International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-14, Issue-1, January 2026
DOI: https://doi.org/10.55524/ijircst.2026.14.1.19
Article ID IJIRE-1421, Pages 179-189
www.ijircst.org

Machine Learning for Secure Cardiovascular Risk Assessment in Distributed Healthcare Environments

Aftab Tariq[1], Michidmaa Arikhad[2], and Adita Sultana[3]

[1, 2, 3] Department of Computer Science and Technology Engineering, American National University, Salem, USA

Correspondence should be addressed to Aftab Tariq; tariqa@students.an.edu

Received: 30 December 2025; Revised: 14 January 2026; Accepted: 29 January 2026

ABSTRACT- Cardiovascular diseases are leading cause of death worldwide. Risk assessment is extremely vital in prevention and treatment, and should be done early and accurately. Machine learning is commonly applied in the past few years to forecast cardiovascular risk based on healthcare data. This information comprises of electronic health records, medical images, wearable devices and genetic information. At the same time, healthcare systems are moving toward distributed environments that use mobile devices, cloud platforms, and the Internet of Medical Things. These systems improve access to care but also create serious problems related to data security and patient privacy. This review summarizes machine learning methods used for cardiovascular risk assessment in distributed healthcare systems. It also explains the main security and privacy challenges in these environments. In addition, the review discusses secure machine learning approaches such as federated learning and differential privacy. Finally, it highlights key research gaps and future directions to support safe and reliable use of machine learning in cardiovascular healthcare.

KEYWORDS- Cardiovascular Disease; Risk Assessment; Machine Learning; Distributed Healthcare; Data Security; Privacy Protection; Federated Learning; Internet of Medical Thing

I. INTRODUCTION AND MOTIVATION

Cardiovascular diseases are the leading cause of illness and death worldwide [1]. They include conditions such as heart attacks, strokes, and heart failure. These diseases affect people in both developed and developing countries. They also place a heavy burden on healthcare systems and national economies. Many cardiovascular events can be prevented if high-risk individuals are identified early [2]. For this reason, accurate cardiovascular risk assessment is a key goal of modern healthcare.

As seen in Figure 1, the rising burden of cardiovascular disease in the world has been increasing since 1990 [3]. In 2023, over 437 million disability-adjusted life years (DALYs) of cardiovascular diseases were reported across the globe [4]. The differences in terms of area, income, and sex are also enormous as indicated in the figure. The low- and middle-income countries have the heaviest burden of the disease and the disease burden is increasing at a faster rate among men than women [5]. These tendencies evidence the fact that there is a great necessity to find early, scalable, and efficient methods of the risk prediction that can be effective on various groups of people.

The traditional cardiovascular risk assessment tools are what are considered to be widely used in practice. They are Framingham Risk Score, ASCVD score and SCORE system. The instruments are founded on limited clinical variables such as age, blood pressure, cholesterol, smoking status and diabetes [6]. Although the above usefulness is there, there are serious limitations of these models. They are typically based on the frozen data which is collected when the patients visit the clinic. They may not cooperate with every population. They also do not quite identify more complex patterns and associations of risk factors [7]. Furthermore, the majority of traditional tools are hospital-centered and they do not imply the application of ongoing data of real life.

The new prediction tool of cardiovascular risks in the recent years is machine learning. The machine learning models allow processing of large and complex data. They get a chance to obtain patterns that are difficult to get with conventional statistical method. These models have been applied onto to electronic health records, medical images, electrocardiograms, wearable sensor data and genetic information [8]. It is discovered that the machine learning models are also more accurate in most occasions than the traditional risk scores. This makes machine learning a possible implementation in the early and individualistic cardiovascular risk assessment.

In the meantime, the healthcare systems are rapidly changing. Care is no longer a prerogative of the hospitals and clinics. The dispersed healthcare facilities are becoming more popular. This includes wearable, mobile health applications, telemedicine and Internet of Medical Things [9]. The data is being collected constantly and submitted as it passes through edge devices and cloud servers, as well as through healthcare facilities. It is also possible that electronic health record interoperability allows the transfer of data to other providers [10]. This action has an advantage of realizing the systems in real time and the long-term prediction of the risks but makes the system more complex.

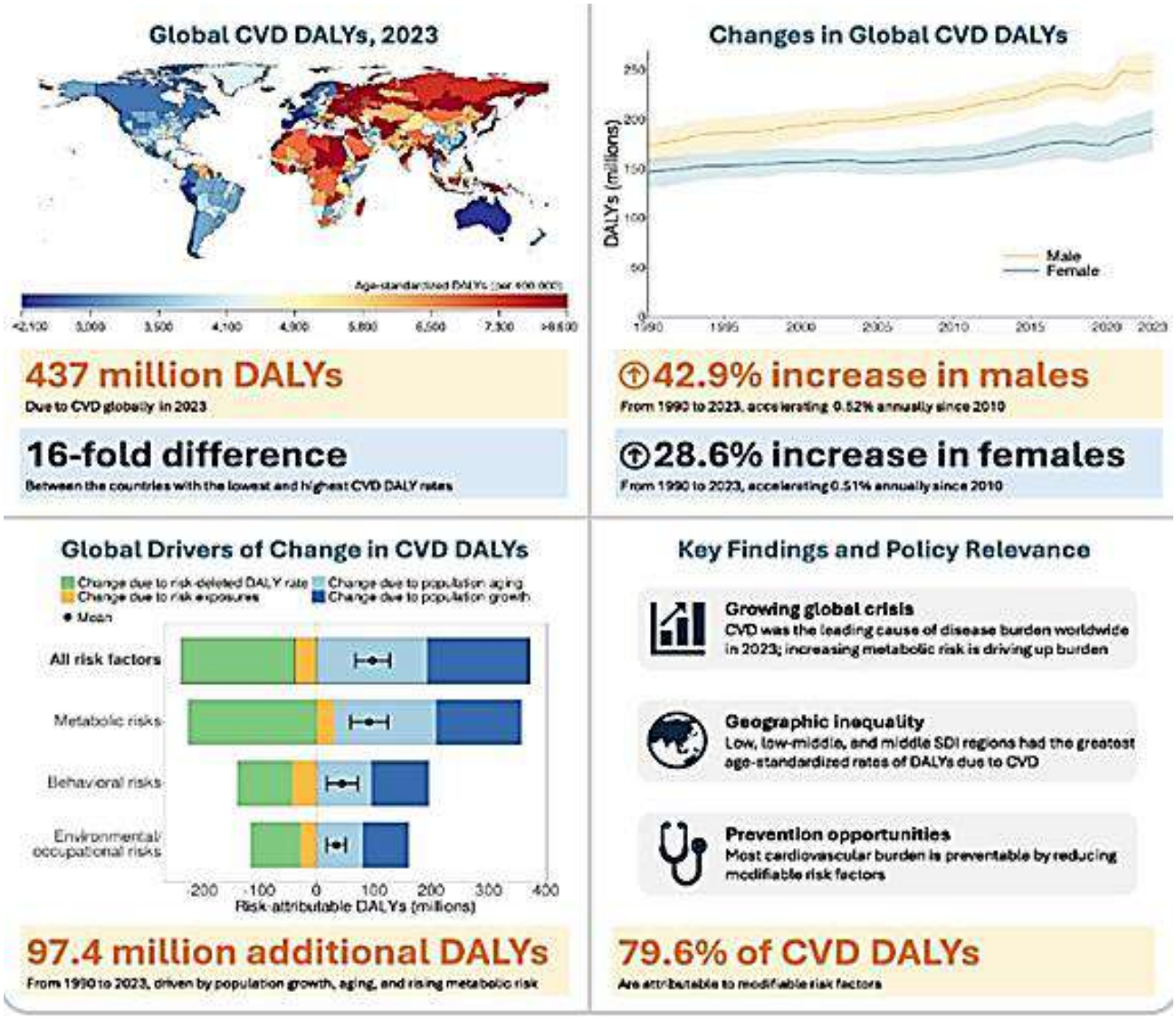

Figure 1: Global Burden of Cardiovascular Disease, Trends, and Risk Factors (1990–2023) [57]

The use of machine learning in medical facilities with a distributed nature poses major security and privacy challenges. Health information is rather delicate. Information leak, data hacking, and improper use of information can have detrimental effects on the patients and can reduce the trust between patients and the healthcare systems [11]. Other types of attacks which are vulnerable to distributed machine learning systems are also present and they are data leaking, data inversion and data poisoning. In addition, it has strict regulations that would require the outstanding protection of patient data. The bulk of the machine learning literature which is available today is focused on understanding how accurate the prediction is but does not devote much focus on these security and privacy risks.

This leaves a gap in research. Even though many machine learning-based cardiovascular risk assessment models have been proposed, the literature of the applicability of such models within a distributed healthcare environment is not as widespread. Security and privacy are an issue that is typically considered as a secondary issue. The comprehensive examination of connections between machine learning solutions, cardiovascular risk assessment, distributed healthcare system, and protection of information still needs to be carried out.

This is what the purpose of this review will be. In the present paper, the critical overview of machine learning approaches in evaluating cardiovascular risks has been provided. It examines main sources of healthcare information and structures of distributed system. It also looks into major security and privacy concerns in distributed environments. In addition, the review also addresses secure and privacy sensitive machine learning. Finally, it identifies the gaps in the literature and future research directions to enable the use of machine learning in cardiovascular healthcare in a safe and reliable manner.

II. CLINICAL FOUNDATIONS OF CARDIOVASCULAR RISK ASSESSMENT

A. Traditional Cardiovascular Risk Models

The cardiovascular risk assessment is a way of identifying individuals who would develop a heart disease in the future. It is used by the doctors to avoid severe complications like heart attacks and strokes [12]. Over the years, this evaluation has been made upon conventional risk models. The models find application in most hospitals

and clinics globally. They assist doctors in making decisions about patients that require treatment and lifestyle changes.

The Framingham Risk Score is one of the most widespread models. It was made based on the findings of a longitudinal study in the US. This model approximates the probability of the heart disease development within a decade. It takes the simplest of details like age, sex, blood pressure, cholesterol level, smoking status and diabetes. The other popular model is ASCVD risk score. It is primarily in use in the United States and has its emphasis on the risk of heart attack and stroke [13]. Doctors in Europe tend to rely on the SCORE system which approximates the risk of death due to cardiovascular disease. The QRISK model is usually utilized in the United Kingdom. QRISK encompasses the same factors plus the social and health conditions.

These models are famous due to ease of use. They do not entail complicated equipment or technology. Physicians are able to estimate risk with the help of easy charts or web-based calculators. These models have contributed to the reduction of heart disease because they assist in making decisions during treatment. They are however founded on predetermined formulas. They base their assumption on the assumption that everybody will respond to the same factors in a similar manner. They are also based on average behaviors of huge masses of people as opposed to individual behavior.

B. Key Risk Factors and Clinical Data

Cardiovascular disease develops due to many risk factors. Some of these factors cannot be changed, while others can be controlled. Age and sex are important non-modifiable factors. Family history also plays a role. People with close relatives who had heart disease are at higher risk. These factors are simple to record but do not explain the full picture of disease risk.

Many important risk factors are related to metabolism. These include high blood pressure, high cholesterol, obesity, and diabetes. These conditions place stress on the heart and blood vessels over time [14]. Behavioral factors also strongly affect heart health. Smoking, unhealthy diet, low physical activity, and excessive alcohol use increase cardiovascular risk [15]. Environmental factors such as air pollution and poor living conditions also contribute to disease development.

According to Figure 1, the majority of the burden of cardiovascular disease is attributed to the changed risk factors. Approximately 79.6 percent of the cardiovascular DALYs were associated with factors that can be mitigated or controlled in 2023 [16]. This implies that a lot of heart problem can be avoided in case the risks factors are identified early. It also emphasizes the necessity of periodic and not singlest observation.

Risk assessment is immensely conducted with clinical data. Blood tests will give information regarding cholesterol, glucose and inflammation. Electrocardiograms indicate heart beats issues. Heart structure and blood flow are found using medical imaging, including echocardiography and CT scans. Over the last several years, wearable devices have brought new forms of information. These gadgets monitor the heart rate, level of activity and sleep patterns. EHRs archive their historic patient records. Collectively, these data sources represent a big and complicated image of patient health.

C. Limitations and Unmet Clinical Needs

Though the traditional risk models are effective, they possess a number of weaknesses. Population bias is one of the greatest issues. A large number of models were built based on any particular regions or even ethnic groups. Consequently, they might not suit any population. This may result in wrong risk assessment among women, younger patients or individuals with other backgrounds.

The other issue is that it is not customized. Conventional models would use the same approach to patients with the same risk factors. They fail to put into full consideration individual differences in lifestyle, genetics or environment. These models also involve the use of fixed data. Risk factors tend to be quantified within one hospital visit. This method disregards the time variation in risk. It does not also take real life daily data.

The modern healthcare generates massive and wide-ranging data. This complexity cannot be easily addressed using traditional models. They have problems with high-dimensional data and complicated variable correlations. They are also not able to mix data of different types like images, signals and text records. Due to these limitations, not all patients get the risks predicted accurately.

These problems demonstrate the necessity to use new methods of cardiovascular risk evaluation. Risk models should be versatile, tailored, and capable of accessing a large amount of data. They should also be representative of the real world. It is relevant to comprehend the advantages and shortcomings of conventional clinical models prior to implementing machine learning solutions. This is a clinical underpinning that helps to make sure that the emerging practices are safe, meaningful and relevant to the patient care.

III. MACHINE LEARNING TECHNIQUES FOR CARDIOVASCULAR RISK PREDICTION

A. Use of Machine Learning in Cardiovascular Risk Prediction

There exists the increased application of machine learning to forecast cardiovascular risk. This is because the issue of cardiovascular disease is affected by many factors, which have complicated interactions [12]. Traditional models are not easily used to describe these interactions. The machine learning models are supposed to learn patterns directly by data [17]. The more data one has, the better they become. This makes them relevant to the contemporary healthcare systems in which big data are common.

The current cardiovascular risk assessment is undergone by a heterogeneous data ecosystem as Figure 2 indicates. It shows that data is presented by a vast number of sources, such as electronic health records, medical images, wearable gadgets, and environmental data. The machine learning models may integrate the different forms of data into a single system of prediction. The ability to process different data is one of the main advantages of machine learning in cardiovascular care.

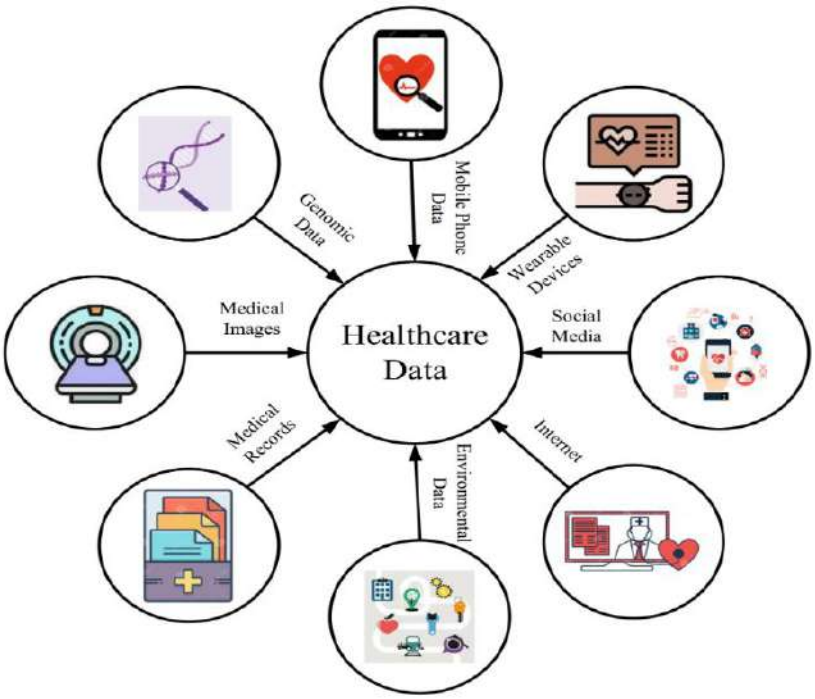

Figure 2: Multimodal Healthcare Data Sources for Cardiovascular Risk Assessment

B. Classical Machine Learning Approaches

Machine learning models which are mostly used in cardiovascular risk prediction are classical models. These are learning techniques that are monitored. This implies that they learn labeled data, in which the result is known. Logistic regression is also one of the simplest models. It can be learnt quickly and easily. It is commonly applied as a reference in medical research [18]. Logistic regression is effective in cases where relationships between variables are not complex. It, however, has difficulty with complicated patterns.

Other common methods include support vector machines. They operate via identification of a demarcation that divides high-risk and low-risk patients [19]. Support vector machines are effective with small and medium-sized data sets. They have special functions known as kernels that can be used to deal with non-linear relationships. They are however hard to interpret and involve careful choice of parameters.

Random forest models have also been popular. Many decision trees constitute a random forest. A tree makes a prediction and the final decision is made based on the combination of all trees. Random forests are able to process large data sets and mixed data sets [20]. They are resistant to noise and missing values. This renders them helpful in data of electronic health records. XGBoost and other gradient boosting algorithms are related in that they construct trees sequentially [21]. The trees are all concerned with correcting the past mistake of the previous trees. Such models are frequently highly accurate on cardiovascular risks prediction tasks.

The classical machine learning models have been based on feature engineering. This implies that input variables should be chosen and prepared well by experts. At this stage, clinical knowledge is significant. Even a strong algorithm may suffer because of the poor design of its features.

C. Deep Learning Methods

An advanced machine learning model can be deep learning models. They make use of several layers in order to extract complex patterns in raw data. Deep learning can be particularly applied to high-dimensional data, including images, signals and time-sequences data [22]. Deep learning has demonstrated good performance in various fields in cardiovascular research.

Medical imaging is also popular with convolutional neural networks. They are put on CT images, MRI images and echocardiography images. The models learn automatically significant visual characteristics of the heart structure and functioning. They minimise the manual feature extraction [23]. Convolutional neural networks have been employed in heart disease detection and cardiac functionality assessment and cardiovascular future event prediction.

Recurrent neural networks and long short-term memory models are created to work with sequential data. They are typically applied to electrocardiogram and wearable sensor data [24]. Such models are time-varying, including the pattern of the heart rhythm and its activity. This matter is significant since cardiovascular risk is not fixed [25]. It varies according to the daily behavior and health statuses. Deep learning models are able to learn such temporal patterns directly using data.

Deep learning lays emphasis on the representation learning rather than on the feature engineering. The model also acquires useful representations automatically, instead of manually selecting features. This saves human time but makes the models more complicated. Deep learning models can be very large in size as well as have high-computational requirements. They are as well less decipherable as compared to classical models.

D. Model Interpretability and Explainable Artificial Intelligence

One of the most important problems of healthcare machine learning is interpretability. Doctors must know why a model is arriving at a particular prediction [26]. Trust on the system is low without reasons. It is particularly relevant to cardiovascular risk prediction, in which long-term treatment depends on decisions.

This issue is solved with explainable artificial intelligence techniques. SHAP is a famous technique that describes the contribution of each input features towards a prediction [27]. It demonstrates how individual patient risks are increased or reduced by elements. The other method is LIME which describes the behavior of models locally by approximating complex models by simpler ones [28]. These aids in bridging machine learning prediction and clinical reasoning.

The interpretability techniques enhance the transparency and facilitate clinical judgment. But they put additional complexity on the system. They must use them as well with caution so as not to give misleading explanations. Nonetheless, despite these issues, machine learning needs explainability in order to be adopted in practice in cardiovascular care.

E. Model Evaluation and Validation

The machine learning models in healthcare applications are important to evaluate. Some of the prevalent performance measurements are accuracy, sensitivity, and specificity, and the area under the curve [18]. Sensitivity indicates the ability of the model to identify the high-risk patients. Specificity is used to determine the extent to which it reaches low-risk patients. They both are significant in the assessment of cardiovascular risk.

It is also important that the methods of validation are employed. Independent datasets should be used to test the models and make them generalized [29]. When training, cross-validation is usually employed. Before clinical use, external validation is required [30]. Most researches have good findings but are not tested in the real cases. This curtails their practical effect.

To conclude, machine learning offers effective cardiovascular risk prediction tools. Classical models are easy and understandable [19]. Complex data is more accurate with deep learning models. Clinical use has to be safe and effective, and it cannot be achieved without explainability and adequate evaluation.

IV. DISTRIBUTED HEALTHCARE ENVIRONMENTS AND DATA ECOSYSTEMS

A. Distributed Healthcare System Architecture

Healthcare is no longer something that is being practiced in hospitals. It is currently practiced concurrently in numerous locations. The patients are also observed at home, at work place and in their daily activities [31]. All this is made possible by the fact that healthcare systems are becoming distributed. Distributed healthcare system implies that information is gathered and processed in various locations unlike the central location.

These systems possess three significant parts. The initial layer is also referred to as the edge layer. This layer consists of the wearable, mobile phones and home monitoring equipment [32]. These gadgets monitor the simplest medical information including heart rate, steps, blood pressure and even sleep patterns. The second layer is the fog layer. The local servers form this layer and they are local data centers areas or hospital systems. It manages information in a place that is near to collection. This will decrease the response time and provide quicker response. The third is the cloud layer. It is a layer that holds extensive data and executes complex machine learning models. It possesses an excellent computing power and it permits long term analysis.

The layers utilize machine learning models. Coupe of easy duties might be performed at the periphery. The more complicated operations are performed in the fog or cloud. This organization assists in the up scaled medical care to a huge number of patients. It also simplifies real time monitoring of cardiovascular hazard [33]. Nonetheless, the data and processing of the system is hard to manage due to its sharing with numerous locations.

B. Data Sources and Data Flow in Distributed Healthcare

There are numerous types of data that distributed healthcare systems rely on. The Internet of Medical Things is one of such resources. IoMT consists of wearable gadgets, smartwatches, heartwatches, and connected healthcare gadgets [34]. Such devices gather health information on a continuous basis. The information is then transferred to other neighboring systems to process it.

Another key source of data is electronic health records. EHR contains patient history, diagnosis, test results, medications, and doctor notes. EHR data shared in a distributed system involves sharing between hospitals and clinics. This data can be exchanged by different systems using interoperability [35]. This will assist in establishing a full picture of patient health in the long term.

Wearables provide details of daily life. They document the physical activity, the changes in heart rate and the quality of sleep [9]. Heart health is also influenced by environmental factors like air pollution, temperature, etc. Such behavioral data as diets and exercise offer valuable background. The different sources of data are brought together in a single system as depicted in Figure 2.

Such a combination of data is used by machine learning models to predict cardiovascular risk. Hypernyymous models tend to be more effective. Table 1 demonstrates this trend with ensemble models and deep learning techniques having access to multimodal data. The large number of sources of data used assists in enhancing the accuracy of prediction, but it makes the systems more complex.

Table 1: Summary of Machine Learning Models Used for Cardiovascular Risk Prediction

Model Type	Common Algorithms	Data Used	Main Strength	Main Limitation
Classical ML	Logistic Regression, SVM	EHR, lab data	Simple and easy to explain	Limited accuracy for complex data
Ensemble ML	Random Forest, XGBoost	EHR, wearables	High accuracy and robustness	Less transparent
Deep Learning	CNN, RNN, LSTM	Images, ECG, sensors	Learns complex patterns	Hard to interpret
Hybrid Models	ML + DL	Multimodal data	Best overall performance	High system complexity

As shown in Table 1, ensemble methods and deep learning models usually perform better than traditional statistical models, especially when multiple data sources are available.

C. Challenges of Distributed Healthcare Systems

Distributed healthcare systems have many issues. One of the greatest challenges is fragmentation of data. Health information is put in many places in diverse ways. This data is difficult to incorporate in a single-system. The absence of good data quality and lack of information reduce the efficiency of machine learning models.

Another problem is system coordination. There will be a need to move information between edge devices, local servers and cloud systems. Connection failure and network delay can be imposed on real-time monitoring [36]. This is applicable in the cardiovascular care where time is paramount.

Security and privacy are also threatened on distributed systems. Communication occurs across a large number of devices and networks. All the transfer points consider the risk of data leakage [11]. There is increased difficulty in controlling access. When the data is transferred more often it is harder to guarantee the privacy of the patients.

There are also practical issues of deployment. Machine learning models should be updated with new data. Models cannot be updated easily in a high number of devices. The computers may not be powerful enough as machines [37]. The medical staff may fail to prepare on handling such systems.

In conclusion, the modern cardiovascular risk forecasting can be applied in the distributed healthcare environment. They can allow collecting data in real time and analyzing it at a large scale. In the meantime, they are also associated with data integration, coordination and management problems. These concerns should be addressed and after this, secure solutions and privacy sensitive solutions should be adopted and this is discussed in the subsequent section.

V. SECURITY AND PRIVACY CHALLENGES IN DISTRIBUTED MACHINE LEARNING FOR HEALTHCARE

A. Privacy Risks in Distributed Healthcare Data

The data of health care is highly sensitive. It holds personal and medical data of patients. This data is gathered in large numbers in numerous different places and distributed in distributed healthcare systems. This puts the privacy issues at risk. The data can be stored in wearable devices, mobile phones, hospital servers, and also in cloud platforms [38]. Every place raises the risk of leakage of the data.

Figure 3 represents a classical distributed healthcare system with IoMT devices providing cardiovascular data on a continuous basis on edge, fog, and cloud layers. There is a high data flow between networks and devices in this system. In this movement, data may be intercepted, copied and abused. Patients can even be recalled by name even in the absence of the names. This is referred to as the re-identification. It occurs with the combination of different datasets.

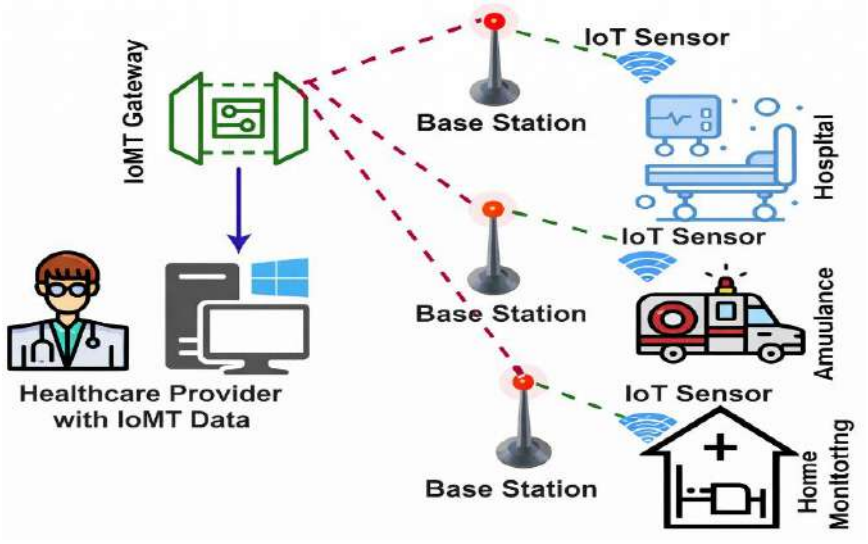

Figure 3: Distributed Healthcare Architecture with IoMT-Enabled Data Flow

The other risk is data leakage. The leakage may be as a result of inadequate security settings, ineffective access controls or system crash. The access points in a distributed system are hard to monitor [39]. One mistake can reveal huge data volumes. This issue is aggravated by the continuous monitoring data of wearables. Such streams of data expose patterns of daily life habits, health condition, and location.

There are also the increasing privacy risks brought about by cross-institutional data sharing. Various systems and standards can be applied in hospitals and clinics [40]. In case of the sharing of data between institutions, it might not be subjected to the same protection rules. Patients are usually not aware of the storage and use location of their data. This diminishes the confidence in online healthcare.

B. Security Threats in Machine Learning Systems

Other such security threats of machine learning systems exist besides the old-time data breach. These attacks are targeted at the models. Model inversion is one of the common threats. In the given attack, an attacker attempts to get access to patient sensitive information with the help of a trained model [41]. Although no one has a practical access to the information, there are instances when one can make an educated assumption of personal information.

The other threat is data poisoning. False or malicious data is in this case introduced during the training of the model. This makes the model develop the inaccurate patterns. This will bring about the risk projections of pseudomathhematics in the medical field. The biased model can also classify the risky patients either as not risky or vice versa. This can harm patient safety.

The other issue on concern is adversarial attacks. It is accomplished by distorting the input data by including minor variations in order to confound the model. This is due to the fact that these changes are something that humans are not familiar with but can transform the model prediction [42]. In order to explain, addition of any noise to ECG signals can cause inaccuracy of classification. The distributed systems have a difficulty in detecting such attacks since the information might be obtained in different sources.

Particularly sensitive are edge devices. The security of wearables and sensors will be low. They are not necessarily highly coded and changed. An edge device can supply false information into the system in case it is spoilt. This impacts on the whole learning process. Sharing and remote access the cloud layers and the fog are also threatened by remote access and shared infrastructure.

Table 1: Common Security and Privacy Threats in Distributed Healthcare ML

Threat Type	What Happens	Main Risk
Data leakage	Data is exposed or stolen	Loss of patient privacy
Re-identification	Patients are identified again	Privacy violation
Model inversion	Data is inferred from models	Sensitive data exposure
Data poisoning	Fake data corrupts training	Wrong predictions
Adversarial attack	Input data is manipulated	Model failure

Table 2 summarizes key cybersecurity threats in healthcare AI systems, explaining what happens in each case and the associated risks.

C. Regulatory and Ethical Challenges

There are stringent laws and regulations that govern healthcare data. The presence of such rules is to safeguard patient rights and privacy. Healthcare systems in a lot of countries have to comply with the laws, including HIPAA and GDPR. This is because these laws govern the collection, storage, sharing, and processing of data [43]. Breaking these rules may cause legal fines and mistrust.

Compliance is more challenging with distributed machine learning systems. The information can span the boundaries between institutions and countries. There are various rules which each location can have. It is difficult to keep track of data location and access by whom. All uses of patient data may not be clearly consented to by patients [44]. This brings about ethical issues.

Another difficulty is transparency. Black boxes are typical of machine learning models. Doctors might not know the way decisions are made. Patients might not have faith in the recommendations that they cannot articulate [45]. This is a deficiency of transparency, which increases accountability. In the case of mistakes, there is no clarity as to whom to hold responsible.

Fairness is also a key issue. Biased results can be obtained by using models that have been trained on biased data. Some groups can be given poorer predictions. This has the potential to increase health inequality. Machine learning should be ethically used fairly, transparently, and accountably.

D. Trust and Accountability in Clinical Use

In healthcare, trust is a key aspect. Physicians have to rely on the system. The predictions should be believed by the patients. The violation of privacy or security will make the loss of trust rather fast. Making up trust is extremely challenging.

The distributed machine learning systems should be able to explain it and offer substantial protection. Physicians must be aware when to use predictions [46]. The patients must be assured that their information is secure. There should be accountability measures that will help correct mistakes and abuse.

In short, there are great advantages to using distributed machine learning systems in cardiovascular risk prediction. Nevertheless, they also come up with serious security and privacy issues. Such challenges are data leakage, model attacks, regulatory constraints and trust problems. These issues have to be tackled in order to make machine learning safe to scale. In the next section, solutions, which are secure and privacy-saving, are discussed to conquer these challenges.

VI. SECURE AND PRIVACY-PRESERVING MACHINE LEARNING APPROACHES

A. Federated Learning for Cardiovascular Risk Prediction

Federated learning is one of the most important solutions for privacy protection in healthcare machine learning. In this approach, patient data does not leave its original location. Instead of sending data to a central server,

machine learning models are sent to local devices or hospitals. These models are trained locally using patient data. Only the model updates are shared, not the raw data.

In cardiovascular risk prediction, federated learning is very useful. Hospitals, clinics, and wearable devices can all train a shared model without exposing patient records. This allows learning from large and diverse populations while keeping data private [47]. Federated learning also supports cross-institutional collaboration. Different hospitals can work together even if they cannot share data directly.

Federated learning minimizes the threat of data leakage and re-identification. The data remains local; therefore, it is not easily accessible to attackers. It is also useful in compliance with regulations since the data of patients is kept locally. Federated learning is however not easy to implement. It needs a robust intersystem communication [48]. The updates on models should be synchronized. The quality of data and the power of devices may vary and impact performance.

Federated learning, despite all these difficulties, is perceived as one of the fundamental approaches to secure cardiovascular risk assessment. It strikes a compromise between power in learning and privacy protection unlike conventional centralized methods.

B. Cryptographic and Privacy-Preserving Techniques

Federated learning is not the only method of cryptographic protection of healthcare data. Secure multi-party computation is one of the techniques. SMPC is able to give the opportunity to calculate along with a number of parties who do not disclose their individual information. The encrypted values are visible to each party only. The end result is accurate but the data used is concealed.

SMPC can be executed in situations in healthcare where the risk scores of various hospitals desire to be jointly computed. Every hospital makes its patient information confidential. This lowers the level of trust among the institutions [49]. Nonetheless, SMPC is frequently computationally intensive as well as complicated to communicate. This restricts its big system scalability.

Another popular technique is the differential privacy. It operates by introducing little noise to data or model outputs. It is hard to distinguish individual patients. Differential privacy has assertive mathematical guarantees [50]. It guards against re-identification even in case of the union of datasets.

Different privacy aids in safeguarding patient identity in cardiovascular risk prediction. But noise may decrease the accuracy of models. It is hard to strike the balance of privacy and performance. Excessive noises damage predictions. The lack of noise undermines the protection of privacy.

Healthcare data security is also enhanced with the help of blockchain technology. Blockchain has a shared and resistant to tampering record of transactions. It is commonly used in the healthcare industry in access control and data sharing control [51]. Blockchain will guarantee privacy of information to authorized users. It also develops a trail of audit that enhances accountability.

Blockchain does not directly protect data content. Instead, it controls who can access data and when. It also increases transparency. However, blockchain systems can be slow and hard to scale. Energy use and system complexity are also concerns.

Table 2: Security and Privacy Techniques in Distributed Healthcare Machine Learning

Technique	Main Idea	Privacy Protection	Impact on Accuracy	Scalability
Federated Learning	Train models locally	High	Low to moderate loss	High
Differential Privacy	Add noise to data	Very high	Moderate loss	High
SMPC	Compute on encrypted data	Very high	Low loss	Low
Blockchain	Control data access	Indirect	No impact	Moderate

In the above Table 3 contrasts major privacy-preserving techniques used in distributed healthcare machine learning, highlighting their strengths and limitations for cardiovascular risk prediction.

C. Trade-offs Between Accuracy, Privacy, and Scalability

No single privacy-preserving method is perfect. Each approach involves trade-offs. Improving privacy often reduces accuracy. Increasing security can reduce system speed. Improving scalability may reduce control over data use.

Federated learning offers a good balance. It protects raw data and allows learning from large populations. However, it may suffer from uneven data quality. Differential privacy provides strong protection but can lower model performance. SMPC provides excellent privacy but struggles with large datasets. Blockchain improves trust and transparency but does not protect data content directly.

Accuracy is of great importance in cardiovascular healthcare. Inaccurate prognoses are detrimental to the patients. Simultaneously, one should not disregard privacy.

The patients should be confident that their information is secure. There is also the need of scalable systems to enable large population and deployment in a real world.

Due to such trade-offs, hybrid solutions tend to be suggested. Federated learning in relation to differential privacy can be coupled together, as an example. Models are trained locally and access control is done through blockchain. These integrated solutions are more protective and have performance that is acceptable.

To conclude, feasible machine-based cardiovascular risk prediction is possible using privacy-preserving and secure methods of machine learning. Federated learning, cryptographic approach and blockchain technologies all have significance. Knowledge of their capabilities and their weaknesses can be used in developing safer and more effective healthcare systems. The following paragraph covers the outstanding issues and research directions.

VII. OPEN CHALLENGES, RESEARCH GAPS, AND FUTURE DIRECTIONS

A. Open Challenges and Research Gaps

Despite the high potential of machine learning in cardiovascular risk assessment, there are many challenges. One of these challenges is bias in models and data. The healthcare statistics are often grounded on small populations. There are those groups that are over represented and there are those groups that do not exist. In turn, machine learning models may work with some patients and fail with other patients. This introduces the issue of fairness and can improve health inequality [52]. The issue of prejudice is especially critical in the case of distributed systems where the data quality and the levels of its availability differ between the regions.

The other significant problem is generalizability. Small or local data is used to train most machine learning models and test them. It is possible that the models are not applicable in new hospitals or other countries. The model will reduce reliability due to the differences in lifestyle, the variation in access to healthcare, and the pattern in diseases. The use of models on scale cannot be considered safe unless the models are well externally validated.

Scalability is also a major problem. In the actual healthcare systems, systems contain millions of patients and devices. The development of distributed machine learning systems must be capable of operating with large volumes of data, updating on a frequent basis, and possess minimal computing capacity [53]. The edge devices are low power and low storage devices. Performance issues are system failure and network delays. The majority of the solutions proposed at the experiments are good in testing but fail in practice.

There is clinical invalidity. Technical performance and not clinical impact have a lot of research devoted to it [53]. High accuracy is not always a good sign of patient outcomes. Doctors need to have an argument that machine learning can help improve a decision-making process and quality of care. It is also difficult to make part of the clinical working processes [54]. The systems must also be user friendly and must address the existing practices.

Another important problem is explainability and privacy. Explainable models can be used to explain the predictions. Transparency is low in privacy preserving procedures. Good privacy and good explanations are difficult to meet. It is an open research problem that is a trade-off.

B. Future Research Directions

This needs to be done through systemized research in order to devise solutions to these issues in future. Firstly, more representative and differentiated datasets have to be obtained. The collaboration between the institutes and the nations is able to limit bigotry. Privacy-sensitive algorithms such as federated learning can help this cooperation [55]. Second, extensive testing in practice should be studied. The models are to be experimented within other health care settings. The approval of external validation will be a matter of course. Long-term studies are necessary to measure actual clinical benefit in order to have better clinical benefit [56]. Third, the design must be capable of being expanded at the start. Edge devices are in need of light models and efficient training processes. Reliability and robustness of the systems should be improved. Fourth, explainable and privacy-friendly models should be developed together. The new strategies should provide clear explanations besides protecting patient data. This will lead to adoption and trust. Finally, interdisciplinary work needs to be undertaken in the future. Collaboration among clinicians, data scientists, engineers, as well as policymakers are required. The collaboration will also be applicable in ensuring that the machine learning systems are safe, just, and beneficial in reality medical practices.

VIII. CONCLUSION

The article has examined the machine learning methods to achieve the assessment of cardiovascular risk in a distributed care environment. Heart diseases continue to remain a major health challenge in the global context. Prevention and treatment are all dependent on the early and correct prediction of risks. The traditional risk models are grounded on good clinical basis and have major limitations. They are performed on static information and limited risk variables.

The machine learning offers distinctive and dynamic healthcare data analysis tools. Classical models are transparent and simple. Deep learning models constitute complicated patterns, which are trained on images, signals, and time-series data. The distributed healthcare system creates the possibility of gathering information and processing it in real-time and at high scale. However, they pose serious security and privacy risks too.

Such challenges as privacy of data, system security, regulation and trust were found in this review. It has also discussed secure and privacy-safe solutions, federated learning, and differential privacy, secure computation, and blockchain-based access control. The two methods have accuracy, privacy and scalability trade-offs.

The main takeaway is clear. Machine learning has the potential to improve cardiovascular risk assessment but only the security and privacy are discussed as design-related issues. The object of concern to researchers must be impartiality, validation, and practical implementation. Practitioners must manage the balance between innovation, trust and safety of the patients. Responsible machine learning and the future of cardiovascular care are secure.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] A. Roth, V. Fuster, and G. A. Mensah, “The Global Burden of Cardiovascular Diseases and Risk Factors,” *Journal of the American College of Cardiology*, vol. 74, no. 20, pp. 2529–2532, Nov. 2019. Available from: https://doi.org/10.1016/j.jacc.2019.10.009

[2] V. L. Roger, “Epidemiology of Heart Failure: A Contemporary Perspective,” *Circulation Research*, vol. 128, no. 10, pp. 1421–1434, May 2021. Available from: https://doi.org/10.1161/CIRCRESAHA.121.318172

[3] N. Boskovic *et al.*, “Comparison of SCORE and SCORE 2 risk prediction tools in contemporary very high-risk European population,” *European Heart Journal*, vol. 43, no. Supplement_2, Oct. 2022. Available from: https://doi.org/10.1093/eurheartj/ehac544.2281

[4] L. J. Laslett *et al.*, "The Worldwide Environment of Cardiovascular Disease: Prevalence, Diagnosis, Therapy, and Policy Issues," *Journal of the American College of Cardiology*, vol. 60, no. 25, pp. S1–S49, Dec. 2012. Available from: https://doi.org/10.1016/j.jacc.2012.11.002

[5] Chong *et al.*, "Global burden of cardiovascular diseases: projections from 2025 to 2050," *European Journal of Preventive Cardiology*, vol. 32, no. 11, Sep. 2024. Available from: https://doi.org/10.1093/eurjpc/zwae281

[6] J. A. A. G. Damen *et al.*, "Prediction models for cardiovascular disease risk in the general population: systematic review," *BMJ*, vol. 353, p. i2416, May 2016. Available from: https://doi.org/10.1136/bmj.i2416

[7] R. Ibarra *et al.*, "Cardiovascular Disease Detection Using Machine Learning," *Computación y Sistemas*, vol. 26, no. 4, pp. 1661–1668, Dec. 2022. Available from: https://doi.org/10.13053/cys-26-4-4422

[8] S. Wan, F. Wan, and X. Dai, "Machine learning approaches for cardiovascular disease prediction: A review," *Archives of Cardiovascular Diseases*, vol. 118, no. 10, pp. 554–562, Oct. 2025. Available from: https://doi.org/10.1016/j.acvd.2025.04.055

[9] S. N. Yoon, D. Lee, and Y. Shin, "Innovative Healthcare Wearable Device Usage and Service Enhancement," *Global Business Finance Review*, vol. 25, no. 2, pp. 1–10, Jun. 2020. Available from: https://doi.org/10.17549/gbfr.2020.25.2.1

[10] P. Bonato, "Advances in wearable technology and its medical applications," in *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*, Aug. 2010. Available from: https://doi.org/10.1109/IEMBS.2010.5628037

[11] M. Nankya, Y. Usman, A. Upadhyay, R. Chataut, and A. Mugisa, "Security and Privacy in E-Health Systems: A Review of AI and Machine Learning Techniques," *IEEE Access*, vol. 12, pp. 1–5, Jan. 2024. Available from: https://doi.org/10.1109/ACCESS.2024.3469215

[12] D.-I. Kasartzian and T. Tsiampalis, "Transforming Cardiovascular Risk Prediction: A Review of Machine Learning and Artificial Intelligence Innovations," *Life*, vol. 15, no. 1, p. 94, Jan. 2025. Available from: https://doi.org/10.3390/life15010094

[13] Ghaem, M. J. Zibaeenezhad, M. Sayadi, S. Khosravaniardakani, N. Parsa, and I. Razeghian-Jahromi, "Association of classic cardiovascular risk factors with myocardial infarction and ischemic stroke: a cross-sectional analysis of the Shiraz Heart Study," *International Journal of Cardiology: Cardiovascular Risk and Prevention*, vol. 23, p. 200332, Sep. 2024. Available from: https://doi.org/10.1016/j.ijcrp.2024.200332

[14] M. M. Hussain, U. Rafi, A. Imran, M. U. Rehman, and S. K. Abbas, "Risk Factors Associated with Cardiovascular Disorders," *Pakistan BioMedical Journal*, vol. 7, no. 2, pp. 03–10, Feb. 2024. Available from: https://doi.org/10.54393/pbmj.v7i02.1034

[15] Goldsborough, E. Tasdighi, and M. J. Blaha, "Assessment of cardiovascular disease risk: a 2023 update," *Current Opinion in Lipidology*, vol. 34, no. 4, pp. 162–173, May 2023. Available from: https://doi.org/10.1097/MOL.0000000000000887

[16] M. M. Haque and A.-Z. Nelson, "Global, Regional, and National Burden of Cardiovascular Diseases and Risk Factors in 204 Countries and Territories, 1990–2023," *Journal of the American College of Cardiology*, Sep. 2025. Available from: https://doi.org/10.1016/j.jacc.2025.08.015

[17] R. Reátegui, C. Tandazo-Malla, R. Suárez, and L. Ramírez-Cerna, "Cardiovascular risk prediction via ensemble machine learning and oversampling methods," *Scientific Reports*, vol. 15, Dec. 2025. Available from: https://doi.org/10.1038/s41598-025-30895-5

[18] Ogunpola, F. Saeed, S. Basurra, A. M. Albarrak, and S. N. Qasem, "Machine Learning-Based Predictive Models for Detection of Cardiovascular Diseases," *Diagnostics*, vol. 14, no. 2, p. 144, Jan. 2024. Available from: https://doi.org/10.3390/diagnostics14020144

[19] T. Banerjee and İ. Paçal, "A systematic review of machine learning in heart disease prediction," *Turkish Journal of Biology*, vol. 49, no. 5, pp. 600–634, Oct. 2025. Available from: https://doi.org/10.55730/1300-0152.2766

[20] T. Liu, A. Krentz, L. Lu, Y. Wang, and V. Curcin, "Benchmarking survival machine learning models for 10-year cardiovascular disease risk prediction using large-scale electronic health records," *Digital Health*, vol. 12, Jan. 2026. Available from: https://doi.org/10.1177/20552076251408534

[21] T. Vu *et al.*, "Machine Learning-Based Prediction of Coronary Heart Disease: Comprehensive Insights from the Suita Study (Preprint)," *JMIR Cardio*, Oct. 2024. Available from: https://doi.org/10.2196/68066

[22] M. Tsai, K. Chen, and P. Chen, "Harnessing Electronic Health Records and Artificial Intelligence for Enhanced Cardiovascular Risk Prediction: A Comprehensive Review," *Journal of the American Heart Association*, Mar. 2025. Available from: https://doi.org/10.1161/JAHA.124.036946

[23] B. A. Tama, D. H. Kim, G. Kim, S. W. Kim, and S. Lee, "Recent Advances in the Application of Artificial Intelligence in Otorhinolaryngology-Head and Neck Surgery," *Clinical and Experimental Otorhinolaryngology*, vol. 13, no. 4, pp. 326–339, Nov. 2020. Available from: https://doi.org/10.21053/ceo.2020.00654

[24] Oporto, D. Mauricio, N. Maculan, and G. Uribe, "Challenges in the Classification of Cardiac Arrhythmias and Ischemia Using End-to-End Deep Learning and the Electrocardiogram: A Systematic Review," *Diagnostics*, vol. 16, no. 1, p. 161, Jan. 2026. Available from: https://doi.org/10.3390/diagnostics16010161

[25] N. Tasmurzayev *et al.*, "Digital Cardiovascular Twins, AI Agents, and Sensor Data: A Narrative Review from System Architecture to Proactive Heart Health," *Sensors*, vol. 25, no. 17, p. 5272, Aug. 2025. Available from: https://doi.org/10.3390/s25175272

[26] Y. Feng, H. Kunz, and K. Dziopa, "Interpretable Lifestyle-Based Machine Learning Models for Ten-Year Cardiovascular Risk Prediction Using Data from the UK Biobank," Feb. 2026. Available from: https://doi.org/10.64898/2026.01.26.26344438

[27] T. Gan, S. Wang, G. Mo, S. Li, Y. Lu, and J. Li, "Machine learning prediction and SHAP interpretability analysis of heart failure risk in patients with hyperuricemia," *Frontiers in Cardiovascular Medicine*, vol. 12, Dec. 2025. Available from: https://doi.org/10.3389/fcvm.2025.1689607

[28] S. Ahmed, M. S. Kaiser, M. S. Hossain, and K. Andersson, "A Comparative Analysis of LIME and SHAP Interpreters with Explainable ML-Based Diabetes Predictions," *IEEE Access*, vol. 13, Jan. 2024. Available from: https://doi.org/10.1109/ACCESS.2024.3422319

[29] Wilimitis and C. G. Walsh, "Practical Considerations and Applied Examples of Cross-Validation for Model Development and Evaluation in Health Care: Tutorial," *JMIR AI*, vol. 2, no. 1, p. e49023, Dec. 2023. Available from: https://doi.org/10.2196/49023

[30] B. Norgeot *et al.*, "Minimum information about clinical artificial intelligence modeling: the MI-CLAIM checklist," *Nature Medicine*, vol. 26, no. 9, pp. 1320–1324, Sep. 2020. Available from: https://doi.org/10.1038/s41591-020-1041-y

[31] Rajagopal and P. K. T. Subramanian, "AI augmented edge and fog computing for Internet of Health Things (IoHT)," *PeerJ Computer Science*, vol. 11, p. e2431, Jan. 2025. Available from: https://doi.org/10.7717/peerj-cs.2431

[32] R. Sundar *et al.*, "Heart health prediction and classification: An IoMT and AI collaborative model," *MATEC Web of Conferences*, vol. 392, p. 01142, Jan. 2024. Available from: https://doi.org/10.1051/matecconf/202439201142
[33] Akhmetov, Z. Latif, B. Tyler, and A. Yazici, "Enhancing healthcare data privacy and interoperability with federated learning," *PeerJ Computer Science*, vol. 11, p. e2870, May 2025. Available from: https://doi.org/10.7717/peerj-cs.2870
[34] S. Gupta, S. Kumar, K. Chang, C. Lu, P. Singh, and J. Kalpathy-Cramer, "Collaborative Privacy-preserving Approaches for Distributed Deep Learning Using Multi-Institutional Data," *RadioGraphics*, vol. 43, no. 4, Apr. 2023. Available from: https://doi.org/10.1148/rg.220107
[35] Thacharodi *et al.*, "Revolutionizing healthcare and medicine: The impact of modern technologies for a healthier future—A comprehensive review," *Health Care Science*, vol. 3, no. 5, Oct. 2024. Available from: https://doi.org/10.1002/hcs2.115
[36] K. Danach, A. H. Khalaf, A. Rammal, and H. Harb, "Enhancing DDBMS Performance through RFO-SVM Optimized Data Fragmentation: A Strategic Approach to Machine Learning Enhanced Systems," *Applied Sciences*, vol. 14, no. 14, p. 6093, Jul. 2024. Available from: https://doi.org/10.3390/app14146093
[37] R. Santos *et al.*, "A Secure and Trustworthy Federated Learning Platform as a Service Model for Stroke Management in European Clinical Centers," *IEEE Access*, vol. 13, pp. 212035–212057, 2025. Available from: https://doi.org/10.1109/ACCESS.2025.3641035
[38] R. Saidi, I. Rahmany, S. Dhahri, and T. Moulahi, "A Privacy-Enhanced Framework for Chest Disease Classification using Federated Learning and Blockchain," *IEEE Access*, vol. 12, 2024. Available from: https://doi.org/10.1109/ACCESS.2024.3419084
[39] Alabdulatif, I. Khalil, and M. S. Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," *Applied Sciences*, vol. 12, no. 21, p. 11039, Oct. 2022. Available from: https://doi.org/10.3390/app122111039
[40] S. M. Narayan, N. Kohli, and M. M. Martin, "Addressing contemporary threats in anonymised healthcare data using privacy engineering," *npj Digital Medicine*, vol. 8, no. 1, Mar. 2025. Available from: https://doi.org/10.1038/s41746-025-01520-6
[41] T. M. Ara, K. S. Sidhu, S. Dass, and S. Saha, "SoK: Privacy-aware LLM in Healthcare: Threat Model, Privacy Techniques, Challenges and Recommendations," *arXiv*, Jan. 2026. Available from: https://doi.org/10.48550/arXiv.2601.10004
[42] Kurniawan, M. G. Putra, D. L. Hakim, and M. Ariyanto, "Temporal Adversarial Attacks on Time Series and Reinforcement Learning Systems: A Systematic Survey, Taxonomy, and Benchmarking Roadmap," *Preprints.org*, Jan. 2026. Available from: https://doi.org/10.20944/preprints202601.0598.v1
[43] S. Barbaria *et al.*, "Advancing Compliance with HIPAA and GDPR in Healthcare: A Blockchain-Based Strategy for Secure Data Exchange in Clinical Research Involving Private Health Information," *Healthcare*, vol. 13, no. 20, p. 2594, Oct. 2025. Available from: https://doi.org/10.3390/healthcare13202594
[44] S. R. Abbas, Z. Abbas, A. Zahir, and S. W. Lee, "Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration," *Healthcare*, vol. 12, no. 24, p. 2587, Dec. 2024. Available from: https://doi.org/10.3390/healthcare12242587
[45] B. Weiner, I. Dankwa-Mullan, W. A. Nelson, and S. Hassanpour, "Ethical challenges and evolving strategies in the integration of artificial intelligence into clinical practice," *PLOS Digital Health*, vol. 4, no. 4, p. e0000810, Apr. 2025. Available from: https://doi.org/10.1371/journal.pdig.0000810
[46] M. Goisauf *et al.*, "Trust, Trustworthiness, and the Future of Medical AI: Outcomes of an Interdisciplinary Expert Workshop," *Journal of Medical Internet Research*, vol. 27, p. e71236, Jun. 2025. Available from: https://doi.org/10.2196/71236
[47] Ryu, M. Lee, S. Kim, J. H. Kim, and H. Yang, "Federated Learning for Cardiovascular Disease Prediction: A Comparative Review of Biosignal- and EHR-Based Approaches," *Healthcare*, vol. 13, no. 21, p. 2811, Nov. 2025. Available from: https://doi.org/10.3390/healthcare13212811
[48] T. A. Sathi *et al.*, "Explainable Federated Learning for Multi-Class Heart Disease Diagnosis via ECG Fiducial Features," *Diagnostics*, vol. 15, no. 24, p. 3110, Dec. 2025. Available from: https://doi.org/10.3390/diagnostics15243110
[49] Ali and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Deleted Journal*, vol. 4, no. 2, pp. 20–62, May 2024. Available from: https://doi.org/10.58496/mjcs/2024/006
[50] B. Bent *et al.*, "The digital biomarker discovery pipeline: An open-source software platform for the development of digital biomarkers using mHealth and wearables data," *Journal of Clinical and Translational Science*, vol. 5, no. 1, pp. 1–8, Jul. 2020. Available from: https://doi.org/10.1017/cts.2020.511
[51] T. Meurers *et al.*, "A quantitative analysis of the use of anonymization in biomedical research," *npj Digital Medicine*, vol. 8, no. 1, May 2025. Available from: https://doi.org/10.1038/s41746-025-01644-9
[52] L. B. Elvas, A. Almeida, and J. C. Ferreira, "The Role of AI in Cardiovascular Event Monitoring and Early Detection: Scoping Literature Review," *JMIR Medical Informatics*, vol. 13, p. e64349, Mar. 2025. Available from: https://doi.org/10.2196/64349
[53] N. H. Alhumaidi, D. Dermawan, H. F. Kamaruzaman, and N. Alotaiq, "The Use of Machine Learning for Analyzing Real-World Data in Disease Prediction and Management: Systematic Review," *JMIR Medical Informatics*, vol. 13, p. e68898, Jun. 2025. Available from: https://doi.org/10.2196/68898
[54] Mehmood, F. Mehmood, and J. Kim, "Towards Explainable Deep Learning in Computational Neuroscience: Visual and Clinical Applications," *Mathematics*, vol. 13, no. 20, p. 3286, Oct. 2025. Available from: https://doi.org/10.3390/math13203286
[55] Petreska, "Cardiovascular disease prediction with machine learning techniques," *Journal of Cardiology & Current Research*, vol. 17, no. 2, pp. 41–51, Apr. 2024. Available from: https://doi.org/10.15406/jccr.2024.17.00603
[56] Choudhury *et al.*, "Advancing Privacy-Preserving Healthcare Analytics: Implementation of the Personal Health Train for Federated Deep Learning (Preprint)," *JMIR AI*, vol. 4, May 2024. Available from: https://doi.org/10.2196/60847
[57] M. Krumholz, "The global burden of cardiovascular disease: not just a mirror, but a compass," *Journal of the American College of Cardiology*, 2025. Available from: https://doi.org/10.1016/j.jacc.2025.09.1584