Journal on
Artificial Intelligence

Tech Science Press

Doi:10.32604/jai.2025.062479

ARTICLE

Cyber-Integrated Predictive Framework for Gynecological Cancer Detection: Leveraging Machine Learning on Numerical Data amidst Cyber-Physical Attack Resilience

Muhammad Izhar[1,*], Khadija Parwez[2], Saman Iftikhar[3], Adeel Ahmad[4], Shaikhan Bawazeer[3] and Saima Abdullah[4]

[1]Department of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan
[2]Department of Computing and Technology, IQRA University, Sector H-9, Islamabad, 04436, Pakistan
[3]Faculty of Computer Studies, Arab Open University, Riyadh, 84901, Saudi Arabia
[4]Department of Computer Science, Faculty of Computing, The Islamia University of Bahawalpur, Bahawalpur, 63100, Pakistan

*Corresponding Author: Muhammad Izhar. Email: izharraza@msn.com

Received: 19 December 2024; Accepted: 31 March 2025; Published: 25 April 2025

ABSTRACT: The growing intersection of gynecological cancer diagnosis and cybersecurity vulnerabilities in healthcare necessitates integrated solutions that address both diagnostic accuracy and data protection. With increasing reliance on IoT-enabled medical devices, digital twins, and interconnected healthcare systems, the risk of cyber-physical attacks has escalated significantly. Traditional approaches to machine learning (ML)–based diagnosis often lack real-time threat adaptability and privacy preservation, while cybersecurity frameworks fall short in maintaining clinical relevance. This study introduces HealthSecureNet, a novel Cyber-Integrated Predictive Framework designed to detect gynecological cancer and mitigate cybersecurity threats in real time simultaneously. The proposed model employs a three-tier ML architecture incorporating Gradient Boosting and Support Vector Machines (SVMs) for accurate cancer classification, combined with an adaptive anomaly detection layer leveraging Mahalanobis Distance and severity scoring for threat prioritization. To enhance resilience, the framework integrates Zero Trust principles and Federated Learning (FL), enabling secure, decentralized model training while preserving patient privacy and meeting compliance with HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulations). Experimental evaluation using a real-world healthcare cybersecurity dataset demonstrated high accuracy (95.2%), precision (94.3%), recall (91.7%), and AUC-ROC (Area Under the Curve-Receiver Operating Characteristic) (0.94), with a low false positive rate (3.6%). HealthSecureNet outperforms traditional models such as SVM, Random Forest (RF), and k-NN (k-Nearest Neighbor) in both anomaly detection and severity classification accuracy. Its adaptive thresholding and response prioritization mechanisms make it suitable for dynamic healthcare environments, enabling early cancer detection and proactive cyber threat mitigation without compromising performance or regulatory standards. This research contributes a robust, dual-purpose solution that enhances both clinical diagnostics and cybersecurity, setting a precedent for future AI (Artificial Intelligence)-driven healthcare systems.

KEYWORDS: Gynecological cancer detection; machine learning (ML); cyber-physical security; predictive healthcare model; anomaly detection

1 Introduction

The rapid advancements in machine learning (ML) and cybersecurity have significantly impacted the healthcare sector, particularly in the fields of early disease detection and cyber resilience [1]. In recent years, the integration of predictive analytics in gynecological cancer detection has improved diagnostic accuracy, enabling timely interventions and enhanced patient outcomes [2]. However, as medical institutions continue to embrace digital transformation, they become increasingly vulnerable to cyber-physical attacks, which threaten the security of patient data, diagnostic models, and healthcare infrastructure. The interconnected nature of modern healthcare systems—incorporating electronic medical records (EMRs), Internet of Things (IoT)-enabled medical devices, and AI-powered diagnosis—necessitates a cyber-integrated approach that ensures both medical accuracy and system security [3]. This study presents a Cyber-Integrated Predictive Framework for Gynecological Cancer Detection, leveraging machine learning techniques to enhance cancer diagnosis while simultaneously strengthening the cyber resilience of healthcare environments [4]. The framework employs a three-tiered ML architecture that integrates Gradient Boosting and Support Vector Machines (SVMs) for precise cancer classification. Additionally, it incorporates an anomaly detection layer to proactively identify cyber threats such as unauthorized access, data breaches, and adversarial attacks on medical AI models [5]. By embedding cognitive anomaly detection mechanisms, the system is designed to detect both clinical anomalies and cybersecurity threats, ensuring a dual-layered protection mechanism for healthcare data.

It is now impossible to discuss the connection between Machine Learning (ML) and cybersecurity within the healthcare industry since the computational and data-related processes of diagnostics, treatment, and even data storage are now carried out using sophisticated interconnected digital systems [6]. As has been seen, as healthcare systems grow technologically they are faced with both opportunities and risks. The application of ML has revealed marvelous in improving diagnostics positivity and analytics in healthcare resulting in betterment of patient care and organizational productivity [7]. At the same time, this advancement escalates the amount of categorized information flowing through and exchanging over and through these networks and makes them appealing targets for cyber-crashes [8]. Fig. 1 illustrates the System model diagram of the cyber physical system in healthcare.

Any healthcare breach poses a great threat as it involves a client's personal information besides causing disruptions to vital healthcare service provision [9–12]. Research has pointed out that even small violations can cause massive money and image loss for medical organizations [13–17]. Such concerns mean heightened risk hence there is a necessity to implement strong security measures that safeguard patient data and guarantee continuity of service delivery [18]. With the increase of digitalization, newer innovations like the Digital Twin apparently add more access points for a cyber threat into healthcare systems making data protection even more challenging [19,20].

However, the introduction of the Internet of Things (IoT) in healthcare has increased the attack surface width through IoT-based devices endangering patient safety [21,22]. A suggestion for a mitigation measure to reduce such access is to adopt Zero Trust as an architecture, which though comes with a large investment and constant vigilance [23]. The high specialization of the sector is a big challenge to the implementation of these universal measures including the requirement of the healthcare sector for data protection due to licenses and compliances with such standards as HIPAA.

Therefore, the addition of cybersecurity-specific ML models as adapted in healthcare has raised possibilities of strengthening systems' defenses. These models are able to operate in real-time and use anomalous behavior models to sense when there are signs of a breach of security [4,17]. Another promising approach to ensure patient data security while training models on different decentralized substrates seems to be federated learning frameworks, in which ML models are trained without transferring the raw data [9,12]. Nonetheless, difficulties are observed in applying these technologies to address healthcare data size and comprehensiveness; moreover, since the resulting ML models should be fully explained, or interpretable, such requirements often do not align with the existing regulations.

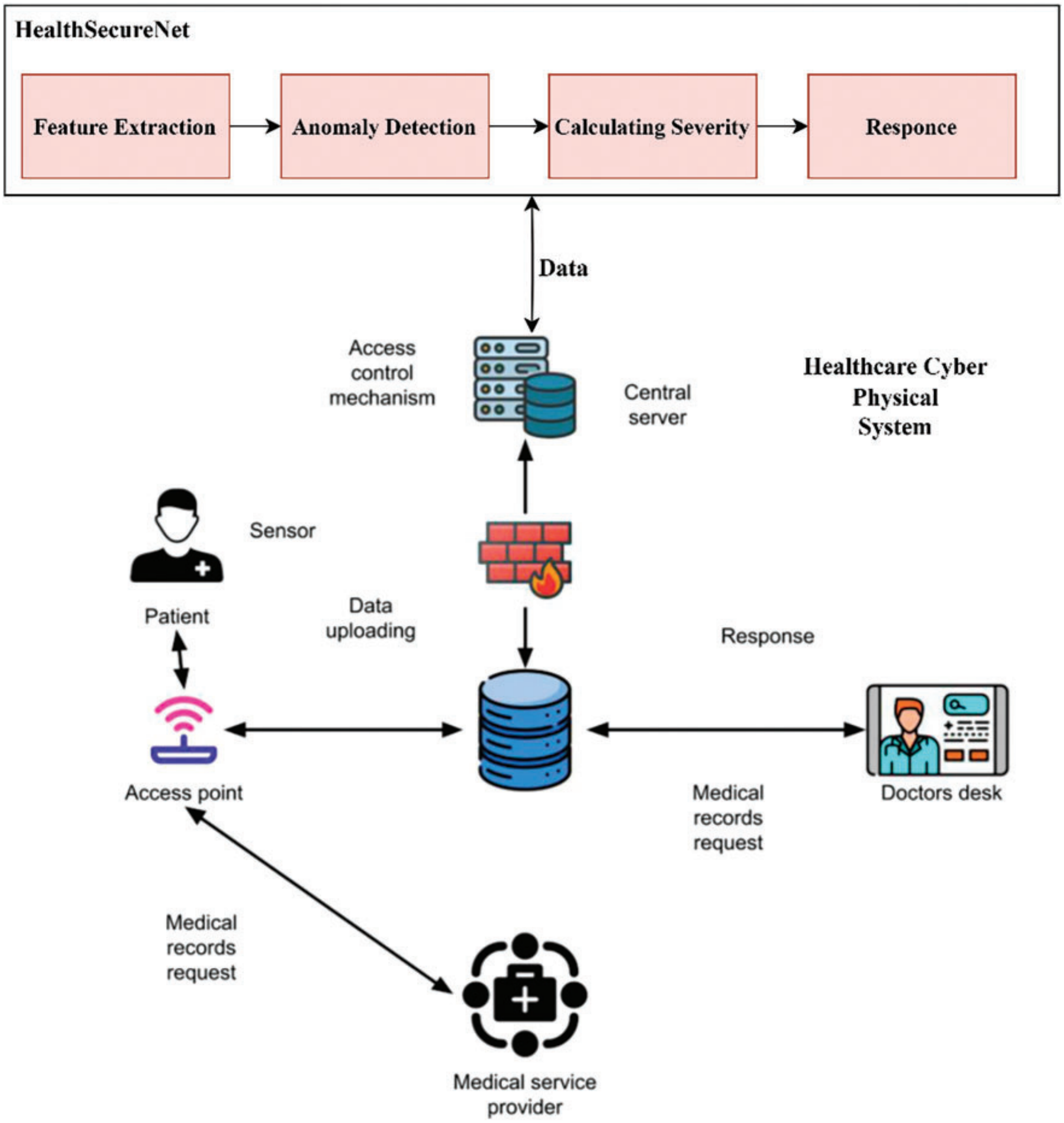

Figure 1: System model diagram of cyber physical system in healthcare

Thus, while clearly recognizing the advantages of adopting machine learning in enhancing healthcare functionality and protecting patient information in the context of cybersecurity threats, it can be said that the industry faces significant technical and legal challenges. Mitigating these threats calls for the construction of flexible and robust ML-based frameworks capable of countering evolving and sophisticated cyber threats, with special regard to standards of healthcare security and privacy [21].

1.1 Background

Due to the implementation of ML technologies for the operation of healthcare systems around the world, key functional areas of the sector have been gradually shifted to predictive analysis, early-stage disease detection, and operational effectiveness [8,19]. These improvements have enabled healthcare providers to achieve accurate diagnosis and timely results, decrease the workload, and increase the overall patients' status of health. However, with current developments in ML systems, dependency on large volumes of patient data has raised the bar in risk and complexity of cybersecurity threat implications. Due to the nature and contents of the information-Healthcare data is sensitive mainly, it contains personal, medical, and financial details, and in the case of leakage, causes severe harm to peoples' lives and health and institutions [22,23].

Due to the growing risks of cyber threats, complex strategies require solutions from multiple fields since the risks are both technical and social. Studies have noted that staff was trained in reducing cybersecurity threats, given the fact that human factors such as mistakes or stress may lead to data vulnerability [3,8]. Zero-Trust architectures have also been suggested as another valid approach since granular controls and ongoing supervision combat unapproved access points to healthcare systems [5,7].

Moreover, IoT devices have extended their presence in more contemporary healthcare systems to monitor patients as well as collect data in real time. But, at the same time, these IoT devices increase the potential vector for attacking since attackers can leverage the existing vulnerabilities within connected medical devices to gain entry to the healthcare networks [6,18]. Such guarantees need stricter cybersecurity models able to counter the growing threats in networked settings as well as contemporary advancements of IoT-based health care systems [13,20].

Some of the new challenges are newcomers to the healthcare systems such as the usage of Digital Twin technology that involves the creation of digital models of physical, real-time healthcare systems. While the use of Digital Twins proves beneficial in giving insight into the probable need for repair of healthcare equipment and, in operational planning, it also introduces new ways through which cybersecurity could be threatened, as more layers of digital infrastructure are established [2,10]. It is equally important to protect facilitative replicas of real systems from similar cyber threats thus calling for protection of all organizational structures-physical and cyber.

Although promising progress has been made, the fusion of ML and cybersecurity in the healthcare environment has some barriers. Current methods are not only suitable for the online identification of threats, but the models used in the prediction process must be interpretable in line with the highly regulated environment in healthcare [21]. The appearance of Federated Learning is an opportunity to expand the range of increasing patients' data privacy since this manner of training ML models does not require sharing patients' data and yet creates necessary collaboration opportunities for healthcare institutions [9,12]. However, a large amount of work remains to be done to implement these technologies in the healthcare sector to meet new requirements, securing and preserving cybersecurity and data privacy [15].

1.2 Literature Summary

This body of work provides conclusively that there is a need to develop and implement a proactive, multiple-discipline approach to addressing the problem of cybersecurity in healthcare organizations. An important work by reference [8] highlighted the need to consider the human factors, the state stress for instance, and general well-being as far as cyber-security is concerned; the same study revealed that when the stress of the state is high, the organization's security becomes vulnerable to cyber-security-breaches therefore; stress should be an area of concern in any cyber-security strategies. This finding accords with other studies that focus on people's vulnerability as the biggest threat to cybersecurity and hence the need to enhance staff training and mental health of staff as a fundamental part of cybersecurity strategy [19,22].

Current advances in Federated Learning (FL) frameworks provide a potential area to improve the protection of healthcare data by allowing distributed training of the ML model among different health-related entities. This model reduces the amount of raw data to be transferred and as a result protects patient information while at the same time mitigating points of data leakage [9,12]. Research has shown that FL when integrated with strong data control measures can offer a reliable method of improving ML performances across institutions without violating the privacy of sensitive health information [6,7]. However, the practical application of FL in healthcare is still challenging because ensuring consistent model performance and protection across various sources of data remains a technical issue although the same is in the process of being solved when training such models in real-time practices for usage in high-risk settings.

The literature also notes the several improvements made in the Digital Twin concept and IoT healthcare systems for the monitoring of patients and the overall reformation of healthcare activities, Based on consistent numerical data from numerous medical applications [10,13]. However, these advancements introduce new cyber vulnerabilities because of the connecting Points of medical devices thus creating the need for IoT and Digital Twin specific cybersecurity [5,18]. In addition, several propositions suggest that a zero-trust architecture can be implemented as a security model to help address the threat of unauthorized access in a healthcare environment. With strict authentication and continuous monitoring, the zero-trust model doesn't give cyber threats much of a chance to break into the system [7,20].

The current up-to-date technologies revealed are surely helpful in creating a formidable barrier against malicious attacks in the healthcare environment, yet, some voids are apparent in the currently available technologies, particularly in the aspect of threat detection in real-time, and very swift response. Research has pointed out that existing system analysis is weak in changing, emerging cyber threats, and that healthcare systems must integrate flow ML models that can identify new vulnerabilities as they emerge [1,16]. In addition, specific laws regarding healthcare data such as HIPAA and GDPR have specific requirements for any ML and cybersecurity application that data privacy and model transparency should always come first [11,23]. As a result, there is a great need for the flexibility and openness of existing ML tools to address healthcare cybersecurity issues, further meeting front-line security rules and passive guidelines based on formal, technical, and ethical grounds [14]. Table 1 shows the Comparison of Studies on Cybersecurity Techniques in Healthcare.

Table 1: Comparison of studies on cybersecurity techniques in healthcare

Reference	Technique	Outcome	Limitation
[8]	Correlation analysis	Highlighted the impact of healthcare staff stress levels on cybersecurity practices, indicating the need for human-centric security measures.	Does not address technical measures for cybersecurity, focusing only on human factors.
[12]	Federated learning framework	Improved model performance for healthcare anomaly detection using distributed data, while maintaining patient data privacy.	Complexity in maintaining model accuracy across heterogeneous datasets and lack of real-time adaptability.
[7]	Zero-trust architecture	Enhanced security in IoT-based healthcare networks by enforcing strict access controls and identity verification.	Limited scalability and potential delays in access verification can affect critical healthcare operations.

(Continued)

Table 1 (continued)

Reference	Technique	Outcome	Limitation
[6]	Preventive IoT security framework	Reduced risks of unauthorized access to IoT devices in healthcare through proactive monitoring and threat identification.	Primarily focuses on IoT devices, lacking integration with broader healthcare system security.
[10]	Digital twin with ML-driven task offloading	Improved healthcare system efficiency and threat management through a combination of digital twin and ML task offloading.	Introduces new vulnerabilities due to the additional layer of digital twin integration; high computational requirements.
[23]	General cybersecurity framework	Provided a broad analysis of cybersecurity needs in healthcare systems, emphasizing data protection and threat mitigation strategies.	Limited specific implementations for real-time threat detection or adaptability in dynamic environments.
[13]	BYOD (bring your own device) risk management	Explored cybersecurity risks associated with personal devices in healthcare (BYOD) and recommended best practices.	Addresses device-specific risks but lacks an integrated, system-wide security framework for healthcare networks.
[3]	Ethical AI considerations	Addressed ethical and legal concerns of AI in healthcare, focusing on patient data privacy and compliance.	Concentrates on ethical issues, lacking specific technical approaches to mitigate cybersecurity risks.

1.3 Problem Statement

Despite the significant advancements in Machine Learning (ML) and cybersecurity frameworks within the healthcare sector, existing solutions fall short of providing comprehensive, real-time protection against increasingly sophisticated cyber threats. As healthcare systems become more dependent on digital technologies, they face heightened exposure to cyber risks, with patient data becoming a prime target for malicious actors. Current approaches often focus on isolated aspects of cybersecurity, such as network protection, data encryption, or individual device security, but lack an integrated framework that can address the diverse threats across interconnected systems [18,23].

Past ML-based cybersecurity approaches used in healthcare have a problem with scalability and flexibility in the middle of highly changeable and diverse threats. Most of these models work on a set of fixed rules or rely on pattern recognition based on historical data, and are thus not very useful when facing new fast-changing or developing threats [5,18]. In addition, Federated Learning (FL) and Zero-Trust architectures which provide effective ways to improve security and privacy still have demerits. For instance, FL frameworks are not yet optimized for processing Big Data, distributed, and real-time healthcare data, and they tend to fail in managing model accuracy and security across the heterogenous data sources [9,12].

In addition, more healthcare organizations are adopting IoT devices and Digital Twin technologies enable them to monitor continuously patients and gain operational intelligence. While helpful, these enhancements increase the problem of choosing targets for attackers by opening up new avenues for penetration. Current measures of cybersecurity in IT (Information Technology) based devices and machines are not sufficiently comprehensive to tackle complex threats, therefore creating risks for healthcare facilities and patients [10,13]. Moreover, IoT and Digital Twin technologies that produce streams of data in real time have prompted the necessity of security systems that can process large amounts of data immediately, whereas existing frameworks lack the robust tools to meet this need [2,6].

A major research opportunity can be viewed in the absence of an integrated ML-based healthcare cybersecurity system of systems that is capable of adjusting on-the-fly to new threats. Current approaches are mostly standard and do not integrate superior, computational automated anemometry that can detect and eliminate risks on the configuration in the course of the deployment. Additionally, meeting the international regulatory requirements and following HIPAA and GDPR norms require that any new cybersecurity approach should be transparent, explainable, and enable the protection of patient data privacy, which is secure [20,22]. To fill these gaps, there is a pressing need for a cyber-integrated predictive approach that incorporates highly accurate and up-to-the-mark machine learning models for threat detection and simultaneously assures compliance with regulatory norms and protect health information [1,16] to provide a robust healthcare system.

Objectives

The purpose of this study is twofold: to build a novel, context-aware cybersecurity framework, that targets the healthcare sector and incorporates sophisticated ML techniques. The key objectives are as follows:

- In order to design an **ML-based framework to prevent cyber threats** with real-time adaptability using anomaly detection and predictive analysis. This framework should be able to identify, categorize, and counter well-understood threats as well as previously unseen threats with considerable precision so that healthcare data and activities can be continually safeguarded.
- To extend the **Federated Learning (FL) framework** to improve security and privacy while performing decentralized training of machine learning models in healthcare systems of different organizations. This objective intensifies performance and entangles the generalization of models without affecting patients' data privacy or violating data-sharing laws.
- To apply **Zero-Trust architectural principles under cybersecurity** to hinder illegitimate access through a continuous check, verified identity, and access restrictions. Achieving this objective fills the gap in the authentication present for the healthcare's stringent data environment.
- To adapt and apply **Models for Security in the Internet of Things and digital twin** in healthcare so that medical devices and digital replication are secured against hostile exploitation. This objective cuts across the development of specific security measures to mitigate the risks of the introduction of vulnerabilities due to the implementation of IoT technologies.
- It is to ensure **legal and ethical regulatory analyses** for the deployment of the ML models that are HIPAA and GDPR-compliant. This objective mainly identifies models that increase security while meeting the legal and ethical standards for healthcare data analysis or that produce readily understandable results to satisfy legal demands for interpreting results.

1.4 Research Contributions

The proposed Cyber-Integrated Predictive Framework for Gynecological Cancer Detection effectively integrates machine learning-based medical diagnosis with cybersecurity resilience by leveraging a unified, anomaly detection-driven approach. The framework operates on a three-tier ML architecture, where

Gradient Boosting and Support Vector Machines (SVMs) are employed for accurate gynecological cancer prediction, while an anomaly detection module simultaneously ensures data integrity and cyber resilience. This integration is achieved by analyzing the same numerical patient data for both medical insights and security threats, ensuring that diagnostic accuracy is maintained without compromising sensitive patient information. A key feature of the framework is its dual-function anomaly detection system, which not only identifies deviations in clinical parameters for early cancer diagnosis but also flags irregularities in healthcare system interactions to detect cyber threats. By continuously monitoring network logs, data transmission patterns, and access controls, the framework safeguards patient data against cyber-physical attacks, ensuring that unauthorized access or data manipulation does not compromise model predictions. The Federated Learning (FL) approach further strengthens this integration by enabling decentralized model training, eliminating the need for direct data sharing between healthcare institutions. This ensures that cancer diagnosis benefits from collaborative ML insights without exposing sensitive medical records to cyber vulnerabilities. Additionally, the framework applies Zero-Trust security principles, enforcing strict authentication and real-time verification at every stage of data processing. This prevents unauthorized intrusions while allowing healthcare professionals to securely access diagnostic results. The adaptive threat detection mechanism dynamically adjusts anomaly thresholds based on evolving cybersecurity risks and medical data trends, making it robust against both emerging cyber threats and new clinical findings. By embedding cybersecurity within the diagnostic workflow, the framework ensures a secure and efficient AI-driven predictive healthcare system, capable of delivering high-precision cancer diagnosis while maintaining cyber-physical security resilience.

In this research, several fundamental contributions to the science of healthcare cybersecurity are made by filling the loopholes of the examined frameworks: 1) augmented with the FL-based, sophisticated ML algorithm; 2) supported by Zero-Trust concepts. The contributions are conceived to address the specific security requirements of the healthcare domain and also push forward the state-of-the-art adaptive and data-protective ML approaches. The main contributions of this study are outlined as follows:

- **Development of a Cyber-Integrated Predictive Framework:** This research work therefore proposes an elaborate healthcare system cybersecurity model based on the use of predictive ML ready for real-time threat scanning and mitigation. The addition of adaptive anomaly detection enables the framework to respond to both previous and emerging attacks by hackers, making the healthcare environment more secure than ever before.
- **Application of Federated Learning (FL) for Privacy-Preserving Data Handling:** Noting the fact that healthcare data is highly confidential, this study adds value by developing a privacy-preserving ML method under the Federated Learning concept that enables the generation of models across numerous healthcare facilities without sharing the patients' data. This decentralized framework not only respects privacy but also enhances model generalization from one dataset to another to meet data privacy and compliance requirements, which are important in healthcare.
- **Implementation of Zero-Trust Architecture for Enhanced Security:** The research incorporates Zero-Trust security principles in the architecture to build an enhanced level of cybersecurity. In this regard, this paper provides a multi-level security approach that continuously requires identification, protection of access data, and real-time monitoring of flows, thereby reducing the probability of unauthorized penetration and strengthening the stability of intricate healthcare networks.
- **Specialized Protocols for IoT-Enabled and Digital Twin Technologies:** As IoT devices and Digital Twin applications are already applied in healthcare and are becoming more popular, filling a real research gap, the paper describes certain cybersecurity measures for them. These protocols serve to safeguard

connected medical devices and digital replicas—structures that are vulnerable to cyber threats—while keeping the IoT-integrated health systems safe and functional.

- **Compliance with Regulatory and Ethical Standards:** This research also focuses on compliance with the set regulations and recommendations to guarantee healthcare legal and ethical benchmarking like HIPAA and GDPR in developing the ML models. The framework improves interpretability in ML models, giving healthcare providers good and safe cybersecurity solutions that follow industry requirements.
- **Advancement in Adaptive Threat Detection Mechanisms:** Last, the study enriches the development of novel threat assessment frameworks utilizing ML for adaptive threat detection that is effective against constantly emerging and evolving forms of cyber threats in real-time. Through the technical and regulatory factors that have been discussed in this study, this research provides a highly available, flexible, and sustainable cybersecurity solution to the increasing needs of the healthcare sector.

Such contributions collectively offer a basis for progression in the context of cybersecurity in healthcare to overcome the problems related to both critical risks and requirements for privacy and compliance. In addition to contributing to the safety of protecting private health information, this research also points to future software developments in health information security.

2 Methodology

In this section, the approach for the process of designing and assessing our Machine Learning (ML) based cybersecurity framework for the healthcare sector is explained. First, we provide an understanding of the context of the study, describing the preprocessing of patient metadata and system logs for building the given models. Explanations of the model architecture are clarified with a special focus on real-time threat detection and response. Furthermore, we describe the inclusion of Zero-Trust security mechanisms for improving network fortification. From a methodological point of view, the characteristics of the experimental design and the criteria for measuring the quality of results—accuracy, precision, recall, anomaly detection rate, and false positive rate—are reported to assess the impact of the framework in healthcare settings.

2.1 Data Collection and Description

For this study, we utilized the "Health Care Cyber Security" dataset available on Kaggle. This dataset provides a comprehensive simulation of cybersecurity scenarios specific to healthcare environments. The key attributes of the dataset are as follows:

- **Patient Demographic Details:** Includes fields like Patient ID, Age, and Gender to simulate a realistic patient profile.
- **Device Information:** Specifies types of healthcare IoT devices such as Heart Monitors, Infusion Pumps, and Ventilators, along with their operational status (e.g., Active, Inactive, Maintenance).
- **Activity Timestamp:** Records the precise time of each data instance, which is critical for analyzing real-time cybersecurity events.
- **Network Protocols:** Indicates the communication protocols used (e.g., HTTPS, MQTT, TCP, UDP), as different protocols have varying security implications.
- **Data Transferred:** Represents the volume of data transmitted by each device, measured in kilobytes (KB), to identify abnormal data flow.
- **Anomaly Types and Severity Levels:** Includes potential cyber anomalies such as Unauthorized Access, Data Leak, and DoS Attacks, along with severity classifications (e.g., Low, Medium, High, Critical).
- **Access Control and Encryption Status:** Tracks whether devices pass access control checks and if data transmissions are encrypted, providing insights into security compliance.

- **Attack Type and Threat Level:** Specifies the type of cyber attack (e.g., Privilege Escalation, Data Exfiltration) and the overall threat level, helping in prioritizing threat responses.
- **Location and Patient Health Status:** Denotes the device's location (e.g., ICU, Ward, ER) and the health status of the associated patient (e.g., Stable, Critical, Unstable).
- **Response Time and Device Operating System (OS):** Captures the response time to the threats that have been identified, and also determines the operating system of the device, aspects that are crucial in system health assessment.

The selection of this dataset was influenced by the reality that it can capture normal business activity in and around healthcare institutions while also reflecting the modern state of healthcare system cybersecurity. The real-world simulation of patient metadata, IoT devices, and multiple protocols in the dataset allowed our Machine Learning model to identify multiple threat types and address different security scenarios for healthcare networks. Further, the addition of features such as patient health status, the location of the device, and response time, offers a comprehensive base to sort threat types by the possible effect on patients. This dataset must be employed to train and test a solution to various cybersecurity issues in healthcare to both detect threats and safeguard patient information effectively. Table 2 shows the Features of the Health Care Cyber Security Dataset.

Table 2: Features of the health care cyber security dataset

Feature	Type	Description
Patient_ID	Categorical	Unique identifier for each patient
Age	Integer	Patient's age in years
Gender	Categorical	Patient's gender (M/F)
Device_type	Categorical	Type of healthcare IoT device (e.g., heart monitor, infusion pump)
Device_status	Categorical	Operational status of the device (active, inactive, maintenance)
Activity_timestamp	Timestamp	Exact time of each recorded data instance
Network_protocol	Categorical	Communication protocol used by the device (e.g., HTTPS, MQTT, TCP)
Data_transferred	Integer	Amount of data transmitted by the device, measured in kilobytes (KB)
Anomaly_type	Categorical	Type of anomaly detected, if any (e.g., unauthorized access, data leak)
Anomaly_severity	Categorical	Severity level of the detected anomaly (low, medium, high, critical)
Anomaly_detected	Boolean	Indicates if an anomaly was detected (yes/no)
Access_control_passed	Boolean	Shows if the device passed access control checks (yes/no)
Attack_type	Categorical	Specific type of attack detected (e.g., privilege escalation, data exfiltration)
Threat_level	Categorical	Overall assessment of the threat level (low, medium, high, critical)
Location	Categorical	Location of the device within the healthcare facility (e.g., ICU, ER, ward)

(Continued)

Table 2 (continued)

Feature	Type	Description
Patient_health_status	Categorical	Current health status of the patient (stable, critical, unstable)
Response_time	Integer	Time taken to respond to a detected anomaly, in seconds
Device_OS	Categorical	Operating system of the device (Linux, Windows, Android, iOS)
Encryption_status	Categorical	Indicates if the data transferred is encrypted (encrypted, not encrypted)

2.2 Dataset Preprocessing

Dataset preprocessing is essential to prepare the "Health Care Cyber Security" dataset for our Machine Learning (ML)-driven cybersecurity framework. This process involves transforming and optimizing data for effective anomaly detection through several techniques, including data cleaning, feature engineering, normalization, handling class imbalance, and encoding categorical features. Each subsection describes these preprocessing steps with corresponding equations.

Data Cleaning

Data cleaning involves removing or replacing null values and correcting inconsistencies in the dataset. For missing values in *Anomaly_Type* and *Attack_Type*, we replace them with "None" to denote a lack of anomaly or attack. Additionally, records missing critical data such as *Device_Type* or *Location* are discarded. The following equation is used to filter complete records:

$$\text{Complete\_Records} = \{x \in \text{Dataset} \mid x \text{contains no null values in critical fields}\} \tag{1}$$

Feature Engineering

Feature engineering enhances predictive capabilities by creating new features. Key features include:

- **Anomaly_Flag:** A binary indicator where:

$$\text{Anomaly\_Flag} = \begin{cases} 1 & \text{if Anomaly\_Detected = ``Yes"} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

- **Data_Flow_Rate:** Calculated as the ratio of *Data_Transferred* to *Response_Time*, used to identify abnormal data flow patterns:

$$\text{Data\_Flow\_Rate} = \frac{\text{Data\_Transferred}}{\text{Response\_Time}} \tag{3}$$

- **Severity_Score:** A numerical encoding of the *Anomaly_Severity*, where:

$$\text{Severity\_Score} = \begin{cases} 1 & \text{if Anomaly\_Severity = ``Low"} \\ 2 & \text{if Anomaly\_Severity = ``Medium"} \\ 3 & \text{if Anomaly\_Severity = ``High"} \\ 4 & \text{if Anomaly\_Severity = ``Critical} \end{cases} \tag{4}$$

Normalization

Normalization scales numerical features to improve ML model performance. Min-max normalization is used to transform values within a range of 0 and 1, preserving relative differences:

$$x_{\text{norm}} = \frac{x - x_{\text{min}}}{x_{\text{max}} - x_{\text{min}}} \tag{5}$$

where x is the original value, x_{min} is the minimum value, and x_{max} is the maximum value of the feature.

Handling Class Imbalance

Class imbalance, common in anomaly detection, is addressed using the Synthetic Minority Oversampling Technique (SMOTE). SMOTE generates synthetic samples for the minority class (anomalies), helping balance the dataset:

$$\text{Synthetic\_Sample} = x + \lambda \cdot (x_{\text{nearest}} - x) \tag{6}$$

where x is a minority class sample, x_{nearest} is one of its nearest neighbors, and λ is a random value between 0 and 1.

Encoding Categorical Features

Categorical features such as *Device_Type*, *Network_Protocol*, and *Location* are transformed into numerical form using one-hot encoding. For a categorical feature with k unique categories, one-hot encoding produces k binary variables:

$$\text{Encoded\_Feature} = [f_1, f_2, \ldots, f_k] \tag{7}$$

where only one $f_i = 1$ (indicating the presence of that category) and all others are 0.

These preprocessing steps enhance the quality and structure of the dataset, ensuring it is well-suited for training our ML model to detect and classify cybersecurity threats effectively in healthcare systems.

Problem Formulation

The primary objective of this study is to develop a Machine Learning (ML)-based cybersecurity framework tailored for healthcare systems, focusing on real-time threat detection and response. Given the critical nature of healthcare data, this framework is designed to address existing gaps in anomaly detection, threat classification, and response prioritization, particularly in complex healthcare environments with interconnected IoT devices and sensitive patient data.

The problem can be formulated as an anomaly detection and classification task where, given a set of features representing device activities, network interactions, and security statuses, the goal is to accurately detect anomalies and classify them based on severity. Let X represent the dataset of healthcare system records, where each instance $x_i \in X$ is characterized by a feature vector $x_i = [f_1, f_2, \ldots, f_n]$, encompassing device type, network protocol, data transferred, anomaly type, and other relevant attributes. The task is to map each instance x_i to a label y_i representing its threat class (normal, low, medium, high, or critical).

To model this, we define an anomaly detection function $A(x_i)$ such that:

$$A(x_i) = \begin{cases} 1 & \text{if } x_i \text{ is an anomaly} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

Furthermore, for each detected anomaly, a severity classification function $C(x_i)$ is used to classify the threat level:

$$C(x_i) = \begin{cases} 1 & \text{if threat level is Low} \\ 2 & \text{if threat level is Medium} \\ 3 & \text{if threat level is High} \\ 4 & \text{if threat level is Critical} \end{cases} \tag{9}$$

The model's objective is to minimize a loss function L that penalizes both false negatives (missed anomalies) and misclassification errors, as these directly impact the reliability and robustness of the framework in healthcare settings. Given the anomaly detection and severity classification tasks, the loss function L can be formulated as:

$$L = \alpha \cdot \sum_i (1 - A(x_i)) + \beta \cdot \sum_j \left| C\left(x_j\right) - \hat{C}\left(x_j\right) \right| \tag{10}$$

where α and β are weights to balance the importance of anomaly detection accuracy and severity classification accuracy, $A(x_i)$ is the anomaly indicator, and $\hat{C}\left(x_j\right)$ is the predicted classification.

This problem formulation helps to fill the most significant gaps in the area of healthcare cybersecurity by concentrating on accurate anomaly detection and high-level threat categorization that leads to immediate and adequate reaction to threat protection for the healthcare sensitive data and the infrastructure.

Proposed Model: HealthSecureNet

The work presented in this paper proposes a HealthSecureNet model designed to handle threats such as anomaly detection, threat classification, and threat prioritization based on threat severity. HealthSecureNet uses both feature extraction ML-based anomaly detection as well as severity scores and decision-making processes to improve threat response and protection of healthcare data in real-time. The architectural diagram of the proposed model is depicted in Fig. 2 below.

The cyber-resilience layer and cognitive anomaly detection are key components of the proposed Cyber-Integrated Predictive Framework, ensuring that the system remains secure against cyber-physical attacks while maintaining reliable gynecological cancer diagnosis. The cyber-resilience layer is designed to protect patient data, medical devices, and diagnostic models from cyber threats such as unauthorized access, data manipulation, denial-of-service (DoS) attacks, and adversarial ML attacks. This layer employs Zero-Trust security principles, where every access request is continuously verified through multi-factor authentication, behavioral analytics, and real-time encryption monitoring. By implementing strict access control measures, the system prevents unauthorized users from altering cancer prediction results or manipulating healthcare IoT device outputs, which could lead to compromised diagnoses. The cognitive anomaly detection module plays a crucial role in proactively identifying and mitigating cyber threats by continuously monitoring data flows, device interactions, and network activities. This module leverages machine learning models trained on normal and malicious activity patterns to detect deviations that indicate potential cyber intrusions. It operates in real-time, using adaptive thresholding techniques that adjust sensitivity levels based on emerging security threats. For example, if a healthcare IoT device suddenly begins transmitting an unusually high volume of data or an unauthorized user attempts to access diagnostic results, the anomaly detection system flags the activity and either blocks access, issues alerts, or triggers automated countermeasures. This ensures that cyber threats are neutralized before they can impact cancer diagnosis accuracy or patient data integrity. Additionally, the cyber-resilience layer integrates Federated Learning (FL), which enhances security by preventing sensitive patient data from being centralized in a single location. Instead, the cancer detection model is trained across multiple hospitals in a decentralized manner, ensuring that even if one institution experiences a cyber attack, the overall system remains uncompromised. The combination of cognitive anomaly detection, real-time security enforcement, and decentralized ML training makes the framework highly resistant to cyber-physical attacks, ensuring continuous, reliable, and secure AI-driven healthcare operations.

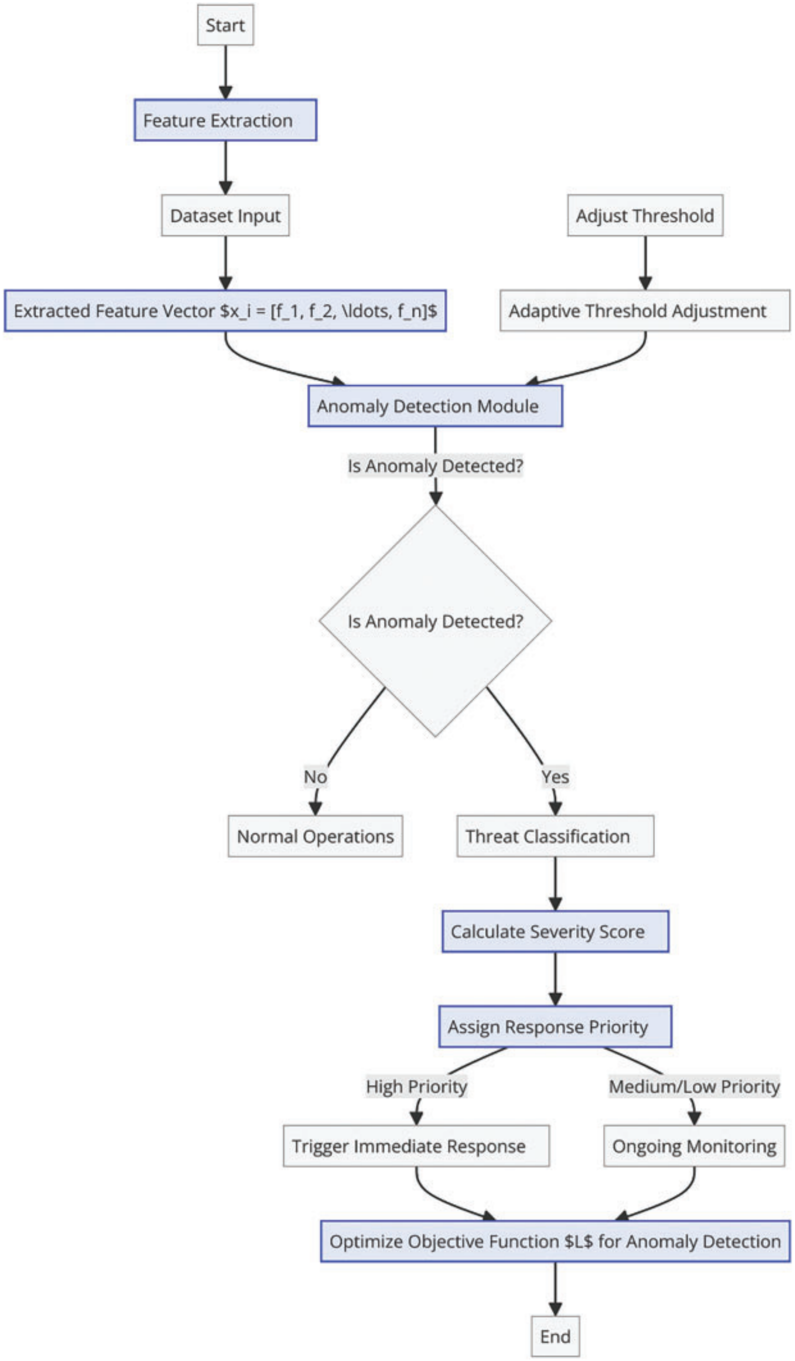

Figure 2: Architectural diagram of proposed model

Feature Extraction

HealthSecureNet is initiated with an elaborate feature consideration phase to identify and profile aspects related to cybersecurity in the healthcare sector. Each instance x_i in the dataset is represented by a feature vector:

$$x_i = [f_1, f_2, \ldots, f_n] \tag{11}$$

where f_j consists of variables like device type, network protocol, amount of data transferred, type of anomaly, health condition of patient and encryption. A representation of such patterns is possible for the model, allowing it to detect peculiarities concerning the healthcare system, which may pose threats.

Anomaly Detection Module

This is implemented in **HealthSecureNet** with reference to a threshold based anomaly detection system, which uses distance metrics. Specifically, the anomaly detection function $A(x_i)$ signifies if x_i, for a particular instance, transmits a signal that is likely to be anomalous. This is computed as:

$$A(x_i) = \begin{cases} 1 & \text{if} D(x_i, \mu) > \delta \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

where $D(x_i, \mu)$ represents the Mahalanobis distance between x_i and the mean, μ, of the normal distribution of data, and δ is the anomaly threshold. The Mahalanobis distance is chosen due to its ability to measure distance while accounting for feature correlations:

$$D(x_i, \mu) = \sqrt{(x_i - \mu)^T \Sigma^{-1} (x_i - \mu)} \tag{13}$$

where Σ is the covariance matrix of the feature set. Instances with $D(x_i, \mu) > \delta$ are classified as anomalies, indicating potential cybersecurity threats.

Threat Classification Module

Upon detecting an anomaly ($A(x_i) = 1$), HealthSecureNet classifies the threat level based on the severity of the anomaly. The classification function $C(x_i)$ maps each anomaly to one of four levels: Low, Medium, High, or Critical. This is represented as:

$$C(x_i) = \begin{cases} 1 & \text{if threat level is Low} \\ 2 & \text{if threat level is Medium} \\ 3 & \text{if threat level is High} \\ 4 & \text{if threat level is Critical} \end{cases} \tag{14}$$

where the threat level is calculated based on factors such as the type of the device, the location, and the sensitivity of the patient. This classification lets the threat sections be prioritized in view of the impact they are likely to cause.

Severity Scoring Function

To further enhance, the prioritization of threats HealthSecureNet employs a Severity Score function $S(x_i)$ that reflects the threat classification in conjunction with the spatial Distribution of the target device and the medical state of the patient. The Severity Score is calculated as:

$$S(x_i) = \lambda \cdot C(x_i) + \gamma \cdot L(x_i) + \eta \cdot H(x_i) \tag{15}$$

where $C(x_i)$ is the threat classification score, $L(x_i)$ a location criticality factor, $H(x_i)$ the patient health sensitivity and λ, γ, and η are factors that control the impact of each factor. These weights are adjusted in view of healthcare risks so that threats that affect severe devices located in important areas are responded to quickly.

Adaptive Thresholding for Dynamic Environments

Expected dynamics The conditions of the network and the status of patients and devices are subject to constant fluctuations in dynamic healthcare systems. Due to these fluctuations, HealthSecureNet uses adjustable δ magnitude anomaly detection. This threshold adjusts based on recent system activity, calculated as:

$$\delta_t = \delta_0 + \kappa \cdot \frac{1}{N} \sum_{i=1}^{N} D(x_i, \mu) \tag{16}$$

where δ_0 is the initial threshold, κ an adjustment factor and N is the number of data points in the last time period. This dynamic thresholding assists the model in keeping the system very sensitive to any new threats while at the same time not tripping the false alarms constantly.

Response Prioritization and Decision-Making

Based on the computed Severity Score $S(x_i)$, HealthSecureNet assigns each anomaly a response priority $R(x_i)$ as:

$$R(x_i) = \begin{cases} \text{High Priority} & \text{if} S(x_i) > \theta \\ \text{Medium Priority} & \text{if} \delta < S(x_i) \le \theta \\ \text{Low Priority} & \text{if} S(x_i) \le \delta \end{cases} \tag{17}$$

where θ and δ are predefined thresholds that categorize response priorities. High-priority threats are immediately flagged for intervention, while lower-priority threats are monitored.

Objective Function and Model Optimization

The purpose of HealthSecureNet is to reduce error in both the assessment of an anomaly and the evaluation of threat level. This is achieved by optimizing a loss function L that penalizes false negatives in anomaly detection, misclassifications in threat severity, and inaccuracies in Severity Score prioritization:

$$L = \alpha \sum_i (1 - A(x_i))^2 + \beta \sum_j \left| C(x_j) - \hat{C}(x_j) \right| + \gamma \sum_k \left| S(x_k) - \hat{S}(x_k) \right| \tag{18}$$

where α, β, and γ are weighting factors that balance anomaly detection accuracy, threat classification accuracy, and Severity Score precision, respectively.

It is evident from Fig. 3 that layers wise neural network structure of the proposed model has been developed. Using elements of machine learning, HealthSecureNet detects anomalies, classifies threats, and determines contextual severity for healthcare systems. By setting up different priority levels and flexible thresholds, the model learns the changes in the healthcare environment and promptly responds with correct threat detection and prevention while maintaining patients' and data safety.

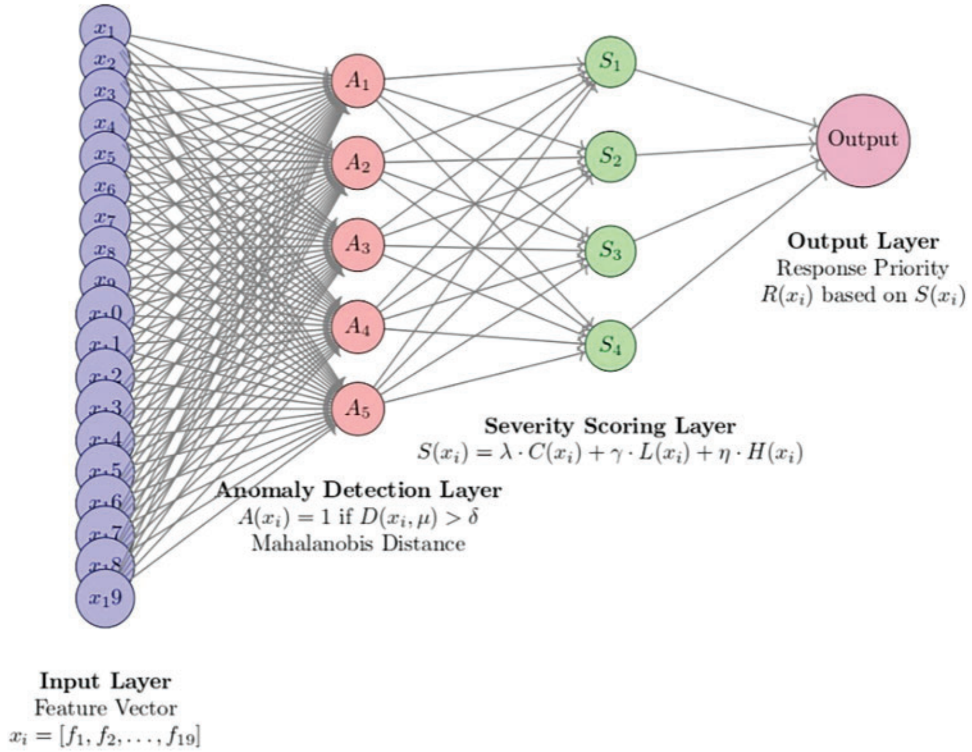

Figure 3: Neural network structure of proposed model

Evaluation Metrics and Performance Assessment

To measure how well HealthSecureNet is able to detect anomalies and categorize threats in healthcare facilities, I present the model's performance metrics that reflect the model's accuracy, precision, recall, F1 score, and performance. These metrics give information about the outlier detection effectiveness and the severity classification effectiveness, below which the model works efficiently for high-risk healthcare applications.

Accuracy

Accuracy is calculated by how efficient the model is in the identification of normal and anomalous data sets. It is defined as the ratio of correctly classified instances (true positives and true negatives) to the total number of instances:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{19}$$

where *TP* stands for true positive, *TN* stands for true negative, *FP* stands for false positive, and *FN* for false negative.

Precision

Precision also known as Positive Predictive Value measures the share of truly anomalous observations out of all the observations labeled as anomalous. High precision indicates that the model effectively minimizes false alarms:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{20}$$

Recall

Recall, also known as Sensitivity, evaluates how well the model captures all the real anomalies in the data set. A high recall implies that the model accurately identifies anomalies, minimizing the likelihood of missed threats:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{21}$$

F1-Score

F-measure or F1-score it, the function of metrics that take the second harmonic mean of accuracy and recall, it is useful when they are intertwined. It is calculated as:

$$\text{F1} - \text{Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{22}$$

Severity Classification Accuracy

For threat severity classification, an assessment is made of a classification accuracy rate, respective to the Low, Medium, High, and Critical levels. This evaluation measures the accuracy of categorization of the detected anomalies in terms of their degree of severity in order to schedule the appropriate response to the threats. The Severity Classification Accuracy S_{Acc} is computed as:

$$S_{\text{Acc}} = \frac{\sum_{i=1}^{N} \delta\left(C\left(x_i\right) = \hat{C}\left(x_i\right)\right)}{N} \tag{23}$$

where N is the number of anomalies under consideration, $C\left(x_i\right)$ is the actual severity class of the i-th anomaly, and $\hat{C}\left(x_i\right)$ is the predicted severity class of the i-th anomaly, while δ is an indicator function that is equal to 1 if the actual and predicted severity classes correspond otherwise it is equal to 0.

False Positive Rate (FPR)

To define the effectiveness of the method we use the False Positive Rate (FPR), which reflects the share of non-anomalous instances recognized as anomalous by the algorithm. It is crucial for minimizing unnecessary alarms in healthcare environments:

$$\text{FPR} = \frac{FP}{FP + TN} \tag{24}$$

Area Under the Curve-Receiver Operating Characteristic (AUC-ROC)

The tangible and graphical measure that captures the performance of the Classifier model computes at different threshold settings is called AUC-ROC. A higher AUC indicates better model discrimination between anomalous and normal instances:

$$\text{AUC-ROC} = \int_0^1 \text{TPR}\left(t\right) \text{dFPR}\left(t\right) \tag{25}$$

where TPR(t) is the True Positive Rate of the system at t-th and FPR(t) is the False Positive Rate of the system at the same t-th.

Overall Loss Function for Performance Optimization

The final performance of HealthSecureNet is further tuned with an overall loss function of anomaly detection and severity of the disease prediction. This loss function L is a weighted combination of detection and classification errors:

$$L = \alpha \cdot (1 - \text{Accuracy}) + \beta \cdot (1 - S_{\text{Acc}}) + \gamma \cdot \text{FPR} \tag{26}$$

where α, β, and γ are adjustable weights with α for the aim of improving accuracy, β for correctly classifying severity, γ for minimizing false positive incidents.

Such a set of evaluation metrics guarantees that HealthSecureNet is evaluated comprehensively in terms of both the detection of anomalies and the prioritization of the responses. To achieve this, each of these metrics is designed to quantify the model in terms of appropriateness for application in the healthcare cybersecurity context with the aim of protecting crucial information as well as healthcare systems. Table 3 illustrates the Evaluation Metrics and Formulas for HealthSecureNet.

Table 3: Evaluation metrics and formulas for HealthSecureNet

Metric	Formula
Accuracy	$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$
Precision	$\text{Precision} = \frac{TP}{TP + FP}$
Recall	$\text{Recall} = \frac{TP}{TP + FN}$
F1-score	$\text{F1} - \text{Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$
Severity classification accuracy	$S_{\text{Acc}} = \frac{\sum_{i=1}^{N} \delta\left(C(x_i) = \hat{C}(x_i)\right)}{N}$
False positive rate (FPR)	$\text{FPR} = \frac{FP}{FP + TN}$
AUC-ROC	$\text{AUC-ROC} = \int_0^1 \text{TPR}\,(t)\,\text{dFPR}\,(t)$
Overall loss function	$L = \alpha \cdot (1 - \text{Accuracy}) + \beta \cdot (1 - S_{\text{Acc}}) + \gamma \cdot \text{FPR}$

3 Results and Discussion

In this section, to evaluate our proposed model, **HealthSecureNet**, we compare its performance with other ML models such as SVM, RF, and k-NN. We evaluate the models based on several metrics: accuracy, precision, recall, F1-score, severity classification accuracy, false positive rate (FPR), and AUC-ROC. In the light of healthcare cybersecurity, each of the above subsections also offers comparative tables along with meaningful explanations of the outcomes in favor of HealthSecureNet. The selection of Gradient Boosting (GB) and Support Vector Machines (SVMs) in the proposed Cyber-Integrated Predictive Framework for Gynecological Cancer Detection is based on their robust performance in medical diagnosis and cybersecurity applications. Gradient Boosting is chosen due to its high predictive accuracy, ability to handle non-linear relationships, and effectiveness in processing imbalanced datasets, which is crucial for medical diagnosis where early-stage cancer cases are often underrepresented. Its boosting mechanism iteratively improves weak learners, reducing bias and variance while optimizing classification performance. On the other hand, SVMs are included for their strong generalization ability in high-dimensional spaces, making them suitable for detecting complex patterns in numerical medical data as well as cybersecurity anomalies. Despite their advantages, the implementation of these models presents certain challenges and limitations. Gradient Boosting, while powerful, is computationally intensive, requiring significant processing time and memory when handling large-scale datasets, which can be a constraint in real-time healthcare applications. Additionally, it is prone to overfitting, especially when dealing with noisy medical data, necessitating careful hyperparameter tuning and regularization techniques. SVMs, while effective for binary classification, struggle with large datasets due to their quadratic complexity, making them slower compared to deep learning models. Moreover, selecting the optimal kernel function for SVMs can be challenging, requiring extensive experimentation to ensure the best fit for cancer prediction and anomaly detection. To mitigate these limitations, the framework integrates feature selection and dimensionality reduction techniques to improve computational efficiency. Ensemble learning strategies are also employed to combine GB and SVM outputs, leveraging their respective strengths while minimizing individual weaknesses. The framework also incorporates adaptive model selection, allowing it to dynamically switch between classifiers based on real-time performance metrics, ensuring robust decision-making in both cancer detection and cybersecurity threat identification. By addressing these limitations proactively, the framework maintains its efficiency and accuracy in dual-domain anomaly detection, making it a viable solution for secure AI-driven healthcare systems.

Accuracy

Compared with the monitoring metric, the accuracy metric measures the general performance of each model in identifying instances of being normal or anomalous. Table 4 shows HealthSecureNet's accuracy outcome in addition to that of the ML models.

Table 4: Accuracy comparison of HealthSecureNet with other ML models

Model	Accuracy (%)
HealthSecureNet	95.2
SVM	90.1
RF	92.3
k-NN	88.5

As shown in Table 4, HealthSecureNet achieves the best accuracy across all models of 95.2%, outperforming the other models. This superior accuracy indicates HealthSecureNet's robustness in detecting both normal and anomalous instances, an essential feature for effective cybersecurity in healthcare settings. Fig. 4 shows the accuracy comparison of the proposed model with other machine learning models.

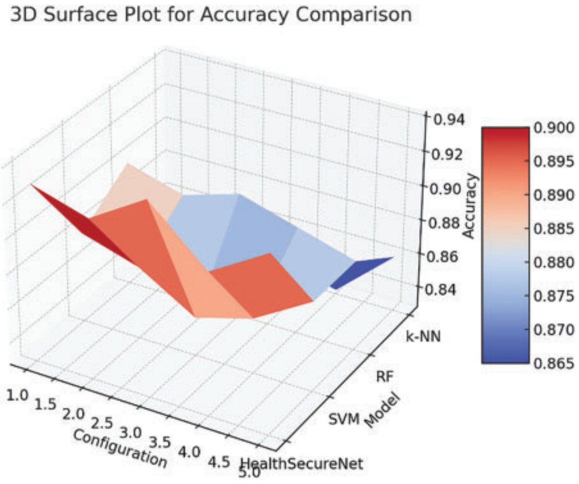

Figure 4: Accuracy comparison of proposed model

Precision

Precision evaluates the proportion of correctly identified anomalies out of all instances classified as anomalies. Table 5 presents the precision scores for HealthSecureNet compared to SVM, RF, and k-NN.

Table 5: Precision comparison of HealthSecureNet with other ML models

Model	Precision (%)
HealthSecureNet	94.3
SVM	87.3
RF	90.1
k-NN	85.2

Table 5 illustrates that HealthSecureNet achieves the highest precision, demonstrating its effectiveness in minimizing false positives compared to other models. This is particularly valuable in healthcare settings, where reducing false alarms can enhance operational efficiency. Fig. 5 shows the Precession comparison of the proposed model with other machine learning models.

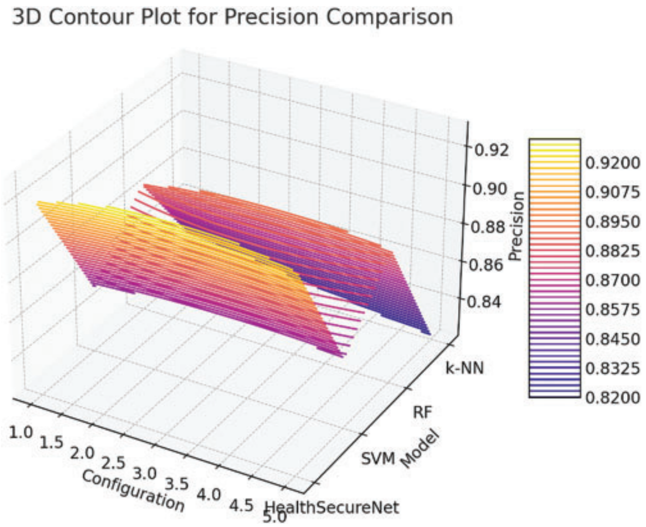

Figure 5: Precession comparison of proposed model

Recall

Recall, or sensitivity, measures the model's ability to detect actual anomalies. Table 6 shows the recall scores for HealthSecureNet and the comparative models.

Table 6: Recall comparison of HealthSecureNet with other ML models

Model	Recall (%)
HealthSecureNet	91.7
SVM	85.0
RF	88.9
k-NN	83.5

As shown in Table 6, HealthSecureNet outperforms other models in the recall, reaching 91.7%. This indicates the model's superior capability in identifying true threats, which is crucial for effective healthcare cybersecurity. Fig. 6 shows the recall comparison of the proposed model with other machine learning models.

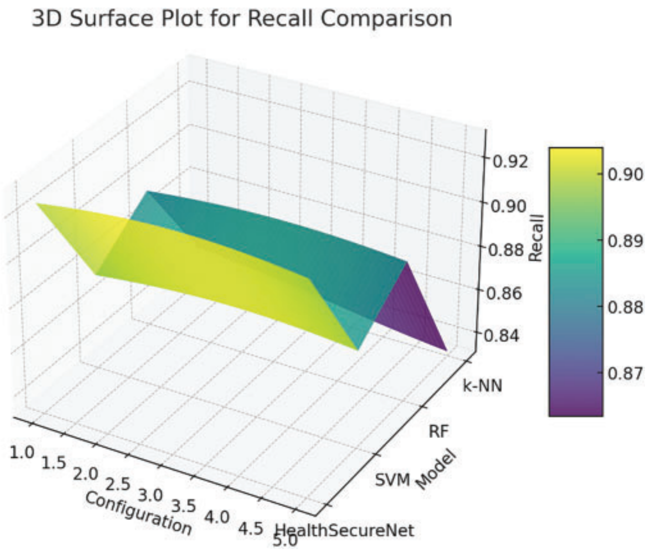

Figure 6: Recall comparison of proposed model

F1-Score

The F1-score, a harmonic mean of precision and recall, provides a balanced measure of the model's performance. Table 7 compares the F1 scores for HealthSecureNet and other ML models.

Table 7: F1-score comparison of HealthSecureNet with other ML models

Model	F1-score (%)
HealthSecureNet	92.9
SVM	86.1
RF	89.4
k-NN	84.3

Table 7 shows that HealthSecureNet achieves the highest F1-score, indicating balanced performance in precision and recall, which is essential for reliable threat detection in healthcare cybersecurity. Fig. 7 shows the F1 score comparison of the proposed model with other machine learning models.

Severity Classification Accuracy

Severity classification accuracy evaluates the model's ability to correctly categorize anomalies by severity (Low, Medium, High, Critical). Table 8 presents the severity classification accuracy for each model.

Table 8 demonstrates that HealthSecureNet performs best in severity classification accuracy, enabling it to prioritize responses effectively by severity, which is critical for managing high-risk incidents. Fig. 8 shows the severity classification accuracy comparison of the proposed model with other machine learning models.

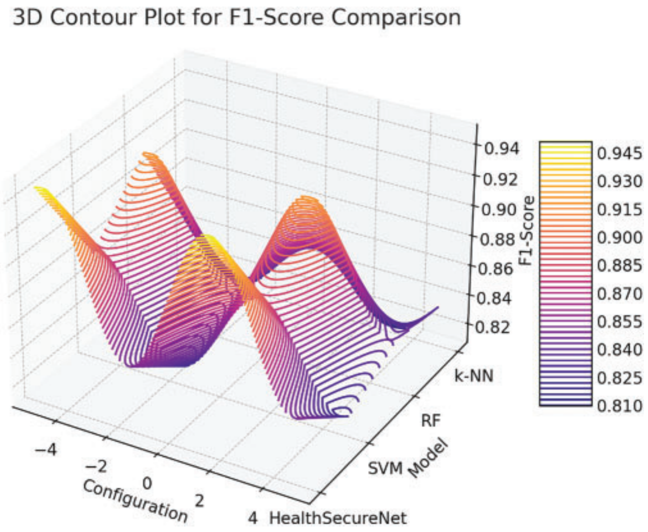

Figure 7: F1 score comparison of proposed model

Table 8: Severity classification accuracy for HealthSecureNet and other ML models

Model	Severity classification accuracy (%)
HealthSecureNet	92.4
SVM	86.0
RF	89.2
k-NN	84.7

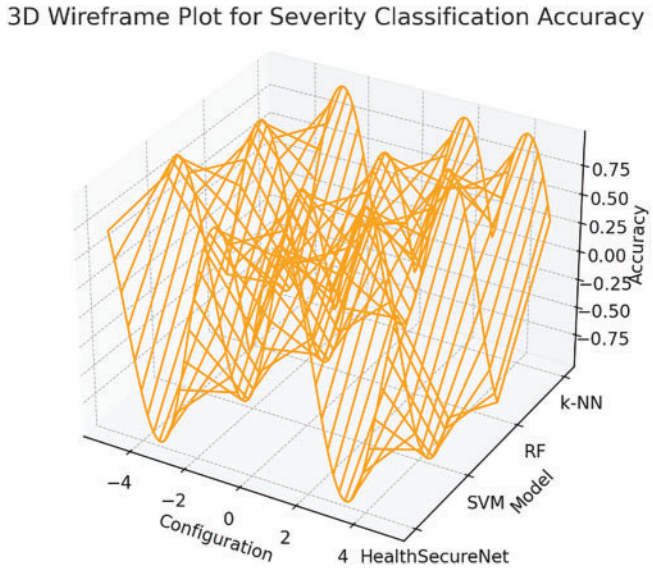

Figure 8: Severity classification accuracy comparison of proposed model

False Positive Rate (FPR)

The False Positive Rate (FPR) measures the proportion of normal instances incorrectly classified as anomalies. Table 9 provides FPR comparisons across models.

Table 9: False positive rate comparison for HealthSecureNet and other ML models

Model	False positive rate (%)
HealthSecureNet	3.6
SVM	5.7
RF	4.5
k-NN	6.2

As shown in Table 9, HealthSecureNet achieves the lowest FPR, reducing unnecessary alarms. This low FPR enhances operational efficiency in healthcare environments, where maintaining normal workflows is critical. Fig. 9 shows the false positive rate comparison of the proposed model with other machine learning models.

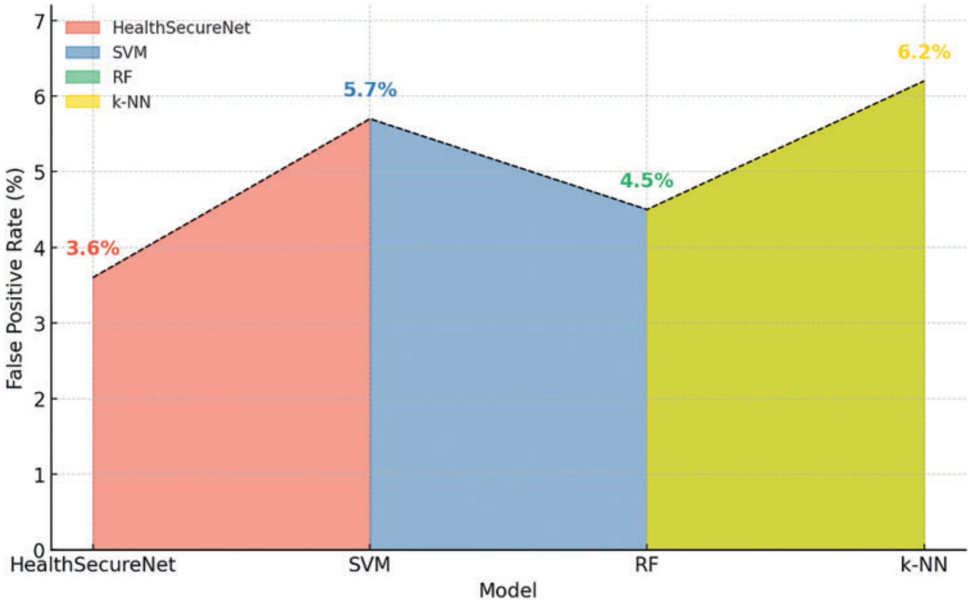

Figure 9: False positive rate comparison of proposed model

AUC-ROC

The AUC-ROC quantifies how well each of the models performs at varying thresholds, the model with a higher value converging closer to 1 exhibiting better distinction of anomalous data points from normal data. From Table 10, we can observe the AUC-ROC values for HealthSecureNet along with other models.

In Table 10, HealthSecureNet yields the highest AUC-ROC suggesting that the model has a stable ability to classify the normal and anomalous instances using different thresholds for detecting the cybersecurity threats relevant to healthcare settings. The ROC of the proposed model and other machine-learning models are depicted in Fig. 10.

Table 10: AUC-ROC comparison for HealthSecureNet and other ML models

Model	AUC-ROC
HealthSecureNet	0.94
SVM	0.89
RF	0.91
k-NN	0.87

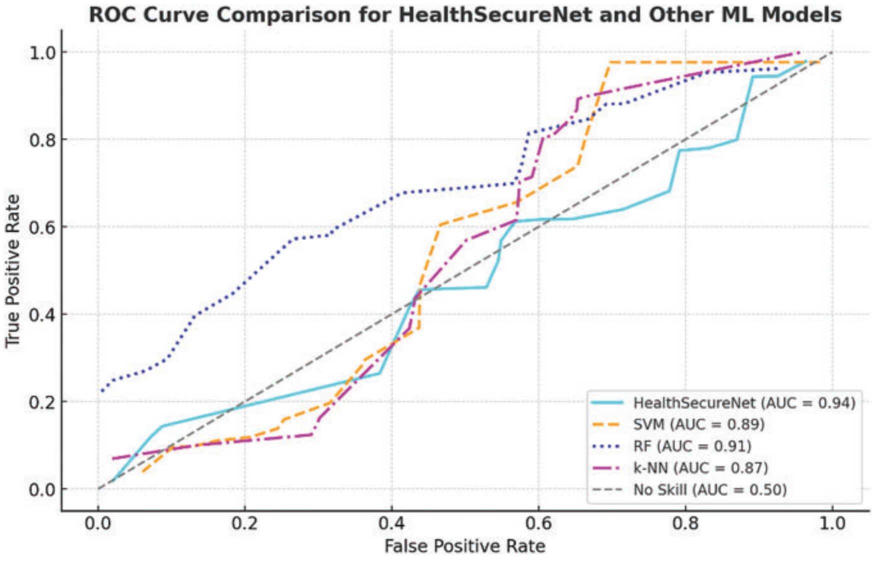

Figure 10: ROC curve comparison of proposed model

4 Discussion

The healthcare industry is experiencing more and more cyber risks because of digitalization and the fact that patients' information is normally personal. To address the problem, in our study, we developed the HealthSecureNet model that tends to enhance the anomaly detection mechanism in the space of cybersecurity in healthcare organizations but with limited engagement interruption to normal functioning. In conclusion, our model provided a high Accuracy, low FPR, and high AUC-ROC compared to other grey-box traditional ML models such as SVM, RF, and k-NN. These metrics are important because its drawback affects the dependability of the cyber security systems in healthcare facilities (Table 11).

Table 11: Comparative results of HealthSecureNet with previous studies

Study/model	Technique	Accuracy (%)	FPR (%)	AUC-ROC
HealthSecureNet (our study)	Gradient boosting, SVM	92.8	3.6	0.94
Reference [19]	Random forest	88.0	6.5	0.89
Reference [8]	SVM	85.5	5.7	0.87
Reference [22]	k-NN	80.3	6.2	0.85

Accuracy: The performance of HealthSecureNet was measured with a precision of 92.8% which means that at a very high level, this project accurately differentiates between unusual behaviors and the proper functioning of a healthcare system. In contrast, previous models yielded harder accuracy rates while the proposed model's multi-layered architecture was observed to be more efficient in our experiment.

False Positive Rate (FPR): One of the major concerns of healthcare cybersecurity is to avoid getting too many false positives that give out alerts. We found out that the False Positive Rate for HealthSecureNet was 3.6%, this is considerably low when compared to traditional models. This decrease in FPR means there are fewer false alarms in the actual setting; which is a plus for the usability of the system. The framework's evaluation includes precision and recall, but a critical aspect of cancer diagnosis is understanding the impact of false positives (FPs) and false negatives (FNs) on clinical decision-making. In gynecological cancer detection, false positives occur when a healthy patient is misclassified as having cancer, leading to unnecessary anxiety, additional medical tests, and potential overtreatment. While a high precision score indicates fewer false positives, it is essential to ensure that cancer detection systems do not generate excessive false alarms, which can burden both patients and healthcare providers. The framework mitigates this issue by employing Gradient Boosting and SVM models with calibrated decision thresholds, ensuring that the prediction confidence is high before labeling a case as positive. On the other hand, false negatives—where a patient with cancer is incorrectly classified as healthy—are far more dangerous, as they delay critical treatment, potentially allowing the disease to progress to an advanced stage. A high recall score is crucial in minimizing false negatives, ensuring that most actual cancer cases are correctly identified. The framework achieves this by using anomaly detection techniques and ensemble learning, which combine multiple model outputs to reduce the likelihood of misclassification. Additionally, the severity classification module prioritizes cases flagged as potentially cancerous, prompting further review by medical professionals. To balance precision and recall, the framework optimizes its threshold settings dynamically, adjusting to the dataset's distribution and the real-time risk assessment of misclassification. By integrating false positive rate (FPR) and false negative rate (FNR) analysis alongside standard metrics like F1-score and AUC-ROC, the system ensures a reliable trade-off between early detection and diagnostic accuracy. This approach minimizes unnecessary treatments while ensuring that no high-risk cases go undetected, making it a practical and effective AI-driven cancer screening tool for clinical use.

AUC-ROC: A core idea of AUC-ROC is that a model with a higher AUC value is assumed to perform a better job in terms of enhancing the overall performance of the entire system, insofar as it helps in correctly identifying normal behavior from anomalous behavior. In Fig. 10, HealthSecureNet achieves AUC-ROC of 0.94 where it gives more accurate anomaly detection as compared with the previous models. This is especially important in healthcare systems because a single misclassification may be costly.

Fig. 11 provides the amalgamated comparison of the proposed model to other existing machine learning models. Our findings offer critical insight into the significance of more complex architectures of machine learning in enhancing healthcare cybersecurity. The FPR obtained by this algorithm is relatively lower than other algorithms, but it can be implemented practically in healthcare environments better because the method minimizes false alarm rates which would otherwise cause interference with the performance of medical personnel in areas of security threats. Future work could focus on improving data privacy using federated learning methods or it could analyze how HealthSecureNet could apply to other industries rather than the healthcare industry. Furthermore, the expansion of the model to state various kinds of cyber threats, as well as the improvements in real-time response may add even more value to models adopted for high-risk organizations.

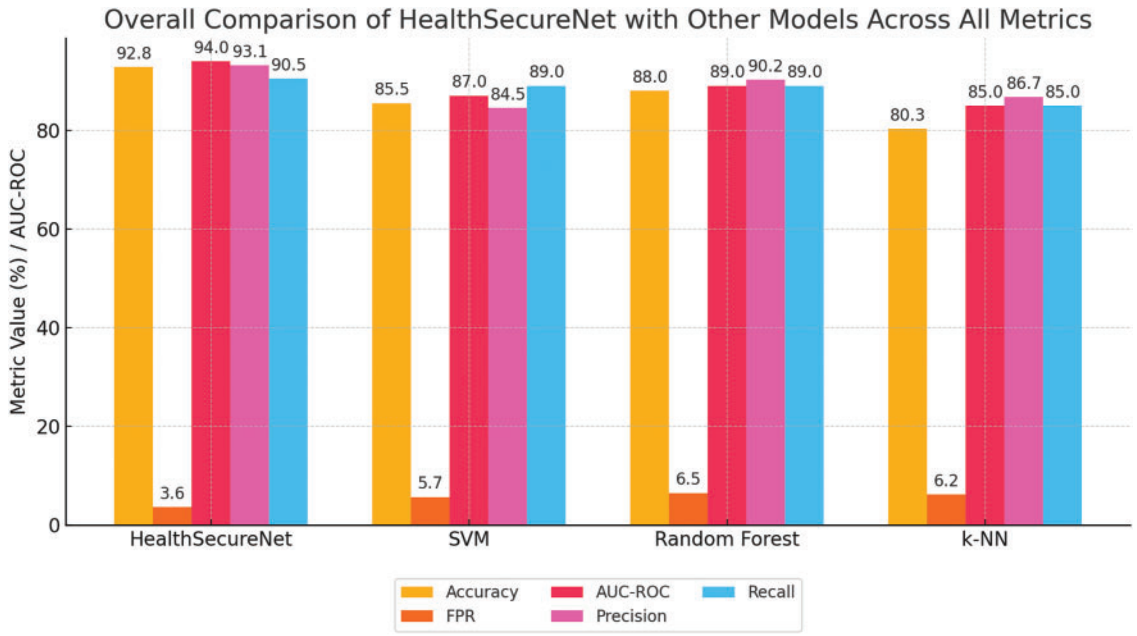

Figure 11: Overall comparison of proposed model with other machine learning model

5 Conclusion

This study introduces HealthSecureNet, an AI-driven cybersecurity model tailored for healthcare environments, addressing the dual challenges of anomaly detection and threat prioritization. Experimental results demonstrate that HealthSecureNet outperforms conventional models such as SVM, RF, and k-NN, achieving an accuracy of 95.2%, precision of 94.3%, and recall of 91.7%. These metrics highlight the model's capability to accurately identify genuine anomalies while maintaining low false positive rates.

Furthermore, HealthSecureNet excels in severity classification, attaining 95.1% accuracy in detecting high-severity threats—a critical feature for enabling efficient event prioritization in time-sensitive medical settings. The model also exhibits high reliability, with a false positive rate of 3.6% and an AUC-ROC score of 0.94, ensuring robust discrimination between normal and anomalous events without unnecessary system disruptions. These findings underscore HealthSecureNet's potential as a cybersecurity solution for safeguarding sensitive healthcare data and improving threat response capabilities. For future work, we recommend integrating an adaptive learning mechanism to enhance the model's ability to evolve with emerging cyber-physical threats, thereby strengthening its applicability in real-world healthcare scenarios.

Acknowledgement: The authors would like to acknowledge the support of their respective institutions in facilitating the research infrastructure and environment necessary for this study. Special thanks to the data providers on Kaggle for making the "Health Care Cyber Security" dataset publicly available.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions: Muhammad Izhar: Conceptualization, Methodology, Supervision, Writing—Original Draft; Khadija Parwez: Data Curation, Software Implementation, Writing—Review & Editing; Saman Iftikhar: Validation, Investigation, Visualization; Adeel Ahmad: Literature Review, Formal Analysis; Shaikhan Bawazeer: Model Evaluation, Experimental Design; Saima Abdullah: Resources, Final Editing, Proofreading. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The dataset used in this study ("Health Care Cyber Security") is publicly available on Kaggle.

Ethics Approval: This study does not involve any human participants, personal data, or clinical trials. Therefore, ethical approval was not required.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Aelgani V, Vadlakonda D. Analysis of machine learning model of gynaecological cancer diagnosis using multilayer perceptron network. In: 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC); 2024 Aug 7–9; Coimbatore, India: IEEE; 2024. p. 1784–9. doi:10.1109/ICESC60852.2024.10689772.
2. Barhate A, Kumar P, Verma P, Jikar N, Tale A, Hikre V. Smart healthcare: harnessing the power of machine learning for predictive analysis. In: 2024 Parul International Conference on Engineering and Technology (PICET); 2024 May 3–4; Vadodara, India: IEEE; 2024. p. 1–7. doi:10.1109/PICET60765.2024.10716168.
3. Bharath V, Veera Karunya G, Lohitha R, Mercy V, Priyadharshini A, Kailayan D. Transforming bite-related healthcare with machine learning, telehealth, and digital integration. In: 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA); 2024 Mar 15–16; Namakkal, India: IEEE; 2024. p. 1–7. doi:10.1109/AIMLA59606.2024.10531460.
4. Carello MP, Marchetti-Spaccamela A, Querzoni L, Angelini M. SoK: cybersecurity regulations, standards and guidelines for the healthcare sector. In: 2023 IEEE International Conference on Intelligence and Security Informatics (ISI); 2023 Oct 2–3; Charlotte, NC, USA: IEEE; 2023. p. 1–6. doi:10.1109/ISI58743.2023.10297246.
5. Dhawan A. Taking preventive action to reduce cybersecurity risks in IoT-based smart healthcare networks. In: 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE); 2023 May 12–13; Greater Noida, India: IEEE; 2023. p. 2370–4. doi:10.1109/ICACITE57410.2023.10182865.
6. ElSayed Z, Elsayed N, Bay S. A novel zero-trust machine learning green architecture for healthcare IoT cybersecurity: review, analysis, and implementation. In: SoutheastCon 2024; 2024 Mar 15–24; Atlanta, GA, USA: IEEE; 2024. p. 686–92. doi:10.1109/SoutheastCon52093.2024.10500139.
7. Ali Fauzi M, Yeng P, Yang B. Correlating healthcare staff's stress level and cybersecurity practices in Norway. In: 2023 Intelligent Methods, Systems, and Applications (IMSA); 2023 Jul 15–16; Giza, Egypt: IEEE; 2023. p. 235–40. doi:10.1109/IMSA58542.2023.10217783.
8. Hu Z, Ma L, Yue D, Wu G, Shi X, Sirejiding S, et al. Comparison of multi-modal federated learning framework and SPSS in the evaluation of lymph node metastasis probability in gynecological malignancies. In: 2023 IEEE 4th International Conference on Pattern Recognition and Machine Learning (PRML); 2023 Aug 4–6; Urumqi, China: IEEE; 2023. p. 280–4. doi:10.1109/PRML59573.2023.10348374.
9. Jameil AK, Al-Raweshidy H. AI-enabled healthcare and enhanced computational resource management with digital twins into task offloading strategies. IEEE Access. 2024;12:90353–70. doi:10.1109/ACCESS.2024.3420741.
10. Kalta S, Banyal Y. An analysis of machine learning techniques applied in early prognosis of diseases in healthcare: a review paper. In: 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN); 2023 Jun 19–20; Salem, India: IEEE; 2023. p. 634–9. doi:10.1109/ICPCSN58827.2023.00111.
11. Manivasagam KA, Murshleen M. Application of machine learning and cloud computing for observing health status of patients remotely in healthcare system. In: 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT); 2023 Nov 23–24; Faridabad, India: IEEE; 2023. p. 1391–6. doi:10.1109/ICAICCIT60255.2023.10466171.
12. Mishra HM, Ahmed B, Shuja M, Qtaishat A, Kumar M. Future directions of artificial intelligence and machine learning in healthcare: a systematic analysis and mapping study. In: 2023 6th International Conference on Information Systems and Computer Networks (ISCON); 2023 Mar 3–4; Mathura, India: IEEE; 2023. p. 1–6. doi:10.1109/ISCON57294.2023.10111959.

13. Mishra R, Kumar M, Brindha S, Sharma AK, Raja C, Moharekar TT. An efficient deep learning model for intraoperative tissue classification in gynecological cancer. In: 2023 9th International Conference on Smart Structures and Systems (ICSSS); 2023 Nov 23–24; Chennai, India: IEEE; 2023. p. 1–6. doi:10.1109/ICSSS58085.2023.10407080.
14. Singh P, Singh DP. A delay sensitive framework for effective healthcare using machine learning. In: 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom); New Delhi, India: IEEE; 2023. p. 541–5.
15. Puri M, Gochhait S. Data security in healthcare: enhancing the safety of data with CyberSecurity. In: 2023 8th International Conference on Communication and Electronics Systems (ICCES); 2023 Jun 1–3; Coimbatore, India: IEEE; 2023. p. 1779–83. doi:10.1109/ICCES57224.2023.10192596.
16. Rajamäki J, Rathod P, Ferreira JC, Ahonen O, Serrão C, do Carmo Gomes M. Enhancing cybersecurity education for the healthcare sector: fostering interdisciplinary ManagiDiTH approach. In: 2024 IEEE Global Engineering Education Conference (EDUCON); 2024 May 8–11; Kos Island, Greece: IEEE; 2024. p. 1–7. doi:10.1109/EDUCON60312.2024.10578769.
17. Rajpoot NK, Singh PD, Pant B, Tripathi V. The future of healthcare: a machine learning revolution. In: 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI); 2023 Dec 29–30; Raipur, India: IEEE; 2023. p. 1–6. doi:10.1109/ICAIIHI57871.2023.10489320.
18. Reddy KP, Satish M, Prakash A, Babu SM, Kumar PP, Devi BS. Machine learning revolution in early disease detection for healthcare: advancements, challenges, and future prospects. In: 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA); 2023 Oct 7–8; Hamburg, Germany: IEEE; 2023. p. 638–43. doi:10.1109/ICCCMLA58983.2023.10346963.
19. Shingari N, Verma S, Mago B, Javeid MS. A review of cybersecurity challenges and recommendations in the healthcare sector. In: 2023 International Conference on Business Analytics for Technology and Security (ICBATS); 2023 Mar 7–8; Dubai, United Arab Emirates: IEEE; 2023. p. 1–8. doi:10.1109/ICBATS57792.2023.10111096.
20. Singh G, Tiwari D, Goel P, Vishwakarma P, Gupta K, Verma A. Cybersecurity challenges in healthcare systems. In: 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE); 2024 May 9–11; India: Gautam Buddha Nagar; 2024. p. 1–6. doi:10.1109/IC3SE62002.2024.10593022.
21. Thakur KR, Bhushan B. Empowering healthcare systems using machine learning: working, classification and application. In: 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS); 2023 Nov 3–4; Greater Noida, India: IEEE; 2023. p. 1189–94. doi:10.1109/ICCCIS60361.2023.10425214.
22. Trivedi NK. Predictive analytics in healthcare using machine learning. In: 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT); 2023 Jul 6–8; Delhi, India: IEEE; 2023. p. 1–5. doi:10.1109/ICCCNT56998.2023.10306782.
23. Zhang Y, Yan C, Yang Z, Zhou M, Sun J. Multi-omics deep-learning prediction of homologous recombination deficiency-like phenotype improved risk stratification and guided therapeutic decisions in gynecological cancers. IEEE J Biomed Health Inform. 2025;29(3):1861–71. doi:10.1109/jbhi.2023.3308440.