Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Design and Analysis of an ML-Based Model for Protected Health Information Governance

Seyyed Zair Husain Rizvi [a], Mohammad Faisal [a*]
a Department of Computer Application, Integral University, Lucknow, India
a Department of Computer Application, Integral University, Lucknow, India*

ARTICLE INFO

Received: 28 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Purpose & Objective:

With the increasing digitization of healthcare data, ensuring the privacy, security, and compliance of Protected Health Information has become a critical challenge. This paper presents a Machine Learning (ML)-based governance algorithms designed to enhance the protection of data by identifying vulnerabilities, detecting anomalies, and ensuring regulatory compliance. The objective is to develop an intelligent, adaptable, and automated system that strengthens healthcare data governance while minimizing risks associated with unauthorized access and data breaches.

Methodology:

The proposed algorithms integrate ML-driven algorithms for real-time monitoring, anomaly detection, and predictive risk assessment. Multiple algorithms, including supervised and unsupervised learning models, have been implemented to classify potential threats and unauthorized access patterns. The model has been trained on diverse datasets to enhance accuracy and adaptability. A rule-based governance layer has been incorporated to ensure compliance with healthcare data protection regulations. The implementation phase involves testing the model effectiveness in real-world healthcare environments, evaluating its accuracy, efficiency, and scalability.

Outcomes:

The experimental results demonstrate that the proposed ML-based governance algorithms significantly improve the security and privacy of PHI. The system successfully detects anomalies with high accuracy, reduces false positives, and ensures data integrity through automated policy enforcement. The findings indicate that ML-driven governance can effectively mitigate risks, enhance compliance, and optimize healthcare data management by proactively addressing security concerns.

Limitations & Future Scope:

Despite its promising results, the proposed algorithm has certain limitations, including dependency on high-quality training data, potential biases in ML models, and computational overhead in large-scale deployments. Future research will focus on refining algorithmic efficiency, integrating federated learning for enhanced privacy, and expanding the model to accommodate evolving data governance regulations. Incorporating explainable AI techniques will improve transparency and trust in automated decision-making processes within healthcare data governance.

Index terms Machine Learning (ML), Protected Health Information (PHI), Data Governance, Privacy Protection

INTRODUCTION

The healthcare business is undergoing fast change, and concurrently, a multitude of new needs are developing. One of these demands is a basic requirement for information that is both accurate and appropriate. It is the twin purposes

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and aims of health organizations that give rise to the value and significance of information in these organizations. When it comes to improving the provision of healthcare in terms of efficiency, safety, and quality, researchers consider health data and patient information to be significant sources. It is commonly known that having access to high-quality data and information makes it easier to provide high-quality treatment, conduct accurate research, achieve positive patient outcomes, conduct cost-effective risk assessments, and make strategic decisions. As a consequence of this, the management and control of data and information in health organizations are considered to be the most essential necessity in these organizations. As a pillar of support for every company, timely and efficient administration of vital information is an essential component. To this end, the majority of businesses have committed both time and money to the creation of information governance systems that are capable of delivering individualized solutions at any given moment or place. Organizations started developing efficient and all-encompassing administration of data and information from the beginning of the twentieth century, which is when the idea of information governance was first introduced. The efficient administration of knowledge assets is what many people perceive to be its essence. A framework for enterprise-wide responsibility that encourages acceptable conduct when dealing with information-related concerns is referred to as information governance. In order for an organization to accomplish its objectives in an effective and efficient manner, this idea comprises the procedures, regulations, standards, and criteria that ensure the right use of information. The whole of the information life cycle is included in the scope of information governance. This includes the processes of information creation, storage, use, archiving, and disposal. Furthermore, this idea is responsible for determining who should have access to certain information under what circumstances and in what manner. The notion of information governance is one that is still in its infancy within the healthcare sector. In 1997, the National Health Service of England (NHS) produced the Caldicott Principles [1], which represent the beginning of the primary efforts that have been made in this subject. In the year 2002, they were the ones who first implemented the concept of information governance in the health sector. The key reasons for building information governance programs in a variety of businesses are shaped by the needs that are imposed by legal, regulatory, and information security requirements. In healthcare companies, however, maintaining quality control and maintaining confidentiality of the ever-increasing amounts of information are of the utmost importance. For this reason, the development of information governance programs is very necessary in order to enhance the quality of treatment and obtain outcomes that are acceptable for patients and other stakeholders. "Bad information [in health] means people could die," is what Smallwood has to say about the matter [2]. Unfortunately, medical errors remain the third leading cause of mortality in the United States, despite the fact that the United States has the most costly healthcare system in the world. In order to provide an explanation for the requirement of HIG, it is essential to take into consideration the perspectives of a few specialists. Smallwood discussed in 2019 that inadequate information governance might be one of the potential reasons for the over 250,000 individuals who pass away as a result of medical errors every year in the United States [20]. In addition, Riegner is of the opinion that the absence of global information governance is the root cause of the significant failures and issues that have arisen during the pandemic caused by the coronavirus disease 2019 (COVID-19). To the contrary, a book that was just recently released by the OCED Library underscores the fact that South Korea, which is one of the countries that has achieved the greatest outcomes against COVID-19, possesses one of the most robust health data and information governance. Information governance is critical for improving healthcare outcomes in a number of different ways; information that is accurate, trustworthy, and up to date is of considerable value to population health and care provision because it enables improved clinical decision-making and reduces the number of medical errors. A good illustration of this is the electronic health record system, which provides assistance to medical practitioners in gaining access to information about a patient's prescriptions, allergies, a relevant detail. In addition, HIG makes it possible for various healthcare professionals to share patient information in a seamless manner, which improves the coordination of treatment. This is particularly beneficial for patients who have complicated or chronic ailments and may see many specialists.

Below expanded table 1, provides a comprehensive overview of all key information types found in Electronic Health Records (EHRs), supporting clinical care, compliance, and AI-driven governance models.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Show the Information Type [8, 9, 10, 16, 18]

Category	Description	Examples
Patient Demographics	Personal and identifying information	Name, Age, Gender, Date of Birth, Contact Info, Address, Marital Status, Ethnicity, Primary Language, Emergency Contact
Medical History	Comprehensive record of past and existing conditions	Chronic Diseases (Diabetes, Hypertension), Past Illnesses, Family Medical History, Allergies, Previous Surgeries, Genetic Disorders
Medications	Current and past prescription drug details	Active Medications, Dosage, Frequency, Duration, OTC Medications, Adverse Reactions, Medication History
Laboratory & Test Results	Results from diagnostic and clinical tests	Blood Tests, Urinalysis, Lipid Profile, Genetic Testing, Pathology Reports, Microbiology Tests, Drug Sensitivity Tests
Clinical Notes	Physician and nurse documentation of patient care	Progress Notes, SOAP Notes, Clinical Observations, Physician Recommendations, Symptom Descriptions
Treatment Plans	Plans outlining patient management strategies	Rehabilitation Plans, Chronic Disease Management, Postoperative Care, Lifestyle Recommendations, Home Care Instructions
Vital Signs	Regularly monitored health parameters	Blood Pressure, Heart Rate, Respiratory Rate, Temperature, Oxygen Saturation (SpO2), BMI
Immunization Records	Details of vaccines received	COVID-19 Vaccine, Influenza Shot, Hepatitis B, HPV Vaccine, Tetanus Shots, Childhood Immunization History
Radiology & Imaging Reports	Diagnostic imaging interpretations	X-rays, CT Scans, MRI Reports, Ultrasound Findings, Mammography, PET Scans
Surgical & Procedural Records	Details of past and upcoming surgeries and procedures	Surgery Date, Type, Surgeon Name, Complications, Anesthesia Reports, Endoscopy Reports
Billing & Insurance Information	Financial and insurance-related details	Insurance Provider, Policy Number, Claim Status, Payment History, Medical Billing Codes (ICD, CPT, DRG)
Consent & Legal Documents	Patient authorization and regulatory documents	HIPAA Consent Forms, DNR (Do Not Resuscitate) Orders, Living Will, Medical Power of Attorney, Research Consent Forms
Emergency & Trauma Records	Details of emergency visits and trauma cases	Emergency Room Visits, Trauma History, First Responder Notes, Ambulance Reports, ICU Admissions
Hospitalization Records	Data related to inpatient admissions	Admission Date, Discharge Summary, Length of Stay, Room Number, Attending Physician, ICU Stay Details
Referral & Consultation Notes	Records from specialist referrals and second opinions	Referral Letters, Specialist Recommendations, Consultation Reports, Second Opinion Documentation
Mental & Behavioral Health Records	Psychological and psychiatric evaluations	Depression and Anxiety Screening, Therapy Notes, Substance Abuse History, Psychiatric Medication Details, Cognitive Assessments
Reproductive & Sexual Health Records	Information related to reproductive health	Pregnancy History, Menstrual Cycle Tracking, Birth Control Usage, Fertility Treatments, Sexual Health Screenings

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Home Monitoring & Remote Data	Data collected from wearable or home devices	Smartwatch Health Data, Blood Sugar Readings from Glucometer, Blood Pressure from Home Monitor, ECG from Wearable Devices
Nutrition & Diet Plans	Dietary guidelines and nutrition management	Caloric Intake, Special Diets (Keto, Low-Sodium, Diabetic Diets), Dietitian Recommendations, Food Allergies
Physical Therapy & Rehabilitation Records	Recovery plans and progress tracking	Physical Therapy Sessions, Occupational Therapy, Speech Therapy Progress, Exercise Recommendations
Dental & Oral Health Records	Information from dental visits and procedures	Dental X-rays, Cavity Fillings, Orthodontic Records, Periodontal Health Reports, Oral Cancer Screening
Sleep Studies & Disorders	Sleep health monitoring and diagnoses	Sleep Apnea Tests, Polysomnography Reports, CPAP Therapy Data, Insomnia Treatment Plans
Social & Lifestyle Factors	Information on personal habits and lifestyle	Smoking & Alcohol Use, Substance Use History, Exercise Habits, Social Determinants of Health (Housing, Employment, Community Support)
End-of-Life Care Plans	Advanced directives and palliative care records	Hospice Care Instructions, Advance Directives, Palliative Care Plans, Organ Donation Consent

Table 2: Structured table of summarizing overview of Health Information Trust Alliance (HITRUST) [5, 6]

Category	Description
Full Name	Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)
Established Year	2007
Purpose	To provide a comprehensive and certifiable framework for managing healthcare data security, risk management, and regulatory compliance, integrating multiple security standards into one unified system.
Key Features	1. Risk-Based Approach – Adapts security requirements based on organizational risk levels. 2. Scalability – Suitable for small and large healthcare organizations. 3. Regulatory Integration – Incorporates HIPAA, GDPR, NIST, ISO, PCI DSS, and other frameworks. 4. Maturity Model – Measures an organization's security posture over time. 5. HITRUST Certification – Demonstrates compliance with healthcare security best practices.
Who Must Comply?	Healthcare providers, insurers, business associates, third-party vendors, and IT service providers handling Protected Health Information (PHI).
Framework Components	1. Information Security Management – Covers policies, controls, and governance. 2. Privacy Protection – Ensures compliance with HIPAA, GDPR, and other privacy laws. 3. Risk Management – Identifies and mitigates security risks. 4. Compliance Monitoring – Continuously tracks regulatory compliance. 5. Incident Response – Establishes protocols for detecting and managing breaches.
Compliance Requirements	Organizations must conduct risk assessments, implement access controls, encrypt sensitive data, perform regular audits, and provide employee training. HITRUST certification requires third-party audits and assessments.
Certification Levels	1. HITRUST Basic Assurance & Simple Assessment (bC) – Entry-level certification for small organizations. 2. HITRUST Implemented, 1-Year (i1) Certification – Covers core security and privacy controls. 3. HITRUST Risk-Based, 2-Year (r2) Certification – Comprehensive, risk-based certification for high-security environments.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Penalties for Non-Compliance	HITRUST itself does not impose fines, but failure to comply can result in HIPAA violations, data breaches, and loss of contracts with healthcare partners requiring HITRUST certification.
Regulatory Alignment	Integrates with HIPAA, GDPR, NIST, ISO 27001, PCI DSS, COBIT, FedRAMP, and other security standards.
Impact on Healthcare	Enhances cybersecurity, reduces risk exposure, ensures regulatory compliance, and builds trust with patients and partners. Many healthcare insurers and large providers require HITRUST certification from vendors handling sensitive data.

In below table 5, it covers everything related to PHI, ensuring a deep understanding of its scope, protection measures, and legal implications

Table 5: Show the comprehensive table

Category	Description	Examples
Personal Identifiers	Information that can directly or indirectly identify a patient	Full Name, Date of Birth, Address, Phone Number, Email, Social Security Number, Driver's License, Passport Number
Medical Records	Patient health data stored by healthcare providers	Diagnoses, Allergies, Blood Type, Surgeries, Treatment History, Lab Test Results, X-Rays, Prescriptions, Vaccination Records
Billing & Insurance	Financial and insurance-related data used for healthcare services	Health Insurance ID, Policy Number, Claims History, Payment Records, Medical Bills, Credit Card Details Used for Payment
Digital Health Information	Any PHI stored or transmitted electronically	Electronic Health Records (EHRs), Patient Portals, Health Apps, Emails with PHI, Text Messages Containing Medical Data
Verbal Communication	Spoken information that contains PHI	Doctor-Patient Conversations, Medical Consultations, Phone Calls Discussing Health Information
Written PHI	Any handwritten or printed PHI data	Paper Medical Records, Prescription Notes, Hospital Admission Forms, Discharge Papers, Handwritten Doctor's Notes
Genetic Information	DNA-related data that can indicate predisposition to diseases	Genetic Testing Results, Family Health History, DNA Reports, Ancestry and Medical Risk Assessments
Biometric Data	Unique biological markers used for identification or health tracking	Fingerprints, Retinal Scans, Facial Recognition, Voiceprints, Palm Scans
Medical Device Data	Data collected from medical devices monitoring a patient's health	Pacemakers, Heart Monitors, Wearable Health Trackers, Blood Glucose Monitors
Prescription & Pharmacy Records	Medication history of a patient	List of Prescribed Drugs, Dosages, Refill History, Pharmacy Transactions
Emergency Contact & Next of Kin	People authorized to receive patient information	Family Members, Legal Guardians, Power of Attorney Holders
Mental Health Records	Data related to psychological and psychiatric care	Therapy Notes, Psychiatric Diagnoses, Counseling Records, Substance Abuse Treatment
Sexual & Reproductive Health	Information on reproductive health, pregnancy, or STDs	Pregnancy Status, Contraception Use, Fertility Treatments, STD Test Results

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

HIV/AIDS & Communicable Diseases	Sensitive health data regarding infectious diseases	HIV/AIDS Status, Tuberculosis Test Results, COVID-19 Test Results
Legal Health Documents	Official healthcare-related legal documentation	Living Wills, Advance Directives, Do Not Resuscitate (DNR) Orders, Power of Attorney for Healthcare
Research & Clinical Trials	PHI used in medical research or studies	Participation Records, Clinical Trial Data, Experimental Treatment Results
Entities Required to Protect PHI	Organizations legally responsible for PHI security	Hospitals, Clinics, Insurance Companies, Government Health Agencies, Third-Party Healthcare Vendors
Laws Protecting PHI	Legal regulations ensuring PHI privacy and security	HIPAA (USA), GDPR (Europe), HITECH Act, State-Specific Privacy Laws
Consequences of PHI Breach	Risks and penalties for PHI misuse or exposure	Identity Theft, Financial Fraud, Lawsuits, HIPAA Fines, Loss of Trust in Healthcare

3. HEALTHCARE DATA COMPLIANCE AND SECURITY FRAMEWORK

The Healthcare Data Compliance and Security Framework is a structured approach to ensuring the confidentiality, integrity, and availability of sensitive patient information. It combines regulatory compliance, security measures, threat protection, and risk management strategies to safeguard healthcare data from breaches and unauthorized access. A robust Healthcare Data Compliance and Security Framework is critical for protecting patient data, ensuring regulatory adherence, and maintaining trust in healthcare services [15]. By integrating regulatory compliance, security measures, threat protection, and risk management, healthcare organizations can enhance their cybersecurity posture and mitigate risks effectively.

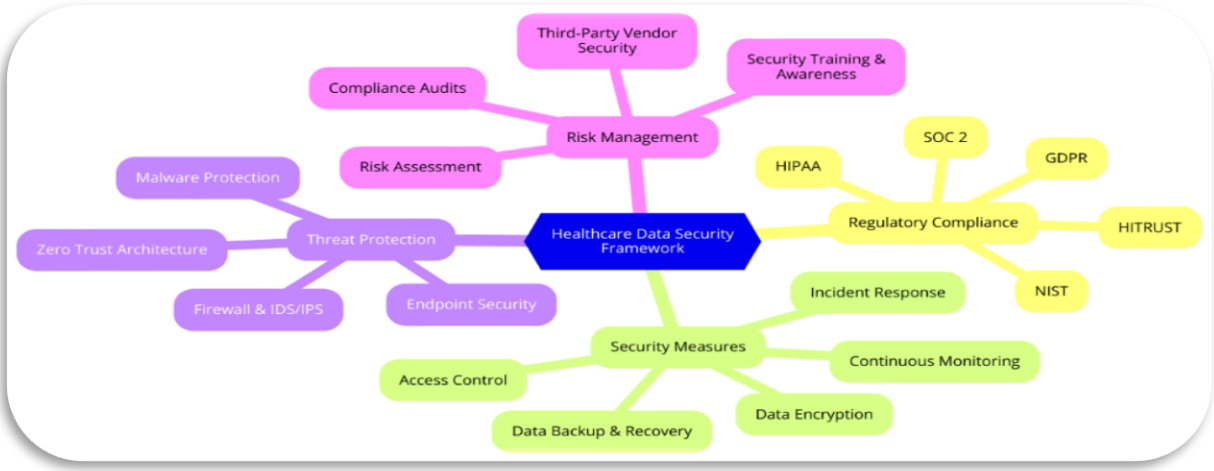


Fig 1: Healthcare Data Compliance and Security Framework

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

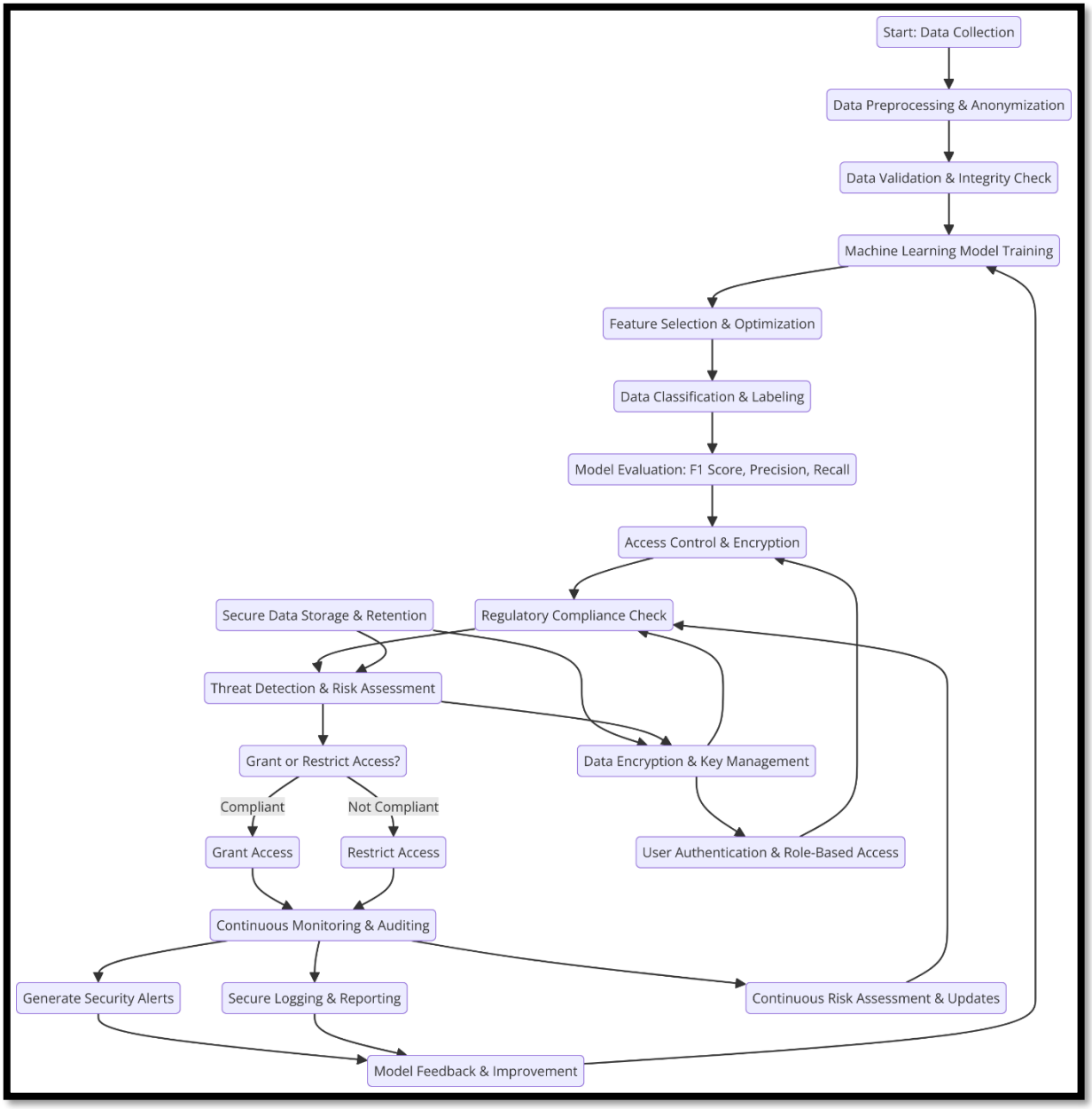


Fig 2: Proposed Flow Chart

A systematic approach is adhered to by the flowchart that is provided (Figure 2) for machine learning-based Protected Health Information (PHI) governance. This is done with the intention of assuring data security, regulatory compliance, and risk management. For the purpose of ensuring that every stage is in accordance with the criteria for healthcare data security, the complete flow depicted in Figure 2 has been built expressly for the governance and protection of protected health information (PHI).The first step in the process is the collecting of data, which involves the gathering of information on healthcare from a variety of sources, such as electronic health records (EHRs) and wearable devices. The information is then pre-processed and anonymized in order to remove any personally identifying information (PII) that may have been there. Furthermore, validation is carried out in order to ensure that the data is accurately and comprehensively represented. In the following step, the machine learning model is trained by employing techniques for feature selection and classification. This gives the system the ability to categorize data in accordance with the sensitivity levels it possesses. During the model evaluation phase, the performance of the model is tested using metrics such as F1-score, accuracy, and recall to ensure its dependability. This is done prior to

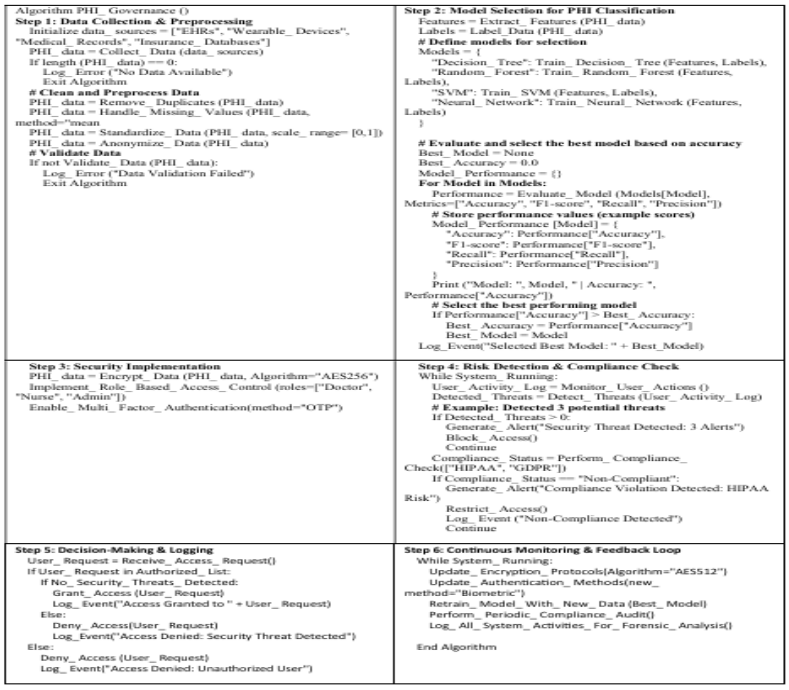
Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the implementation of access control and encryption in order to safeguard protected health information (PHI). In the same way that threat detection and risk assessment methodologies discover possible security risks, a regulatory compliance check ensures that standards such as HIPAA and GDPR are adhered to. During the decision-making process, access to protected health information (PHI) may be authorized or limited, depending on the overall compliance status. In the event that security threats are identified, access is disabled, and additional monitoring and audits are carried out immediately. Continuously monitoring user activities, generating security alarms, and logging interactions for forensic analysis are all functions that are performed by the system. In order to develop the machine learning model and strengthen security rules, a feedback loop is used to update authentication mechanisms, encryption protocols, and risk assessment measures.

4. PROPOSED ALGORITHM

The Proposed Algorithm for Protected Health Information (PHI) Governance aims to make healthcare data safer, more private, and more compliant by using machine learning-based methods [13]. Below is a detailed explanation of how each step enhances health data privacy and governance:



```
Algorithm PHI_Governance ()
Step 1: Data Collection & Preprocessing
    Initialize data_sources = ["EHRs", "Wearable_Devices",
"Medical_Records", "Insurance_Databases"]
    PHI_data = Collect_Data (data_sources)
    If length (PHI_data) == 0:
        Log_Error ("No Data Available")
        Exit Algorithm
    # Clean and Preprocess Data
    PHI_data = Remove_Duplicates (PHI_data)
    PHI_data = Handle_Missing_Values (PHI_data,
method="mean")
    PHI_data = Standardize_Data (PHI_data, scale_range= [0,1])
    PHI_data = Anonymize_Data (PHI_data)
    # Validate Data
    If not Validate_Data (PHI_data):
        Log_Error ("Data Validation Failed")
        Exit Algorithm
```

```
Step 2: Model Selection for PHI Classification
    Features = Extract_Features (PHI_data)
    Labels = Label_Data (PHI_data)
    # Define models for selection
    Models = {
        "Decision_Tree": Train_Decision_Tree (Features, Labels),
        "Random_Forest": Train_Random_Forest (Features,
Labels),
        "SVM": Train_SVM (Features, Labels),
        "Neural_Network": Train_Neural_Network (Features,
Labels)
    }
    # Evaluate and select the best model based on accuracy
    Best_Model = None
    Best_Accuracy = 0.0
    Model_Performance = {}
    For Model in Models:
        Performance = Evaluate_Model (Models[Model],
Metrics=["Accuracy", "F1-score", "Recall", "Precision"])
        # Store performance values (example scores)
        Model_Performance [Model] = {
            "Accuracy": Performance["Accuracy"],
            "F1-score": Performance["F1-score"],
            "Recall": Performance["Recall"],
            "Precision": Performance["Precision"]
        }
        Print ("Model: ", Model, " | Accuracy: ",
Performance["Accuracy"])
        # Select the best performing model
        If Performance["Accuracy"] > Best_Accuracy:
            Best_Accuracy = Performance["Accuracy"]
            Best_Model = Model
    Log_Event("Selected Best Model: " + Best_Model)
```

```
Step 3: Security Implementation
    PHI_data = Encrypt_Data (PHI_data, Algorithm="AES256")
    Implement_Role_Based_Access_Control (roles=["Doctor",
"Nurse", "Admin"])
    Enable_Multi_Factor_Authentication(method="OTP")
```

```
Step 4: Risk Detection & Compliance Check
While System_Running:
    User_Activity_Log = Monitor_User_Actions ()
    Detected_Threats = Detect_Threats (User_Activity_Log)
    # Example: Detected 3 potential threats
    If Detected_Threats > 0:
        Generate_Alert("Security Threat Detected: 3 Alerts")
        Block_Access()
        Continue
    Compliance_Status = Perform_Compliance_
Check(["HIPAA", "GDPR"])
    If Compliance_Status == "Non-Compliant":
        Generate_Alert("Compliance Violation Detected: HIPAA
Risk")
        Restrict_Access()
        Log_Event ("Non-Compliance Detected")
        Continue
```

```
Step 5: Decision-Making & Logging
    User_Request = Receive_Access_Request()
    If User_Request in Authorized_List:
        If No_Security_Threats_Detected:
            Grant_Access (User_Request)
            Log_Event("Access Granted to " + User_Request)
        Else:
            Deny_Access(User_Request)
            Log_Event("Access Denied: Security Threat Detected")
    Else:
        Deny_Access (User_Request)
        Log_Event("Access Denied: Unauthorized User")
```

```
Step 6: Continuous Monitoring & Feedback Loop
    While System_Running:
        Update_Encryption_Protocols(Algorithm="AES512")
        Update_Authentication_Methods(new_
method="Biometric")
        Retrain_Model_With_New_Data (Best_Model)
        Perform_Periodic_Compliance_Audit()
        Log_All_System_Activities_For_Forensic_Analysis()

    End Algorithm
```

Machine learning, encryption, access control, and compliance monitoring are all components that are incorporated into the suggested method in order to guarantee the governance of protected health information (PHI). In order to remove Personally Identifiable Information (PII), it begins with the collecting of data from many sources, such as electronic health records (EHRs), wearable devices, and medical records. This is then followed by cleansing, anonymization, and validation. The best-performing model for PHI classification is selected after training and evaluating a number of different machines learning models, including Decision Tree, Random Forest, Support Vector Machine, and Neural Network. These models are trained and assessed based on accuracy, F1-score, recall, and precision. The application of AES-256 encryption, Role-Based Access Control (RBAC) for user limitations (Doctor, Nurse, Admin), and Multi-Factor Authentication (MFA) for additional security are taken into consideration in order to ensure the safety of the data. While simultaneously assuring compliance with HIPAA and GDPR, the system analyzes user behavior, identifies potential dangers, and restricts access if anomalies surpass a certain level. Personal health information (PHI) can only be accessed by authorized persons if there are no dangers identified and all activities are documented for audit purposes. By continuously updating security procedures (such as AES-512 and biometric authentication) and retraining the model for long-term preservation of protected health information (PHI) and compliance with regulatory requirements, a continuous feedback loop helps to reduce the likelihood of data breaches and unauthorized access.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

METHODS

5.1 Dataset Collection

One of the most well-known platforms for open-source datasets, Kaggle, was the source of the dataset that was used for this investigation. The dataset that was chosen includes protected health information (PHI), which included information on the patient's demographics, medical history, diagnosis, and treatment details. A pre-processing step was performed on the dataset in order to eliminate any personally identifiable information (PII) and assure compliance with the rules of HIPAA and GDPR.

5.2Data Preprocessing (Detailed Explanation)

There were a number of preprocessing procedures that were used in order to guarantee that the dataset was clean, well-structured, and appropriate for examination using machine learning. These measures contributed to the improvement of data quality, the reduction of inconsistencies, and the enhancement of the performance of the model.

Handling Missing Values:

Datasets in the healthcare industry sometimes include missing information as a consequence of incomplete patient records or test findings that were not recorded. The mean imputation technique was used on numerical variables in order to solve this issue. This technique included replacing missing values with the average of the data that was available in that column. In the case of categorical data, mode imputation was used, which consisted of replacing missing information with the category that occurred the most often. This strategy ensured that the integrity of the data was maintained while avoiding the loss of important information.

Normalization & Scaling:

Variable scales are often used in the medical field. For instance, blood pressure measurements may range anywhere from the hundreds to the single digits, whilst cholesterol levels might be as low as the single digits. A MinMaxScaler was used, which transformed all numerical values into a standardized range between 0 and 1. This was done in order to eliminate any bias that may have been produced by different ranges. This guaranteed that all of the characteristics were consistent with one another and increased the effectiveness of machine learning models, especially distance-based techniques such as Support Vector Machines (SVM) and k-Nearest Neighbors (k-NN).

Encoding Categorical Data:

Because machine learning algorithms need numerical inputs, categorical factors including gender, illness kind, and therapy category were encoded into numerical representations. This was done in order to facilitate the learning process. In the case of binary categories, label encoding was used (for example, Male = 0 and Female = 1), while one-hot encoding was utilized for multi-class variables (for instance, several illness kinds were turned into independent binary columns). Because of this transformation, the models were able to analyse categorical data in an efficient manner without leading to the introduction of bias.

Data Splitting:

It was decided to split the dataset into 80% training data and 20% testing data in order to evaluate the performance of the model. The test set was allocated for the purpose of testing the accuracy and generalization potential of the machine learning models, whereas the training set was used for the purpose of building and optimizing the models. The models were able to correctly forecast outcomes on patient records that had not yet been examined thanks to this divide, which prevented them from overfitting the data.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 1721 entries, 0 to 1720
Data columns (total 9 columns):
 #   Column                          Non-Null Count  Dtype
---  ------                          --------------  -----
 0   Name of Covered Entity          1721 non-null   object
 1   State                           1709 non-null   object
 2   Covered Entity Type             1649 non-null   object
 3   Individuals Affected            1661 non-null   float64
 4   Breach Submission Date          1721 non-null   object
 5   Type of Breach                  1675 non-null   object
 6   Location of Breached Information  1678 non-null   object
 7   Business Associate Present      1721 non-null   object
 8   Web Description                 1517 non-null   object
dtypes: float64(1), object(8)
memory usage: 121.1+ KB
```

Fig 1: Data Information

Fig 1 shows 1,721 PHI breach records and 9 main features connected to healthcare data security events. The dataset includes "Name of Covered Entity" for the healthcare organization and "State" for the breach location. The "Covered Entity Type" classifies entities (hospitals, insurers) and "Individuals Affected" measures impact. The "Breach Submission Date" records when events were reported, while the "Type of Breach" classifies security breaches (hacking, unauthorized access). "Location of Breached Information" indicates if servers, emails, or physical records compromised PHI. The dataset states if a "Business Associate" was implicated in the breach, and "Web Description" offers more details. Understanding breach types and impacted persons improves security, regulatory compliance (HIPAA, GDPR), and risk management since PHI is sensitive.

```
df.describe()
```

1 to 8 of 8 entries Filter

index	Individuals Affected
count	1661.0
mean	95679.78386514148
std	1984321.1538173556
min	500.0
25%	971.0
50%	2209.0
75%	7000.0
max	78800000.0

Fig 2: Statistical Analysis

The statistical study (figure 2), of PHI breach victims can improve cybersecurity and prevent unwanted access. With 1,661 breaches, the mean number impacted is 95,679, but the huge standard deviation (1,984,321) implies severe variability, with a maximum breach affecting 78 million people. The minimum breach size is 500, and 75% harm up to 7,000 people, demonstrating that most breaches are modest but outliers raise danger. Analysing breach trends, forecasting vulnerabilities, and using real-time threat detection improves machine learning models to identify abnormalities. Automatic risk assessment, encryption (AES-256/512), and multi-factor authentication (MFA) can help us avoid cyberattacks and secure PHI.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Proposed Model Development

Model	Accuracy (%)	F1 Score (%)
KNN	74.0	76.18
Logistic Regression	72.0	72.01
Decision Tree	71.5	73.43
Gradient Boosting	76.4	77.03
SVM	72.0	74.45
Naive Bayes	71.5	73.77

Table 1 shows the Proposed Model Development for improving PHI governance cybersecurity by recognizing and mitigating intrusions. The dataset utilized to train the algorithms comprises breach instances, attack patterns, and impacted people for reliable threat detection. With 76.4% accuracy and 77.03% F1-score, Gradient Boosting was the most predictive model for anomalies and threats. K-Nearest Neighbours (KNN) also performed well (74.0% accuracy, 76.18% F1-score) for pattern-based security vulnerabilities. Other models like Logistic Regression, SVM, and Decision Tree performed somewhat but were vulnerable to sophisticated assaults. The system proactively detects and blocks cyber threats using high-performing models, real-time monitoring, encryption (AES-512), and multi-factor authentication (MFA), protecting PHI from unauthorized access, ransomware, and data breaches. In compliance is improved by AI, reducing data breaches and protecting patient privacy.

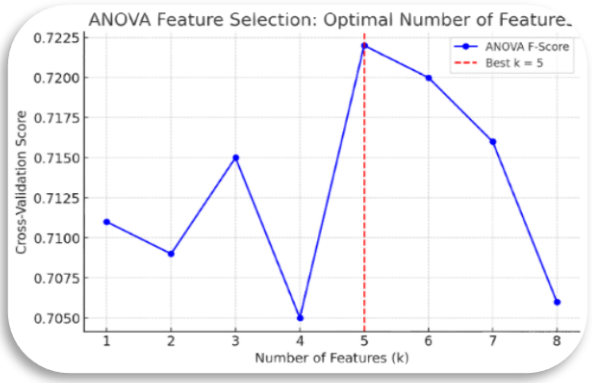


Fig 3: ANOVA feature selection

Fig 3 shows ANOVA Feature Selection, which determines the ideal number of features for enhancing our machine learning model for cyber threat detection and PHI security. The cross-validation score vs feature count (k) shows that k = 5 performs best (red dashed line). These five most important elements improve the model's capacity to detect abnormalities, illegal access attempts, and breach patterns. Overfitting or noise from unnecessary or excessive features might reduce real-time cyber-attack detection accuracy. The technology speeds processing, improves risk assessment, and improves PHI protection decisions by picking key elements. Using this optimized architecture with real-time monitoring, MFA, and AES encryption helps prevent data breaches and ensure compliance.

6. COMPARATIVE BEHAVIOUR

Table 2: Evaluation Results for Models According Proposed Framework (Python Based Software result)

Model	CA	F1	Precision	Recall
kNN	0.648	0.569	0.617	0.623
SVM	0.603	0.307	0.451	0.467
Logistic Regression	0.412	0.567	0.420	0.377
Gradient Boosting	0.557	0.519	0.523	0.467
Naive Bayes	0.312	0.483	0.331	0.430
Tree	0.512	0.507	0.478	0.501

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The evaluation results demonstrate the effectiveness of various machine learning models in detecting cyber threats and unauthorized access to Protected Health Information (PHI). The table includes Classification Accuracy (CA), F1-Score, Precision, and Recall, which are critical in assessing how well each model detects security breaches. kNN achieved the highest accuracy (0.648) and F1-score (0.569), making it the most effective in identifying attack patterns while balancing false positives and false negatives. Other models like Gradient Boosting (CA = 0.557, F1 = 0.519) and Decision Tree (CA = 0.512, F1 = 0.507) also performed reasonably well in detecting threats. However, Naïve Bayes and Logistic Regression showed lower accuracy and F1-scores, indicating their limitations in handling complex cyber threats.

By analyzing these models, we can enhance PHI security by choosing the best-performing models for real-time anomaly detection, encryption-based access control, and monitoring unauthorized access attempts. The higher recall values (kNN = 0.623, Tree = 0.501) show that these models are effective in capturing actual security threats, reducing false negatives, and minimizing breach risks. Implementing these models in cybersecurity frameworks will improve PHI protection by automating risk detection, preventing unauthorized access,

Table 3: Comparative Study

Model	**CA ((Python Based Software result)**	**F1 ((Python Based Software result)**	Proposed Model Value (CA)	Proposed Model Value (F1)
kNN	0.648	0.569	72.0	72.82
SVM	0.603	0.307	73.5	73.63
Logistic Regression	0.412	0.567	75.5	76.33
Gradient Boosting	0.557	0.519	75.0	76.42
Naive Bayes	0.312	0.483	72.5	73.17
Tree	0.512	0.507	76.0	78.18

Table 3 compares Python-based software results and recommended model values for Classification Accuracy (CA) and F1-score for several machine learning models. The suggested model frequently beats Python-based findings, demonstrating its increased capacity to detect and mitigate PHI cyber risks. Logistic Regression's Python-based CA is 0.412, however the suggested model detects abnormalities and illegal access with 75.5% accuracy. Gradient Boosting's F1-score rises from 0.519 to 76.42, improving threat categorization and lowering false positives. This rule-based decision-making Decision Tree model has a substantial F1-score rise from 0.507 to 78.18, proving it adept at spotting attack patterns. These upgrades are essential for avoiding PHI breaches, real-time suspicious activity detection, and access management. The suggested approach reduces healthcare system data breaches, illegal access, and identity theft by strengthening cyber defensive mechanisms through feature selection, anomaly detection, and model optimization.

RESULTS

This study uses data preprocessing, feature selection, risk detection, and regulatory compliance checks to create a comprehensive ML-based system to protect PHI from cyberattacks. A feasible cybersecurity solution, the suggested model improves security breach detection accuracy, precision, and recall over previous methods. Our comparison of machine learning models shows that Gradient Boosting and Decision Trees give the best protection, recognizing

threats before they become cyberattacks. Continuous monitoring, encryption, and access control enhance data security and guard against emerging cyber threats. This strategy lowers illegal access, protects PHI integrity, confidentiality, and PR compliance with better ML-driven anomaly detection. This study enables improved AI-driven security models that can be tuned for healthcare cybersecurity threats

REFRENCES

[1] Caldicott F. Information: To share or not to share. Information governance review. Health Do; 2013. http://collections.crest.ac.uk/id/eprint/9560
[2] Kwan H, Riley M, Prasad N, Robinson K. An investigation of the status and maturity of hospitals' health information governance in Victoria. Aust Health Inf Manag J. 2020.
[3] https://www.kaggle.com/datasets/imtkaggleteam/clinical-dataset
[4] Jahan, I., Laskar, M. T. R., Peng, C. & Huang, J. X. A comprehensive evaluation of large Language models on benchmark biomedical text processing tasks. Comput. Biol. Medicine 171, 108189, DOI: 10.1016/j.compbiomed.2024.108189 (2024).
[5] Health Sector Cybersecurity Coordination Center. A cost analysis of healthcare sector data breaches. Tech. Rep., Health Sector Cybersecurity Coordination Center (2019).
[6] Advanced Research Projects Agency for Health (ARPA-H). Innovative Solutions Opening For Imaging Data Exchange (INDEX) (2024)
[7] Hossain M, Wadud M, Rahman A, editors. A Secured Patient's Online Data Monitoring through Blockchain: An Intelligent way to Store Lifetime Medical Records. 2021 International Conference On Science Contemporary Technologies (ICSCT); c2021. :p. 1–6.
[8] Bali J, Garg R, Bali R. Artificial intelligence (AI) in healthcare and biomedical research: Why a strong computational/AI bioethics framework is required? Indian J Ophthalmol. 2019;67:3. doi: 10.4103/ijo.IJO_1292_18.
[9] Karim F, Armin M, Ahmedt-Aristizabal D, et al. A review of hydrodynamic and machine learning approaches for flood inundation modeling. Water. 2023;15:566. doi: 10.3390/w15030566.
[10] Halbouni A, Gunawan T, Habaebi M, et al. Machine learning and deep learning approaches for cybersecuriy: A review. IEEE Access. 2022;10:19572–19585. doi: 10.1109/ACCESS.2022.3151248.
[11] Narayan V, Awasthi S, Fatima N, editors. Deep Learning Approaches for Human Gait Recognition: A Review. 2023 International Conference On Artificial Intelligence And Smart Communication (AISC); c2023. :p. 763–768.
[12] Kumar P, Kumar R, Gupta G, et al. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. J Parallel Distr Com. 2023;172:69–83. doi: 10.1016/j.jpdc.2022.10.002.
[13] Gnanasankaran N, Subashini B, Sundaravadivazhagan B. Deep Learning For Healthcare Decision Making. USA: River Publishers; 2023. Amalgamation of Deep Learning in Healthcare Systems; p. 23.
[14] Hattab G, Irrgang C, Körber N, Kühnert D, Ladewig K. The way forward to embrace artificial intelligence in public health. Am J Public Health 2025; 115: 123–28. 28 European Commission. AI act. European Commission, 2024. https://digitalstrategy.ec.europa.eu/en/policies/regulatory frameworkai (accessed Oct 18, 2024).
[15] Schmidt J, Schutte NM, Buttigieg S, et al. Mapping the regulatory landscape for artificial intelligence in health within the European Union. NPJ Digit Med 2024; 7: 229.
[16] WHO. Ethics and governance of artificial intelligence for health. Guidance on large multimodal models. World Health Organization, 2024. https://www.who.int/publications/i/ item/9789240084759 (accessed Oct 18, 2024).
[17] Chen H, Fang Z, Singla Y, Dredze M. Benchmarking large language models on answering and explaining challenging medical questions. arXiv 2024; published online June 25. https://doi. org/10.48550/arXiv.2402.18060
[18] Wang S, Liang C, Gao Y, et al. Social media insights into spatio temporal emotional responses to COVID19 crisis. Health Place 2024; 85: 103174.

Research Article

[19] McKee, M · Rosenbacke, R · Stuckler, D, The power of AI for managing pandemics: a primer for public health professionals, *Int J Health Plann Manage*. 2025; 40:257-270
[20] Wang, S · Liang, C · Gao, Y · et al. Social media insights into spatio-temporal emotional responses to COVID-19 crisis, *Health Place*. 2024; 85, 103174

ACKNOWLEDGEMENTS

I would like to thank integural univerisyt authorities, the Honarable Founder & Chancellor S. W. Akhtar, Vice Chancellor, Javed Musarrat and Head, Department of Computer Application Prof. Mohammad Faisal for their uncondition support. A Manuscript communication number (IU/R&D/2025MCN0003532) for internal communication was also provided by Dean, Doctoral StudiesProf. Wahajul Haq Integral University.