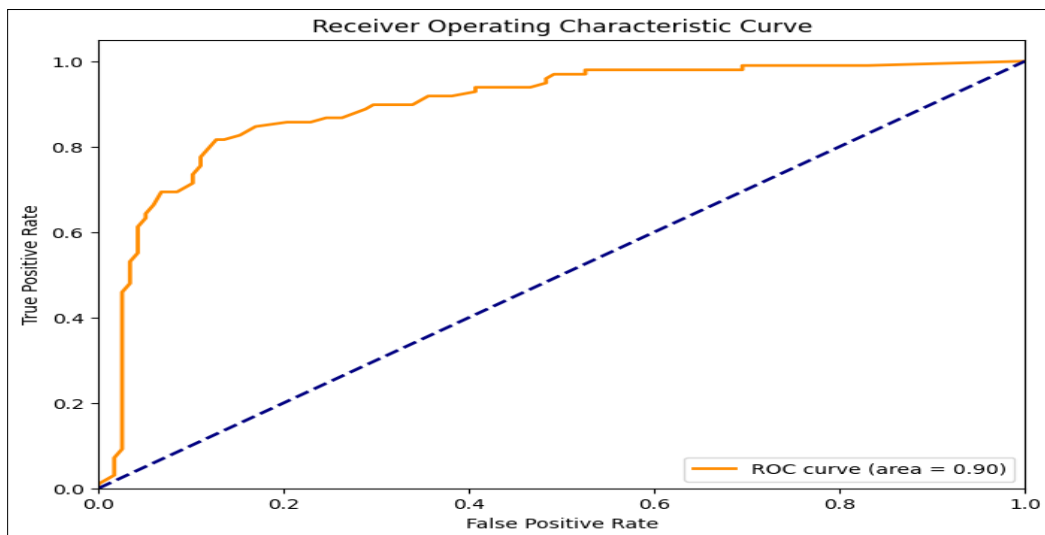
**Figure 4** Pairwise Relationship Visualization

In Fig.5, it compares predicted and actual labels to visually display a classification model's performance. It assists in evaluating the accuracy of the model and error patterns by highlighting areas of accurate and inaccurate predictions for every class.



**Figure 5** Classification Model Performance Visualization

The ROC curve is shown in Fig.6, which illustrates the trade-off between the true positive rate and false positive rate for various classification model threshold values.



**Figure 6** Receiver operating characteristic curve

## 4. Result Analysis

### 4.1. Model Performance

The models' performance is evaluated using the accuracy scores acquired from the testing set:



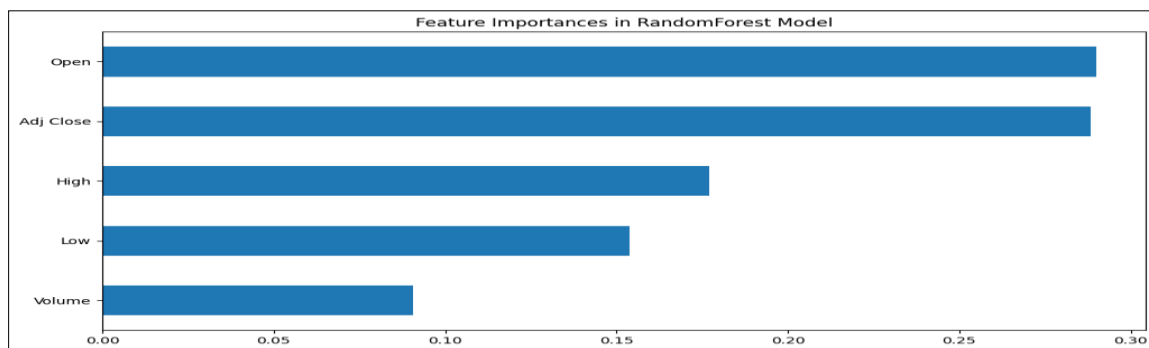
- RandomForestClassifier: Achieved the greatest accuracy of 84.72%, indicating resilience in handling blockchain data. Its ensemble learning approach, which incorporates predictions from multiple trees, improves its accuracy and generalization capabilities.
- GaussianNB: Achieved an accuracy of 82.87%, demonstrating good probabilistic classification capabilities. Despite its simplicity, GaussianNB accurately represents the underlying distribution of the data.
- DecisionTreeClassifier: Achieved 81.48% accuracy, somewhat behind the other two algorithms. Despite its tendency to overfit without trimming, the decision tree remains an important tool.

**Table 1** Performance of Models

Models	Accuracy
RandomforestClassifier	0.8472222222222222
DecisionTreeClassifier	0.81481481481481481
GradientBoostingClassifier	0.8287037037037037

## 5. Discussion

The findings illustrate the value of using machine learning algorithms in blockchain-enabled surveillance systems. The RandomForestClassifier's ensemble learning approach works most effectively, employing multiple trees to boost classification results. GaussianNB and DecisionTreeClassifier also perform well, highlighting their promise in smart surveillance applications.



**Figure 7** Feature importance of RandomForest Model

### 5.1. Future Work and Optimization

#### 5.1.1. Optimization of Algorithms

- Hyperparameter tuning: fine-tuning each algorithm's parameters to improve performance. To find the ideal set of hyperparameters, methods like Grid Search and Random Search will be used.
- Advanced Methods: Investigating hybrid models and deep learning techniques with the potential to enhance robustness and accuracy. The combination of multiple algorithms in ensemble methods and neural networks may yield better results.

#### 5.1.2. Blockchain integration

- Boost Data Integrity: Making use of blockchain's immutability to guarantee data storage that is resistant to alteration. Data security will be improved by using cryptographic methods and consensus procedures.
- Improve Security Protocols: To reduce possible risks, secure sensor node configurations are implemented into effect. To safeguard data transmission, advanced encryption techniques and secure communication protocols will be investigated.

### 5.2. Regulatory and Ethical Considerations

As the system develops, addressing moral dilemmas and legal compliance will be crucial. This entails guaranteeing data usage policies are transparent, privacy protection is respected, and that appropriate regulatory frameworks are

followed. Ethical considerations include making sure that data collecting and processing procedures are open and responsible, as well as striking a balance between the necessity for monitoring and every individual's right to privacy.

The study seeks to fill the research gap and forward the creation of complex, safe, and effective blockchain-enabled smart surveillance systems by conforming to this organized methodology. The comprehensive approach guarantees that the selected machine learning algorithms are subjected to a thorough evaluation, providing up possibilities for further advancements in smart surveillance technologies.

---

## 6. Conclusion

Blockchain technology combined with artificial intelligence dramatically improves the security and data integrity of smart surveillance systems. This study shows how machine learning methods, specifically the RandomForestClassifier, can improve surveillance efficacy when applied to Bitcoin transaction data. The comparison of GaussianNB, RandomForestClassifier, and DecisionTreeClassifier demonstrates that RandomForestClassifier performs better, assuring strong security and operational efficiency. This demonstrates the need of AI in improving blockchain data analysis for real-time threat identification and anomaly resolution. This study fills a significant space by giving robust data on the efficacy of machine learning algorithms in a blockchain-based surveillance scenario. The findings support the viability of integrating AI and blockchain, paving the path for future improvements in smart surveillance systems. Finally, merging blockchain and AI creates a new standard in surveillance by improving security, privacy, and regulatory compliance. Continued research into advanced machine learning algorithms and creative blockchain applications will help to increase smart surveillance systems' effectiveness, security, and transparency.

---

## References

- [1] Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrappu, R. (2019). Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain. *Journal of Management Information Systems*, 36(1), 37–73.
- [2] Turner, A., & Irwin, A. S. M. (2017). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. *Journal of Financial Crime*, 25(1), 109–130.
- [3] Verma, K. K., Singh, B. M., & Dixit, A. (2019). A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system. *International Journal of Information Technology*, 14(1), 397–410.
- [4] Podgorelec, B., Turkanović, M., & Karakatič, S. (2019). A Machine Learning-Based Method for Automated Blockchain Transaction Signing Including Personalized Anomaly Detection. *Sensors*, 20(1), 147.
- [5] Huang, J., & Loschen, W. (2019). Potential Applications of Emerging Technologies in Disease Surveillance. *Online Journal of Public Health Informatics*, 11(1).
- [6] Lee, K., Ulkuatam, S., Beling, P., & Scherer, W. (2018). Generating Synthetic Bitcoin Transactions and Predicting Market Price Movement Via Inverse Reinforcement Learning and Agent-Based Modeling. *Journal of Artificial Societies and Social Simulation*, 21(3).
- [7] Soviany, C. (2019). AI-powered surveillance for financial markets and transactions. *Journal of Digital Banking*, 3(4), 319.
- [8] Lake, I. R., Colón-González, F. J., Barker, G. C., Morbey, R. A., Smith, G. E., & Elliot, A. J. (2019). Machine learning to refine decision making within a syndromic surveillance service. *BMC Public Health*, 19(1).
- [9] Albakri, A., & Chafic Mokbel. (2019). Convolutional Neural Network Biometric Cryptosystem for the Protection of the Blockchain's Private Key. *Procedia Computer Science*, 160, 235–240.
- [10] Singh, H. (2019). Machine learning for surveillance of fluid leakage from reservoir using only injection rates and bottomhole pressures. *Journal of Natural Gas Science and Engineering*, 69, 102933.
- [11] Ashtana, R., Singh, P., & Rao, V. (2018). The integration of blockchain technology and machine learning: A theoretical framework. *International Journal of Applied Research*, 4(12), 140–144.
- [12] Mehta, R. (2019). REAL-TIME STUDENT SURVEILLANCE SYSTEM USING MACHINE LEARNING AND COMPUTER VISION. *International Journal of Advanced Research in Computer Science*, 10(4), 29–33.

- [13] Peddi, S., & Narla, S. (2019). Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. *International Journal of Advanced Research in Computer Science*, 15(1). ISSN 2319-5991.
- [14] Peddi, S., & Narla, S. (2018). Advancing geriatric care: Machine learning algorithms and AI applications for predicting dysphagia, delirium, and fall risks in elderly patients. *International Journal of Advanced Research in Computer Science*, 6(4).