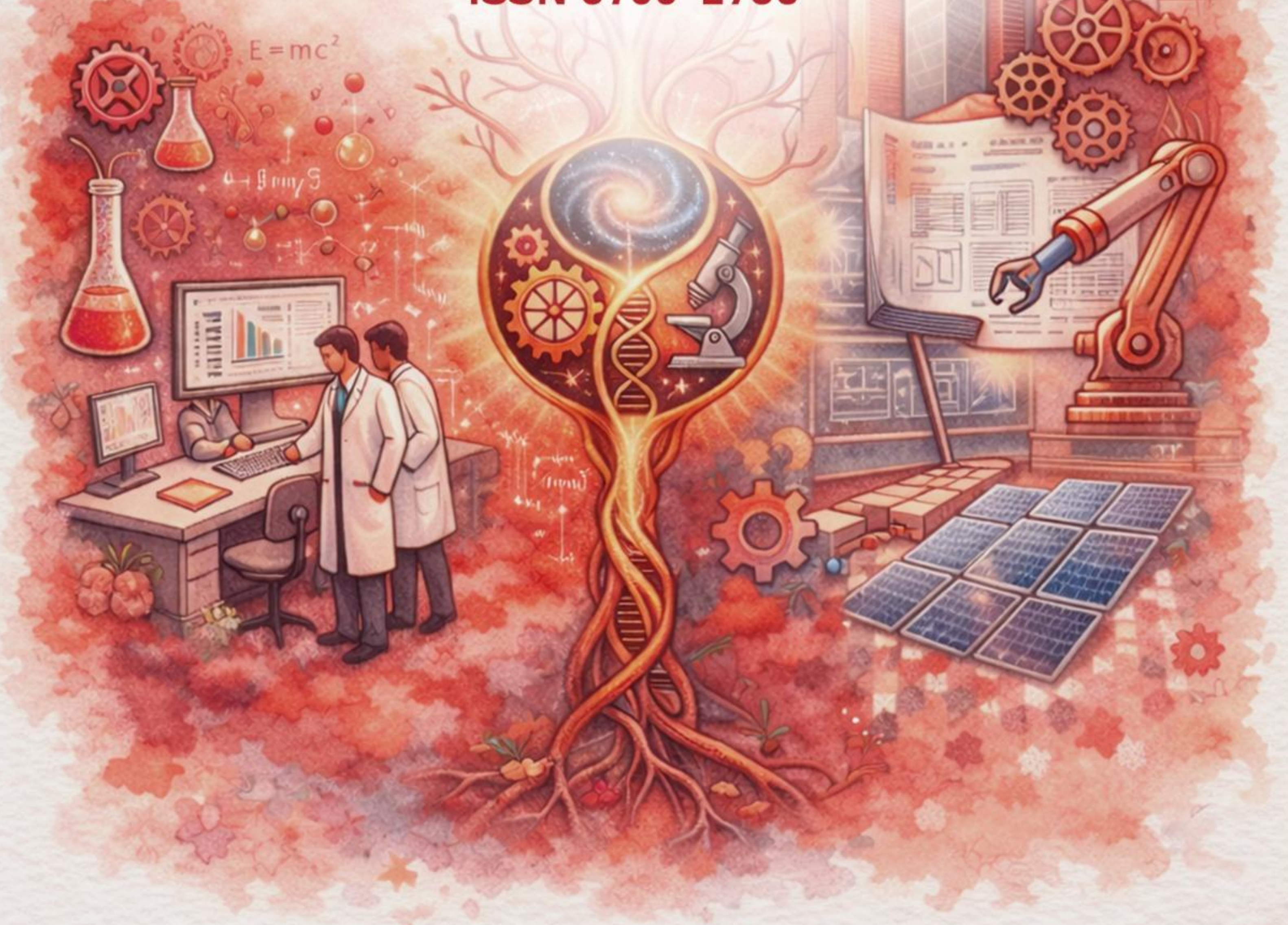
Stardom University

Stardom Scientific Journal of Natural and Engineering Sciences

- Stardom Scientific Journal of Natural and Engineering Sciences -
Peer Reviewed Scientific Journal published twice
a year by Stardom University
1st issue- 4th Volume 2026
ISSN 3756-2980



Stardom Scientific Journal of Natural and Engineering Sciences
Peer Reviewing Committee

Integrating AI Techniques with Cybersecurity Solutions to Build a Smart Diabetic Care System

Res. Maha Abdo Osman Mohamed

(Maha.2560524@std.stardomuniversity.edu.eu)

Dr. Khalid Hamid Bilal

(khalidhamidk9@gmial.com)

Abstract

Diabetes mellitus is one of the most global health challenges, needing early detection and effective management to reduce long-term issues. Artificial intelligence (AI) techniques have shown promising capabilities in predicting diabetes using structured medical data, but most studies have focused on improving predictive accuracy while neglecting cybersecurity (CS) and patients' data protection.

This study suggests an integrated framework that combines machine learning(ML) with cybersecurity (CS) mechanisms. The proposed framework combines AES-256-GCM encryption, SHA-256 integrity verification, and pseudonymization, along with anomaly detection using the Isolation Forest (IF)algorithm to improve data quality.

The model was tested on Pima Indians Diabetes Dataset in three stages: before the integration of cybersecurity (CS), after the integration, after the removal of outliers. Results showed accuracy improving from 74.68% to 82.88%, with ROC-AUC being stable at 0.82–0.84.

The novelty of this study is adding a cybersecurity (CS) layer with a data quality improvement in a unified pipeline, strengthening model reliability. These facts show that achieving a balance between predictive accuracy, data quality, and cybersecurity (CS) is crucial for developing trustworthy AI-based medical systems that will work for real-world healthcare systems.

Keywords: Diabetes prediction (DP), Artificial Intelligence (AI), Cybersecurity (CS), Differential Privacy (DP), Encryption, Random Forest (RF), Health Data Protection, Anomaly Detection, ROC-AUC.

Abbreviation

AI Artificial Intelligence

ML Machine Learning

RF Random Forest

DP Differential Privacy

AES Advanced Encryption Standard

AES-256-GCM Advanced Encryption Standard (256-bit) – Galois/Counter Mode

SHA-256 Secure Hash Algorithm 256-bit

IF Isolation Forest

ROC Receiver Operating Characteristic

AUC Area Under the Curve

ROC-AUC Area Under the Receiver Operating Characteristic Curve

E2EE End-to-End Encryption

SVM Support Vector Machine

CNN Convolutional Neural Network

CGM Continuous Glucose Monitoring

NLP Natural Language Processing

API Application Programming Interface

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

TN True Negative

TP True Positive

FN False Negative

FP False Positive

1. Introduction

Chronic diseases- most notably diabetes mellitus—represent one of the most pressing global health challenges of the twenty-first century, affecting hundreds of millions of individuals worldwide and imposing an escalating burden on healthcare systems and national economies [8]. Owing to its complex nature, diabetes requires continuous monitoring, early diagnosis, and timely therapeutic intervention to reduce long-term complications and improve patients' quality of life.

Recently, the healthcare sector went through a rapid digital transformation driven by advances in artificial intelligence (AI), which has become a powerful tool for analyzing large volumes of medical data and supporting clinical decision-making [6]. Machine learning (ML) algorithms, such as Random Forest (RF) and neural network–based models, have proved strong capabilities in predicting diabetes using structured clinical data [26] [25]. These models enable the extraction of meaningful patterns from patient datasets, thereby providing for early detection and risk [20] [23].

Despite these improvements, combining AI into healthcare systems introduces significant cybersecurity (CS) challenges. Medical data are among the most sensitive categories of information and weak to a wide array of threats, including data poisoning attacks, input manipulation, data breaches, and re-identification risks [10]. Such threats can compromise patient privacy and undermine the reliability of predictive models, potentially leading to incorrect medical decisions.

Current literature shows that most AI-driven medical studies focus mainly on improving predictive accuracy while overlooking critical facets of security and privacy [19]. This gap limits the practical placement of such systems in real-world environments. A clear research gap emerges from treating AI and cybersecurity as separate domains, resulting in systems that are either highly accurate but insecure or secure yet inferior in performance.

The objective of this study is intended to fill the gap by proposing an integrated framework that combines machine learning(ML) techniques with cybersecurity (CS)mechanisms for diabetes prediction. The framework requires reliable predictive performance while maintaining data confidentiality, integrity and privacy throughout all stages of processing.

The scientific contribution of this research is to embed a comprehensive cybersecurity(CS) layer into the machine learning (ML) pipeline including data protection techniques and abnormality detection techniques to improve data quality. Moreover, this study provides a powerful set of evaluation metrics like accuracy, precision, recall, F1-score, and ROC-AUC for a more balanced and realistic judgment in the presence of imbalanced medical datasets [22] [24].

This study differs from the conventional methods that only emphasize improving the performance indicators. It emphasizes the importance of balancing predictive accuracy, data security and model strength. By analyzing the interaction between data quality, protection mechanisms, and model action, the study helps to gain a deep understanding of how to improve trustworthy AI systems for healthcare applications.

The study is divided into the following parts: Section 2 discusses the related work. Section 3 outlines the methodology. Section 4 experimental results. Section 5 discussion of the findings, recommendations and directions for future work.

2. Literature Review

Recent research on diabetes prediction has provided clear diversity in methodological approaches, from advanced artificial intelligence (AI)models to low-cost techniques, connected medical systems, and traditional data mining algorithms. Several studies have focused on deep learning (DL) models—or convolutional neural networks (CNNs)—which rely on high-quality medical data and have shown strong diagnostic performance in experimental settings [15] [22]. But their need to complex base and sensitive datasets limits their applicability in resource-constrained environments, and most of these studies have not incorporated effective mechanisms for data protection or lifelong security [10] [19].

While the other research has explored the use of voice analysis and behavioral data as low-cost tools for early diabetes detection [13] [1]. While these approaches are accessible and easy to use, they often lack accuracy in comparison to more advanced models and raise some concerns about the privacy and protection of biometric data [2] [14].

A further and a new line of work has checked continuous glucose monitoring (CGM) systems, which provide real-time data that helps on disease management [18] [24]. But, despite their clinical value, the constants dependence on these systems and on connected devices and wireless networks exposes them to cybersecurity (CS) risks, such as data exposure or manipulation [5] [10]. This highlights the need for strong security in transmission, storage and processing of data [7] [3].

Overall, traditional data mining algorithms such as J48 and Random Forest (RF) continue to be widely used due to their suitability for structured medical datasets [9] [12]. Although these models often provide good to excellent performances, they are still very sensitive to noisy or abnormal data, especially in the absence of anomaly detection or data integrity assurance mechanisms [16] [11].

Comparison Between Previous Studies and the Current Study

Table 1

Study \approach	Type of data used	Technique \model	strength	Limitation \weaknesses	Cybersecurity aspect	Position of the current study
CNN-based ultrasound study	Advanced biomedical data based on high-frequency ultrasound	Convolutional neural networks (CNN)	High diagnostic accuracy, strong ability to extract complex patterns	Require specialized equipment and advanced technical infrastructure; limited scalability in routine practice	Cybersecurity was not considered a core component of system design	The current study differs by using structured clinical data that is more practical, while integrating a comprehensive cybersecurity layer
Voice-based diabetes detection study	Audio recording collected via smartphones	Machine learning models for voice feature analysis	Low cost, widely accessible, suitable for preliminary screening	Moderate accuracy; results may be affected by external factors; sensitivity of biometric data	Significant privacy risks related to voice data and identity recognition	The current study outperforms by emphasizing data privacy, integrity, and secure prediction
Continuous glucose monitoring (CGM) studies	Real-time continuous monitoring and analytical system	Continuous monitoring and analytical system	Real-time tracking and clinical decision support	Dependence on connected devices requires infrastructure and a relatively high cost	Vulnerable to communication threats such as data interception and manipulation	The current study is less dependent on connected devices and focuses more on securing data lifecycle within the system
J48 and traditional data mining approaches	Structured medical data	J48 and data mining algorithms	Interpretable, fast execution, suitable for structured datasets	Sensitive to data quality and noisy inputs; vulnerable to data contamination or manipulation	Typically lacks integrated cybersecurity mechanisms	The current study shares the use of structured data but differs by incorporating a security layer and anomaly detection mechanisms
Current study	Pima Indians diabetes (768 records, 9 features)	Random forest with a secure processing pipeline	Balanced performance and practical applicability; integration of cybersecurity with machine learning	Limited by dataset size and population specificity	Includes AES-256-GCM encryption, SHA-256 integrity verification, pseudonymization, simplified differential privacy, anomaly detection, and audit logging	Provide a comprehensive contribution by combining diabetes prediction, data protection, and performance improvement through anomaly removal

Research Gap

Most current studies focus on improving accuracy while neglecting the integration of cybersecurity (CS) and patients' data safety. These aspects are often treated as separate issues without analyzing their combined impact on a model's performance. This resulted in a gap in developing unified, secure, and reliable predictive systems, particularly in the context of imbalanced medical datasets.

Research Contributions

Suggesting a unified multi-layered base that integrates data preprocessing, cybersecurity (CS) mechanisms, and predictive modeling in a single system.

1-Combining advanced cybersecurity (CS) techniques, like AES-256-GCM encryption, SHA-256 integrity verification, and pseudonymization, to ensure data protection.

2-Adding the Isolation Forest (IF)algorithm to improve data quality and strengthen the stability of the predictive software.

3-Testing models by using more than one metric, like Accuracy, Precision, Recall, F1-score, and ROC-AUC.

4-Analyzing the impact of cybersecurity (CS) integration and improved data quality on model performance.

5-Showing that the synergy between cybersecurity (CS)and data quality improvement contributes to a better model robustness and ensures applicability in real-world healthcare environments

3. Methodology

3.1 Research Design

This study focuses on an experimental research design to review a machine learning (ML)based diabetes prediction model within a secure analytical base. The main objective is to check how integrating cybersecurity (CS) mechanisms and data quality improvement affects predictive performance and model reliability.

The proposed system is structured as a multi-layer pipeline comprising five stages: data acquisition, preprocessing, cybersecurity (CS) integration, model development, and evaluation. This design enables a controlled comparison across testing conditions and isolates the effect of each component on the system performance [3] [5].

Figure 1: System Architecture This architecture ensures secure data processing and reliable prediction outcomes.

3.2 Description of the dataset

The test was performed using the Pima Indians Diabetes Dataset, a popular structured medical dataset for binary classification [12]. The dataset contains: 768 records, 8 numerical features: Pregnancies, Glucose, Blood pressure, Skin thickness, Insulin, BMI, Diabetes Pedigree Function, and Age

Target variable (Outcome): non-diabetic =0 | Diabetic=1

The dataset is imbalanced in class, with non-diabetic cases being more frequent, that affects the model bias and testing [21].

3.3 Data Preprocessing

The following pre-processing steps were implemented to assure data quality and reliability:

3.3.1 handling Invalid Values

Zero values in medical features (Glucose, Blood pressure, Skin thickness, Insulin, BMI) were treated as missing values and were considered physiologically invalid [4].

3.3.2 Missing Value Imputation

The missing values were replaced by median, due to its stability against outliers and skewed distributions [17].

3.4 Cybersecurity layer

The incorporation of a cybersecurity (CS) layer assisted in maintaining data integrity and preventing its unauthorized access [10].

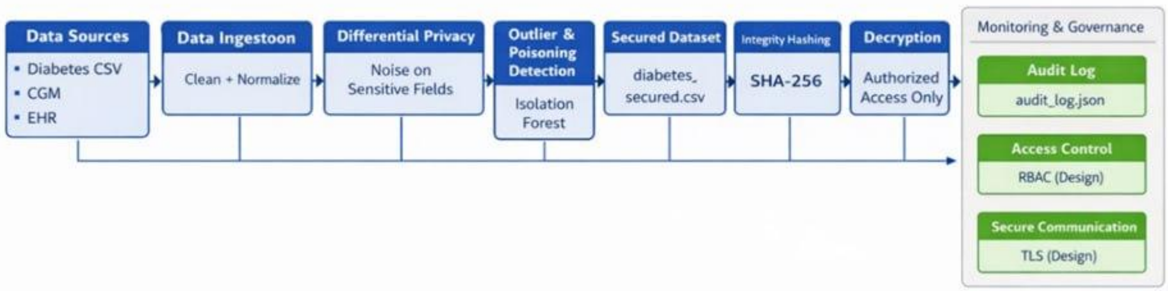


Figure 2: Secure data processing and cybersecurity pipeline for AI-Based healthcare system

3.4.1. Pseudonymization

Sensitive identifiers were replaced with anonymized representations to avoid direct identification [2].

3.4.2 Encryption (AES-256-GCM)

AES-256-GCM was used to encrypt data which provides confidentiality as well as validation so that the patients' information is protected from unauthorized access [5].

3.4.3 Integrity Verification (SHA-256)

Data integrity was verified by computing SHA-256 hash values before and after processing. Any mismatch is an indication of data tampering [14].

3.4.4 Differential privacy (DP)

A simplified differential privacy (DP) approach was applied to selected numerical features with controlled Gaussian noise. The noise level was calibrated to preserve statistical utility while reducing the risk of re-identification [7].

3.4.5 Threat Model

The system considers potential threats including Data leakage, Data tampering, Re-identification attacks.

These threats are mostly shown through encryption, hashing, and anonymization mechanisms integrated throughout the pipeline [10].

3.5 Outlier Detection and handling

To improve data quality, the Isolation Forest (IF)algorithm was used to detect anomalies [16] [1].

Model configuration: n_estimators=100 contamination=0.05 | random_state=42

Each instance was scored as abnormal and outliers were flagged with a binary variable (Outlier Flag).

Detected outliers: 39 records (5.08 %)

There are two testing scenarios to be reviewed With outliers, Without outliers

This allows to analyze the effect of data quality on the model performance.

3.6 Development of the Model

Random Forest(RF) classifier was selected based on: Noise stability, capability to model nonlinear relationships, high performance on structured medical datasets compared to models like logistic regression and SVM [4] [12]. Model Configuration: **random_state=42.**

Hyperparameter Optimization:

Hyperparameter tuning was done with Grid Search CV (5-fold cross validation). But performance gains were modest, revealing that data quality plays a bigger role than parameter tuning.

3.7 Train–Test Split

The dataset was split into:

80% training

20% testing

Using:

test_size = 0.2

random_state = 42

This ensures reproducibility and balanced evaluation.

3.7 Evaluation Metrics

Model performance was assessed using four standard materials derived from the confusion matrix

Accuracy: Overall correctness of the model predictions.

Precision: Proportion of correctly predicted positive cases.

Recall (Sensitivity): Ability of the model to correctly identify diabetic cases.

F1-score: Harmonic mean of Precision and Recall.

ROC-AUC: Overall discriminative capability across multiple classification thresholds. [11].

These materials are based on the following conditions:

- TP (True Positive): Diabetic cases correctly classified
- TN (True Negative): Nondiabetic cases correctly classified
- FP (False Positive): Nondiabetic cases incorrectly classified as diabetic
- FN (False Negative): Diabetic cases incorrectly classified as non-diabetic

The metrics are computed using the following formulas:

- accuracy=(TP+TN)/(TP+TN+FP+FN)
- Precision=TP/(TP+FP)
- Recall=TP/(TP+FN)
- F1-score=2×(Precision×recall)/ (Precision+recall)

3.9. Experimental Protocol

The overall workflow of the proposed framework can be summarized as follows:

- Load the data set
- Data preprocessing and missing value imputation
- Use pseudonymisation techniques
- Encrypt the data with AES-256-GCM
- Check data integrity with SHA-256
- Isolation Forest for Anomaly Detection
- Train a Random Forest model
- Use multiple metrics to evaluate model performance
- Compare results for different experimental scenarios

3.10 Environment of Implementation

All experiments were performed using Python 3.11.

The libraries used are:

- Data processing using Pandas and Numpy
- Scikit-learn for machine learning and outlier detection
- Hashlib and Cryptography for cybersecurity mechanisms
- Matplotlib and Seaborn for visualization

All experiments were conducted in a controlled environment to ensure reproducibility and consistency of the experimental results.

The proposed methodological framework incorporates machine learning, cybersecurity techniques and data quality improvement into a single analytical pipeline. This framework guarantees reproducibility, security and robustness, thus making the proposed framework highly suitable for real-world healthcare applications where both predictive performance and data protection are crucial.

4. Results

4.1 Dataset Description and Experimental Setup

The experimental evaluation was conducted using the Pima Indians Diabetes Dataset, widely used structured medical dataset for diabetes prediction tasks. The dataset consists of:

768 records

8 numerical predictive features

(Pregnancies, Glucose, Blood Pressure, Skin Thickness, Insulin, BMI, Diabetes Pedigree Function, Age)

A binary target variable (Outcome):

Nondiabetic=0

Diabetics = 1

The prediction task was formulated as a binary classification problem.

Data were split into 80% training, 20% testing.

with a fixed random seed (random state = 42) to improve reproducibility.

Three testing scenarios were reviewed: Baseline model (before cybersecurity integration), After integrating the cybersecurity layer (with outliers retained), After removing outliers found by Isolation Forest

4.2 Baseline Model Performance (Before Cybersecurity Integration)

In the baseline stage, the Random Forest (RF) model was trained after standard preprocessing Performance: Accuracy: 74.68%, ROC-AUC: ≈ 0.82

Class-wise performance:

Table 2

class	precision	Recall	F1-scor
Non-diabetic (0)	**0.81**	**0.79**	**0.80**
Diabetic (1)	**0.64**	**0.67**	**0.65**

The model showed stronger performance in pointing non-diabetic cases. This imbalance is added to class imbalance, where the majority class (non-diabetic) dominates the dataset, leading to biased learning behavior.

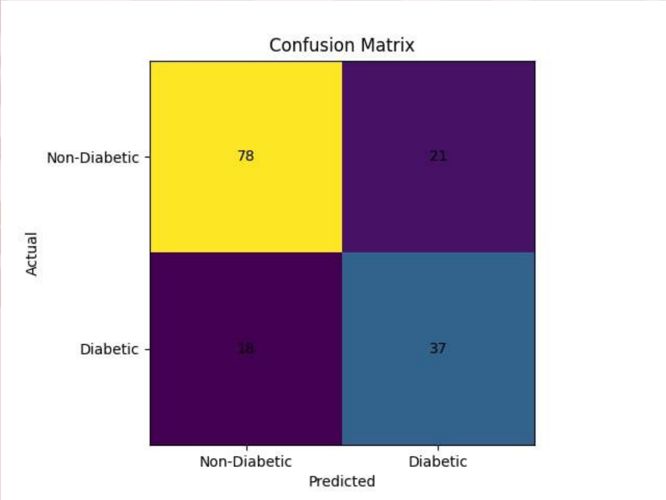


Figure 2: Confusion Matrix of the Random Forest model showing classification performance for diabetic and non-diabetic cases.

4.3 Performance After Cybersecurity Integration (With Outliers)

After integrating the cybersecurity layer—which included: AES-256-GCM encryption, SHA-256 integrity verification, Pseudonymization improved data handling

The model was retrained using the same data split.

Results: Accuracy: 75.97%, ROC-AUC: 0.827, Diabetic class performance: Precision: ~0.67, Recall: ~0.69, F1-score: ~0.68

The results showed a modest improvement, particularly in detecting cases of diabetes.

The ROC-AUC stability indicates that the cybersecurity (CS) layer did not degrade discriminative ability and may have assisted on improving data consistency.

4.4 Outlier removal performance

The Isolation Forest (IF) algorithm identified: 39 anomalous records, Representing 5.08% of the dataset, upon removal of these outliers and re-training the model: Accuracy: 82.88%, ROC-AUC: 0.8271-0.831

The all-performance metrics were improved including Precision, Recall and F1-score.

This large improvement confirms that the spurious records were noise that negatively affecting the model’s learning.

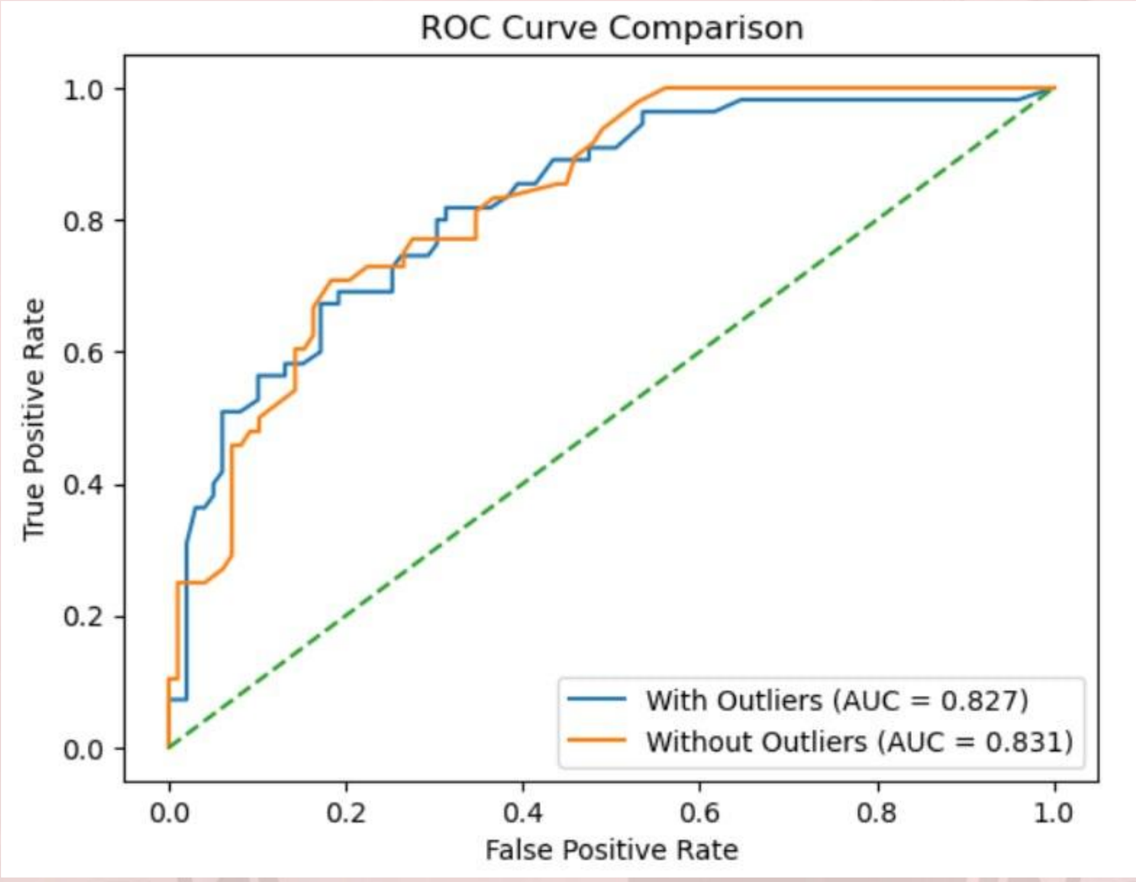


Figure 3

The ROC curve illustrates the model's discriminative performance before and after outlier removal. The AUC value improved from 0.827 to 0.831, indicating a slight enhancement in classification capability.

4.5 Comparative Analysis

Table 3

Scenario	Accuracy	ROC-AUC
Baseline	74.68%	0.82
With Cybersecurity	75. 97%	0.8271
After Outlier Removal	82.88%	0.8271–0.8314

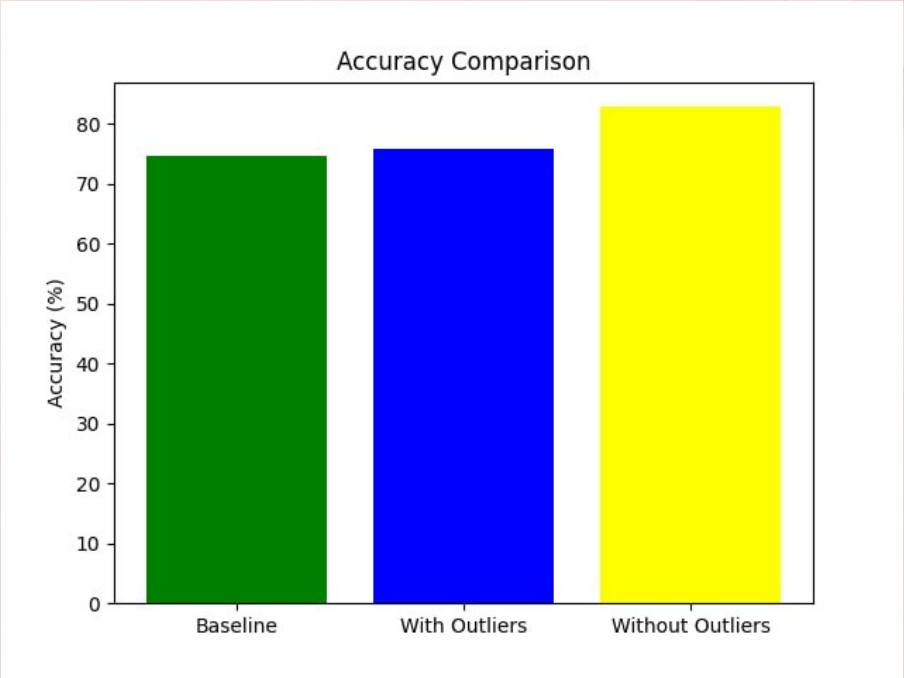


Figure 4: Comparison of model accuracy across different experimental scenarios.

Interpretation:

- The cybersecurity (CS) layer contributed to incremental performance improvement.
- Outlier removal had the largest impact on predictive accuracy.
- Data quality remains a critical determinant of model performance.

4.6 Key Observations

- Class imbalance caused the model to favor non-diabetic predictions.
- The model consistently performed better in the non-diabetic class.
- Recall for diabetic cases improved after cybersecurity (CS) integration.
- ROC-AUC remained stable, confirming robust discriminative ability.
- Accuracy alone is insufficient for evaluating medical models.

The findings show that integrating cybersecurity (CS) mechanisms into the machine-learning (ML) pipeline not only ensures data protection but also helps improve data quality and model stability. The removal of outliers was the most important factor for performance improvement, which highlights the importance of data quality for the development of reliable medical prediction systems.

5. Discussion

5.1 Discussion of general results

The outcomes of this study reveal that the predictive performance of machine learning (ML) models in medical applications is not only based on the selection of the algorithm but is also directly affected by two essential factors: data quality, cybersecurity (CS) integration [3][10]. The model was evaluated in three consecutive stages to provide a systematic investigation of the effect of both the cybersecurity (CS) procedures and the handling of outliers on the performance. A set of measurable evaluation criteria was utilized to assure balanced and rigorous handling [10] [21], including Accuracy, Precision, Recall, F1-score, and ROC-AUC.

5.2 Baseline Performance Analysis

In the baseline stage, the accuracy of the Random Forest (RF) model was 74.68% and the discriminative ability was ROC-AUC = 0.827 [22] [19]. Moreover, the findings were significantly different among classes, with the non-diabetic class being effective (Precision = 0.81, Recall = 0.79, F1 = 0.80) than the diabetes one (Precision = 0.64, Recall = 0.67, F1 = 0.65).

This disparity is attributed to the occurrence of class imbalance when the majority class dominates the dataset leading to inaccurate predictions [21]. The weak Recall for the diabetic class indicated unfound cases (false negatives), which are especially important in medical settings, as missed diagnosis might increase clinical risks.

5.3. Effect of the integration of cybersecurity (CS)

The accuracy improved to 75.97% with the addition of the cybersecurity (CS) layer and better analytical capability (ROC-AUC = 0.82). The diabetic class also improved modestly, showing that more positive instances were identified.

The results support the fact that addition of measures like encryption, integrity verification, and pseudonymization does not significantly impact prediction performance [5] [14]. Instead, they help in increasing data consistency and lowering noise and reinforce system reliability in medical situations where rigorous data security is required [10].

5.4 Effect of Outlier Detection and Removal

Outlier elimination (39 records, 5.08% of the sample) resulted in a significant performance gain. Accuracy improved to 82.88% with gains across all assessment parameters and a little rise in ROC-AUC (≈ 0.827–0.831).

This means outliers were noise interfering with the learning process and their removal helped the model to learn from more representative data [16] [1]. Caution is required, as some outliers may correspond to rare but clinically valid cases. These records are sensitive to several medical patterns. Also, regular detection must be used to balance data purification with the preservation of clinically significant signals.

5.5 Model Discrimination and ROC-AUC

The ROC-AUC metric progressively improved during the three stages (≈0.82→0.8271→0.8314), indicating an enhanced classification capability. Metric is particularly beneficial for medical applications, since it evaluates performance across several thresholds rather than a single categorization criterion [24] [19].

5.6 Trade-Offs in Performance Metrics

The accuracy has clearly increased but the study reveals that accuracy alone is not sufficient for reviewing and testing medical models. Focusing on effective evaluation. Recall for the diabetic class to reduce false negatives. Multi-metric testing is a trade-off between reducing false negatives (clinically critical) and false positives (operationally important) ([21]

This study's findings indicate that data quality, particularly outlier removal, has the greatest impact on improving predictive performance, but incorporating cybersecurity(cs) enhances the model's stability and data reliability without compromising its results. Therefore, to design effective medical AI systems, it is necessary to find the right balance between prediction performance, data quality and information security.

Besides the conventional performance measures, an additional validation phase was carried out to evaluate the reliability of the developed prediction model. The model outputs were visually compared to the confusion matrices and ROC curves for the three experimental stages [11]. This was confirmed visually and in the numerical data, with better class separation and fewer misclassifications, especially after the application of the cybersecurity (CS) layer and removal of outliers.

The model was compared with the baseline models and the traditional methods given in the literature which gave external validation to the results [22] [19]. The adoption of visual examinations, quantitative measures and comparison with literature adds confidence to the presented approach and verifies its practical applicability in real life healthcare settings.

5.7 Comparison Between Previous Studies

Few earlier research, especially those based on CNN-based architectures, have shown high accuracy levels, up to 98% in some circumstances. These models are based on very complicated computer models which raise the overall cost and computational burden, therefore restricting their applicability in real-world clinical systems [15].

By contrast, voice-analysis approaches have achieved a more moderate percentage of accuracy than the former, ranging between 70% and 75%. They are readily available, however they rely on very sensitive biometric speech data and thus raise questions of privacy and data protection [13].

Continuous glucose monitoring (CGM) systems give real-time physiological data of high resolution and considerable clinical significance. The use of expensive sensors and complex digital architectures makes them inaccessible and difficult to widely implement, especially in resource-scarce healthcare settings [18].

Some traditional machine-learning (ML) algorithms like J48 have been reported to obtain an accuracy level of 85% in some studies but their performance has been known to deteriorate when faced with complicated or noisy medical datasets, thereby rendering them uncompetitive with more advanced models [9].

In comparison to these investigations, the model in this work achieved 74.68% accuracy in the baseline scenario that climbed to 82.88% after enhancing data quality through outlier removal. Competitive results are obtaining the simplicity of the Random Forest(RF) model and the usage of only structured clinical data, not requiring specialist sensors or high-cost imaging modalities.

More notably, whereas most of the prior research focused on the prediction performance, they rarely incorporated explicit cybersecurity (CS) methods. On the other hand, the current study proposes a completely integrated cybersecurity (CS) layer, which comprises encryption, integrity verification and pseudonymization, which increases system stability and keeps compliance with data-protection needs in real-world healthcare systems.

the suggested basis uniquely integrates data-quality improvement (by aberrant detection and removal) with stable cybersecurity(CS) protections, a dual integration not addressed in prior research. “This is a major scientific contribution and takes the study closer to achieving secure and reliable.

6. Conclusion

This study focused on developing an integrated base that combines machine learning(ML) with cybersecurity (CS)to improve diabetes prediction while keeping the balance between predictive performance and data protection. Using the Random Forest (RF)classifier and the Pima Indians Diabetes dataset, the model was tested across three scenarios: before integrating the cybersecurity layer, after its integration, and following the removal of abnormal records.

The baseline model reached an accuracy of 74.68%, with noticeable variation between the two classes due to class imbalance. After adding the cybersecurity(CS) layer, performance improved slightly to 75.79%, indicating that the security mechanisms didn’t weaken the model’s predictive capability; but, they actually stabilized and improved data quality.

Following the application of the Isolation Forest (IF)algorithm and the removal of abnormal records, accuracy increased greatly to 82.88%, highlighting the crucial role of data quality in improving machine-learning (ML)performance. Other tests like Precision, Recall, F1-score and ROC-AUC also showed improvements in the discrimination ability of the model.

Overall, the findings confirm that adding cybersecurity (CS)within the AI pipeline not only strengthens data protection but also positively influences data consistency and predictive performance. but the results also showed the need for caution in medical applications, as false negatives (missed diabetic cases) may have serious clinical complications.

In summary, this study helps in improving the concept of AI–cybersecurity (CS)integration and underscores the importance of data quality, balance, and security in developing reliable intelligent healthcare systems.

7.Recommendations

Based on the findings of this study, the following recommendations are proposed:

1. Address Class Imbalance

To improve the model's ability to find diabetic cases and increase Recall for the minority class, it is recommended to apply techniques such as: SMOTE (Synthetic Minority Over-sampling Technique), Class weighting.

2. Use Evaluation Metrics

Accuracy alone is not enough in medical applications. Other holistic test includes: Precision, Recall, F1-score, ROC-AUC

This allows for a true analysis of model performance, especially for high risk classes.

3. Use Cross-Validation

K-Fold Cross-Validation is recommended to improve reliability of results and minimize effect of data partitioning on performance.

4. Improve Outlier Handling

Although removing abnormal values improved performance, it is advisable to: Analyze the impact of each abnormal record before removal, Consider more robust approaches (e.g., robust models) instead of a direct one.

5. Expand the Dataset

To improve model accuracy in general, future work must have: Real clinical datasets from hospitals, Multiple datasets to increase diversity.

6. enhance the Cybersecurity Layer(CS)

The security base can be improved through: Adding Federal Learning for data privacy during training, using advanced Differential Privacy(DP) techniques, merging mechanisms to find attacks like data poisoning.

7. View More Advanced Models

Future work could explore the performance of more advanced deep-learning models such as Neural Networks, LSTM, Transformers. Compare with Random Forest(RF).

8. Practical Deployment

The system can be extended into: A Clinical Decision Support System (CDSS), A smart application for monitoring diabetic patients.

Conclusion: achieve high predictive performance in medical AI systems needs more than just choosing an appropriate model, it demands a careful integration of data quality, cybersecurity(CS), and understanding review metrics. This study provides a foundation for developing more secure, accurate, and trustworthy AI-driven healthcare.

8. Reference

1. Abousaber, I., Abdallah, H.F. and El-Ghaish, H. (2024) ‘Robust predictive framework for diabetes classification using optimized machine learning on imbalanced datasets’, *Frontiers in Artificial Intelligence*, 7, pp. 1–12.
2. Ahuja, N., Zhao, X. and Williams, K. (2023) ‘Pseudonymization techniques for secure medical data sharing’, *Journal of Medical Systems*, 47(2), pp. 1–14.
3. Battineni, G., Sagaro, G.G. and Amenta, F. (2022) ‘Data preprocessing strategies for healthcare machine learning’, *Healthcare Analytics*, 2, pp. 100–112.
4. Biau, G. and Scornet, E. (2021) ‘A random forest guided tour’, *TEST*, 30, pp. 1–43.
5. Chen, Y., Zhang, L. and Wang, H. (2023) ‘AES-256-GCM encryption for secure healthcare data transmission’, *IEEE Access*, 11, pp. 45012–45025.
6. Deng, Y., Zhang, H., Li, J. and Zhou, M. (2025) ‘Artificial intelligence in diabetes care: from predictive analytics to generative AI and implementation challenges’, *Frontiers in Endocrinology*, 16, pp. 1–14.
7. Dwork, C. and Roth, A. (2020) ‘The algorithmic foundations of differential privacy’, *Foundations and Trends in Theoretical Computer Science*, 9(3–4), pp. 211–407.
8. Esmaeilyfard, R. and Bayati, M. (2025) ‘Enhancing AI-driven forecasting of diabetes burden: a comparative analysis of deep learning and statistical models’, *Scientific Reports*, 15(2), pp. 1–12.
9. Eyasu, T. (2020) ‘Performance evaluation of J48 classifier for diabetes prediction’, *International Journal of Computer Applications*, 176(12), pp. 1–6.
10. Gordon, W.J., Fairchild, A. and Buntin, M. (2022) ‘Cybersecurity challenges in modern healthcare systems’, *Health Affairs*, 41(3), pp. 354–362.
11. Grandini, M., Bagli, E. and Visani, G. (2023) ‘Metrics for multi-class classification: An overview’, *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 13(2), pp. 1–25.
12. Haque, M.I., Rahman, M.M., Islam, M.S. and Rahman, M.A. (2023) ‘Machine learning-based diabetes prediction using structured clinical data’, *BMC Medical Informatics and Decision Making*, 23(1), pp. 1–14.
13. Kaufman, S. (2023) ‘Voice-based biomarkers for diabetes detection: Opportunities and privacy concerns’, *Digital Health*, 9, pp. 1–10.
14. Kumar, S., Singh, R. and Verma, A. (2022) ‘Ensuring data integrity in healthcare systems using SHA-256 hashing’, *Journal of Information Security and Applications*, 68, pp. 1–9.
15. Lee, J. (2024) ‘Deep CNN architectures for diabetes prediction: Performance and limitations’, *Computers in Biology and Medicine*, 170, pp. 1–10.

16. Li, X. and Xu, Y. (2023) ‘Isolation Forest-based anomaly detection in medical datasets’, *Expert Systems with Applications*, 219, pp. 1–12.
17. Luque, A., Carrasco, A., Martín, A. and de las Heras, A. (2020) ‘The impact of class imbalance in classification performance metrics’, *Pattern Recognition*, 91, pp. 216–231.
18. Martens, T. (2021) ‘Continuous glucose monitoring: Clinical value and limitations’, *Diabetes Technology & Therapeutics*, 23(5), pp. 350–360.
19. Mohsen, F., Al-Absi, H.R.H., Yousri, N.A., El Hajj, N. and Shah, Z. (2023) ‘A scoping review of AI-based methods for diabetes risk prediction’, *NPJ Digital Medicine*, 6(1), pp. 1–15.
20. Paul, R., Singh, A. and Kumar, P. (2025) ‘Comparative analysis on diabetes using ensemble machine learning models on Pima Indians dataset’, *Journal of Healthcare Informatics Research*, 9(1), pp. 1–18.
21. Saito, T. and Rehmsmeier, M. (2022) ‘The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets’, *PLOS ONE*, 17(2), pp. 1–15.
22. Shin, J., Kim, J., Lee, C., Yoon, J.Y., Kim, S. and Song, S. (2022) ‘Development of various diabetes prediction models using machine learning techniques’, *Diabetes & Metabolism Journal*, 46(2), pp. 251–262.
23. Sim, J., Park, H. and Choi, S. (2025) ‘Integrated biomarker analysis and next-generation AI for precision diabetes prediction’, *Springer Nature Medicine*, 12(4), pp. 1–15.
24. Sun, Q., Cheng, X., Han, K., Sun, Y., Ren, H. and Li, P. (2025) ‘Machine learning-based assessment of diabetes risk’, *Applied Intelligence*, 55, pp. 1–15.
25. Tao, L., Chen, Y. and Wang, Z. (2025) ‘Multi-task learning for diabetes prediction using structured datasets’, *Springer Nature Computer Science*, 6(3), pp. 1–10.
26. Wu, X. (2022) ‘Transformer-based frameworks for diabetes prediction’, *Springer Lecture Notes in Computer Science*, pp. 112–124.

Stardom University

STARDOM UNIVERSITY

S D U

Stardom Scientific Journal of Natural and Engineering Sciences

- Stardom Scientific Journal of Natural and Engineering Sciences -
Peer Reviewed Scientific Journal published twice
a year by Stardom University
1st issue- 4th Volume 2026
ISSN 3756-2980