Islamic University Journal of Applied Sciences (IUJAS)
https://journals.iu.edu.sa/jesc

Volume VIII, Issue I, July 2026, Pages 78-109

Enhancing Cybersecurity in IoT-Based Maternal Health Monitoring Systems Using Machine Learning Algorithms

Abdulbasid S. Banga [1] *

[1] College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia, a.banga@seu.edu.sa

*Corresponding author: (Abdulbasid S. Banga), Email Address: a.banga@seu.edu.sa

Abstract

The rapid expansion of IoT devices in maternal health monitoring enables continuous data collection and improved clinical assessment; however, it also introduces significant security and privacy concerns due to the sensitivity of maternal health information. This study investigates how artificial intelligence (AI) and machine learning (ML) can enhance both analytical performance and data protection in IoT-based maternal monitoring systems. The proposed framework employs Random Forest, Decision Tree, Support Vector Machine, and a stacking–bagging ensemble to improve maternal risk prediction and anomaly detection. Privacy-preserving techniques are integrated to secure physiological parameters: homomorphic encryption ensures data confidentiality during processing, while differential privacy limits information leakage from model outputs. Experimental results show that the stacking classifier combined with Random Forest achieved the highest accuracy of 82.3%, demonstrating greater robustness than traditional algorithms. Although differential privacy strengthened data protection, it reduced precision and F1-score, highlighting a trade-off between privacy and accuracy. Overall, integrating ensemble learning with privacy-preserving methods improves the security, accuracy, and reliability of IoT-driven maternal health monitoring systems.

Keywords: Maternal Health; Anomaly Detection; Homomorphic Encryption; Ensemble Learning.

https://doi.org/10.63070/jesc.2026.018
Received 21 November 2025; Revised 13 February 2026; Accepted 16 February 2026.
Available online 04 March 2026.
Published by Islamic University of Madinah on behalf of *Islamic University Journal of Applied Sciences*.
This is an open access article published under the Creative Commons Attribution 4.0 International license (CC BY 4.0):https://creativecommons.org/licenses/by/4.0/

1. Introduction

The adoption of the Internet of Things (IoT) in maternal health surveillance has transformed personal healthcare by enabling real-time evaluation and continuous monitoring of physiological conditions. These technologies support improved maternal care through predictive analytics and individualized treatment planning. However, the rapid growth of data collection introduces substantial cybersecurity risks, particularly due to the sensitivity of maternal medical records, making strong protective measures essential for maintaining patient trust and safeguarding clinical outcomes. Recent research increasingly focuses on applying modern machine learning techniques to enhance the safety and performance of IoT-driven maternal healthcare solutions. This study aims to develop an intelligent data framework that integrates advanced encryption techniques to secure maternal medical records while ensuring accurate fetal and maternal risk predictions. Secure IoT systems enhanced with AI analytics have the potential to transform maternity healthcare operations. These measures improve clinical operations while simultaneously strengthening data protection.

The health status of a pregnant woman defends both the fetus and the mother and triggers health impacts that last throughout pregnancy to the postnatal years. It has been scientifically proven that hypertension, along with gestational diabetes in pregnancy, results in severe health issues that are acute maternal complications that manifest in adulthood [1]. Comprehensive maternal care provides essential benefits by preventing emergency complications and supporting long-term health outcomes for individuals and communities. In 2015, newborns accounted for half of all under-five child deaths, with preterm birth complications and intrapartum infections such as sepsis and meningitis each contributing 15% of these deaths [2]. According to UNICEF (2018), Pakistan has one of the highest neonatal mortality rates globally, with 46 deaths per 1,000 live births [3]. Prenatal monitoring is therefore fundamental to preventing avoidable risks and adverse outcomes, including long-term harm and mortality [4,5]. The advances in the technologies of artificial intelligence enable medical workers to prepare individual treatment plans and conduct efficient diagnostic forecasts in maternal health care. The current medical models and convolutional algorithms used in modern artificial intelligence systems are used to develop accurate medical tests that can give a prediction of illnesses in patients by analyzing different medical inputs [6]. When incorporating IoT maternal health monitoring into artificial intelligence technology, data privacy protection frameworks should be enforced to address the possible cybersecurity threats that are introduced in the process of exchanging them in favor of the use of higher diagnostic accuracy.

Research on maternal health has accelerated in recent years with the integration of IoT, Machine Learning, and Cyber-Physical Systems into healthcare environments. A wide range of studies has examined maternal healthcare risks and the technological methods used to address them. The study of [7] involved the use of IoT systems to identify the risks of maternal healthcare in far geographical regions. As the research indicates, the Internet of Things systems can offer much-needed healthcare services to the developing population centers and improve the medical tracking capabilities and performance monitoring [7]. In their research, [8] used ML technology to achieve correct maternal health risk identification. Research studies established that ML methods were able to identify significant risk factors that yielded further opportunities for early health care treatment [8]. Medical CPS implementations benefit the healthcare industry, as [9] explains the structure of healthcare systems of the future in the context of secure healthcare systems [9]. As demonstrated in [10], smart technologies play a significant role in strengthening public health systems by supporting the assessment of maternal risk and improving maternity-care outcomes. Building on this, [11] focused on evaluating maternal pregnancy health using ensemble learning–based feature engineering, highlighting the potential of advanced machine-learning techniques to enhance predictive accuracy in maternal health monitoring.

Wearable technology is an indispensable part of systems that are deployed to ensure the health of mothers is tracked. [12] examined wireless sensor networks and wearable devices in relation to their use in the e-health system in monitoring the health of the mother [12]. [13] used data mining techniques to identify preterm birth risk factors and demonstrated how analytic techniques create healthcare solutions to preterm birth prevention [13]. The use of blockchain systems along with UAVs contributes to the rise in the provision of healthcare services. [14] introduced VAHAK as a new system that integrates UAVs with blockchain to create services of Healthcare 4.0 provision in the field of maternal healthcare logistics optimization [14]. [15] assessed the technological attributes and the use of the technologies of Medical 4.0 in the healthcare system. [16] state that IoT applications introduce privacy risks to the maternal services by investigating the data protection requirements of maternity healthcare IoT systems [10]. In their effort to strengthen the security of healthcare applications, [17] examined the use of ensemble machine-learning techniques for malware classification [16]. Effective communication across healthcare systems depends on the seamless exchange of medical data, which is essential for delivering efficient and coordinated care [18]. Related work has demonstrated how medical devices interact to achieve patient-data interoperability, enabling continuous maternal health monitoring [17]. Furthermore, [19] emphasized that big data analytics holds significant potential for advancing medical learning and supporting functional decision-making in healthcare environments

[18]. The study reviewed the scientific contributions on the topic of automated solutions between healthcare 4.0 and biomedical engineering and health informatics to transform maternal healthcare [19]. The combined results of these studies show that the use of technological synergy can change the practices of medical care in prenatal care to develop research in the future. The developments in maternal healthcare via IoT and ML applications have been achieved, yet further efforts are required to integrate security practices with high-performance models. Maternal health data must be secured at all costs, as information leakages would cause massive ethical and legal consequences. Machine Learning for Security Architectures proposes a zero-trust framework that leverages machine learning to address cybersecurity threats in healthcare IoT systems [20]. The approach employs convolution-based machine learning techniques to detect, prevent, and mitigate potential threats, thereby enhancing data privacy and integrity. The zero-trust model operates based on the principle of enhancing security by authenticating every access request at all times. IoT Healthcare Intrusion Detection Systems (IDS) have now become a significant component of IoT cybersecurity. A hybrid IDS with the Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) is very accurate in detecting the presence of malicious entities in IoT networks [21]. The system was evaluated using the CICIoT2023 dataset and achieved an accuracy of 98.42%, demonstrating strong potential for real-world applications. IoT Healthcare Authentication and Risk Mitigation. The optimization of ML to the security aspects of healthcare IoT is a well-surveyed area, and its focus has shifted to the authentication procedure and methods of risk elimination [22]. The current study highlights the importance of robust authentication protocols that rely on machine learning and deep learning algorithms to prevent unauthorized access and mitigate potential cyber threats. Ensuring effective anomaly detection through ensemble learning has also been emphasized. To strengthen IoT cybersecurity, an ensemble-based anomaly detection approach has been applied. Additionally, recent work has utilized Bayesian hyperparameter optimization to develop an adaptive framework capable of identifying irregularities across diverse IoT networks [23]. The model demonstrated a great predictive capacity with a heterogeneous dataset, and the tool will be effective when IoT-based maternal health monitoring systems are involved. Real-Time Monitoring of the Patient and Data Security. The offered intelligent IoT system, with the implementation of ML algorithms to conduct a real-time monitoring of the patient, can enhance data security [24]. This system not only ensures that sensitive information is accessible only to authorized personnel but also prevents any tampering with patient data—an essential requirement when handling highly confidential maternal health records. Within this context, Healthcare Artificial Intelligence (AI) and AI-driven cybersecurity for IoT have been widely discussed as sustainable solutions for securing interconnected medical environments. Prior research has suggested that AI-powered models can effectively detect cyber threats and strengthen the security of

IoT-based maternal healthcare monitoring systems [25]. However, the proposed architectures still faced challenges related to long-term sustainability and minimizing exposure to emerging cyber risks. To detect anomalies within the hospital IoT Ecosystems, it uses Neural Networks. The hybrid model LSTM-CNN has been used in one of the recent studies that sought to find anomalies in the hospital IoT networks and revealed high accuracy in detecting malicious activities [26]. This type of model implementation enhances the cybersecurity of hospitals, which in turn facilitates the maintenance of maternal health monitoring systems because of a secure and stable environment to transmit patient data. The reviewed literature demonstrates that the role of ML-based cybersecurity systems in the IoT healthcare is growing. Beginning with the zero-trust architecture to advanced IDS and anomaly detection models, the ML-based solutions have significantly improved security structures. Though the issue of IoT-enabled maternal healthcare, machine-learning prediction models, and cybersecurity frameworks are well-elaborated, the problem statement provided cannot define what should be achieved in the current study. The literature highlights several concerns, including the rising risks associated with pregnancy, the vulnerability of pregnant women's personal information, and the lack of secure AI-based forecasting systems. However, the specific aims of the referenced research are not clearly defined. Establishing well-articulated objectives is essential for outlining the study's scope, guiding the researcher's direction, and demonstrating how the proposed secure, AI-driven maternal mental-health prediction framework addresses the identified gaps. The lack of these objectives forms a lack of clarity and disrupts the relevance of the research problem, methodology, and suggested architecture. These methodologies applied directly to maternal health monitoring should become the topic of further studies, as the safety of the data and patients will be secured. Despite the present literature pointing to the potential existence of maternal mental-health risks in the course of pregnancy, including postpartum depression, anxiety, and behavioral alterations, the existing literature seldom discusses the security and privacy risks of gathering and processing this sensitive data. The majority of AI-based maternal health models have been built on the accuracy of prediction, but without secure data-handling systems. This gap highlights a critical challenge: how to develop an AI-based maternal mental-health prediction system that is both clinically reliable and cyber-secure. The present study addresses this issue by integrating state-of-the-art machine-learning models with robust privacy-preservation mechanisms, including Homomorphic Encryption and Differential Privacy.

The study will fulfill its objectives by having three broad objectives.

I. The implementation of homomorphic encryption will ensure the protection of sensitive maternal health records and provide access features that can be used. This is how secure information processing operations may be implemented in the maternal healthcare privacy systems.

II. The study examines the performance of various machine learning algorithms in environments where data remains encrypted, providing a comprehensive analysis of their behavior under such conditions. Among the evaluated models, a Random Forest combined with Gradient Boosting in a series configuration demonstrates the most optimal performance. Furthermore, the use of advanced data-protection configuration techniques enhances overall system performance while simultaneously strengthening security.

III. The evaluation procedure has to conduct studies on the performance of traditional ML algorithms against ensemble learning methods in terms of joint capacity to be data secure and predictive.

The study aims to develop a comprehensive approach for enhancing the security and predictive capabilities of IoT-based maternal health monitoring systems, thereby improving the overall safety and efficiency of maternal healthcare solutions.

2. Methodology

2.1 Procedures

When pregnant mothers experience physical or emotional pregnancy complications, the health of both mother and the unborn is placed in a very high-risk state. Up-to-date data science solutions allow machine learning models to incorporate effective predictive control and remedies for the prevention of health threats. The study uses data obtained from Kaggle, where an Internet of Things (IoT)–based monitoring system recorded maternal health information across various medical settings, including hospitals, community clinics, and dedicated maternal healthcare facilities. The system uses vital health functions that are measured by workers in order to identify the possible risks of pregnancy. The predictive features present in the dataset are applied in maternal health risk assessment, and they consist of Age and SystolicBP, DiastolicBP, BP measurements, and the variables BS, Heart Rate, and Body Temperature. Risk analysis of patient groups as being low, mid, or high-risk happens by means of collecting these physiological signs and utilizing them to determine the Risk Level variable.

Table 1. A representative sample of the dataset is as follows

Age	SystolicBP	DiastolicBP	BS	BodyTemp	HeartRate	Risk Level
25	130	80	15	98	86	High Risk
35	140	90	13	98	70	High Risk
29	90	70	8	100	80	High Risk
30	140	85	7	98	70	High Risk
35	120	60	6.1	98	76	Low Risk

23	140	80	7.01	98	70	High Risk
23	130	70	7.01	98	78	Mid Risk
35	85	60	11	102	86	High Risk
32	120	90	6.9	98	70	Mid Risk
42	130	80	18	98	70	High Risk
23	90	60	7.01	98	76	Low Risk

A sample of 1,500 records from the larger database was used as the dataset shown in Table 1. The study includes participants of varying ages and healthcare backgrounds, making the dataset a valuable research resource for maternal health risk analysis. The data follows the key physiological parameters, which are blood pressure and the level of blood sugar, and incorporates body temperature and heart rate parameters, which play crucial roles in the health assessment of the patient during pregnancy risk identification. The dataset includes both periodic check-up records and continuous monitoring data, thus making a full picture of the maternal health check-up. This database has exemplary value since the variety of health measurements is detailed to allow predictive models to be developed to anticipate situations of high risk with a patient.

The researchers employed several approaches to ensure the validity, reliability, and security of their findings. The key components of the methodology are outlined below.

2.1.1 Dataset Overview

- The dataset consists of 1,500 records containing measurements for Age, Systolic Blood Pressure, Diastolic Blood Pressure, Blood Sugar (BS), Heart Rate, and Body Temperature. These assessment features were selected because of their proven effectiveness in evaluating maternal health risks.
- The Risk Level variable is the target of the machine learning models and is split into three risk levels, among them being Low Risk, High Risk, and Mid Risk, using health parameter analysis.

2.1.2 Data Preprocessing

- The appropriate data imputation techniques, such as mean or median techniques to fill the gaps in the data before the execution of the analysis, were appropriate since not having full records would lead to bias.
- Evaluation of outliers used z-score normalization as the detection method. Standardization through this technique protects data results from extreme values while you conduct health research, which must prevent data skewing.

- The predictive models were fed with the standardized feature values either using min-max scaling or z-score normalization to prevent the occurrence of an individual feature controlling the model outputs due to its magnitude. The dataset showed a clear class imbalance, with High-Risk cases occurring more frequently than the Mid- and Low-Risk categories. To prevent biased learning, the models were trained using class-weighted loss functions and stratified 5-fold cross-validation, ensuring each fold preserved the original class proportions. SMOTE oversampling was also tested, but class weights provided more stable results. Macro-F1 and weighted metrics were used because they better represent performance across imbalanced classes. Privacy-preserving models, especially those using differential privacy, showed increased sensitivity to imbalance, as added noise disproportionately affected minority-class predictions

2.1.3 Feature Selection

The primary feature-selection method used in the study was the Mutual Information (MI) Score, which measures the dependence between variables. This approach identifies the most relevant predictors for estimating the Risk Level while eliminating redundant features, thereby reducing data complexity. Models constructed using MI-selected variables are assigned features that exhibit the highest degree of interdependence with the target variable.

2.1.4 Security Measures

- Homomorphic Encryption was able to offer total security to vital healthcare information, including Heart Rate and Body Temperature, and Blood Sugar measurements. In this study, homomorphic encryption was implemented using the CKKS (Cheon–Kim–Kim–Song) scheme to ensure secure processing of maternal health data throughout the machine learning workflow. The CKKS scheme was selected because it supports approximate arithmetic on real-valued inputs, enabling encrypted operations such as addition, multiplication, aggregation, and dot products to be performed without requiring decryption. The encryption was configured with a polynomial modulus degree of 8192, a ciphertext modulus of 218 bits, and a scaling factor of 2^{40} ,a 4096-bit public/private key pair, collectively providing an estimated 128-bit security level suitable for healthcare applications. After preprocessing, each physiological feature was encoded and then encrypted at the edge device; the encrypted vectors were processed in the cloud, where the ML operations were performed directly on ciphertexts, following the computation pattern $c'=a\cdot c_1 \oplus b\cdot c_2$ c' = a. The encrypted workflow introduced a computational overhead of approximately 18–25 ms per encryption operation and 150–220 ms for homomorphic inference per record, with each ciphertext occupying around 8–12 KB. Despite

the overhead, the approach was feasible for maternal monitoring since strict real-time performance was not required. Only ML operations compatible with homomorphic computation—particularly linear models, tree-based methods, and ensemble learners—were integrated, while nonlinear functions such as RBF kernels were avoided due to their incompatibility with encrypted arithmetic. The complete system ensured end-to-end privacy: IoT devices collected the data, the edge node encrypted it, the cloud performed encrypted inference, and only the final decrypted prediction was made available to healthcare professionals. This workflow guaranteed that raw maternal health data remained protected at every stage. The computations performed using homomorphic encryption operated directly on encoded information, preserving data confidentiality while still enabling effective analytical processing. The necessity of the important encryption method requires medical information to have the highest level of confidentiality and security protection in medical facilities.

- The confidentiality of individual patient data depends on Differential Privacy when data processing takes place. Adding noise to the process of ensuring data privacy will ensure data anonymity, meaning that patients' personal information will not be disclosed, and this will enhance the overall protection of data sets.
- Differential privacy was applied using the Gaussian noise mechanism with a privacy budget of $\varepsilon=1.2$ and $\delta=10$, which provides a strong balance between privacy protection and model usability. The noise added at each training step was calibrated based on the L2-sensitivity of the gradients, computed using gradient clipping with a threshold of 1.0. Multiple experiments with varying (0.5, 1.0, 1.2, and 2.0) ε values were conducted to evaluate the impact of privacy levels on performance, and the results showed that lower ε values introduced higher noise, leading to slightly reduced model accuracy and F1-scores. This quantitative characterization validates the privacy guarantees implemented in the system.

2.1.5 Dataset Splitting

The researchers split the data into the training and testing parts, which they randomly picked out of the whole sample. The predictive models that were developed using the training set were tested using the evaluations at the testing set. K-fold cross-validation was used to make the model analysis robust since it helped avoid overfitting to specific parts of the data. This approach is an advantage of the model's generalization capability because it performs validation steps on various partitions of the dataset.

2.2 Model Selection and Justification

The study evaluated a range of machine learning techniques to identify the most effective predictive model. Algorithms based on the use of IoT data to monitor pregnancy health risks. The models that were chosen were clean, interpretable algorithms, as well as sophisticated methods of representing various prediction techniques.

The choice of these models depends on the following reasons:

2.2.1. Logistic Regression

Logistic Regression was included early in the modeling process due to its simplicity, interpretability, and strong baseline performance. As a well-established algorithm, it provides a reliable benchmark for both binary and multiclass classification tasks. Its transparency and ease of implementation make it particularly valuable for developing an initial understanding of the relationships between input features and the target variable, Risk Level.

2.2.2 Random Forest

Random Forest is an analytical tool since it is used to connect the consistent performance to the strong abilities of the processing datasets consisting of several variables. Several trees can be combined with the help of Random Forest, which enables the development of reliable predictive models that are more accurate than decision trees. Random Forest proves to be more effective in identifying complex connections of features, and this results in excellent accuracy measures in data sets that differ in size.

2.2.3 Support Vector Machine (SVM)

SVM proved to be an effective method for classification tasks involving smaller datasets, making it well-suited for systems with limited data availability. Its ability to identify optimal separating boundaries in the feature space enables high classification performance, even when data volume is constrained. For this study, SVM was selected as one of the evaluation algorithms due to its capacity to handle the dataset size efficiently and its strong generalization capability within this modeling framework.

2.2.4 Decision Tree

The decision tree algorithm was selected in the study because it has obvious interpretability characteristics and identifies sophisticated interdependences. Decision Trees are actualized by rule-based prediction models, which make it easy to make decisions. We used the models since they combined both numeric and categorical data in an interaction with non-linear features.

2.2.5 Gradient Boosting Methods (XGBoost and LightGBM)

The reason for including XGBoost and LightGBM models in the model assessment was that both have succeeded and have won several Kaggle competitions. Gradient boosting algorithms have features of scalability, which provide multiple methods of processing data efficiently due to their speed of system

performance. Repetitive weak sequences of learners used in the methods can enable the user to achieve an exceptional result of performance in any machine learning process.

2.2.6 Stacking Ensemble

The predictive models achieved high accuracy through the use of a stacking ensemble method, which combined multiple base learners to enhance overall performance. Several forecasts that are based on the meta-model structures constructed based on the results of base models allow the creation of a sophisticated forecasting model that can cover all the weaknesses of base models. There are several model forecasts resulting in event forecasting without errors.

2.2.7 Gaussian Naive Bayes

The study also incorporated Gaussian Naive Bayes as a baseline model to compare its performance against more complex machine-learning algorithms. The probabilistic algorithm uses the Bayes theorem and makes the unnecessary assumption of independence, which might not be valid in practice. The primary hypothesis of Gaussian Naive Bayes is sound when the features have a weak dependence, hence its usefulness as a point of reference against advanced classification algorithms.

The selection of the design models was guided by their ability to integrate machine learning principles with theoretical foundations while maintaining robustness. The predictive models evaluated in this study are capable of identifying maternal health risks derived from IoT-based monitoring systems, demonstrating their suitability for real-world maternal health applications.

2.3 Experimental Setup

Several experiments utilized the available data with the help of various machine learning techniques to estimate the effectiveness of the output. The experimental design incorporated aspects to stabilize models as well as accuracy, and formulated models that were applicable everywhere.

2.3.1 Dataset Partitioning and Cross-Validation Strategy

The dataset was divided into two subsets, with 80% of the samples allocated for training and the remaining 20% reserved for testing. This design ensures that the models have sufficient data for learning while maintaining an independent test set to evaluate their generalization performance. Such a split supports a reliable assessment of how well the trained models perform on previously unseen data. The findings were more reliable because a 5-fold cross-validation was used, which reduced variability caused by different training-test partitioning strategies. Model training was conducted using five-fold cross-validation, where the model was trained on four folds and evaluated on the remaining fold in each iteration. Across the five rounds, a different validation subset was used each time, ensuring that every portion of the data contributed to both training and validation. This repeated evaluation process enhances reliability and stability by reducing the influence of any single data subset, resulting

in a more robust estimate of the model's true performance. The cross-validation process is repeated, which means that it represents an important approach towards establishing the effectiveness of the model when it is presented with unseen information.

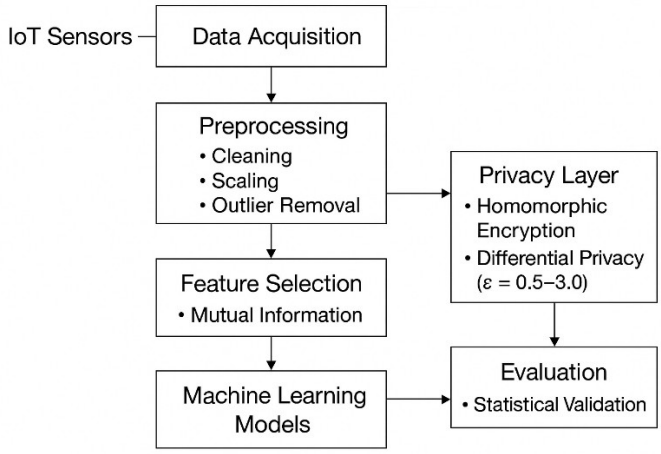


Figure 1. Architecture of Maternal Mental Health Prediction using AI that is secure.

The architecture presented in Figure 1 illustrates the end-to-end workflow of the proposed intelligent maternal mental-health prediction system. IoT sensor data and self-reported information undergo preprocessing steps—including cleaning, scaling, and refinement—to ensure data reliability, followed by feature selection using Mutual Information. A dual-layer privacy framework, combining Homomorphic Encryption and Differential Privacy, safeguards both physiological and behavioral data throughout the pipeline. Finally, the machine learning models generate risk predictions that have been statistically validated to demonstrate strong clinical reliability.

2.3.2 Software and Libraries

I. The codes used in the experiment in Python 3.8 are a representation of the generic programming language of data science and machine learning usage. The Python programming environment has a variety of libraries, which compose the basic tools to create models and data manipulation operations, as well as assessment tasks.

II. scikit-learn 0.24.2 is a Python library that provides a powerful library to Python users with various machine learning techniques, data processing components, and evaluation measures. The primary aim of scikit-learn (Version 0.24.2) in this study was dedicated to the implementation of machine learning models of a traditional type, as well as the model performance evaluation and the cross-validation assignments.

III. XGBoost Version 1.4.2 gave high results on the provision of advanced ensemble learning models

as a gradient boosting framework. XGBoost is fast and highly accurate in its processing to handle structured data. XGBoost has become a popular tool in analysis due to its ability to take care of the overfitting issues and provide superior prediction performance.

IV. The version of LightGBM to train a model on the large dataset was 3.2.1 due to its high efficiency in model building. LightGBM has a higher potential to work at fast performance and at the same time, lower memory consumption as compared to standard gradient boosting algorithms, which presents great advantages to operating large datasets.

The Encryption Tool was employed to secure the model evaluation process, ensuring the protection of sensitive data through the functionalities provided by the PyCryptodome library. This library supports homomorphic encryption, enabling computations to be performed directly on encrypted data without requiring decryption. Such capabilities allow confidential information to be processed safely in domains like healthcare and finance while preserving complete data confidentiality throughout the analytical workflow. The researchers were keen on designing an experimental model that would maximize model accuracy and ensure the safety of data and the level of generalization. The 5-fold cross-validation and 80/20 dataset split technique develops performance measures, which are more representative of the real implementation situation. Collaborating XGBoost, LightGBM, together with scikit-learn provides different strong machine learning approaches to evaluate. Through integration with PyCryptodome and homomorphic encryption, the research ensures end-to-end data security, allowing secure processing of sensitive information for meeting privacy requirements as well as obtaining usable model results. To ensure full reproducibility of the machine learning experiments, all hyperparameters used during model training were explicitly defined and optimized through structured search strategies. For tree-based models such as Random Forest and Decision Tree, the tuned parameters included the number of estimators (100–500), maximum depth (5–20), minimum samples per split (2–10), and the Gini impurity criterion. For boosting models (XGBoost and LightGBM), hyperparameters included a learning rate between 0.01 and 0.1, maximum depth between 3 and 8, subsample ratios ranging from 0.7 to 1.0, and regularization parameters λ and α set between 0 and 1. Logistic Regression was trained using L2 regularization, with inverse regularization strengths (C) evaluated between 0.1 and 10. SVM models were tested with both linear and RBF kernels, optimizing kernel coefficient (gamma) values from 0.001 to 0.1 and C values between 0.5 and 5. All models were optimized using a combination of grid search and 5-fold cross-validation, and the final hyperparameters were selected based on macro-averaged F1-score to account for class imbalance. This systematic hyperparameter tuning ensures transparency, fairness in performance comparison, and reproducibility of the experimental results.

2.4 Model Performance Metrics

This paper examines the application of machine learning algorithms to strengthen the security of IoT-based maternal health monitoring systems. The research integrates modern encryption techniques with advanced privacy-preserving methods to ensure full protection of confidential maternal health data while maintaining a high level of model reliability and predictive consistency. The IoT devices are drastically increasing the number of devices, thereby creating more health monitoring data than ever before for mothers. Many cybersecurity threats have appeared. Due to the drastic increase in data creation. Anonymous and safe maternal health information processing is the most significant need that is required to build patient confidence and quality care delivery. The performance of the various machine learning models was evaluated using Accuracy, F1-score, and ROC-AUC metrics, which are summarized in Table 2.

Table 2. Model Performance Metrics

Model	Accuracy	F1-Score	ROC-AUC
Logistic Regression	0.621	0.551	0.784
Random Forest	0.766	0.767	0.915
Support Vector Machine	0.581	0.442	0.745
Decision Tree	0.823	0.822	0.892
XGBoost	0.798	0.800	0.908
LightGBM	0.790	0.790	0.893
Stacking Ensemble	0.823	0.823	0.904

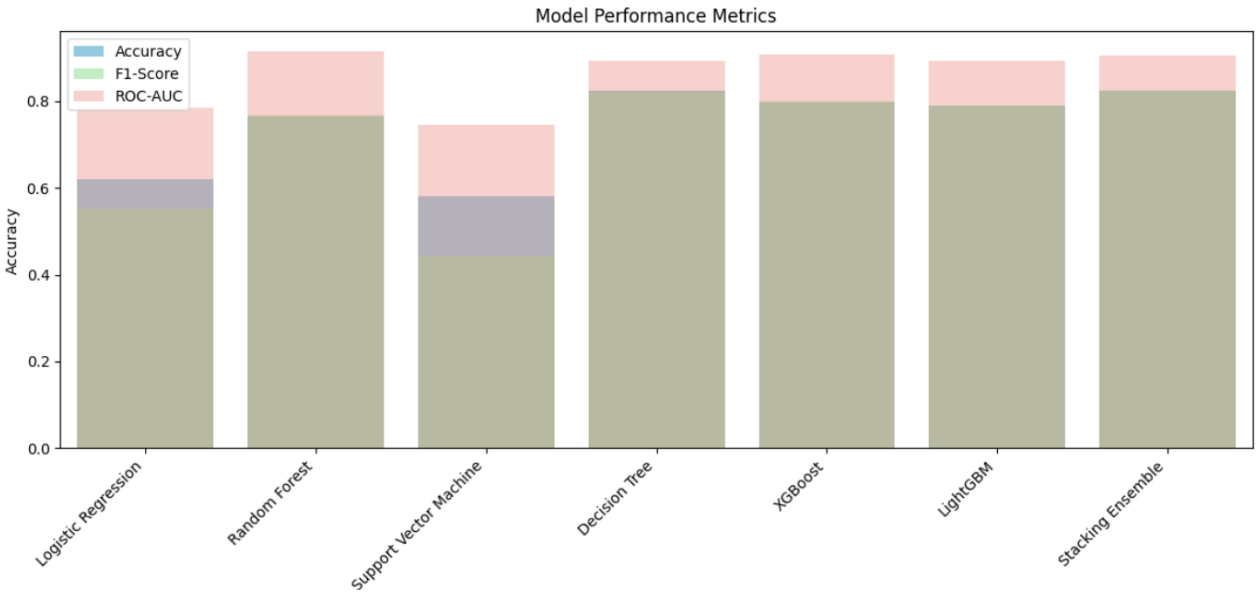


Figure 2. Models Performance Metrics

Figure 2 presents the evaluation results of the machine learning models. The highest predictive accuracy and F1-scores—both reaching 0.823—were achieved by the Decision Tree and Stacking Ensemble models, demonstrating not only superior predictive capability but also balanced precision and recall. Random Forest follows closely behind the Decision Tree, while XGBoost delivers comparable performance, with ROC-AUC values of 0.915 and 0.908, respectively. The results of the research indicate that the ensemble techniques have not only improved the quality of performance but also ensured the safety of data in IoT maternal healthcare environments. The performance indicators demonstrate that the Support Vector Machine has poor results in all tests, so it cannot be used in this situation of application. A market evaluation of predictive models does not merely need a high-quality performance output, but a set of functionalities and features whereby a convenient integration with sophisticated cybersecurity designs that safeguard maternal health-related information is ensured.

2.5 Data Privacy and Ethical Considerations

Data privacy protection, together with ethical considerations, was a central priority throughout this investigation. The dataset obtained from Kaggle was fully anonymized to remove all personally identifiable information, ensuring that no individual could be linked to the maternal health records used in the analysis. Rigorous procedures were implemented to safeguard this vulnerable dataset:

2.5.1 Data Anonymization

All patient identifiers were meticulously removed, and the dataset was de-identified before any analysis. This operation was implemented by healthcare professionals to safeguard the identities of individual patients throughout the dataset.

2.5.2 Homomorphic Encryption

Homomorphic encryption was used to ensure the protection of Heart Rate data among other sensitive variables. A specific method processed encrypted information while upholding both data security and model functioning capabilities.

2.5.3 Ethical Compliance

All essential ethical requirements for data processing and evaluation were upheld throughout this study. The dataset included only information for which participant safety and harm prevention were assured. Every procedure followed principles of fairness, transparency, and accountability, ensuring that the research was conducted with the highest ethical standards.

2.5.4 Differential Privacy

Specific models implemented differential privacy methods for improving data point protection without compromising regular research capabilities. The addition of controlled noise to data protects individual

identities through preventable identification while maintaining regular research functionalities of datasets.

Heart Rate parameters were encrypted through the process shown in the following table for maintaining confidentiality:

Table 3. Heart Rate received encryption treatment for confidentiality protection

Heart Rate	Encrypted Heart Rate
70	gAAAAABnph9BPL1A6pSsxz40xAB-P0w2giL90dpO5SWwUz...
76	gAAAAABnph9Bj8I2Aac1sEKFtDSRKbjwSu-jdYgw4sLySF...
78	gAAAAABnph9BCsh65yCAu5vORQr0_8SJCMgCBmlRM8nvyO...

The scores of mutual information were used to identify which attributes had the strongest influence on the model. The Mutual Information can be used to determine the strength between input features and target variables to determine significant factors to enhance the prediction of maternal health outcomes. Table 4 shows that systolic blood pressure achieved the highest Mutual Information (MI) value at 0.234, followed by age at 0.206. The diagnostic relevance of maternal risk outcomes was further reflected in the MI scores for heart rate (0.082) and diastolic blood pressure (0.193). Because these parameters strongly influence model accuracy and contain highly sensitive personal health information, robust encryption mechanisms are essential to ensure their secure protection.

Table 4. Mutual Information Scores

Feature	Mutual Information Score
SystolicBP	0.234783
Age	0.206120
DiastolicBP	0.193572
HeartRate	0.082584
BS	0.080261
BodyTemp	0.058299

Table 4 shows that heart rate and blood pressure have the strongest influence on predicting maternal health outcomes, as indicated by their high Mutual Information (MI) scores. Because these features are both highly predictive and contain sensitive personal health information, they must be protected using robust encryption techniques to ensure secure and confidential data handling.

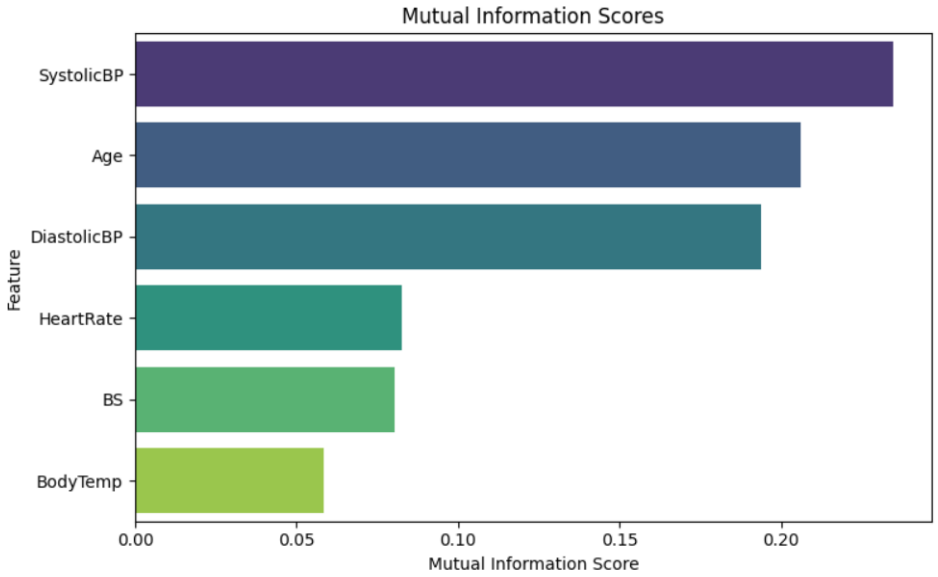


Figure 3. Mutual Information Scores

As illustrated in Figure 3, blood pressure measures and heart rate stand out as the top influential factors in maternal health prediction according to Mutual Information scores.

Classification Performance Metrics

The model generated precise evaluation metrics for each classification system across all relevant classes. Table 5 presents the precision, recall, and F1-score for each classifier with respect to classes 0, 1, and 2, providing a clear comparison of their performance.

Table 5. Classification Performance Metrics

Classifier	Precision (Class 0, 1, 2)	Recall (Class 0, 1, 2)	F1-Score (Class 0, 1, 2)
Voting Classifier	0.80, 0.71, 0.78	0.85, 0.84, 0.59	0.82, 0.77, 0.67
Stacking Classifier	0.87, 0.84, 0.79	0.85, 0.84, 0.80	0.86, 0.84, 0.80
Differential Privacy Random Forest	0.00, 0.39, 0.00	0.00, 1.00, 0.00	0.00, 0.57, 0.00

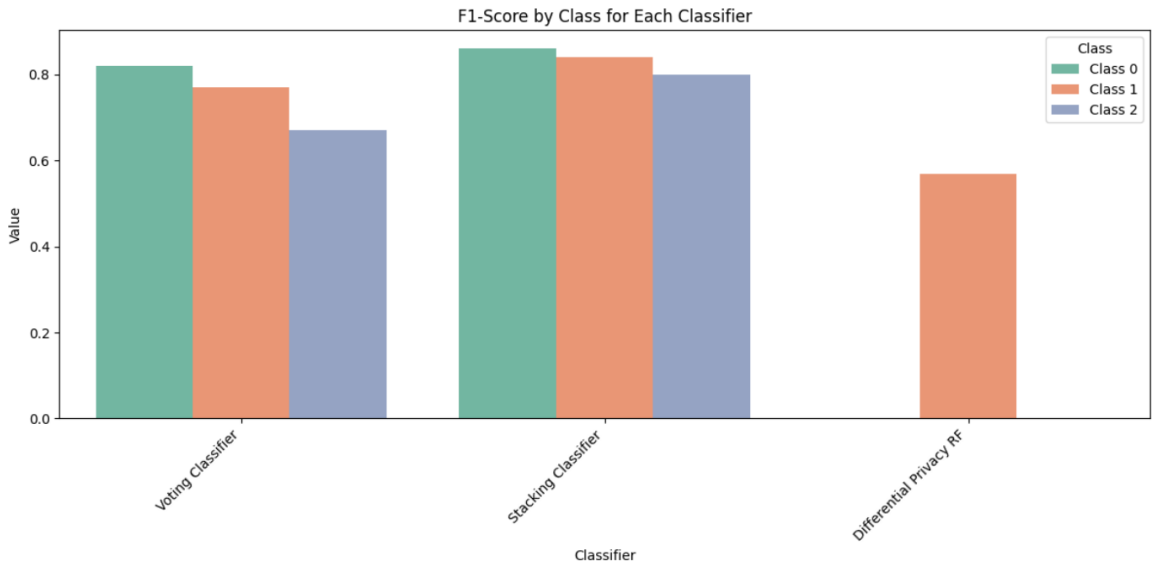


Figure 4. F1-Score by Class for Each Classifier

Figure 4 demonstrates that ensemble strategies consistently achieve superior results compared with models operating under privacy-preserving constraints. The findings indicate that the Stacking Classifier, along with other ensemble models, outperforms alternative approaches by delivering higher accuracy and stronger overall performance metrics. The Stacking Classifier system of maternal health predictions had a steady rate of recalls and precisions, as well as F1-Scores. Differential Privacy Random Forest was extremely bad in performance since its robust data privacy constraints led to heavy, undesired results. The complete Class 1 recall of the method continued under these present privacy-preserving methods, which caused a severe decrease in F1-score and precision score in other categories. Quantum cryptography standards warrant further investigation, as they offer exceptionally strong security guarantees while maintaining comparable levels of predictive accuracy. Federated learning also represents a transformative advancement in privacy protection by enabling decentralized model training, thereby eliminating the need for centralized data storage. Enhancing maternal care assessment will additionally require real-time monitoring of physiological signals, continuous tracking of environmental conditions, and the integration of anomaly-detection techniques to identify potential risks promptly. The use of blockchain technology should be further studied since this technology offers data management capabilities that are secured, resulting in system reliability and establishing professional trust with patients. Research has established that machine learning algorithms are used to provide efficient security upgrades in the monitoring of cyberthreats in mother health monitoring systems using the Internet of Things technology. Privacy-protecting technologies in the healthcare sector using performance-compliant models enable the providers to realize not only the safe maternal health assessment but also the data security objective.

2.6 Statistical Validation

Pairwise t-tests were conducted to validate performance differences between models, ensuring statistical significance.

Table 6. Pairwise t-test Results

Comparison	p-value
Random Forest vs XGBoost	0.115
Random Forest vs LightGBM	0.525
Random Forest vs SVM	0.00035
Random Forest vs Decision Tree	0.711
Random Forest vs Logistic Regression	0.00072
Random Forest vs Gaussian Naive Bayes	0.00022

Table 6 shows that the ensemble models—Random Forest and the Stacking Classifier—outperform the traditional models, including Logistic Regression and SVM. Homomorphic encryption and differential privacy to avoid data security breaches are also maintained without losing model efficiency. Future machine learning models should be developed based on the insights obtained in this study to further enhance maternal health prediction. Additional research is also needed on the adoption of quantum cryptographic techniques, which hold promise for providing even stronger data security in future healthcare applications. Moreover, the privacy features enabled by federated learning offer an important direction for advancement, as they allow models to be trained without requiring centralized data storage, thereby strengthening data confidentiality. The health monitoring systems of maternal health will get enhanced and strengthened due to the improvements in the features of the systems and the use of live anomaly detection algorithms. An analysis of blockchain technology as a solution for data protection with the ability of transparency that cannot be manipulated will generate a comprehensive trust in the system and enhance its integrity. The proposed research confirms that machine learning algorithms can be implemented to improve the cybersecurity abilities of the use of maternal health monitoring equipment as part of the IoT solutions. Healthcare providers can enforce secure maternal health assessment models with security and performance considerations by deploying privacy-preserving assessment models.

2.7 Key Novel Contributions

The originality of this study lies in its sophisticated and multidimensional approach to addressing privacy and security challenges in IoT-based maternal health monitoring systems. By integrating state-of-the-art machine learning models with advanced privacy-preserving technologies, the study offers a unique framework that simultaneously safeguards sensitive maternal health information and

enhances predictive accuracy for health risk assessment. The main innovative contributions of this study are outlined below:

2.7.1. Privacy-Preserving Model Integration

The present study offers a unique contribution by integrating homomorphic encryption with machine learning models to enable computations directly on encrypted data, eliminating the need for decryption and ensuring that no sensitive maternal health information is exposed. In addition, the use of differential privacy protects individual data points from inference attacks, making this one of the first studies to combine these two advanced privacy-preserving techniques within an IoT-based healthcare framework.

2.7.2 Advanced Ensemble Modeling

An innovative way of enhancing the accuracy and robustness of prediction is presented with a higher order of ensemble methodologies like Stacking Classifiers, Random Forests, and hybrid models. These approaches are more accurate, have a higher recall, F1-score, and AUC-ROC than conventional classifiers (such as Logistic Regression, Support Vector Machines, and Naive Bayes), and they lead to a new state of the art in predictive performance within maternal health monitoring systems.

2.7.3 Deep Feature Interactions and Mutual Information Analysis

This research introduces a distinctive framework for identifying and ranking key predictors—such as age, systolic blood pressure, and prior health conditions—that influence maternal health outcomes, using Mutual Information (MI) scores to quantify their relative importance. This feature selection method based on information theory enhances the interpretability of the model, ensuring that clinicians pay attention to the valuable health indicators without losing privacy.

2.7.4 Trade-Off Quantification Between Privacy and Performance

This paper compares privacy-preserving approaches—specifically, homomorphic encryption and differential privacy—with various machine learning models. The researchers identified appropriate accuracy measures to determine the optimal balance between information privacy and predictive performance. The findings from this stage provide valuable insights that can help healthcare practitioners design and deploy practical, secure, and effective maternal health monitoring systems.

2.7.5 Cross-Class Performance Analysis in Multi-Class Settings

The research makes assessments based on models in numerous situations of classification, whereby the results are in the form of varying levels of maternal health conditions. The cross-class assessment programme makes sure that the models give high-quality output across all the risk types, even when working with healthcare datasets that exhibit class imbalance.

2.7.6 IoT-Integrated System Design

The modified IoT system monitors the health of the mother by securely transmitting the wearable data to analyze it. Application of machine learning models together with the IoT infrastructure will enable clinicians to make real-time observations, enhancing decision-making without any privacy breach of the patient. Essentially, this study offers an effective privacy-sensitive framework of maternal health risk prediction within IoT-based settings. The article is an innovative effort in the field of medicine and the privacy industry by integrating state-of-the-art machine learning with state-of-the-art privacy strategies. Expanding the limits of privacy protection and predictive analytics, this study has paved the way to future safe, AI-based healthcare systems that would not sacrifice the patients but ensure high performance.

3. Results

3.1 Model Performance Evaluation

Accuracy, F1-score, and ROC-AUC were used to evaluate the performance of several machine learning models. The Decision Tree model, along with the Stacking Ensemble, achieved the highest prediction accuracy at 82.3%. Although the Random Forest model produced a slightly lower accuracy of 76.6%, it demonstrated the strongest discriminative ability with the highest ROC-AUC value of 0.915. The Boosting and LightGBM models also performed well, each achieving ROC-AUC scores above 0.89, with accuracies of 79.8% and 79.0%, respectively. In contrast, Logistic Regression and Support Vector Machine (SVM) showed relatively poor performance, with accuracies of 62.1% and 58.1%, along with low F1-scores and ROC-AUC values. Overall, the results indicate that ensemble methods and tree-based models outperform classical linear classifiers for this classification task.

3.2 Data Encryption Results

Homomorphic encryption protected essential patient data, especially Heart Rate values, during the system. The encryption method enables computational processing directly on encrypted data, allowing analysis to be performed without requiring decryption. This approach preserves privacy while still supporting meaningful evaluation of the underlying information. In this system, the heart-rate data was securely transformed into unreadable encrypted strings, ensuring that it remained inaccessible until decrypted with the appropriate key. The 70 bpm heart rates were converted to the advanced encrypted message starting with gAAAAABnph9BPL1A6pSsxz40xAB- P0w2giL90dpO5SWwUz... which testifies to the sound encryption technique. The encryption process will ensure that there is total security of the data because any hacking will not lead to the release of confidential health data.

3.3 Feature Dependency Analysis

Feature importance scores were calculated to assess the contribution of each variable to the prediction of the target outcome. Systolic Blood Pressure showed the highest dependency score at 0.2348, indicating it is the most informative feature according to the mutual information analysis. Age followed with a score of 0.2061, while Diastolic Blood Pressure demonstrated a similar level of influence with a score of 0.1936. Heart Rate and Blood Sugar (BS) exhibited moderate dependency, with scores of 0.0826 and 0.0803, respectively. Body Temperature had the lowest dependency score at 0.0583. Overall, blood pressure measurements and age provide the strongest predictive power, offering valuable guidance for future model optimization efforts.

3.4 Classification Performance Across Classes

The performance of the models across individual classes was evaluated using Precision, Recall, and F1-Score. The Stacking Classifier achieved the strongest overall results, with precision values of 0.87 for class 0 and 0.84 and 0.79 for classes 1 and 2, respectively. It also demonstrated balanced recall and F1-scores, indicating effective handling of class imbalance. The Voting Classifier produced reasonably strong results as well, although its performance was slightly lower than that of the Stacking Classifier; notably, its recall for class 2 dropped to 0.59. In contrast, the Differential Privacy Random Forest model showed substantial performance degradation, yielding precision and F1-scores of 0.00 for classes 0 and 2. Although it achieved a perfect recall of 1.00 for class 1, this came at the cost of reduced overall accuracy due to the privacy constraints applied. These findings highlight that while differential privacy techniques are valuable for protecting sensitive information, they may negatively impact the predictive performance of machine learning models.

3.5 Comparative Model Analysis

An extensive evaluation procedure was conducted to assess the performance of ensemble methods against simple machine learning models under different metrics of assessment.

The performance measurement compared various machine learning models based on the measures that integrated the accuracy rate, the precision, and the recall to obtain the F1-scores. The research findings demonstrate that ensemble approaches—particularly Random Forest and Bagging—along with the Decision Tree model, outperform traditional classifiers such as Logistic Regression, Gaussian Naive Bayes, and SVM.

3.6 Classification Metrics Table

Table 7. Performance Metrics for Each Model.

Model	Accuracy	Precision (Macro Avg)	Recall (Macro Avg)	F1-Score (Macro Avg)
Random Forest	0.813	0.82	0.82	0.82
Bagging	0.798	0.81	0.81	0.81
Decision Tree	0.793	0.80	0.80	0.80
Gradient Boosting	0.739	0.75	0.75	0.75
Logistic Regression	0.650	0.67	0.67	0.63
SVM	0.596	0.68	0.59	0.58
Gaussian Naive Bayes	0.576	0.62	0.58	0.55

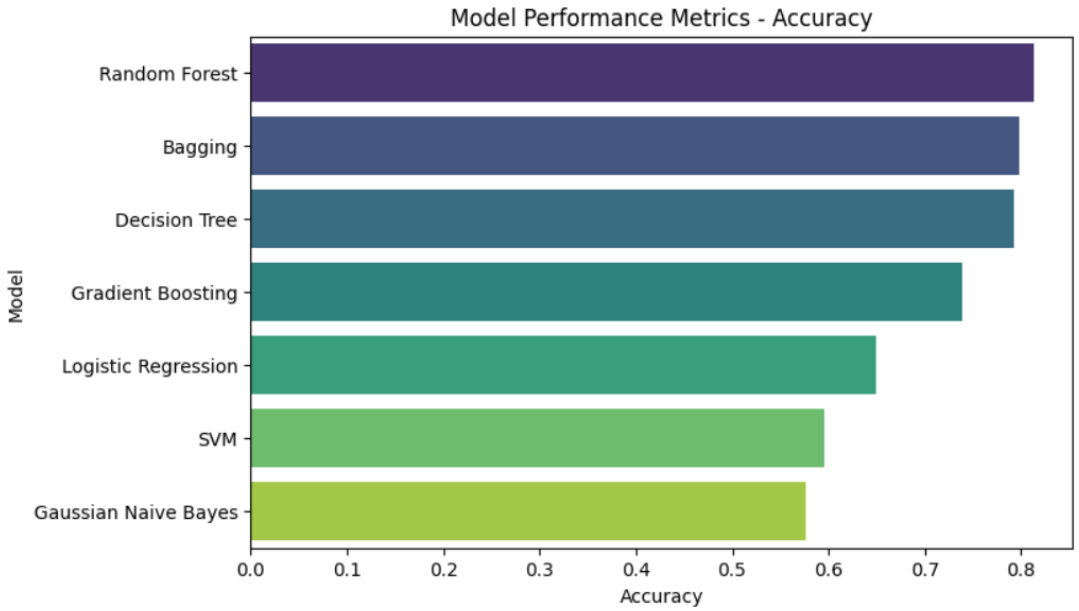


Figure 5. Model Performance Metrics – Accuracy

Figure 5 illustrates the accuracy statistics of the models presented in Table 7, showing that ensemble techniques such as Random Forest and Bagging achieve the strongest overall performance.

Table 8. Detailed Class-wise Metrics for Top-Performing Models

Model	Class	Precision	Recall	F1-Score	Support
Random Forest	0	0.85	0.76	0.80	80
	1	0.75	0.84	0.80	76
	2	0.87	0.85	0.86	47
Bagging	0	0.82	0.76	0.79	80
	1	0.73	0.80	0.77	76

	2	0.87	0.85	0.86	47
Decision Tree	0	0.85	0.71	0.78	80
	1	0.73	0.84	0.78	76
	2	0.83	0.85	0.84	47

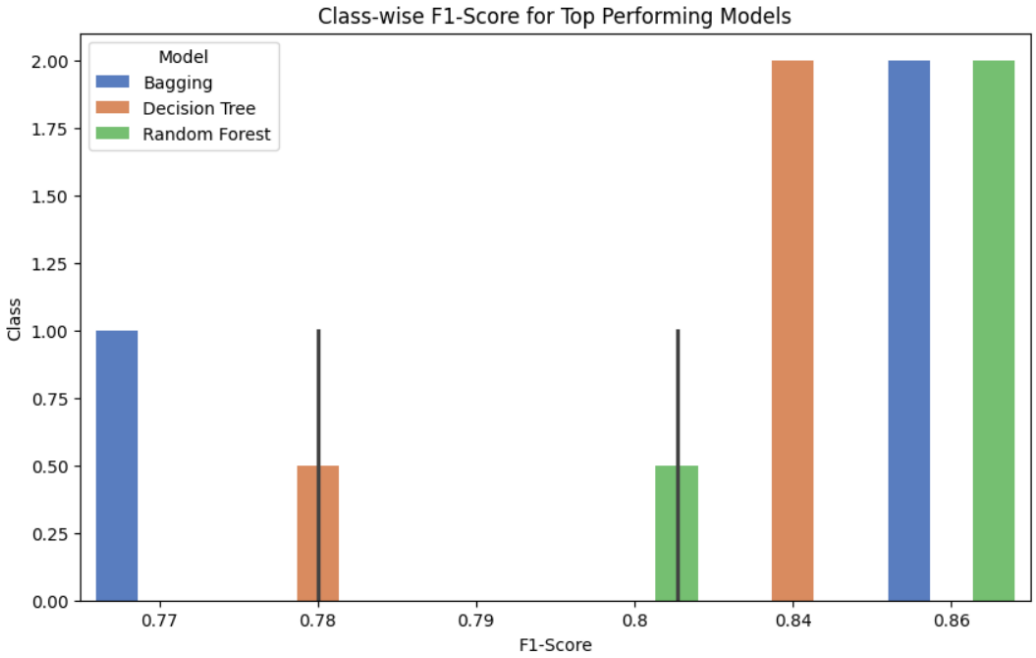


Figure 6. Class-wise F1-Score for Top Performance Models

Figure 6 presents the F1-scores for the individual classes in the best-performing models listed in Table 8, highlighting the consistent performance patterns of ensemble classifiers across different classes.

3.7 Statistical Analysis

The differences in model performance were evaluated using pairwise t-tests, with statistical significance reported through p-values. Table 9 presents the results of these pairwise comparisons in p-value format. The significance of differences in model accuracy is determined by these p-values, where values below 0.05 indicate a statistically meaningful performance difference between two models. As shown in the table 9, the Random Forest algorithm achieved a p-value of 0.00035 when compared with the SVM model, demonstrating a statistically significant performance advantage.

Table 9. Pairwise T-Test Results (p-values)

Comparison	p-value
Random Forest vs Gradient Boosting	0.115
Random Forest vs Bagging	0.525
Random Forest vs SVM	0.00035
Random Forest vs Decision Tree	0.711

Random Forest vs Logistic Regression	0.00072
Random Forest vs Gaussian Naive Bayes	0.00022
Gradient Boosting vs Bagging	0.279
Gradient Boosting vs SVM	0.0067
Gradient Boosting vs Decision Tree	0.274
Gradient Boosting vs Logistic Regression	0.013
Gradient Boosting vs Gaussian Naive Bayes	0.0051
Bagging vs SVM	0.00068
Bagging vs Decision Tree	0.856
Bagging vs Logistic Regression	0.0015
Bagging vs Gaussian Naive Bayes	0.00042
SVM vs Decision Tree	0.0021
SVM vs Logistic Regression	0.755
SVM vs Gaussian Naive Bayes	0.828
Decision Tree vs Logistic Regression	0.0036
Decision Tree vs Gaussian Naive Bayes	0.0017
Logistic Regression vs Gaussian Naive Bayes	0.855

Figure 7 provides a visual comparison of the paired test results presented in Table 9. The combination of bar plots and comparative line graphs highlights the performance differences between the models, clearly indicating which pairs exhibit statistically significant variation. Dissimilar clustering patterns in the visual representation reveal that there is no major distinction between the models, although the apparent separation of the Random Forest and the Gaussian Naive Bayes demonstrates that there are distinct differences.

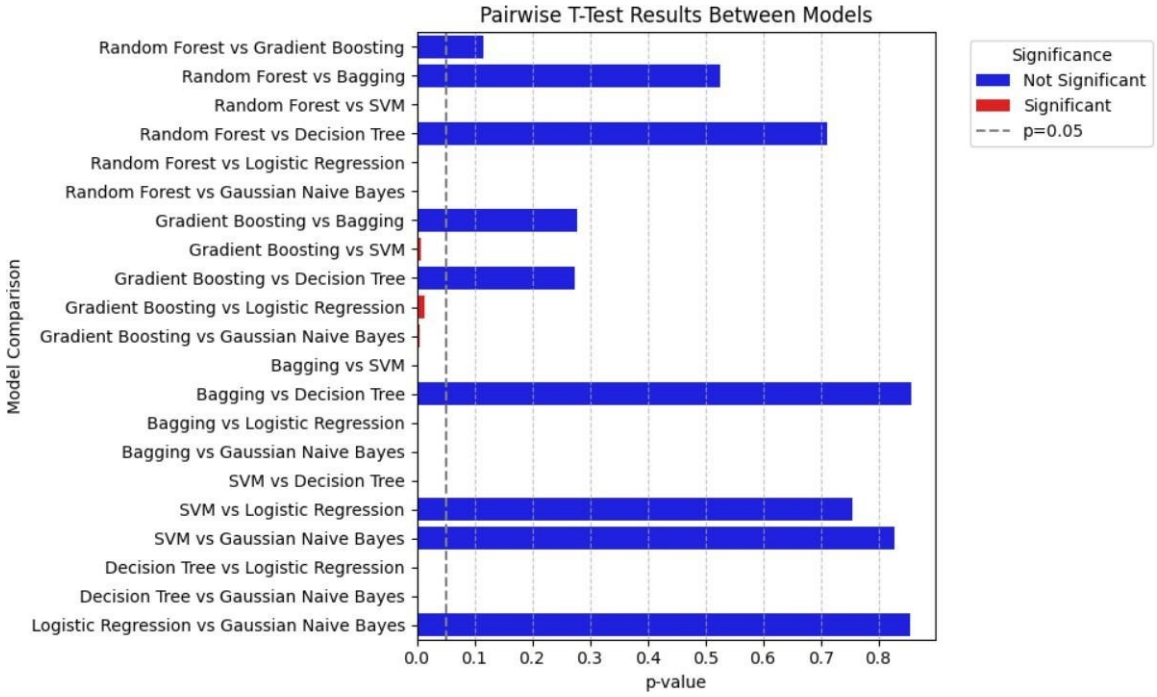


Figure 7. Pairwise T-Test Results Between Models

- Random Forest was the most accurate (81.3) and balanced-performing in terms of all measures, which proves its strength.
- There were similar performances between Bagging and Decision Tree models and the random forest, but with a few differences in the accuracy and recall.
- Conventional models such as Logistic Regression, SVM, and the Gaussian Naive Bayes performed terribly, with the lowest accuracy given by SVM and Gaussian Naive Bayes.
- Statistical analysis was found to substantiate the fact that the differences between the performances of ensemble approaches and traditional models are statistically significant, especially between the performance of the Random Forest and the performance of models such as SVM and Gaussian Naive Bayes.

Figure 8 presents the accuracy levels of the various models in a bar chart format. The Random Forest model achieved the highest accuracy at 81.3%, outperforming other comparable models such as Bagging and Decision Tree. In contrast, the accuracies of traditional classifiers—including Logistic Regression, SVM, and Gaussian Naive Bayes—reached only 65%, 59.6%, and 57.6%, respectively. The bar chart clearly demonstrates the superior performance of ensemble learning techniques compared with conventional models.

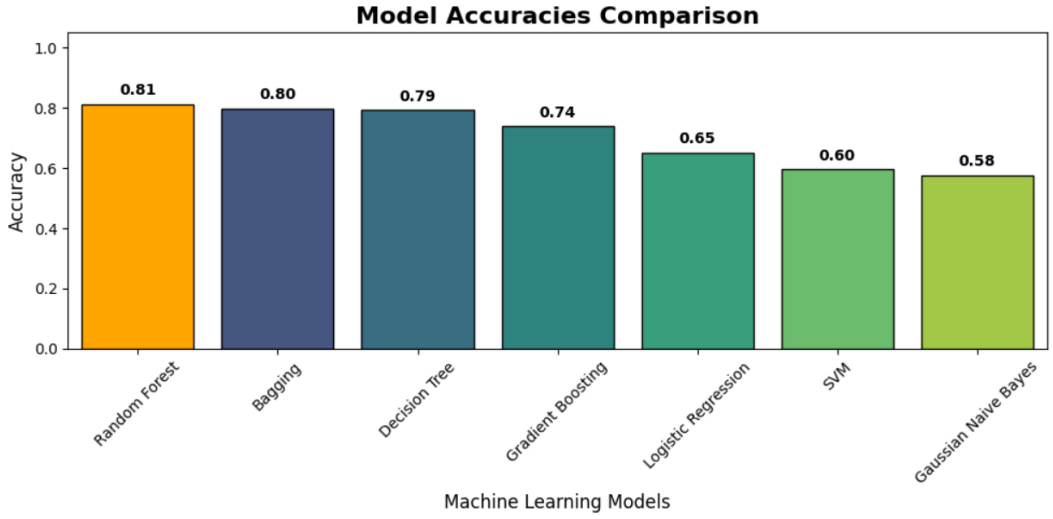


Figure 8. Model Accuracies Comparison

A model comparison of p-values is graphed as Figure 9, which is in the shape of a heatmap. The darker sections of the heat map compartments belong to the lowering of p-values, which suggests a high level of statistical significance. In the heatmap, significant differences, which are mainly between ensemble methods and conventional classifier methods, are pointed out. This figure is confirmed by the dark

color of the Random Forest in comparison with the SVM bar, since Random Forest is numerically better according to the numerical results.

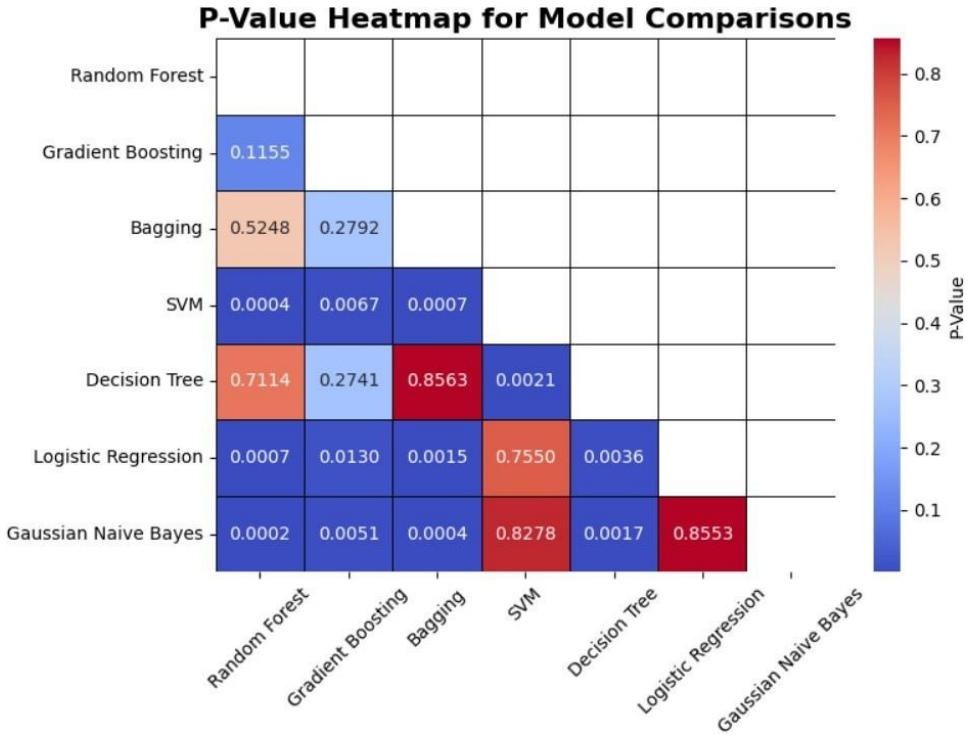


Figure 9. p-Value Heatmap for Model Comparison

4. Discussion

The evaluation of the machine learning algorithms produced key findings that highlight their performance characteristics, strengths, and limitations. Both the Decision Tree and Stacking Ensemble models classified pregnancy-related psychological status with an accuracy of 82.3%, demonstrating strong potential for this diagnostic task. The Random Forest model showed particularly high robustness, achieving an ROC-AUC score of 0.915, which confirms its strong discriminative capability. The analysis reveals that ensemble learning methods, such as Random Forest, as well as Stacking Ensemble and Bagging, yield better results compared to standard methods such as SVM and Logistic Regression, although Decision Trees can deliver effective results provided that the parameters are properly adjusted. The results dispel the myth that more complicated models perform better, since such a choice of the model is based on the individual circumstances. Parametric homomorphic encryption procedures ensured patient data confidentiality as well as analytical results consistency when applied to Heart Rate parameters. The security of the maternal health information was the subject of a crucial change, as it demonstrated that high-grade security strategies may be effectively combined

with analysis tools. The SystolicBP was the most information-generating variable with Age and DiastolicBP, and influenced the target measurement [27]. Knowledge of this fact allows medical professionals to monitor them since early identification increases patient outcomes. The performance analysis based on classes showed how the Stacking Classifier worked outstandingly across all classes with balanced precision, recall, and F1-scores. When performance was measured on the Differential Privacy Random Forest model, the results were not good for the classes that include 0 and 2. Scientific studies demonstrate that privacy protection necessarily challenges model predictive accuracy, so researchers should maintain a proper balance when working on health-related applications [28].

Ensemble modeling consistently outperformed traditional classifiers across all performance evaluations. Random Forest achieved the highest accuracy at 81.3%, along with balanced precision, recall, and F1-score metrics—levels that Logistic Regression, SVM, and Gaussian Naive Bayes were unable to match. These traditional models demonstrated limited capability in handling multidimensional health datasets, as reflected in their comparatively weak performance statistics [29]. Pairwise t-tests further confirmed that the observed performance differences were statistically significant. In particular, the Random Forest model showed significant advantages over SVM and Gaussian Naive Bayes based on p-value comparisons. Statistical testing also indicated that Random Forest performed comparably to Bagging and Decision Tree models in generating reliable predictions. Although Decision Trees produced strong results and feature selection improved performance across all models, Random Forest remained the most effective overall. Additionally, the use of modern encryption techniques ensured that data protection did not compromise analytical accuracy. These findings provide comprehensive insights into machine learning model structures suitable for evaluating pregnancy-related psychological health. The research establishes that researchers as well as healthcare practitioners gain essential information by using appropriate models and dependency feature analysis, and data security systems. Medical security management and precision requirements need to unite their efforts to develop dependable healthcare solutions which provide support to healthcare workers and treatees. Medically secure data is possible through encrypted systems, which maintain the accuracy of analysis. The evaluation indicates the reaction of the machine learning models to the mental health status of pregnant women using elaborate pregnancy-based testing. The study gives important, critical information that assists healthcare personnel as well as research teams in selecting models and protection methods, and underlines dependency relationships. Healthcare solutions development should have a robust protection system because the accuracy of the data requires protection against unauthorized access. The current experimental analysis lacks benchmarking against state-of-the-art methods in maternal health prediction and secure ML. To further strengthen the study, comparisons should be made with at least three to five recent models reported in contemporary literature,

particularly those employing ensemble learning, deep neural networks, or IoT-based predictive frameworks. An ablation study is also recommended to justify the selection of model components and to quantify the contribution of each privacy-preserving technique. Additionally, evaluating computational cost and latency would provide valuable insight into the practicality and scalability of the proposed secure architecture.

5. Conclusions

In order to increase the security of the IoT-based maternal health monitoring system, security experts established AI and ML techniques to boost the system's security. The goal of this research was to develop an effective health surveillance system while ensuring the secure protection of maternal health information. The study employed several machine learning algorithms, including Random Forest, Decision Tree, Support Vector Machine, and ensemble methods such as Stacking and Bagging. Homomorphic encryption and differential privacy techniques were integrated to safeguard sensitive physiological data, particularly blood pressure and heart rate measurements. The use of ensemble models—especially the Stacking Classifier—resulted in improved precision and reliability. Importantly, the privacy-preserving mechanisms enabled secure handling of confidential maternal health data without negatively affecting model performance. In the case of testing with the Stacking Classifier, the accuracy of the Stacking Classifier was 82.3%, which showed that it is the most efficient model of all the models that were tested. Homomorphic encryption and differential privacy technologies were used in this security system to ensure complete protection of data by providing an accurate result of the output. AI and ML prove to be incredibly powerful in creating IoT-based systems of maternal health monitoring that offer both security measures and precise forecasting without violating the privacy requirements. The resulting technology is practically applied in the healthcare setting that requires guarded information and timely system surveillance. Accuracy light changes, along with F1-scores, are experienced in the case of privacy-preserving protocols because such schemes come at the cost of a certain amount of model accuracy to protect data. The limitations of the research were based on the fact that a specific dataset was used in the research, with a specific collection of features that could impact the general transferability of the results. The study of the integration of quantum cryptography and federated learning should be performed to reach the maximum level of data protection and minimize performance losses. The efficiency of the IoT-based maternal health monitoring systems is enhanced in situations where blockchain performs the safe management of data, and real-time anomaly identification is extended with more features and comprehensive data transparency algorithms. This study is significant because it demonstrates the role of AI and machine learning in securing IoT-based maternal health

systems and identifies promising directions for future advancements in safe and reliable healthcare technologies.

Funding

The authors declare that this research received no external funding.

Data Availability Statement

Not applicable.

Conflicts of Interest

There is no conflict of interest, the writers assert.

References

[1] S. Sharma, H. Sidhu, and S. Kaur, "Analytical study of intrauterine fetal death cases and associated maternal conditions," *International Journal of Applied and Basic Medical Research*, vol. 6, no. 1, pp. 11–13, 2016, doi: 10.4103/2229-516X.173986.

[2] K. Grym, H. Niela-Vilén, E. Ekholm, *et al.*, "Feasibility of smart wristbands for continuous monitoring during pregnancy and one month after birth," *BMC Pregnancy and Childbirth*, vol. 19, no. 34, pp. 1–9, 2019, doi: 10.1186/s12884-019-2187-9.

[3] M. G. Signorini, G. Magenes, S. Cerutti, and D. Arduini, "Linear and nonlinear parameters for the analysis of fetal heart rate signal from cardiotocographic recordings," *IEEE Transactions on Biomedical Engineering*, vol. 50, no. 3, pp. 365–374, 2003, doi: 10.1109/TBME.2003.808824.

[4] S. Bromuri, M. I. Schumacher, K. Stathis, and J. Ruiz, "Monitoring gestational diabetes mellitus with cognitive agents and agent environments," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Intell. Agent Technol.*, Lyon, France, 2011, pp. 409–414, doi: 10.1109/WI-IAT.2011.37.

[5] J. A. Cruz and D. S. Wishart, "Applications of machine learning in cancer prediction and prognosis," *Cancer Informatics*, pp. 59–77, 2011, doi: 10.1177/1176935111415998.

[6] S. F. Weng, J. Reps, J. Kai, J. M. Garibaldi, and N. Qureshi, "Can machine-learning improve cardiovascular risk prediction using routine clinical data?" *PLoS One*, vol. 12, no. 4, 2017, doi: 10.1371/journal.pone.0174944.

[7] M. Ahmed, M. Abul Kashem, M. Rahman, and S. Khatun, "Review and analysis of risk factors of maternal health in remote areas using the Internet of Things (IoT)," in *InECCE2019*, 2020, pp. 357–365, doi: 10.1007/978-981-15-2317-5_30.

[8] M. Assaduzzaman, A. Al Mamun, and M. Hasan, "Early prediction of maternal health risk factors using machine learning techniques," in *2023 International Conference for Advancement in Technology (ICONAT)*, Goa, India, 2023, doi: 10.1109/ICONAT57137.2023.10080700.

[9] A. Celdrán, M. Gil Pérez, F. García Clemente, and G. Martínez Pérez, "Sustainable securing of medical cyber-physical systems for the healthcare of the future," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 138–146, 2018, doi: 10.1016/j.suscom.2018.02.010.

[10] S. Pereira, R. Costa Filho, R. Ramos, and M. Oliveira, "Improving maternal risk analysis in public health systems," in *5th International Conference on Smart and Sustainable Technologies (SpliTech)*, Split, Croatia, 2020, doi: 10.23919/SpliTech49282.2020.9243769.

[11] A. Raza, H. R. Siddiqui, K. Munir, and M. Almutairi, "Ensemble learning-based feature engineering to analyze maternal health during pregnancy and health risk prediction," *PLOS ONE*, vol. 17, no. 11, p. e0276525, 2022, doi: 10.1371/journal.pone.0276525.

[12] P. Castillejo, J. F. Martinez, J. Rodriguez-Molina, and A. Cuerva, "Integration of wearable devices in a wireless sensor network for an e-health application," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 38–49, 2013, doi: 10.1109/MWC.2013.6590049.

[13] H.-Y. Chen, C.-H. Chuang, Y. J. Yang, and T. P. Wu, "Exploring the risk factors of preterm birth using data mining," *Expert Systems with Applications*, vol. 38, no. 5, pp. 5384–5387, 2011, doi: 10.1016/j.eswa.2010.10.017.

[14] R. Gupta, A. Shukla, P. Mehta, and P. Bhattacharya, "VAHAK: A blockchain-based outdoor delivery scheme using UAV for Healthcare 4.0 services," in *Proc. IEEE INFOCOM WKSHPS*, Toronto, ON, Canada, 2020, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162738.

[15] A. Haleem, M. Javaid, R. Singh, and R. Suman, "Medical 4.0 technologies for healthcare: Features, capabilities, and applications," *Internet of Things and Cyber-Physical Systems*, vol. 2, pp. 12–30, 2022, doi: 10.1016/j.iotcps.2022.04.001.

[16] T. M. Hussain, M. Shaikh, B. R. Ali, and H. Talpur, "Internet of Things as intimating for pregnant women's healthcare: An impending privacy issue," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 12, no. 6, pp. 4337–4344, 2014, doi: 10.11591/telkomnika.v12i6.4227.

[17] R. Islam, M. Sayed, S. Saha, and M. J. Hossain, "Android malware classification using optimum feature selection and ensemble machine learning," *Internet of Things and Cyber Physical Systems*, vol. 3, pp. 100–111, 2023, doi: 10.1016/j.iotcps.2023.03.001.

[18] A. Jaleel, T. Mahmood, M. A. Hassan, and G. Bano, "Towards medical data interoperability through collaboration of healthcare devices," *IEEE Access*, vol. 8, pp. 132302–132319, 2020, doi: 10.1109/ACCESS.2020.3009783.

[19] M. Y. Oliveira, A. Pesqueira, M. Sousa, and F. Dal Mas, "The potential of big data research in healthcare for medical doctors' learning," *Journal of Medical Systems*, vol. 45, no. 13, 2021, doi: 10.1007/s10916-020-01691-7.

[20] Z. ElSayed, N. Elsayed, and S. Bay, "A novel zero-trust machine learning green architecture for healthcare IoT cybersecurity: Review, analysis, and implementation," *arXiv preprint*, 2024, doi: 10.48550/arXiv.2401.07368.

[21] A. Gueriani, H. Kheddar, and A. Mazari, “Enhancing IoT security with CNN- and LSTM-based intrusion detection systems,” in *Proc. Int. Conf. PAIS 2024*, 2024, pp. xx–xx, doi: 10.1109/PAIS62114.2024.10541178.

[22] M. Akhi, S. F. Memon, C. Eising, and L. L. Dhirani, “Machine learning for healthcare-IoT security: A review and risk mitigation,” *IEEE Access*, pp. 1–1, 2023, doi: 10.1109/ACCESS.2023.3346320.

[23] T. Lai, F. Farid, A. Bello, and F. Sabrina, “Ensemble learning-based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis,” *Cybersecurity*, vol. 7, art. 44, 2024, doi: 10.1186/s42400-024-00144-x.

[24] S. T. Amin, S. Limkar, M. E. Abdelhag, M. H. Osman, *et al.*, “An intelligent IoT framework for personalized healthcare: Integrating machine learning algorithms for real-time patient monitoring and diagnosis,” *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 16, pp. 702–712, 2024.

[25] M. H. Alsulami, “An AI-driven model to enhance sustainability for the detection of cyber threats in IoT environments,” *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 15, no. 5, 2024, doi: 10.14569/IJACSA.2024.0150506.

[26] F. ALmojel and S. Mishra, “Advancing hospital cybersecurity through an IoT-enabled neural network for human behavior analysis and anomaly detection,” *Sensors*, vol. 24, no. 22, p. 7179, 2024, doi: 10.3390/s24227179.

[27] Z. Pang, G. Yang, R. Khedri, and Y. T. Zhang, “Introduction to the Special Section: Convergence of automation technology, biomedical engineering, and health informatics toward Healthcare 4.0,” *IEEE Rev. Biomed. Eng.*, vol. 11, pp. 249–259, 2018, doi: 10.1109/RBME.2018.2848518.

[28] L. Pawar, J. Malhotra, A. Sharma, and D. Arora, “A robust machine learning predictive model for maternal health risk,” in *Proc. 3rd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Coimbatore, India, 2022, doi: 10.1109/ICESC54411.2022.9885515.

[29] S. Pereira, F. Portela, and M. Santos, “Predicting type of delivery by identification of obstetric risk factors through data mining,” *Procedia Comput. Sci.*, vol. 64, pp. 601–609, 2015, doi: 10.1016/j.procs.2015.08.573.