International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-6, November 2025
DOI: https://doi.org/10.55524/ijircst.2025.13.6.19
Article ID IJIRE-1422, Pages 187-197
www.ijircst.org

Machine Learning–Based Anomaly Detection and Homomorphic Encryption for Securing Electronic Health Records in IoT-Enabled Hospitals

Gnanesh Methari[1] and Dr. Iqra Rasool[2]

[1]Department of Information Technology (Cybersecurity), Franklin University, Columbus, United States
[2]Department of Hematology, Chughtai Institute of Pathology, Lahore. Pakistan

Correspondence should be addressed to Gnanesh Methari; Metharignanesh770@gmail.com

Received: 2 November 2025 Revised: 18 November 2025 Accepted: 30 November 2025

ABSTRACT- Internet of Things (IoT) devices are used by hospitals to enhance patient care. Such gadgets gather health information and keep it in Electronic Health Records (EHRs). EHR is highly sensitive information that should be secured. Nonetheless, IoT systems raise security and privacy threats. The threats to hospitals are numerous as they include data breaches, insider abuse, and ransomware attacks. These new risks cannot be dealt with using the traditional security methods.
Machine learning (ML) can contribute to that by identifying abnormal or aberrant behavior within hospitals. Homomorphic encryption (HE) is one of the techniques that can be used to secure the data and perform the calculation on the encrypted data without disclosing it. The combination of ML and HE can enhance security and privacy of healthcare systems. The current review examines the available literature on ML-based anomaly detection and homomorphic encryption in securing EHRs of hospitals through IoT solutions. It outlines the existing practices, citing their shortcomings, and determining where the research remains unfinished and where it should go in the future.

KEYWORDS: Electronic Health Records (EHR), IoT Healthcare Security, Machine Learning Anomaly Detection, Homomorphic Encryption, Privacy-Preserving Analytics, Cybersecurity in Healthcare

I. INTRODUCTION

New digital technologies are changing hospitals. The use of the Internet of Things (IoT) is one of the most significant changes. IoT has medical sensors, wearables, smart monitors, and connected machines [1]. These machines gather patient information on time. This information is used by nurses and doctors to make improved decisions and offer quicker care. Due to IoT, hospitals are becoming smarter and efficient. Electronic Health Records (EHRs) are an important component of the modern health care. EHRs include information about patients, including their medical history, test results, prescriptions, and treatment plans [2]. The data assists the health workers to know the state of the patient and treat them accordingly. Nonetheless, EHR data is very sensitive. In case this information is stolen or modified, it will be detrimental to patients and hospitals. The security of EHRs is thus quite critical. Hospitals have become more vulnerable to security and privacy risks due to the use of IoT devices. The security of many IoT devices is poor [3]. They can use passwords that are not complex or use old software. These weaknesses can be used by attackers to get access to hospital systems. Insider threats are also a challenge to healthcare organizations in which authorized users utilize their access improperly. Moreover, ransomware attacks have been on the rise in the past years. Such attacks have the ability to freeze the hospital systems and require payment to unlock them. These occurrences may interfere with the functioning of the hospital and endanger the lives of patients. Healthcare systems commonly use traditional security methods. They are access control, firewalls, and standard encryption [4]. Although these are effective, there are evident limitations to these methods. There are traditional systems which are based on the established rules and familiar attack models. They have difficulties in identifying new or unfamiliar attacks. There is another weakness of standard encryption. Data should be decrypted first and then it can be analyzed. This puts into danger the processing of sensitive EHR data in cloud or third-party systems. There is a new means of enhancing healthcare security through machine learning. ML systems can learn the normal behavior using data [5]. They can then observe abnormal activities that can be singling out an attack. ML-based anomaly detection may be used in hospitals to track access logs in EHRs, network traffic, and the behavior of IoT devices. This assists in the early detection of threats even in the case when the attack is new or unfamiliar.
Meanwhile, the issue of data privacy protection is a significant challenge. One of the possible solutions to this problem is homomorphic encryption. It enables the data to remain coded in the processing [6]. This implies that one can make calculations without revealing original data. In the case of healthcare systems, this comes in handy. It enables hospitals to examine the EHR data and keep patient information confidential. Machine learning and homomorphic encryption can be used to protect EHR systems with high levels of security. Machine learning is used to identify security threats. Homomorphic encryption is used to secure the privacy of the data [7]. The two will

provide a holistic approach to safe and confidential healthcare environments. Nonetheless, this integration is also challenging. These involve the high cost of computation and delays, particularly in a low resource IoT environment.

The primary aim of the review paper is to research and summarize studies on machine learning-powered anomaly detection and homomorphic encryption of EHR security in IoT-enabled hospitals. The paper compiles the current methods, states their strengths and weaknesses, and outlines the unanswered research gaps. It also provides the direction of future research in this field. The remaining part of this paper is structured as follows. The following section explains the IoT hospital systems and EHR security fundamentals. Subsequent sections are a review of machine learning and homomorphic encryption techniques. The paper subsequently addresses the integrated approaches, open challenges, and research directions in the future, with a conclusion.

II. BACKGROUND AND PRELIMINARIES

Hospitals today utilize a lot of digital technologies. One of the most significant technologies is the Internet of Things or IoT. IoT stands for connected devices that can collect and transmit data via the internet. In hospitals, IOT devices can assist doctors and nurses to monitor and manage healthcare services.

A. IoT Enabled Hospital Architecture

Many devices are connected in a hospital when they have an IoT system. These devices are installed in patient rooms, wards, and operation areas [8]. Common devices are wearable sensors, heart monitors, blood pressure devices, infusion pumps and smart beds. These devices collect health data from patients. Most of the data used by IoT devices is numerical. This includes things like heart rate, body temperature, blood pressure, oxygen level and glucose level. These numbers are gathered on a continuous or periodic basis. This enables hospitals to monitor the patients in real time. After the collection of data, the information is transferred to a nearby system. This system is often referred to as a gateway or edge device. The gateway receives data from several IoT devices and transmits them to the hospital servers or cloud platforms [9]. Cloud systems are used because they can store massive data and complex processing.

Electronic Health Record (EHR) systems are linked to this architecture. EHR systems include the data of the patients in a digital form [2]. This includes numerical sensor data, medical history, lab results, and doctor notes. Doctors and nurses use learning EHR systems to view patient information and update treatment plans. This connected architecture enhances healthcare services. However, it also adds up to the security risks. Each connected device becomes a potential point of attack for attackers.

B. EHR Data Workflow and Lifecycle

EHR data have a defined path within hospital systems. The first step is data input. IoT devices are used to gather patient data. Most of this data is numerical and time related [10]. For example, a heart monitor may record the heart rate every second. The following step is transmitting data. The numbers are transmitted via hospital networks. It may pass through gateways before it arrives at central servers. During this step, data may be vulnerable to attacks if it is not protected appropriately. After it is transmitted, data is stored. EHR data is stored in hospital databases or cloud storage. This stored data may contain long records of numeric levels, such as blood pressure levels daily or oxygen levels through time [11]. This data is very valuable and should be protected from any unauthorized access. The stored data is then used to do data analysis. Doctors use the numbers to comprehend patient conditions. Machine learning systems may also use the analysis of numeric patterns to identify abnormal behavior. For example, sudden changes in heart rate values might be an indicator of medical problems or system issues.

Lastly, the data is used to support decision-making. Doctors use the results of data analysis to make treatment decisions. The data can also be shared with labs, specialists, or insurance providers. At each stage of this workflow, there are security and privacy risks.

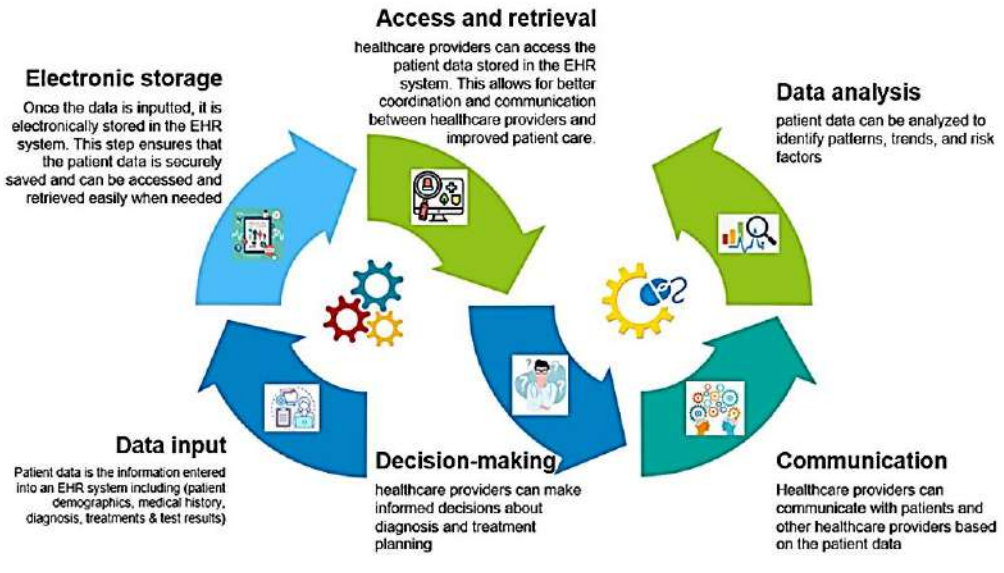

Figure 1: Flow of patient data through EHR

A generic workflow of EHR data collection, storage, analysis and decision-making in a hospital environment is illustrated in Figure 1. This figure describes a cycle of numeric health data going from input devices to storage and analysis systems. It also emphasizes important points where data has to be safeguarded to prevent any misuse or leakage.

C. Threat Model in IoT Enabled Hospitals

IoT-enabled hospitals are faced with numerous security threats. These threats may be external or internal to the hospital.

External attacks are very common. Attackers can use malware, phishing emails, or ransomware. Ransomware attacks are particularly dangerous [12]. They can lock hospital systems down and prevent access to EHR data. This can delay treatment and endanger patient lives in the process. IoT devices are frequently attacked in external attacks. Many devices are not very secure. They may have simple passwords or outdated software. Attackers may use these vulnerabilities to gain access to hospital networks. Insider threats are another serious problem. Insiders are people that already work in the hospital [13]. They can have a say in EHR systems. Some insiders abuse this access deliberately. Others do so by mistake. For example, an employee may access patient information without consent or share login credentials. Unauthorized access occurs when unauthorized attackers or insiders have been granted access without permission. And weak authentication and poor access control increase this risk. Once attackers gain access, they can steal, change or delete number-based health data. These threats illustrate that hospitals require systems which can identify unusual behavior, not merely known attacks.

D. Regulatory and Privacy Issues

Healthcare data is covered by strict laws. These laws are meant to keep patient privacy and ensure safe data handling.

The primary healthcare privacy law in the United States is HIPAA. HIPAA has created a need for hospitals to safeguard patient data and restrict access to authorized users. It also requires the reporting of data breaches [14]. In Europe, there is GDPR for healthcare data. GDPR gives patients great rights over their personal data. It requires the protection of data by organizations, particularly numeric personal data gathered by digital systems [15]. Organizations can incur large fines if they fail to comply. These regulations apply to all phases of the EHR life cycle. Hospitals are responsible for safeguarding data collection, storage, processing and data sharing. This is hard to do in IoT environments where data is constantly moving [16]. Traditional security methods are, in many cases, not sufficient. Hospitals need smarter security systems that can detect threats and protect data at the same time.

This section explains the basic structure of IoT-enabled hospitals, the flow of EHR data, common threats to EHR security and legal requirements. This background is useful in understanding why advanced solutions are required to protect EHR data in modern healthcare systems, including machine learning-based anomaly detection and homomorphic encryption.

III. MACHINE LEARNING–BASED ANOMALY DETECTION

Machine learning is an important tool to enhance security for IoT-enabled hospitals. Hospitals are using a lot of connected devices and digital systems on an everyday basis. These systems generate a huge amount of numerical data [17]. This data consists of patient readings, system logs and network records. Because of the size and speed of this data, manual monitoring is not possible. Machine learning helps hospitals to study this data automatically and find out if there is an abnormal behavior. Anomaly Detection is one of the major tasks in Machine Learning. It is the focus on the identification of behavior that is not consistent with normal behavior patterns [18]. In healthcare systems, anomalies could mean cyber-attacks, system faults, or the misuse of electronic health records. Early detection of such behavior is very important as delays can cause harm to the patient and interrupt the services of the hospital.

A. Anomaly Detection in Healthcare-Bottom Up

Anomaly can be defined as any action or data value that appears to be unusual as compared to normal behavior. In healthcare systems, anomalies can be from medical devices, users or network activity [19]. These anomalies are classified into three major types. Point anomalies are single values of data that are very different from normal values. For example, if a sensor suddenly sends in an extremely high or low number reading, this could be a point anomaly. This may occur due to a device fault or security issue.

Contextual anomalies depend on the situation or time. A value in one situation may appear normal but abnormal in another [20]. For example, regular access to patient records during office hours may be normal but such access late at night may be suspicious. Machine learning models take time and context into account to find this type of anomaly.

Collective anomalies are related to a group of data values. Individual values themselves can be normal. However, when they are viewed together, they exhibit abnormal behavior [21]. For example, changes in network traffic may be a slow cyber-attack if the change is small over a period. Detecting collective anomalies is important to long-term security.

All three types of anomalies are common in IoT-enabled hospitals. Effective security systems must be able to detect each of the types.

B. Machine Learning Workflow for Anomaly Detection

Figure 2 presents a general machine learning-based anomaly detection workflow for healthcare data. It begins with the collection of data and ends with anomaly analysis and alerts. This figure illustrates how the flow of numeric data moves through various steps and how decisions are made.

In the first step, data is collected from various sources. This includes things like the number of sensors from IoT devices, access logs from EHR systems, and network traffic data. These values can be timestamp values, access count values, device status numbers, and packet sizes. In the following step, the data is cleaned and prepared. Missing values are corrected and noisy data is removed.

Numeric values are frequently normalized such that all data is in a similar range. This helps machine learning models work with greater accuracy.
Preparing Data After the data is prepared, it is sent to machine learning models. These models learn what normal behavior is in a hospital. When new data arrives, the model compares it with learned patterns. If the data is consistent with normal behavior, the data is accepted. If it does not match, it is marked as an anomaly.

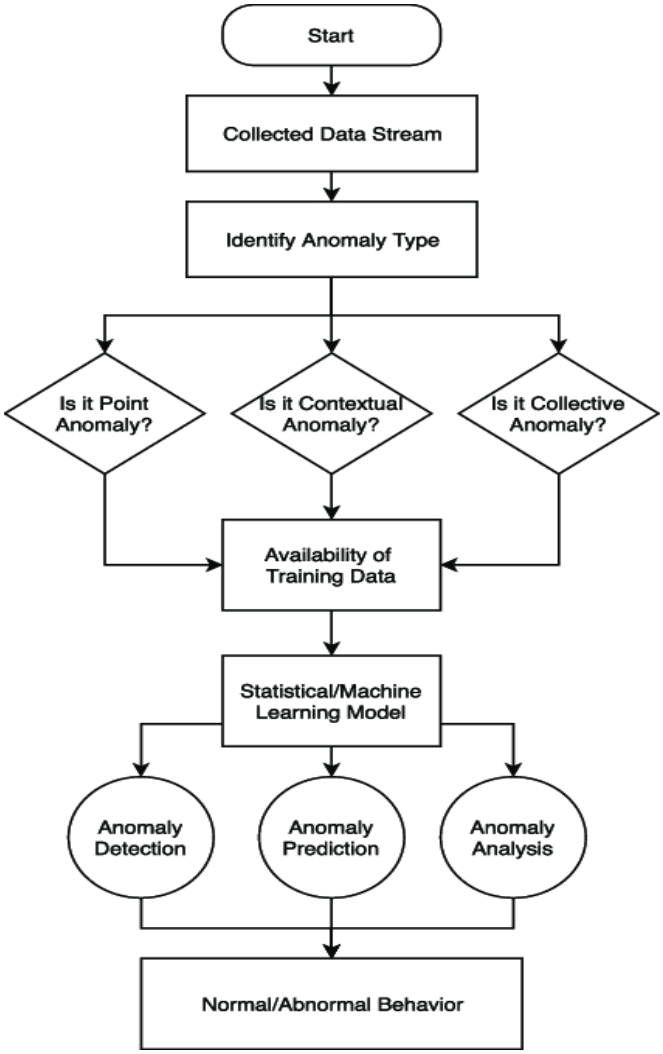

Figure 1: Machine Learning-Based Anomaly Detection Workflow for Healthcare Data

Different decision paths are also shown in Figure 2. Point Anomalies, Contextual Anomalies, and Collective Anomalies Point anomalies, anomalies that are contextual, and anomalies that are collective, follow different analyzing routes. Statistical rules or machine learning models are employed at each stage. Finally, alerts are generated so security teams or hospital employees can quickly respond to them.

C. Supervised Machine Learning Techniques

Supervised machine learning involves the use of data that has been labeled. This means each data record is identified as normal or abnormal. The model then learns from these examples and attempts to predict labels for new data [22]. Common supervised models are deciding on trees, supporting vector machines, and random forests. These models are good at detecting known attacks. If a similar attack has occurred previously, this model can identify it again.
In the case of healthcare systems, supervised learning can identify repeated access to unauthorized systems or known malware behavior. However, this technique has its limitations. Labeled healthcare security data is difficult to collect. Hospitals are not always clear on how they record attacks. Preparing labeled data is also time-consuming and labor-intensive. Due to all these issues, supervised learning alone is insufficient for IoT-enabled hospitals' protection.

D. Unsupervised Machine Learning Techniques

Unsupervised machine learning does not require the use of labeled data. The model analyzes the data and discovers patterns by itself. Anything that does not fit into these patterns is considered an anomaly [23]. Common unsupervised techniques are clustering techniques and isolation-based models. These methods group together similar values of numbers. Data that falls outside these groups is abnormal. Unsupervised learning is useful in healthcare as it can detect new and unknown attacks. It works quite well if attack data is not available. For example, if a medical device starts behaving differently, suddenly, the model will be able to pick up on this change without any previous examples. However, unsupervised models could produce false alarms. Some strange but innocuous behavior may be flagged out as a threat. This can be a heavier workload for those working within the hospital.

E. Semi-Supervised Machine Learning Algorithms

Semi-supervised learning is a combination of both supervised and unsupervised learning methods. The model is trained primarily using normal data. It learns what normal behavior is, and flags something different [24]. This approach is very common in healthcare systems. Normal hospital data is easily collected. Attack data is rare. This is the advantage taken by semi-supervised learning. For example, the model can learn normal access patterns to EHR. If a user suddenly accesses a lot of records in a short period of time, the system notices this as suspicious.
The primary limitation is that the behavior of the hospital can change over the course of time. Models may need to be updated regularly to ensure that they remain accurate.

F. Deep Learning for Anomaly Detection

Deep learning is a more advanced form of machine learning. It uses many layers to learn complex patterns in data. Deep learning models are useful when the data is large and detailed. In IoT enabled hospitals, using deep learning, it is possible to analyze time-based data from sensors [25]. It can spot small changes to the patterns that simple models may miss. This is useful for early detection of attacks. However, deep learning requires more computing power and more memory. Many IoT devices are resource constrained. This makes it difficult to deploy in a real-time environment.

G. Data Sources Used in Healthcare Anomaly Detection

There are many data sources in hospitals that are used by machine learning models. IoT devices give the numbers of the sensors like heart rate, temperature and oxygen level

[26]. EHR systems include logs that indicate who accessed the patient data and when. Network systems are used to get information about traffic such as packet size and connection frequency.
Multiple-data sources to improve the detection accuracy It is also useful to uncover external attacks and insider threats.

H. Evaluation Capability: Performance Metrics

Performance metrics are used to measure the effectiveness of anomaly detection models. Accuracy indicates the accuracy of the predictions. Precision describes the number of detected anomalies that are actual threats [27]. Recall shows the number of actual attacks that are successfully detected. F1-score - The F1-score is a balance between precision and recall.
In healthcare systems, a high recall is very important. Missing an attack can result in serious harm. At the same time, too many false alarms can disrupt the operations of the hospital.

I. Practical Issues: Key Challenges

There are several challenges associated with the use of machine learning-based anomaly detection. One major problem is unbalanced data. Normal data is much more prevalent than attack data. This can impact the accuracy of the model.
Another challenge is explainable. Some models fail to provide a clear picture as to why an alert was generated. Healthcare staff may not believe what they don't understand [28]. Realtime processing is not easy either. IoT systems generate data at very fast pace. Models need to be quick responding to be useful. These challenges indicate that machine learning solutions need to be carefully designed for health care environments.

IV. HOMOMORPHIC ENCRYPTION FOR EHR SECURITY

A lot of patient data is collected by hospitals. This data is saved in Electronic Health Records (EHRs). EHR data is very sensitive. It contains medical history, lab results, prescriptions, and personal information [29]. The protection of this data is very important. Traditional encryption ensures data security while stored and transmitted. However, normal encryption needs data to be decrypted for the processing. Decrypted data is subject to attack. The problem is solved by Homomorphic Encryption (HE). HE can compute data while it remains encrypted. This ensures that patient data is kept private even when doing processing.

A. Introduction to Homomorphic Encryption

Homomorphic encryption is of three primary categories that include homomorphic encryption, partial homomorphic encryption, somewhat homomorphic encryption, and fully homomorphic encryption. Partial Homomorphic Encryption (PHE) only allows one type of operation on encrypted data [30]. For example, it may allow addition or multiplication, but not both. This is easier and faster but not as flexible. Somewhat Homomorphic Encryption (SHE) enables a limited number of operations of addition and multiplication. [31] It can do more complex calculations than PHE but has its limits. Fully Homomorphic Encryption FHE is an access to encrypted data that admits an unlimited number of operations. Doctors or systems can do any computation without decryption of data. FHE is very secure, it is also computationally heavy and slower than others [32].
In the field of healthcare, these kinds of HE can ensure that EHR data is protected and perform important tasks such as analytics, statistics, and sharing between hospitals.

B. Homomorphic Encryption Schemes in Healthcare

There are several HE schemes to be used in healthcare applications.
Paillier Encryption is a partially homomorphic encryption. It is possible to do addition on encrypted data [33]. For instance, if a hospital wants to calculate the total number of patients in different wards, they can calculate the total without decrypting the individual records. BFV (Brakerski/Fan-Vercauteren) includes addition and multiplication on integers. It is frequently used in privacy-preserving analytics where numerical computations are needed on ciphertexts of EHRs [34]. CKKS (Cheon-Kim-Kim-Song) is based on approximate computations. It is useful when processing real numbers, such as average blood pressure, heart rate trends or other numeric health measurements. CKKS can work efficiently with large data sets [35].
These schemes are popular for many applications like cloud-based storage, cross-hospital collaboration and secure machine learning on encrypted data.

C. Applications for Homomorphic Encryption

Encrypted Cloud Storage: Hospitals can store the EHR data in the cloud servers in an encrypted form. The cloud can undergo some calculations without seeing the raw data [36]. For example, the hospital may request a cloud server to calculate the average lab result for all the patients in a ward. The cloud returns the result in encrypted form keeping patient data private. Privacy-Preserving Analytics: Hospitals can utilize HE to perform analytics on sensitive data without the patient records being exposed [37]. For example, a hospital can analyze trends in blood pressure, glucose levels or heart rate for thousands of patients while data are encrypted. Cross-Hospital Data Sharing: Sometimes data will be required to be shared between hospitals or other research centers. HE allows them to share encrypted data safely. The receiving hospital can make computations without having access to raw data about the patient. This allows for cooperative research without losing privacy.

D. Workflow of Homomorphic Encryption

Figure 3 shows the general process to do computations on encrypted EHR data using a homomorphic encryption friendly model.

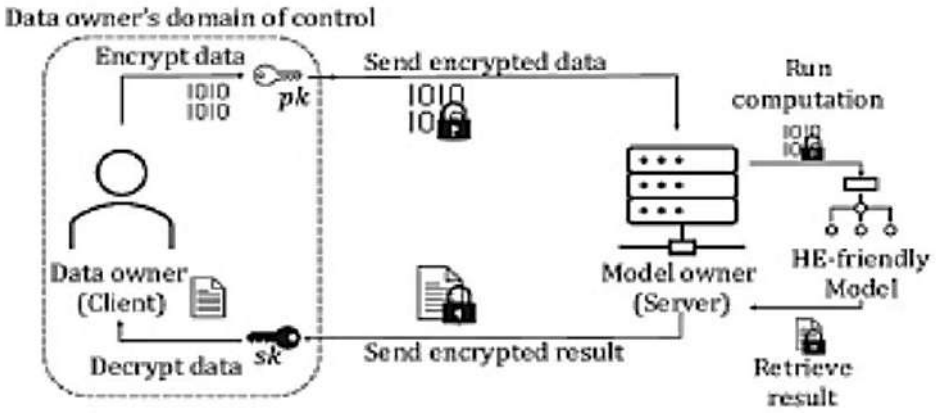

Figure 3: Data Encrypting Process in EHR

- Step 1: Data Encryption - The client which can be a hospital, or a medical system will encrypt the EHR data. Numeric values like lab results, blood pressure readings or heart rates get converted into encrypted numbers. These encrypted numbers cannot be read by anyone except the authorized users that have the key.
- Step 2: Data Transmission - The encrypted information is transmitted to a cloud server or computation platform. The server only receives encrypted data. It cannot view the actual patient information which maintains privacy.
- Step 3: Computation on Encrypted Data - The cloud or server does calculations on the encrypted values. For instance, it can be used for calculating the sum of blood glucose values, average, or simple machine learning models. Because the data is encrypted, the numbers are never visible to the server.
- Step 4: Returning Encrypted Results - After the computation is done, the results are returned in encrypted form to the hospital.
- Step 5: Decryption and Use - The hospital decrypts the results with its private key. The staff can now view the numerical results or results of analysis. At no point was the raw EHR data exposed.

This workflow demonstrates that homomorphic encryption enables processing of numeric and time series health data in a secure manner. It maintains privacy but still allows meaningful computations.

E. Performance Factors

Homomorphic encryption is quite secure, but it has its drawbacks.

HE is computationally more expensive than normal encryption. Operations on encrypted numbers are slower by hundreds or thousands of times. Since computation takes longer, results could take more time to return. This is important in such hospitals where real-time decisions may be required. Encrypted data is very large in size as compared to raw data. For example, a single blood pressure reading could be expanded from a few bytes to hundreds of bytes after encryption. Hospitals require additional storage space. These factors need to be taken into consideration when designing HE systems for IoT-enabled hospitals.

F. Practical Challenges

Hospitals have massive amounts of numeric EHR data generated daily. Applying HE to millions of records is a task that requires scalable computation solutions. Also, HE requires the use of public and private keys. Secure management of these keys is therefore essential. Losing keys can cause data to be inaccessible, while improper sharing can cause shared data to be breached. In addition, HE must integrate with existing hospital software, IoT devices, EHR systems etc. Integration can be challenging due to the heavy computational nature of HE and the lack of support for it in current systems. Despite these challenges, HE is becoming more practical with the modern computing resources and optimized algorithms.

Homomorphic encryption enables hospitals to perform calculations on encrypted EHR data and remain preserved privacy. Different HE schemes are available for supporting different types of numeric computations. HE is used for encrypted storage, privacy-preserving analytics, and the sharing across hospitals. Figure 3 illustrates how data can be encrypted, transmitted for computation, processed in encrypted form, and decrypted after computing results are returned. Numeric health data is always secure. Performance issues such as computation time, latency and storage overhead need to be dealt with. Practical challenges such as scalability, key management, and system integration also require careful planning. HE is an important technology for modern healthcare security. When in combination with machine learning, it can be used to help detect anomalies in EHR data while ensuring patient information remains private. This combination is of vital importance in IoT-enabled hospitals, which produce massive volumes of sensitive number data every day.

V. INTEGRATED ML + HE APPROACHES

There are two primary issues that hospitals have with EHRs. First, data relating to patients is sensitive data and needs to be protected. Second, IoT devices produce a lot of numerical data which may harbor security threats. Using machine learning on its own can detect abnormal behavior. Using encryption alone can protect the confidentiality of data. But each approach has limitations if one is used separately. This is why it is important to combine machine learning (ML) based anomaly detection and homomorphic encryption (HE).

A. Reasons for the Integration of ML and HE

Machine learning requires access to numeric data to detect anomalies. But EHR data is sensitive and cannot be exposed to untrusted systems [38]. Homomorphic encryption enables a computation on encrypted data. This means that ML models can analyze data without having to decrypt it. Combining ML and HE provides security and privacy. Hospitals will have the advantage of detecting attacks and protecting data of the patient simultaneously.

This integrated approach is useful for IoT-enabled hospitals. Sensors are used to create continuous streams of data. And if the data is processed directly in the cloud, it may be intercepted or misused. ML + HE ensures that anomaly detection works even when data remains encrypted.

B. Architecture: Edge vs Cloud Based Secure ML

There are two main buildings for integrating ML and HE in hospitals, which are edge-based and cloud-based. Edge based architecture is used to process data near the IoT devices. This reduces the amount of data that is sent to cloud [39]. It also allows for quicker anomalies to be detected. Encrypted data can be used to run lightweight ML models on edge devices. This is good for real time monitoring such as heart rate or oxygen level. However, edge devices have typically been limited in their computing power. Running complicated HE operations may slow them down.

Cloud based architecture transmits encrypted data to a central server or cloud. Powerful servers are used to perform ML computations on encrypted EHR data [40]. This enables more complicated models and larger data sets. Cloud computing can manage several departments of hospitals simultaneously. But putting encrypted data out to the cloud could result in network delays. Hospitals are caught between security, speed and cost.

Some hospital systems are using a hybrid approach. Simple anomaly detection occurs at edge and detailed analysis is completed in the cloud. This way, sensitive data is protected but real time monitoring continues.

C. Secure ML Inference on Encrypted EHR Data

Secure ML inference means running a machine learning model on data while it remains encrypted. Homomorphic encryption allows addition, multiplication, and other operations on encrypted values [41]. The output is also encrypted and can be decrypted only by authorized personnel.

For example, an EHR dataset may include numeric records of blood pressure, heart rate, and glucose level. A deep learning model can analyze these values while they are encrypted [42]. If the model finds unusual patterns, it flags them as anomalies. The hospital staff can then view results without ever seeing raw sensitive data in the cloud.

This process protects patient privacy and prevents attackers from learning anything from the data. It also allows hospitals to use cloud resources securely. This is especially helpful when hospitals do not have strong computing facilities on-site.

D. Case Studies and Frameworks

Several studies and frameworks indicate that ML + HE integration is feasible for hospitals: IoT Health Monitoring Frameworks. These frameworks employ edge devices to preprocess data, encrypt it using HE, and transmit it to cloud servers for anomaly detection [43]. They can identify abnormal behavior of devices or abnormal readings by patients without sharing sensitive health information. Cloud-Based Secure EHR Systems: There are some cloud platforms where hospitals can store EHRs using encryption. ML models in the cloud analyze encrypted numeric data to find the patterns of abnormal access or abnormal vital signs [44]. Only encrypted alerts are sent to hospital administrators. Real-World Applications: For example, a hospital has sensors on heart rate, and they monitor it in real time. It is the ML model that detects sudden spikes in readings by anomalies through encryption. Alerts are sent instantly to the nurses or doctors. All patient data remains encrypted across the process. These case studies demonstrate how ML + HE can ensure the privacy of patient data, secure hospital networks, and facilitate real-time monitoring.

E. Tradeoffs: Performance vs Security

Combining ML and HE enhances security and privacy. But there are trade-offs. The homomorphic encryption method adds more time in computation [45]. Complex ML models take a lot of time to process encrypted data. This can slow down real-time detection. Hospitals need to achieve a balance. Lightweight models on the edge devices can process data quickly but can potentially miss subtle anomalies. Powerful cloud models can detect more complex anomalies but can create network delays. Another challenge is energy consumption. IoT devices and edge servers may have a short battery life. Performing encryption and ML computations can cause more energy consumption [46]. Hospitals need to take this into account when developing the system. Despite all these trade-offs, the combination that is ML + HE offers stronger security and privacy than using either approach alone. It ensures that hospitals can track patients, identify threats and keep sensitive numeric EHR data in a secure and private manner.

Integrated ML + HE approaches help hospitals to solve two main problems at once: detecting anomalies and protecting sensitive data. Edge based and cloud-based architectures give flexibility in deployment. Secure ML inference on encrypted data enables privacy-preserving analysis. Case studies demonstrate real world feasibility. Hospitals need to control performance, network, and energy trade-offs. Overall, ML + HE integration is an interesting solution for IoT-enabled hospitals dealing with a massive amount of numeric EHR data.

VI. COMPARATIVE ANALYSIS AND SYNTHESIS

Many studies have examined the use of machine learning (ML) and homomorphic encryption (HE) for healthcare security. Each study is on different aspects. Some are focused on security, some on ML techniques, HE types, others on the performance of the system. Comparing these studies helps to understand what works well and where there are problems.

A. Comparison of Anomaly Detection Studies based on ML

ML anomaly detection studies vary as to the nature of the model used. Supervised models, such as decision trees or support vector machines, are good at picking out known attacks. Unsupervised models, such as k-means or autoencoders better detect unknown threats. Semi-supervised models involve mostly normal data and are useful in case of limited labeled attack data. Deep learning models can process large and complex data and require more computing power [47]. Performance measures differ from study to study. Accuracy, precision, recall and F1-score are frequently reported. Some studies focus on a high recall to reduce the risk of missing attacks. Others try to minimize false alarms for the sake of not disturbing hospital operations. Healthcare applicability is also important. Studies with real hospital data or realistic simulation of IoT devices are shown to yield better results in practice. Studies with synthetic data may not reflect real-world challenges.

B. Comparison of studies of Homomorphic Encryption

HE studies are about protecting sensitive EHR data but still being able to perform computations. Some studies use partial HE that can be used only for certain operations. Others use fully homomorphic encryption (FHE), which can perform all types of computations on encrypted data. FHE offers better privacy at the higher cost of increased computing power. Partial HE is quicker but less flexible. Performance is typically measured in computation time, memory use and scalability. Studies have often produced numerical results indicating processing delays. For example, FHE takes for example several seconds to process a patient record, whereas partial HE takes milliseconds. These numbers are important to hospitals that require real-time responses.

The applicability to healthcare depends on whether HE can manage large-scale EHR data and IoT data streams [48]. Some studies are being conducted where HE is combined with cloud computing to manage storage and computation. Others attempt to use edge-computing solutions to minimize delays. Charts can be used to summarize HE types and computation time and scalability for quick comparison.

C. Integration of ML and HE

Few studies combine ML-based anomaly detection and HE. The target is to identify abnormalities without revealing sensitive data. This integration is not without its challenges. One issue is the computation cost. ML models require numbers to train and analyze [49]. HE keeps data encrypted. Processing encrypted data is slower. Hospitals might require more high-powered servers or cloud solutions.

Another challenge is real-time processing. IoT devices are sources of data that produce data 24/7. Delays caused by HE could impact the usefulness of anomaly detection [50]. Some studies propose to employ hybrid methods, where important information is cryptographically processed in real time and less important information is encrypted for later batch processing. A third challenge is interpretability. ML models are already complicated. HE makes it harder for healthcare staff to understand decisions. This can make people less trustworthy of the system.

D. Patterns, Gaps, and Insights

From the reviewed literature, some clear patterns emerge. First, machine learning (ML) models are effective in the detection of anomalies in hospital systems. However, their performance varies with the type of data and amount of data that is available. Second, homomorphic encryption (HE) is used to protect the patient's data and ensure privacy. The bad side is that it complicates the computation time and consumes more resources. Third, the combination of ML and HE is promising. It can be used for security as well as anomaly detection. But for implementing this combination in real-time systems, it is still difficult.

There are also several gaps that emerge from literature. Few studies are based on real hospital data, which comprise both data from IoT devices and from electronic health records [51]. There is little research on how to optimize ML models to work on encrypted data. Also, anomaly detection and HE for IoT devices with limited resources have not been fully explored.

Insights from these studies suggest that hybrid frameworks may be the best way to go. For example, certain research work utilizes partial HE to decrease computation time and uses deep learning to correctly detect anomalies. These studies demonstrate the potential for security and privacy preserving healthcare systems. At the same time, they point out some practical issues of using these systems in real hospitals. This section demonstrates the comparison of ML anomaly detection, and HE studies, the gaps among them and how the combination of both techniques can enhance healthcare security.

VII. OPEN CHALLENGES AND FUTURE DIRECTIONS

Although the use of machine learning and homomorphic encryption can enhance security in IoT-enabled hospitals, there are still several challenges that remain. These challenges must be solved for practical and efficient implementation.

One of the challenges is lightweight homomorphic encryption for IoT devices. Many IoT devices have limited computing power and battery life [35]. Current homomorphic encryption techniques are computationally expensive. Researchers need to develop lighter methods of encryption that will work on small devices without slowing them down.

Another challenge is healthcare security-explainable AI. Many machine learning models are like a "black box." They spot anomalies but it is difficult to see why a decision has been made [52]. Healthcare staff need these systems to be explained to them in a way that they trust. It is important to develop models that are accurate as well as interpretable.

The use of real-time anomaly detection on encrypted data is also a major challenge. Homomorphic encryption is a method of protecting data while it is being processed. However, processing encrypted data takes longer than normal data. This delay can make real-time detection difficult. Solutions are required to process encrypted data at fast rates to allow the attack to be immediately stopped.

Federated learning and HE integration is another promising direction. Federated learning enables the training of models across multiple hospitals, without

exchanging patient data [53] [54]. Combining federated learning with homomorphic encryption can achieve impressive privacy without worsening model performance. This approach is still new and needs more research to be applied to healthcare use. Finally, standardized datasets and compliance with regulations are important for future research. Many of the studies are done with different data sets making it difficult to compare the results. Standard datasets would be useful for researchers who want to test and compare methods. At the same time, all solutions must not contravene laws such as HIPAA and GDPR. Future systems should be designed for regulatory standards from the beginning.

Addressing these challenges will help IoT-enabled hospitals be safer. It will also provide incentive for the adoption of advanced security systems. Researchers should also focus on combining efficient encryption, accurate and explainable anomaly detection, and compliance with healthcare laws.

VIII. CONCLUSION

IoT-enabled hospitals produce a lot of sensitive health data from connected devices. Electronic Health Records (EHRs) hold and facilitate these important decisions for healthcare professionals. However, these systems are at risk of serious security and privacy threats, such as cyberattacks, insider threats, and unauthorized access. Traditional security methods are not sufficient to protect modern healthcare systems. Machine learning based anomaly detection can detect unusual behavior in hospital networks and data systems. It can identify point, contextual, and collective anomalies with supervised, unsupervised or deep learning techniques. This helps hospitals to detect new or unknown threats in a short period of time. Homomorphic encryption makes it possible to have the data encrypted even during the processing phase. It preserves patient privacy and facilitates analysis and decision-making. Combining these two technologies forms a robust framework for secure and private healthcare systems based on the Internet of Things.

This review presented a summary of the recent research in integrating machine learning anomaly detection and homomorphic encryption in hospitals. It addressed the advantages, data sources, workflow, performance metrics, and challenges of current approaches. Key challenges include computational complexity, unbalanced data, real-time processing, and interpretability of machine learning models. Regulatory compliance and standardized data sets are also important for future systems. Future research should focus on lightweight encryption that can be used for IoT devices, real-time anomaly detection on encrypted data, and explainable AI for healthcare staff. Federated learning in combination with homomorphic encryption can further enhance privacy and performance across multiple hospitals. Standard datasets and compliance with HIPAA and GDPR regulations is important for practical implementation as well.

In conclusion, integrating machine learning anomaly detection with homomorphic encryption is a potential solution to protect IoT-enabled hospital systems. It enhances security, maintains privacy of patients, and aids in timely healthcare decisions. Continued research and development in this area will enable healthcare systems to be safer and reliable and help hospitals adopt advanced technologies without sacrificing patient trust or data security.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Andriulo, F. C., M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge computing and cloud computing for internet of things: A review," *Informatics*, vol. 11, no. 4, 2024. Available from: https://doi.org/10.3390/informatics11040071

[2] W. Wang, D. Ferrari, G. Haddon-Hill, and V. Curcin, "Electronic health records as source of research data," *PubMed*, 2023. Available from: https://www.ncbi.nlm.nih.gov/books/NBK597466/

[3] Liu, D. Huang, J. Yao, J. Dong, L. Song, H. Wang, C. Yao, and W. Chu, "From black box to glass box: A practical review of explainable artificial intelligence (XAI)," *AI*, vol. 6, no. 11, pp. 285–285, 2025. Available from: https://doi.org/10.3390/ai6110285

[4] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Computers in Biology and Medicine*, vol. 158, p. 106848, 2023. Available from: https://doi.org/10.1016/j.compbiomed.2023.106848

[5] A. Ali, M. A. Gunavathie, V. Srinivasan, M. Aruna, R. Chennappan, and M. Matheena, "Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare," *Clinical eHealth*, vol. 8, 2025. Available from: https://doi.org/10.1016/j.ceh.2025.04.002

[6] Hildt, "What is the role of explainability in medical artificial intelligence? A case-based approach," *Bioengineering*, vol. 12, no. 4, pp. 375–375, 2025. Available from: https://doi.org/10.3390/bioengineering12040375

[7] Al Badawi and M. Faizal Bin Yusof, "Private pathological assessment via machine learning and homomorphic encryption," *BioData Mining*, vol. 17, no. 1, 2024. Available from: https://doi.org/10.1186/s13040-024-00379-9

[8] Zhai, O. N. Akande, S. Agarwal, and W. Pak, "Security risk assessment of internet of things health devices using DREAD and STRIDE models," *Ain Shams Engineering Journal*, vol. 16, no. 11, p. 103721, 2025. Available from: https://doi.org/10.1016/j.asej.2025.103721

[9] T. Guimarães, R. Duarte, F. Hak, and M. Santos, "Context-aware electronic health record—Internet of things and blockchain approach," *Informatics*, vol. 11, no. 4, pp. 98–98, 2024. Available from: https://doi.org/10.3390/informatics11040098

[10] S. Abdulmalek, A. Nasir, W. A. Jabbar, M. A. M. Almuhaya, A. K. Bairagi, M. A.-M. Khan, and S.-H. Kee, "IoT-based healthcare-monitoring system towards improving quality of life: A review," *Healthcare*, vol. 10, no. 10, p. 1993, 2022. Available from: https://doi.org/10.3390/healthcare10101993

[11] Samariya, J. Ma, S. Aryal, and X. Zhao, "Detection and explanation of anomalies in healthcare data," *National Library of Medicine*, vol. 11, no. 1, 2023. Available from: https://doi.org/10.1007/s13755-023-00221-2

[12] S. Mittal, "Fully homomorphic encryption-based optimal key encryption for privacy preservation in the cloud sector," *Journal of Information Security and Applications*, vol. 91, p. 104048, 2025. Available from: https://doi.org/10.1016/j.jisa.2025.104048

[13] Riou, M. El Azzouzi, A. Hespel, E. Guillou, G. Coatrieux, and M. Cuggia, "Ensuring GDPR compliance and security in a clinical data warehouse: Challenges and insights from a university hospital," *JMIR Medical Informatics*, 2024. Available from: https://doi.org/10.2196/63754

[14] P. Schummer, A. del Rio, J. Serrano, D. Jimenez, G. Sánchez, and Á. Llorente, "Machine learning-based network anomaly detection: Design, implementation, and evaluation," *AI*, vol. 5, no. 4, pp. 2967–2983, 2024. Available from: https://doi.org/10.3390/ai5040143

[15] S. Rani, R. Kumar, B. S. Panda, R. Kumar, N. F. Muften, M. A. Abass, and J. Lozanović, "Machine learning-powered smart healthcare systems in the era of big data," *Diagnostics*, vol. 15, no. 15, pp. 1914–1914, 2025. Available from: https://doi.org/10.3390/diagnostics15151914

[16] Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing," *International Journal of Intelligent Networks*, vol. 3, pp. 16–30, 2022. Available from: https://doi.org/10.1016/j.ijin.2022.04.001

[17] M. Humbert-Droz, P. Mukherjee, and O. Gevaert, "Strategies to address the lack of labeled data for supervised machine learning training with electronic health records," *JMIR Medical Informatics*, vol. 10, no. 3, p. e32903, 2022. Available from: https://doi.org/10.2196/32903

[18] S. M. Varnosfaderani and M. Forouzanfar, "The role of AI in hospitals and clinics: Transforming healthcare in the 21st century," *Bioengineering*, vol. 11, no. 4, pp. 1–38, 2024. Available from: https://www.mdpi.com/2306-5354/11/4/337

[19] F. Agyemang, "Anomaly detection using unsupervised machine learning algorithms: A simulation study," *Scientific African*, vol. 26, p. e02386, 2024. Available from: https://doi.org/10.1016/j.sciaf.2024.e02386

[20] Lee, "Analysis of insider threats in the healthcare industry: A text mining approach," *Information*, vol. 13, no. 9, p. 404, 2022. Available from: https://doi.org/10.3390/info13090404

[21] H. Almotairi, "Application of internet of things in healthcare domain," *Journal of Umm Al-Qura University for Engineering and Architecture*, 2022. Available from: https://doi.org/10.1007/s43995-022-00008-8

[22] Yasuda, T. Shimoyama, and J. Kogure, "Secret computation of purchase history data using somewhat homomorphic encryption," *Pacific Journal of Mathematics for Industry*, vol. 6, no. 1, 2014. Available from: https://doi.org/10.1186/s40736-014-0005-x

[23] Parihar, J. B. Prajapati, B. G. Prajapati, B. Trambadiya, A. Thakkar, and P. Engineer, "Role of IoT in healthcare: Applications, security and privacy concerns," *Intelligent Pharmacy*, vol. 2, no. 5, 2024. Available from: https://doi.org/10.1016/j.ipha.2024.01.003

[24] Habehh and S. Gohel, "Machine learning in healthcare," *Current Genomics*, vol. 22, no. 4, pp. 291–300, 2021. Available from: https://doi.org/10.2174/1389202922666210705124359

[25] T. Madathil, F. K. Dankar, M. Gergely, A. N. Belkacem, and S. Alrabaee, "Revolutionizing healthcare data analytics with federated learning," *Computational and Structural Biotechnology Journal*, vol. 28, pp. 217–238, 2025. Available from: https://doi.org/10.1016/j.csbj.2025.06.009

[26] R. Foorthuis, "On the nature and types of anomalies: A review of deviations in data," *International Journal of Data Science and Analytics*, vol. 12, no. 4, pp. 297–331, 2021. Available from: https://doi.org/10.1007/s41060-021-00265-1

[27] C. Muhoza, E. Bergeret, C. Brdys, and F. Gary, "Power consumption reduction for IoT devices thanks to edge-AI," *Internet of Things*, vol. 24, p. 100930, 2023. Available from: https://doi.org/10.1016/j.iot.2023.100930

[28] T. K. Nguyen, D. H. Duong, W. Susilo, Y.-W. Chow, and T. A. Ta, "HeFUN: Homomorphic encryption for unconstrained secure neural network inference," *Future Internet*, vol. 15, no. 12, p. 407, 2023. Available from: https://doi.org/10.3390/fi15120407

[29] Grünewald et al., "Beyond the numbers: The importance of contextual data when reusing blood pressure data from electronic health records," *Frontiers in Digital Health*, vol. 7, 2025. Available from: https://doi.org/10.3389/fdgth.2025.1664213

[30] R. Almutairi, G. Bergami, and G. Morgan, "Advancements and challenges in IoT simulators: A comprehensive review," *Sensors*, vol. 24, no. 5, pp. 1511–1511, 2024. Available from: https://doi.org/10.3390/s24051511

[31] Bolhasani, M. Mohseni, and A. M. Rahmani, "Deep learning applications for IoT in healthcare: A systematic review," *Informatics in Medicine Unlocked*, vol. 23, p. 100550, 2021. Available from: https://doi.org/10.1016/j.imu.2021.100550

[32] Edemekong, M. Haydel, and P. Annamaraju, "Health insurance portability and accountability act (HIPAA)," *National Library of Medicine*, 2024. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/

[33] Shojaei, E. V. Gjorgievska, and Y.-W. Chow, "Security and privacy of technologies in health information systems: A systematic literature review," *Computers*, vol. 13, no. 2, pp. 1–25, 2024. Available from: https://www.mdpi.com/2073-431X/13/2/41

[34] V. Terziyan, B. Bilokon, and M. Gavriushenko, "Deep homeomorphic data encryption for privacy preserving machine learning," *Procedia Computer Science*, vol. 232, pp. 2201–2212, 2024. Available from: https://doi.org/10.1016/j.procs.2024.02.039

[35] Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, 2021. Available from: https://doi.org/10.1016/j.eij.2020.07.003

[36] Razzaq and M. Shah, "Machine learning and deep learning paradigms: From techniques to practical applications and research frontiers," *Computers*, vol. 14, no. 3, pp. 93–93, 2025. Available from: https://doi.org/10.3390/computers14030093

[37] Rejeb et al., "The internet of things (IoT) in healthcare: Taking stock and moving forward," *Internet of Things*, vol. 22, p. 100721, 2023. Available from: https://doi.org/10.1016/j.iot.2023.100721

[38] El-Yahyaoui and M. D. E. C. El Kettani, "A verifiable fully homomorphic encryption scheme for cloud computing security," *Technologies*, vol. 7, no. 1, p. 21, 2019. Available from: https://doi.org/10.3390/technologies7010021

[39] Jabir, J. Le, and C. Nguyen, "Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors," *AI*, vol. 6, no. 8, pp. 174–174, 2025. Available from: https://doi.org/10.3390/ai6080174

[40] M. Masud et al., "A robust and lightweight secure access scheme for cloud-based e-healthcare services," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, 2021. Available from: https://doi.org/10.1007/s12083-021-01162-x

[41] Beniwal and A. Singhrova, "A systematic literature review on IoT gateways," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 10, 2021. Available from: https://doi.org/10.1016/j.jksuci.2021.11.007

[42] Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," *Symmetry*, vol. 13, no. 5, p. 742, 2021. Available from: https://doi.org/10.3390/sym13050742

[43] M. Zonayed et al., "Machine learning and IoT in healthcare: Recent advancements, challenges and future direction," *Advances in Biomarker Sciences and Technology*, vol. 7, 2025. Available from: https://doi.org/10.1016/j.abst.2025.08.006

[44] Kumari et al., "A comprehensive investigation of anomaly detection methods in deep learning and machine learning," *IET Information Security*, 2024. Available from: https://doi.org/10.1049/2024/8821891

[45] Kupcova, M. Pleva, V. Khavan, and M. Drutarovsky, "A comparative study of partially, somewhat, and fully homomorphic encryption," *Electronics*, vol. 14, no. 23, p. 4753, 2025. Available from: https://doi.org/10.3390/electronics14234753

[46] Zaraket, K. Hariss, M. Chamoun, and T. Nicolas, "Cloud-based private data analytics using secure computation over encrypted data," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 8, pp. 4931–4942, 2022. Available from: https://doi.org/10.1016/j.jksuci.2021.06.014

[47] Y. Majib et al., "Detecting anomalies within smart buildings using do-it-yourself internet of things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 4727–4743, 2022. Available from: https://doi.org/10.1007/s12652-022-04376-w

[48] Krzysztoń, I. Rojek, and D. Mikołajewski, "A comparative analysis of anomaly detection methods in IoT networks: An experimental study," *Applied Sciences*, vol. 14, no. 24, p. 11545, 2024. Available from: https://doi.org/10.3390/app142411545

[49] Y. Lu, T. Zhou, Y. Tian, S. Zhu, and J. Li, "Web-based privacy-preserving multicenter medical data analysis tools via threshold homomorphic encryption," *Journal of Medical Internet Research*, vol. 22, no. 12, p. e22555, 2020. Available from: https://doi.org/10.2196/22555

[50] G.-Y. Kim, S.-M. Lim, and I.-C. Euom, "A study on performance metrics for anomaly detection based on industrial control system operation data," *Electronics*, vol. 11, no. 8, p. 1213, 2022. Available from: https://doi.org/10.3390/electronics11081213

[51] M. Javaid and I. H. Khan, "Internet of things (IoT) enabled healthcare helps to take the challenges of COVID-19 pandemic," *Journal of Oral Biology and Craniofacial Research*, vol. 11, no. 2, pp. 209–214, 2021. Available from: https://doi.org/10.1016/j.jobcr.2021.01.015

[52] Y. Xiao et al., "Privacy protection anomaly detection in smart grids based on combined PHE and TFHE homomorphic encryption," *Electronics*, vol. 14, no. 12, pp. 2386–2386, 2025. Available from: https://doi.org/10.3390/electronics14122386

[53] Zhang and X. Jiang, "Sensitive data detection with high-throughput machine learning models in electronic health records," *AMIA Annual Symposium Proceedings*, 2023, p. 814, 2024. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC10785837/

[54] Manshadi, N. Alafchi, A. Tat, M. Mousavi, and A. Mosavi, "Comparative analysis of machine learning and numerical modeling for combined heat transfer in polymethylmethacrylate," *Polymers*, vol. 14, no. 10, pp. 1996–1996, 2022. Available from: https://doi.org/10.3390/polym14101996