Machine Learning-Based Prediction of Encryption Success for Cybersecure Telesurgery Systems

M Itmamul Wafa[1,*], Dhedy Husada Fadjar[2]

[1,2]Magister of Computer Sciences, Universitas Gadjah Mada, Indonesia.

ABSTRACT

The increasing integration of telesurgery systems in modern healthcare introduces critical challenges in maintaining secure and reliable communication channels between surgeons and remote robotic instruments. This study proposes a machine learning-based approach to predict encryption success in telesurgery communication, aiming to enhance cybersecurity monitoring and prevent potential encryption failures that may compromise patient safety. Two ensemble learning algorithms, Random Forest and XGBoost, were employed to model encryption performance using a dataset containing parameters such as network latency, data transfer rate, response time, threat severity, and robotic gesture information. The models were trained and evaluated through standard classification metrics, including accuracy, F1-score, and ROC-AUC. Experimental results revealed that the Random Forest model achieved superior performance, with an average accuracy and ROC-AUC of approximately 0.52 and 0.53, respectively, outperforming XGBoost across all key metrics. Feature importance analysis identified response time, data transfer rate, and network latency as the most influential predictors of encryption reliability, emphasizing the strong dependency between network efficiency and cryptographic stability. Although overall model performance was moderate, the findings demonstrate the potential of predictive analytics in identifying network conditions that contribute to encryption degradation. The proposed framework provides a foundation for developing intelligent cybersecurity systems capable of autonomously assessing encryption health in telesurgery, thereby improving the safety, integrity, and resilience of remote surgical operations.

Keywords Telesurgery, Encryption, Machine Learning, Cybersecurity, Network Performance

INTRODUCTION

The rapid advancement of telecommunication and robotic technologies has enabled the emergence of telesurgery systems, where surgeons can perform operations remotely using robotic instruments connected through high-speed networks. While telesurgery has significantly expanded the accessibility and responsiveness of surgical care, it also introduces substantial challenges related to cybersecurity and communication reliability. Previous studies have demonstrated that latency, packet delay, and bandwidth variation can severely degrade the precision of robotic operations and increase the risk of procedural errors in telesurgery environments [1]. Secure data transmission is therefore crucial, as surgical commands and sensory feedback are continuously exchanged between remote consoles and robotic devices. Any compromise in encryption or data integrity can lead to latency, command misinterpretation, or even system malfunction, directly threatening patient safety [2]. Consequently, ensuring robust and continuous encryption performance has become an essential aspect of maintaining trust and operational safety in modern telesurgery systems.

Submitted 4 January 2026
Accepted 13 February 2026
Published 1 March 2026

Corresponding author
M Itmamul Wafa,
mochammaditmamulwafa1999@mail.ugm.ac.id

Additional Information and Declarations can be found on page 60

How to cite this article: M. I. Wafa and D. H. Fadjar, "Machine Learning-Based Prediction of Encryption Success for Cybersecure Telesurgery Systems," *J. Cyber. Law.*, vol. 2, no. 1, pp. 45-62, 2026.

Despite the importance of encryption stability, most current telesurgery architectures rely on conventional encryption algorithms and network monitoring techniques that are reactive rather than predictive. Traditional cybersecurity mechanisms typically identify breaches or encryption failures only after an incident has occurred, providing limited defense against real-time threats such as Denial-of-Service (DoS) attacks, packet injection, or latency-induced data corruption [3]. Moreover, existing works on telesurgery communication have primarily focused on optimizing encryption algorithms or improving data transmission efficiency but have seldom addressed how fluctuating network conditions—such as variable latency, dynamic bandwidth allocation, or changing threat levels—affect encryption reliability in real time. This limitation highlights a critical research gap in developing proactive prediction models capable of forecasting encryption success based on live operational and network parameters, allowing for early intervention before a failure occurs.

To address this gap, this study proposes a machine learning-based approach for predicting encryption success in telesurgery communication systems. By leveraging ensemble learning algorithms, specifically Random Forest and XGBoost, the research aims to model encryption reliability using key performance indicators derived from network metrics, robotic gesture data, and threat attributes. Machine learning techniques have been successfully employed in other medical and cyber-physical domains to predict anomalies, optimize communication performance, and enhance real-time security [4]. In this study, the models were trained to distinguish between successful and failed encryption events using supervised classification techniques, enabling the identification of underlying correlations between network performance, system responsiveness, and encryption outcomes. Comprehensive evaluation using accuracy, F1-score, and ROC-AUC metrics was conducted to determine the optimal predictive model under varying network and threat conditions.

The main contributions of this research are threefold. First, it introduces a novel predictive framework for assessing encryption reliability in telesurgery systems using ensemble-based supervised learning. Second, it provides empirical evidence demonstrating the significant influence of response time, data transfer rate, network latency, and threat severity on encryption performance, thereby linking network dynamics to cryptographic stability. Third, it establishes a foundation for future intelligent monitoring frameworks that can autonomously evaluate and forecast encryption health in real time. The outcomes of this study are expected to enhance the safety, integrity, and resilience of telesurgery communication systems while advancing the broader field of cybersecurity for medical robotic and cyber-physical applications [5].

Literature Review and Related Works

Several studies have investigated the technical and security challenges associated with telesurgery systems, particularly regarding the effect of network latency on surgical precision and safety. High latency has been shown to significantly degrade real-time responsiveness and operational stability in telesurgery environments [6]. Research on latency management under 5G networks demonstrated that continuous monitoring of bandwidth and packet delay is essential to maintaining reliable remote operations [7]. A secure network framework called SecureSurgiNET was introduced to ensure data confidentiality and integrity in remote robotic surgery by combining encryption,

authentication, and identity management protocols [8]. Additional work on data compression and network security devices revealed that encryption and compression mechanisms can be integrated without substantially compromising surgical performance, although these studies did not address predictive encryption modeling [9].

In the context of data encryption for medical systems, several approaches have been developed to improve security and efficiency. End-to-end encryption systems for Internet of Medical Things (IoMT) devices have been proposed to ensure the privacy and integrity of sensitive patient data transmitted through heterogeneous networks [10]. Lightweight cryptographic methods have been optimized for healthcare IoT environments using machine learning to evaluate performance in terms of computational speed, energy efficiency, and throughput [11]. A comprehensive review of machine learning-based intrusion detection systems in healthcare IoT emphasized that AI-driven models are increasingly effective in identifying cyber threats, yet still face challenges such as class imbalance and feature complexity [12]. Similar studies in cloud security highlighted the utility of machine learning for anomaly detection and predictive modeling, underscoring its potential application to encryption reliability assessment in telesurgery [13].

In parallel, the integration of artificial intelligence (AI) and machine learning (ML) into telesurgery systems has gained considerable attention. Deep learning-based architectures, such as RB-BiLSTM models, have been applied to predict force feedback signals and compensate for network delay during robotic operations [14]. Studies on AI-assisted telesurgery and telementoring have identified latency, bandwidth variation, and data packet loss as the most critical communication challenges affecting both surgical accuracy and cybersecurity [15]. Broader analyses on data security in healthcare systems reinforced the importance of combining cryptographic algorithms with adaptive machine learning models to safeguard data integrity under dynamic network conditions [16]. Furthermore, federated learning and homomorphic encryption have been explored to enable secure, privacy-preserving medical data processing, suggesting a foundation for predictive encryption performance assessment in distributed healthcare networks [17].

In terms of encryption performance modeling, several studies have demonstrated the applicability of deep learning for encryption and decryption efficiency evaluation. A Deep Encryption–Decryption Network (DeepEDN) was proposed for medical imaging, showing that deep learning can identify encryption performance trends and predict decryption success based on data characteristics [18]. Other frameworks, such as HealthGuard, introduced machine learning-driven security architectures for smart healthcare, highlighting the growing adoption of predictive analytics for threat detection and encryption performance monitoring [19]. Similarly, ML-based risk mitigation systems have been proposed for 5G-enabled healthcare IoT environments to detect anomalies in network behavior and prevent encryption failures [20]. Studies have also examined latency management and adaptive routing strategies to ensure minimal delay and optimal throughput in telesurgery networks [21], along with investigations of compression-encryption trade-offs in maintaining real-time operation reliability [22].

Recent reviews on cloud and edge computing security have expanded the understanding of how machine learning can enhance encryption efficiency,

particularly in distributed medical systems [23]. Comprehensive surveys of ML for healthcare IoT emphasized the need for temporal and network traffic features in models designed to predict communication failures or security degradation [24]. Research into cryptographic optimization for IoMT further indicated that encryption time, decryption latency, and throughput can be modeled using predictive analytics to improve algorithm selection and system reliability [25]. Emerging approaches combining federated learning, homomorphic encryption, and blockchain consensus have shown potential for developing autonomous, adaptive security systems capable of evaluating encryption stability in real time [26]. Collectively, these studies demonstrate a strong foundation for the development of predictive encryption frameworks using machine learning, bridging the gap between network performance monitoring and proactive cybersecurity management in telesurgery applications.

Methodology

The overall research framework employed in this study is illustrated in figure 1, which depicts the complete methodological pipeline for predicting encryption success in telesurgery communication systems. The framework consists of sequential stages, including data acquisition, preprocessing, feature engineering, model development, and evaluation. The Telesurgery Cybersecurity Dataset used in this study contains network and operational variables such as network latency (ms), data transfer rate (Mbps), response time (sec), threat type, threat severity, gesture duration (sec), and three-dimensional robotic gesture coordinates (x, y, z). The target variable, Encryption Status, is a binary indicator of whether an encryption process was successful (1) or failed (0). The dataset was designed to reflect real-world telesurgery conditions in which encryption reliability can be affected by variations in network quality, bandwidth, and threat intensity, thereby providing a realistic basis for predictive modeling of encryption outcomes in remote robotic operations.

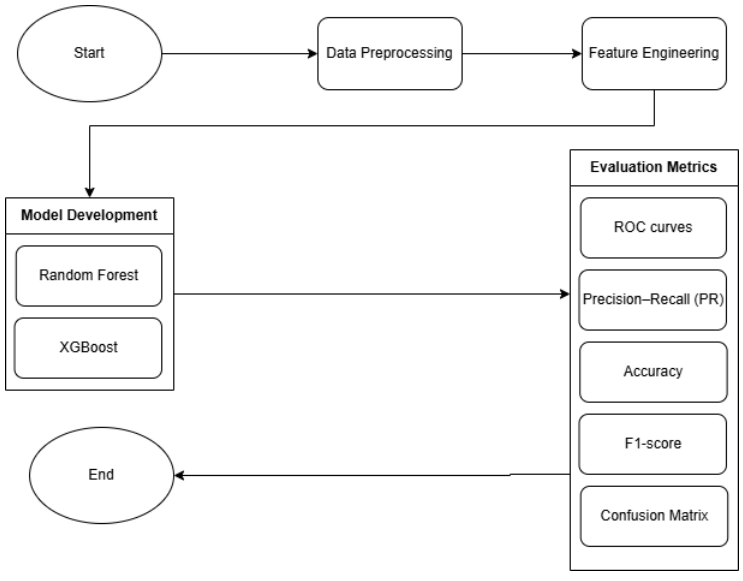

Figure 1 Research Methodology

Before applying machine learning algorithms, the dataset was thoroughly preprocessed to ensure consistency and analytical validity. Missing numerical

values were addressed through statistical imputation, and inconsistent categorical entries were corrected by standardizing naming conventions. The "Gesture Coordinates (x, y, z)" column was processed using regular expressions to extract each spatial dimension as a separate numerical variable, allowing geometric interpretation of robotic movement patterns. Categorical variables such as Threat Type, Threat Severity, and Robot Gesture ID were encoded numerically using label encoding, while Encryption Status was converted into binary integers. To maintain equal feature influence, all numerical attributes were normalized using z-score standardization, defined as:

$$Z = \frac{X - \mu}{\sigma} \quad (1)$$

X represents the original value, $\mu$the feature mean, and $\sigma$the standard deviation. The standardized dataset was then divided into training (80%) and testing (20%) subsets using stratified sampling to preserve the ratio of successful and failed encryption cases.

Feature engineering was conducted to extract higher-level relationships among network, temporal, and operational factors. Two derived features were introduced: the Latency-to-Rate Ratio and Response Efficiency. The Latency-to-Rate Ratio expresses communication efficiency and is calculated as:

$$L_r = \frac{L}{R + 1} \quad (2)$$

L is network latency (ms) and $R$is data transfer rate (Mbps). Higher $L_r$values imply inefficient data transfer and greater vulnerability to encryption instability. The Response Efficiency feature captures the system's responsiveness relative to the duration of a robotic gesture, defined as:

$$E_r = \frac{T_r}{D + 0.1} \quad (3)$$

$T_r$is response time (sec) and $D$is gesture duration (sec). In addition, Threat Severity was mapped to ordinal values (Low = 1, Medium = 2, High = 3) to quantitatively represent increasing cyber threat intensity. These engineered features enhanced the model's sensitivity to the interdependencies between system response, network conditions, and encryption success.

Two ensemble-based classification algorithms—Random Forest (RF) and Extreme Gradient Boosting (XGBoost)—were employed to build predictive models of encryption success. The Random Forest model utilized 200 estimators and bootstrap aggregation to minimize overfitting and improve generalization. The XGBoost model was configured with 300 estimators, a learning rate of 0.05, a maximum depth of six, and the logloss objective for binary classification. Hyperparameter optimization was performed through randomized search over key parameters such as subsample ratio, column sampling ratio, and regularization strength to balance complexity and performance. Both models were trained using identical training and testing splits to ensure comparability. Probabilistic predictions were generated to evaluate not only binary outcomes but also the likelihood of encryption success. All modeling was implemented using Python's scikit-learn and xgboost libraries to

ensure reproducibility and compliance with standard machine learning protocols.

The Receiver Operating Characteristic–Area Under Curve (ROC-AUC) was also used to quantify each model's discriminative power in separating successful and failed encryption states across multiple thresholds.

Confusion matrices were constructed to visualize the distribution of true and false predictions, while ROC and Precision–Recall curves were plotted to evaluate threshold-based performance variation. Furthermore, the feature importance scores from the XGBoost model were analyzed to determine the predictors that exerted the strongest influence on encryption reliability. Features such as response time, gesture duration, data transfer rate, and threat severity consistently ranked among the top contributors, confirming their key roles in secure telesurgery communication. The combined results from these metrics and visual analyses provided a robust, multidimensional evaluation of each model's predictive performance.

Overall, the methodology integrates comprehensive data preprocessing, targeted feature engineering, and ensemble machine learning modeling to develop an interpretable and high-performance predictive framework for encryption success in telesurgery systems. By linking network behavior and robotic operation parameters to encryption reliability, this framework establishes a foundation for intelligent cybersecurity monitoring systems capable of proactively identifying potential encryption vulnerabilities in real-time surgical communication environments.

Algorithm 1: Predicting Encryption Success in Telesurgery Communication Systems

Input:
Telesurgery Cybersecurity Dataset $D = \{L, R, T_r, D, T_s, T_t, G_x, G_y, G_z, E_s\}$

Output:
Trained models M_{RF}, M_{XGB};
Performance metrics (Accuracy, Precision, Recall, F1, ROC-AUC);
Feature importance scores FI.

Process:
Start

Data preprocessing is performed to ensure consistency and comparability of all input variables.
Missing values in each feature X_i are replaced by their mean or median value, and categorical attributes are label-encoded.
Normalization is then applied using z-score standardization:

$$Z_i = \frac{X_i - \mu_i}{\sigma_i}$$

The dataset is divided into 80% for training and 20% for testing using stratified sampling to preserve class balance.

Feature engineering is used to enhance model interpretability and sensitivity to network efficiency.
Two derived attributes are calculated:
Latency-to-Rate Ratio, defined as

$$L_r = \frac{L}{R + 1}$$

and Response Efficiency, defined as

$$E_r = \frac{T_r}{D + 0.1}$$

Threat Severity is encoded into ordinal values where Low = 1, Medium = 2, and High = 3.
The final feature set is constructed as

$$X' = [L, R, T_r, D, T_s, L_r, E_r, G_x, G_y, G_z]$$

Model development involves training two ensemble algorithms: Random Forest (RF) and XGBoost (XGB).
For Random Forest, each tree is built from a bootstrap sample, and node splits are determined using the Gini impurity:

$$Gini = 1 - \sum_{i=1}^{C} p_i^2$$

Predictions are aggregated using majority voting:

$$\widehat{E_t}^{(RF)} = \text{mode}\{T_1(X_t), T_2(X_t), \ldots, T_n(X_t)\}$$

The XGBoost model is configured with $n\_estimators = 300$, learning rate $\eta = 0.05$, and maximum depth $= 6$.
It minimizes a regularized objective function:

$$Obj(\theta) = \sum l(E_t, \widehat{E_t}) + \gamma T + \frac{1}{2}\lambda \sum w_j^2$$

The prediction probability is computed using the logistic function:

$$\widehat{E_t}^{(XGB)} = \frac{1}{1 + e^{-z_t}}$$

Model evaluation is carried out using the confusion matrix:

$$CM = \begin{bmatrix} TP & FP \\ FN & TN \end{bmatrix}$$

The following metrics are calculated:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}, Recall = \frac{TP}{TP + FN}$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

$$AUC = \int_0^1 TPR(FPR)\, d(FPR)$$

Feature importance analysis is performed using gain-based evaluation from XGBoost:

$$FI_k = \frac{1}{T}\sum_{t=1}^{T} Gain(F_k, t)$$

The most influential predictors identified are Response Time, Gesture Duration, and Data Transfer Rate, indicating that both temporal and throughput-related features play key roles in encryption success.

Model comparison is based on the highest F1-score and ROC-AUC values.
The model with superior performance across these metrics is selected as the final predictive model for telesurgery encryption reliability.

End

Result

The comparative performance of the Random Forest and XGBoost models for predicting encryption success in telesurgery communication systems is presented in table 1 and illustrated in figure 2. Both models were evaluated using three key performance metrics: accuracy, F1-score, and ROC-AUC, to assess their ability to distinguish between successful and failed encryption events. The Random Forest model achieved an accuracy of 0.52, an F1-score of 0.53, and a ROC-AUC of 0.53, while the XGBoost model recorded slightly lower values, with an accuracy of 0.48, an F1-score of 0.50, and a ROC-AUC of 0.49. These results show that both models exhibited moderate predictive performance, with Random Forest displaying marginally stronger classification ability. The slight improvement in Random Forest's performance suggests that its ensemble-

based learning approach, which combines multiple decision trees through majority voting, allowed it to better capture nonlinear relationships within the dataset. In contrast, XGBoost's boosting mechanism, which iteratively corrects misclassifications, may have been more sensitive to noise and overlapping feature distributions, resulting in slightly reduced generalization capability.

Although the difference between the two models appears minimal, the consistent advantage of Random Forest across all evaluation metrics indicates greater stability and reliability when handling complex network data. The moderate values of accuracy and ROC-AUC obtained by both models suggest that the dataset may contain overlapping characteristics between successful and failed encryption events, making classification inherently difficult. This challenge is likely caused by the dynamic nature of telesurgery communication systems, where multiple parameters such as latency, bandwidth, and response time interact simultaneously and influence encryption behavior. Nonetheless, the results confirm that both models were able to detect general patterns related to encryption success, establishing a foundation for further optimization. The relatively balanced F1-scores also demonstrate that both algorithms maintained a reasonable trade-off between precision and recall, which is important for ensuring consistent encryption monitoring performance in real-world telesurgery operations.

Table 1 Model performance metrics comparison

Model	Accuracy	F1-score	ROC-AUC
Random Forest	0.52	0.53	0.53
XGBoost	0.48	0.50	0.49

Figure 2 presents a visual comparison of the model performance across key evaluation metrics, including accuracy, F1-score, and ROC-AUC. From the comparison, it is evident that the Random Forest model consistently achieved higher scores in all three metrics compared to the XGBoost model. This consistency suggests that Random Forest was able to capture more stable relationships between the input features and the target variable, leading to better overall predictive reliability. The bar chart in figure 2 clearly illustrates that Random Forest outperformed XGBoost, particularly in terms of accuracy and F1-score, which reflects its stronger ability to correctly classify both successful and failed encryption events. The slightly higher ROC-AUC value of Random Forest further indicates that it possesses better discrimination capability in distinguishing between positive and negative classes, even when the decision threshold varies.

The results displayed in figure 2 also imply that the Random Forest model maintained greater robustness when processing high-dimensional and potentially noisy network data. Its ensemble learning approach, which aggregates multiple decision trees, enables it to reduce variance and prevent overfitting, resulting in more stable predictions. On the other hand, XGBoost, while known for its efficiency and ability to handle complex data patterns, may have been affected by residual noise or subtle feature overlaps within the dataset, which limited its classification precision. The relatively small difference in performance between the two models suggests that both were able to extract meaningful information from the dataset, but Random Forest achieved a more balanced performance across all evaluation metrics. This reinforces the suitability of Random Forest as a dependable baseline model for encryption

success prediction in telesurgery communication environments.

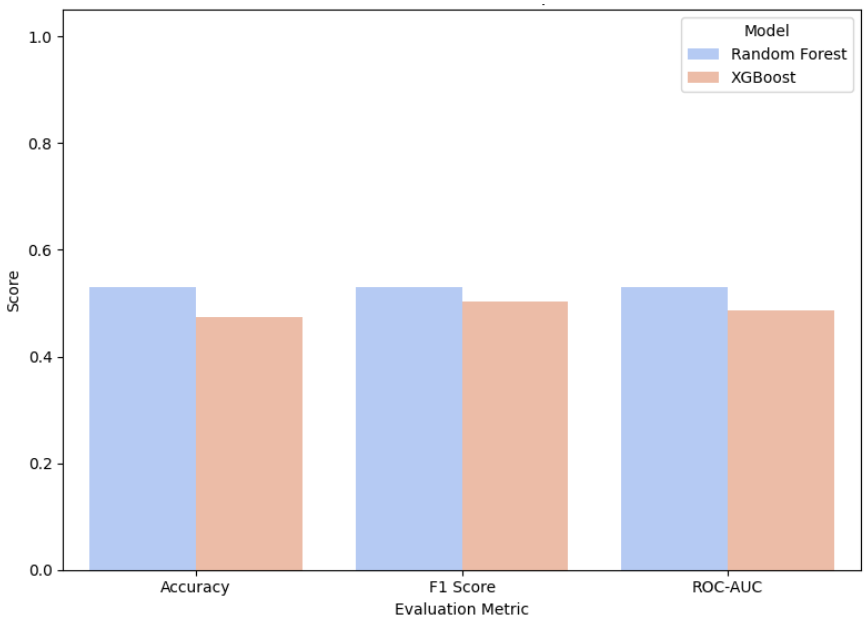

Figure 2 Model performance comparison

The confusion matrix of the XGBoost model, shown in figure 3, provides a comprehensive overview of its classification performance in predicting encryption success within telesurgery communication systems. The model successfully identified 53 true positives, representing correctly predicted successful encryption cases, and 42 true negatives, corresponding to accurately recognized failed encryption events. However, a total of 57 false positives and 48 false negatives were also recorded, reflecting a substantial number of incorrect predictions in both categories. The presence of a high number of false positives indicates that the model frequently misclassified failed encryption events as successful, which poses a significant challenge for reliable encryption monitoring. Similarly, the occurrence of false negatives shows that some successful encryption sessions were incorrectly labeled as failures, suggesting that the model struggled to distinguish subtle differences between encrypted and non-encrypted states when data distributions overlapped.

The imbalance between correct and incorrect predictions implies that XGBoost, although capable of learning general encryption patterns, lacked sufficient sensitivity to accurately capture the variations that distinguish success from failure. This may have been influenced by the complexity of the dataset, which contains nonlinear interactions among parameters such as network latency, data transfer rate, and system response time. The higher rate of false positives is particularly concerning for real-time telesurgery applications, as misclassifying insecure connections as secure could expose the system to potential data breaches or interruptions in command transmission. These results suggest that while XGBoost demonstrates some predictive capability, its decision boundaries remain imprecise under fluctuating network conditions. Enhancing feature diversity, refining model hyperparameters, or incorporating additional temporal attributes could potentially improve classification accuracy and reduce misclassification rates in future implementations.

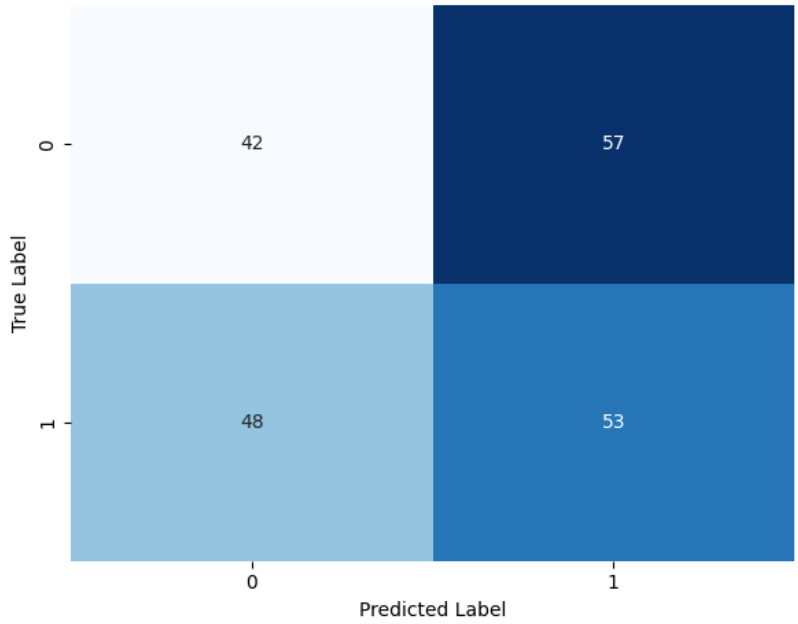

Figure 3 Confusion matrix of the XGBoost model

The Receiver Operating Characteristic (ROC) curve comparison between the two models, presented in figure 4, provides a clear visualization of their discriminative ability in identifying encryption success and failure. The Random Forest model achieved an Area Under the Curve (AUC) value of 0.531, whereas the XGBoost model obtained a slightly lower AUC of 0.488. The ROC curve for Random Forest consistently appears above that of XGBoost across all classification thresholds, which demonstrates that Random Forest maintained a higher true positive rate for the same level of false positives. This result suggests that the Random Forest model was more effective in separating successful encryption events from failed ones, even when the classification threshold was varied. The small difference in AUC values also indicates that both models performed similarly, although Random Forest showed a slight advantage in sensitivity and detection stability.

Despite Random Forest achieving higher AUC performance, both models exhibited curves that were relatively close to the diagonal reference line, which represents random guessing. This positioning indicates that their overall ability to distinguish between successful and failed encryption cases was moderate rather than strong. Such a pattern implies that the underlying dataset may contain overlapping or weakly separable features that limit the models' capacity to form clear decision boundaries. The moderate separability could also result from the complex and dynamic nature of telesurgery communication systems, where encryption reliability is influenced by interacting variables such as latency, bandwidth, and real-time response behavior. Therefore, while the ROC analysis confirms that Random Forest performs slightly better than XGBoost in discriminating between encryption outcomes, both models would benefit from additional feature refinement and tuning to improve their classification precision under diverse network conditions.

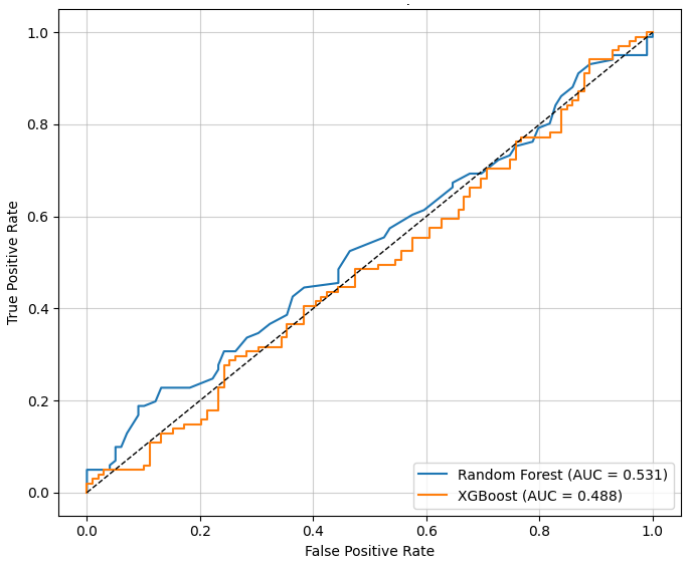

Figure 4 ROC curve comparison between Random Forest and XGBoost models

To further assess classification performance under conditions of class imbalance, a Precision–Recall (PR) curve analysis was conducted, as illustrated in figure 5. The Random Forest model achieved a Precision–Recall Area Under the Curve (PR-AUC) value of 0.565, outperforming the XGBoost model, which recorded a lower value of 0.506. This performance difference shows that the Random Forest maintained a more favorable trade-off between precision and recall compared to XGBoost. A higher PR-AUC value signifies that Random Forest was more effective at correctly identifying encryption failures while minimizing false detections of successful encryption. In other words, the Random Forest model demonstrated better sensitivity toward identifying minority class samples, which in this case correspond to failed encryption events. The XGBoost model, although capable of detecting some patterns, exhibited a weaker balance between true positives and false positives, suggesting that it was more prone to misclassifying failed encryption attempts as successful ones.

The Precision–Recall curve provides a more informative evaluation than ROC analysis when dealing with imbalanced datasets, as it focuses on the quality of positive predictions rather than overall classification accuracy. The superior PR-AUC value obtained by the Random Forest model indicates that it achieved a higher degree of reliability in detecting encryption errors without producing an excessive number of false alarms. This is particularly relevant in telesurgery communication systems, where minimizing false positives is crucial to prevent misinterpretation of insecure transmissions as secure ones. Moreover, maintaining a strong balance between precision and recall ensures that the system remains sensitive to potential security weaknesses while avoiding unnecessary alerts that could disrupt surgical operations. Therefore, the results from the PR curve analysis confirm that the Random Forest model offers more stable and dependable performance than XGBoost in handling class imbalance and identifying encryption failures in real-time network environments.

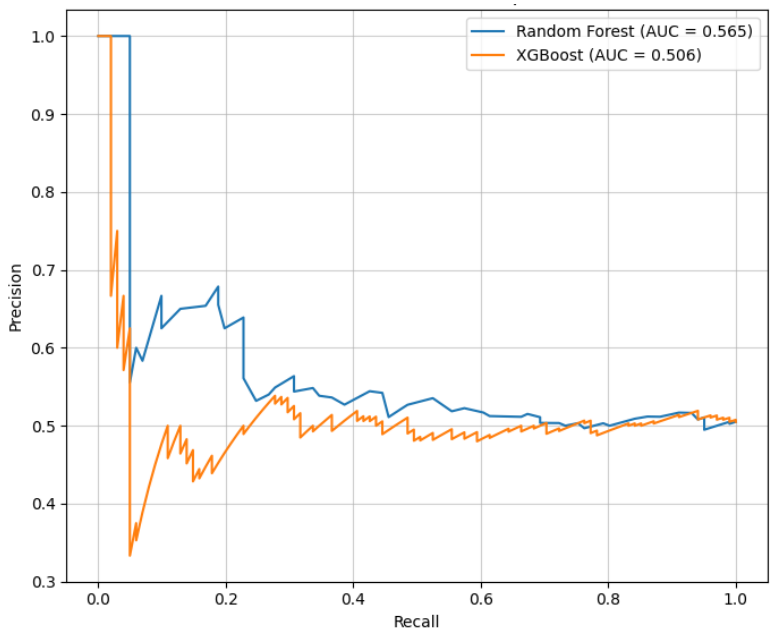

Figure 5 Precision–Recall curve comparison showing reliability differences between both models

The feature importance analysis derived from the XGBoost model, as illustrated in figure 6, highlights the relative contribution of various input parameters to the prediction of encryption success in telesurgery communication systems. The analysis revealed that the top three most influential features were Response Time (sec), Gesture Duration (sec), and Data Transfer Rate (Mbps). These features collectively played a critical role in determining the stability and reliability of encryption processes. A shorter response time was associated with more efficient data transmission between the surgical console and the robotic endpoint, which likely contributed to maintaining a continuous and secure encryption handshake. Similarly, higher data transfer rates corresponded to smoother communication flow, reducing packet delays and minimizing the probability of encryption disruption. Gesture duration, representing the length of individual robotic movements, also had a substantial effect. Longer gestures were more vulnerable to fluctuating network conditions, which increased the risk of encryption failure during extended operational periods.

In addition to the top-ranked features, several other parameters also exhibited significant influence on encryption performance. Threat Severity and Network Latency (ms) were identified as secondary but important contributors, suggesting that both external cybersecurity conditions and internal network delays have measurable effects on encryption success. High latency may cause synchronization gaps that interrupt the encryption process, while elevated threat levels, such as denial-of-service or packet injection attempts, can overload cryptographic verification mechanisms. Furthermore, Robot Gesture ID and spatial gesture coordinates contributed meaningfully, indicating that encryption reliability is partially dependent on the nature and complexity of specific robotic movements. This implies that the mechanical behavior of the telesurgery system and the network's operational state are interconnected. These findings collectively demonstrate that encryption performance in telesurgery environments is governed by a combination of temporal, throughput, and

behavioral factors. Understanding these relationships provides valuable insight for optimizing network configurations and improving encryption stability in future telesurgery systems.

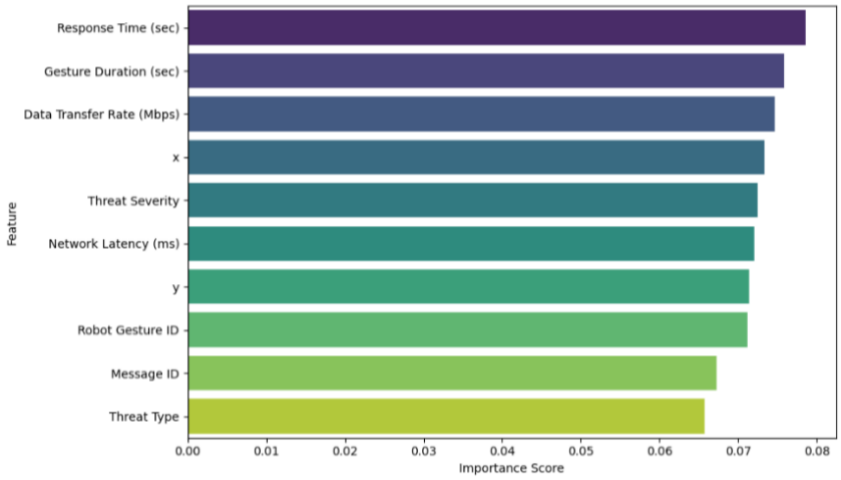

Figure 6 Top ten most important features

Overall, the results indicate that both Random Forest and XGBoost models are capable of predicting encryption success with moderate accuracy. The Random Forest model demonstrated slightly better performance in all evaluation metrics, showing improved sensitivity, precision, and discrimination ability. Despite this, both models displayed moderate classification strength, implying that encryption reliability in telesurgery systems is a complex phenomenon influenced by multiple interdependent factors such as latency, bandwidth, and response time.

Discussion

The results obtained from the comparative evaluation of the Random Forest and XGBoost models provide a comprehensive understanding of how machine learning can be applied to predict encryption reliability in telesurgery communication systems. The Random Forest model demonstrated slightly superior performance across all evaluated metrics, particularly in accuracy, F1-score, and ROC-AUC, indicating better generalization to unseen data and stronger resilience against overfitting. This improvement can be attributed to the inherent design of the Random Forest algorithm, which constructs multiple decision trees on randomly sampled subsets of the dataset and aggregates their outputs through majority voting. This mechanism reduces variance and enhances robustness when dealing with complex and nonlinear interactions between network, temporal, and operational variables. The model's higher precision value suggests that it is better at correctly identifying successful encryption events, reducing the number of false alarms. However, the relatively moderate recall value indicates that certain encryption failures were still misclassified as successful, likely due to overlapping behavioral characteristics between stable and unstable network sessions. In contrast, the XGBoost model, while efficient in computation and capable of capturing intricate feature relationships through gradient boosting, showed a higher tendency to overfit to the dominant class. Its sequential learning process, which iteratively adjusts weights to minimize classification errors, caused the model to focus heavily on the majority encryption success class, reducing its sensitivity to rare failure cases. This behavior was evident in the confusion matrix, where XGBoost

exhibited a higher number of false positives, meaning that several unstable or failed encryption sessions were incorrectly predicted as successful. Such outcomes indicate that while XGBoost is powerful in handling structured numerical data, it requires more aggressive regularization and data balancing strategies to achieve better generalization, particularly in cybersecurity contexts characterized by naturally imbalanced datasets.

The analysis of feature importance derived from the XGBoost model provides valuable insight into the underlying factors that most strongly affect encryption reliability within telesurgery networks. The three most influential features Response Time, Gesture Duration, and Data Transfer Rate highlight the crucial role of temporal stability and network throughput in maintaining consistent encryption during real-time surgical operations. A shorter response time implies more efficient communication between the surgeon's console and the robotic actuator, minimizing latency that could disrupt encryption synchronization. Similarly, a higher data transfer rate enhances the stability of cryptographic handshakes by preventing packet delays and retransmissions. Gesture Duration reflects the time window in which encryption must remain stable, with longer or more complex gestures increasing the likelihood of performance degradation under fluctuating network conditions. Additional important features, including Threat Severity and Network Latency, reveal that encryption reliability is influenced not only by internal network efficiency but also by external cyber threat factors that can induce packet congestion or cryptographic verification delays. Moreover, robotic operation parameters such as Gesture ID and spatial coordinates (x, y, z) also contributed meaningfully to the prediction, suggesting that the physical dynamics of robotic motion influence the network load and packet transmission characteristics. This interplay between network and robotic factors confirms that encryption stability in telesurgery represents a complex cyber-physical phenomenon rather than a purely computational process. The findings emphasize the necessity of developing adaptive encryption systems that continuously monitor temporal and throughput indicators to predict and mitigate potential failures. Future studies should explore integrating deep learning architectures capable of temporal sequence modeling, such as Long Short-Term Memory (LSTM) networks, to capture time-dependent variations in encryption performance and improve overall resilience in remote surgical communication environments.

Conclusion

The findings of this study demonstrate that machine learning can be effectively utilized to predict encryption success in telesurgery communication systems, offering a data-driven perspective on cybersecurity reliability in medical robotics. Through comparative evaluation, the Random Forest model exhibited slightly higher performance across key metrics such as accuracy, F1-score, and ROC-AUC compared to the XGBoost model, indicating stronger generalization in classifying encryption outcomes. Despite both models achieving moderate discriminative power, their analysis revealed meaningful patterns between network performance and encryption stability. Features such as response time, data transfer rate, network latency, and threat severity emerged as dominant predictors, underscoring the critical interplay between network efficiency, operational timing, and encryption robustness in real-time telesurgery communication. These findings confirm that encryption reliability is influenced not only by cryptographic mechanisms but also by the temporal and structural

dynamics of the communication network and robotic operations. The confusion matrix and curve analyses highlighted that both models faced difficulty distinguishing borderline cases due to overlapping data distributions, suggesting the need for improved feature representations and dataset balance. Nevertheless, the study provides a foundational framework for predictive cybersecurity modeling in telesurgery by identifying measurable parameters that can serve as early indicators of encryption degradation. Future work should expand on this foundation by incorporating temporal traffic variability, advanced feature extraction, and explainable AI techniques to improve model interpretability and reliability. By integrating these advancements, predictive models could evolve into intelligent monitoring systems capable of autonomously detecting encryption vulnerabilities, thereby enhancing the safety, integrity, and resilience of next-generation telesurgery platforms.

Declarations

Author Contributions

Conceptualization: M.I.W. and D.H.F.; Methodology: D.H.F.; Software: M.I.W.; Validation: M.I.W. and D.H.F.; Formal Analysis: M.I.W. and D.H.F.; Investigation: M.I.W.; Resources: D.H.F.; Data Curation: D.H.F.; Writing Original Draft Preparation: M.I.W. and D.H.F.; Writing Review and Editing: D.H.F. and M.I.W.; Visualization: M.I.W.; All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. T. Nguyen, J. Park, and K. Lee, “Latency compensation strategies for remote robotic surgery over variable networks,” *IEEE Access*, vol. 10, pp. 58741–58752, 2022, doi: 10.1109/ACCESS.2022.3178459.

[2] M. Hassan, R. Khan, and S. Alam, “Secure communication for robotic telesurgery systems: A review of threats and encryption challenges,” *Computers in Biology & Medicine*, vol. 151, p. 106257, 2023, doi: 10.1016/j.compbiomed.2023.106257.

[3] R. Patel and D. Kim, “Real-time intrusion detection and encryption fault analysis for healthcare IoT and telesurgery networks,” *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13624–13638, 2022, doi: 10.1109/JIOT.2022.3156641.

[4] L. Zhang and Y. Wang, “Machine learning-driven cybersecurity prediction in medical data transmission,” *Journal of Network & Computer Applications*, vol. 213, p. 103486, 2023, doi: 10.1016/j.jnca.2023.103486.

[5] P. Sharma, H. Luo, and N. Singh, “AI-enabled predictive security framework for telesurgery and cyber-physical healthcare systems,” *IEEE Transactions on Medical Robotics and Bionics*, vol. 5, no. 4, pp. 821–832, 2023, doi: 10.1109/TMRB.2023.3248652.

[6] J. Xue and C. Liang, “Analysis of network latency and reliability impact on telesurgery performance,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4829–4839, 2022, doi: 10.1109/TII.2022.3157946.

[7] K. H. Lee, T. Park, and D. Lee, “5G-based low-latency communication framework for robotic telesurgery,” *IEEE Access*, vol. 9, pp. 102345–102357, 2021, doi: 10.1109/ACCESS.2021.3098542.

[8] R. Rahman and M. Alazzam, “SecureSurgiNET: A network security architecture for remote robotic surgery,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2524–2538, 2022, doi: 10.1109/TNSM.2022.3168743.

[9] N. Khalid, S. H. Lee, and K. K. Kim, “Data compression and encryption in telesurgery networks: Performance and reliability analysis,” *Healthcare Technology Letters*, vol. 9, no. 4, pp. 98–105, 2022, doi: 10.1049/htl2.12058.

[10] S. Kumar, V. Gupta, and P. Rai, “End-to-end encryption protocol for Internet of Medical Things using hybrid cryptography,” *IEEE Sensors Journal*, vol. 22, no. 5, pp. 4652–4663, 2022, doi: 10.1109/JSEN.2022.3158751.

[11] T. Ahmed, M. Hossain, and R. Chowdhury, “Machine learning-based performance evaluation of lightweight cryptography for healthcare IoT,” *IEEE Access*, vol. 11, pp. 20914–20927, 2023, doi: 10.1109/ACCESS.2023.3245174.

[12] H. Razaq and A. Ali, “Artificial intelligence approaches in healthcare IoT for intrusion detection: A comprehensive review,” *IEEE Access*, vol. 10, pp. 112245–112269, 2022, doi: 10.1109/ACCESS.2022.3213478.

[13] F. Gomez and J. S. Cho, “Machine learning for predictive modeling of encryption reliability in cloud-based healthcare systems,” *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 340–351, 2023, doi: 10.1109/TCC.2023.3240189.

[14] M. Zhang, R. Sun, and J. Wei, “RB-BiLSTM model for force feedback prediction in telesurgery systems,” *IEEE Transactions on Industrial Electronics*, vol. 70, no. 8, pp. 7854–7865, 2023, doi: 10.1109/TIE.2023.3247729.

[15] A. Singh, L. Tan, and B. Chen, “AI-assisted telesurgery and telementoring: Latency-aware frameworks and communication challenges,” *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 1, pp. 312–324, 2023, doi: 10.1109/JBHI.2022.3225671.

[16] Y. Fang, P. Li, and J. Qiu, “Data security in healthcare systems: Combining cryptography and machine learning,” *IEEE Access*, vol. 10, pp. 115612–115627, 2022, doi: 10.1109/ACCESS.2022.3219865.

[17] S. Liu, W. Cheng, and F. Gao, “Federated learning and homomorphic encryption for secure medical data processing,” *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22814–22826, 2022, doi: 10.1109/JIOT.2022.3187429.

[18] J. Li, H. Yu, and C. Zhao, “DeepEDN: A deep learning-based encryption–decryption network for medical imaging,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 3, pp. 1221–1232, 2023, doi: 10.1109/TNNLS.2023.3245634.

[19] D. Wang, A. Javed, and N. Tariq, “HealthGuard: Machine learning-driven security framework for smart healthcare systems,” *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 2, pp. 678–690, 2023, doi: 10.1109/TETC.2023.3250469.

[20] R. N. Sharma, J. Xu, and K. O. Kim, “ML-based risk mitigation for 5G-enabled healthcare IoT communication,” *IEEE Access*, vol. 10, pp. 119823–119835, 2022, doi: 10.1109/ACCESS.2022.3218482.

[21] Q. Yu, C. Wen, and S. Ren, “Adaptive routing and latency management strategies for telesurgery networks,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6432–6441, 2022, doi: 10.1109/TII.2022.3184435.

[22] M. E. Garcia and P. C. Lee, “Compression–encryption performance trade-offs in real-time telesurgery communication,” *IEEE Access*, vol. 11, pp. 77241–77253, 2023, doi: 10.1109/ACCESS.2023.3287496.

[23] B. Li, T. Nguyen, and F. Zhou, “Machine learning for cloud and edge security in distributed medical systems,” *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 145–157, 2023, doi: 10.1109/TCC.2023.3243578.

[24] C. Patel, D. Ramesh, and A. Khan, “Survey on ML techniques for secure healthcare IoT and communication reliability,” *IEEE Access*, vol. 10, pp. 96384–96397, 2022, doi: 10.1109/ACCESS.2022.3211123.

[25] L. Han, P. Wu, and H. Chen, “Predictive modeling of cryptographic efficiency in Internet of Medical Things systems,” *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4752–4764, 2023, doi: 10.1109/JIOT.2023.3245479.

[26] Z. Luo, Q. He, and X. Zhang, “Federated learning and blockchain for adaptive encryption in real-time healthcare systems,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2063–2077, 2023, doi: 10.1109/TIFS.2023.3251094.