Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Ransomware prediction and detection in healthcare Networking using AI

Dil Tabassum Subha
Master of Science in Business Analytics, Grand Canyon University, USA
Sad Bin Anwar
Masters in Information Technology, Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria, VA 22314
Rakib Hassan Rimon
Business analytics, Grand Canyon university, 3300 W. Camelback Road, Phoenix, AZ 85017
Mohd Jahidul Hoque
Business Analytics, Grand Canyon University, 3300 W. Camelback Road, Phoenix, AZ 85017
Sk Md Zubair
Engineering Management, Trine University, 2900 S Diablo Way Suite D281, Tempe, AZ 85282
Tajbeha Fatema
Mathematics, Jahangirnagar University, Savar,Dhaka 1342
Corresponding Author: Dil Tabassum Subha, **E-mail**: dsubha@my.gcu.edu

| ABSTRACT
The healthcare industry's reliance on interconnected digital systems, electronic health records (EHR), and real-time patient data management makes them a prime target for ransomware attacks, which have become one of the most significant cybersecurity threats facing healthcare organizations today. These attacks can cause major disruption to health care, compromise patient sensitive data, and cause major financial and operational losses. Ransomware detection technologies like signature-based detection are ineffective against advanced and mutating ransomware strains, especially zero-day attacks. Thus, the incorporation of Artificial Intelligence (AI) and Machine Learning (ML) techniques has grown more significant to create intelligent and proactive ransomware detection systems in healthcare networking environments. In this research, a framework for prediction and detection of ransomware attacks in healthcare networks driven by a machine learning algorithm are proposed on the Healthcare Ransomware Dataset. This study emphasizes ransomware attack pattern analysis, ransomware frequency monitoring, ransomware backup's compromised rate, ransomware severity, and ransomware recovery behavior in the healthcare organizations. The machine learning algorithms used consist of Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost, which are all well-known and widely-used models for identifying malicious behaviors and predicting ransomware attacks. The framework proposed consists of a data preprocessing, feature engineering, model training and performance evaluation. The effectiveness of the implemented models is assessed using performance metrics like accuracy, precision, recall, F1-score and ROC-AUC. The research goals are to improve ransomware early detection, reduce false positive rate, and increase cyber security resilience of healthcare networks. The results of this study will likely show that AI-driven predictive cybersecurity systems can have a substantial impact on the effectiveness of ransomware defense, as they allow for quicker detection of threats and proactive measures are taken to minimize them. This study can help develop intelligent healthcare cybersecurity solutions and serve as a basis for future investigations into the use of AI in the development of ransomware defense systems for modern healthcare infrastructures.

| KEYWORDS
Ransomware Detection, Healthcare Cybersecurity, Artificial Intelligence, Machine Learning, Network Security and Threat Prediction

| ARTICLE INFORMATION
ACCEPTED: 01 May 2026 **PUBLISHED:** 12 June 2026 **DOI:** 10.32996/jcsts.2026.8.8.3

I. Introduction

A. *Background*

Ransomware is among the most harmful and spreading cyber threats impacting organizations around the world, especially in the healthcare industry. The operation of today's healthcare systems is increasingly reliant on interwoven digital technologies, cloud computing, electronic health records (EHRs), medical Internet of Things (IoT) devices, and real-time communication networks for effective health care. These technological developments enhance the effectiveness and accessibility of health care services, but they also raise the risk of health care networks to cyber-attacks [1]. Of these threats, ransomware attacks are particularly troubling, because they can encrypt sensitive information, cause disruption to hospital operations, and also call for monetary ransom for the data to be recouped. Health facilities are viewed as high-value targets of cybercrime as they hold critical patient data, which is highly sensitive, and have a need for a system that can be accessible at all times for emergencies and clinical operations [2]. Once the ransomware is successful, it can disrupt medical treatments, delay surgeries, impact patient safety, and result in significant financial and reputational harm. As ransomware continues to change and adapt, traditional cybersecurity solutions such as signature-based antivirus and rule-based IDS are unable to keep up with recent ransomware variants and zero-day attacks. The adoption of Artificial Intelligence (AI) and Machine Learning (ML) technologies is proving to be a key solution in enhancing cybersecurity systems with intelligent threat prediction and automated cyber detection capabilities [3]. AI models use real-time analysis of the network behavior, to detect anomalies, malicious patterns and predict potential ransomware attacks [4]. The key objective of this work is to create an AI-based ransomware prediction and detection framework for the healthcare networking system with the provided Healthcare Ransomware Dataset. This research is intended to reduce the resilience of healthcare systems to ransomware attacks using machine learning approaches that will analyze and identify the behaviour of ransomware attacks and bolster early threat detection systems.

B. *Problem Statement*

Ransomware is a growing threat to healthcare organizations, leading to disruptions in healthcare services, compromises of sensitive patient health information, and hefty monetary losses. Ransomware is mainly detected by traditional cybersecurity systems, which use signature-based detection, which are useless against new ransomware variants and zero-day attacks. This trend of tight integration of healthcare networks, cloud systems and IoT medical devices has exacerbated the cybersecurity risks in healthcare settings. Furthermore, the threat detection process is delayed and existing security frameworks are not as effective due to suboptimal predictive capabilities [5]. Hence, an intelligent and proactive cybersecurity solution with Artificial Intelligence and Machine Learning (AI/ML) techniques to help strengthen cybersecurity resilience by anticipating and detecting ransomware attacks within healthcare networking environments is a critical need.

C. *Objective of the Study*

The objective of this study are

- To examine ransomware attack patterns and behaviors in the healthcare networking environment.
- To build a framework for a digital AI tool to predict and detect ransomware attacks in the healthcare environment.
- Using machine learning techniques, identify important factors in cyber security that affect ransomware attacks [6].
- To evaluate the effectiveness of different AI algorithms in detecting ransomware threats.
- To enhance early identification of ransomware threats, and reduce false positive detection rates.
- To boost healthcare cyber-security resiliency with smart predictive analytics.
- To make recommendations to improve ransomware defence strategies in healthcare organisations.

D. *Research Questions*

Following these questions are guides to this study:

- What are the chances of using AI to predict and detect ransomware in a healthcare networking system?
- What is the most accurate machine learning algorithm for detecting ransomware threats in the healthcare environment?
- Which cybersecurity aspects are the greatest challenges to ransomware in a healthcare organization?
- What is the added value of AI behavioral analysis in early identification and defense against ransomware attacks on networks?

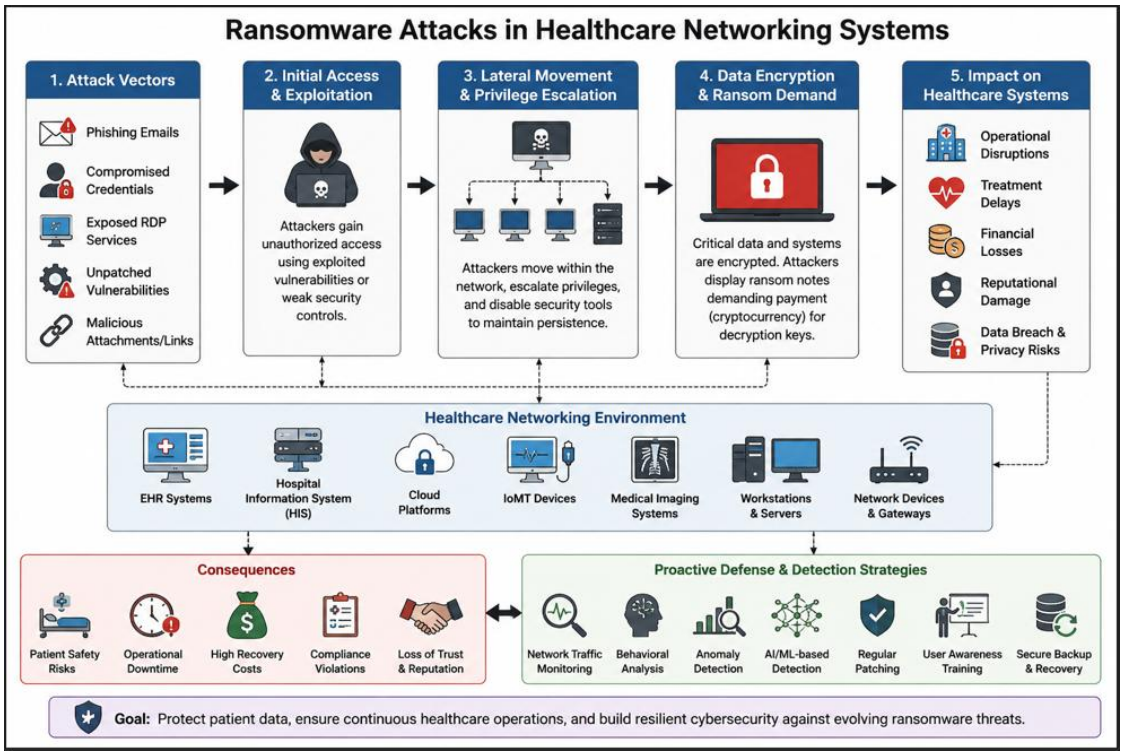
E. *Significance of the Study*

This study is notable given ransomware attacks are currently among the biggest cybersecurity issues for health care organizations around the world. The healthcare sector relies extensively on interdependent digital infrastructures, electronic health records (EHRs), and cloud-based healthcare technologies to ensure effective patient care and healthcare system management [7].Hospitals, clinics, and medical research institutes increasingly rely on complex digital infrastructures, electronic health records (EHRs), and cloud-based healthcare technologies to deliver efficient care to patients and healthcare system management. But along with the digital transformation of healthcare infrastructures, there have been significant increases in cybersecurity vulnerabilities, including cyber networks becoming targets for cybercriminals. A ransomware attack can truly cause a disruption of critical healthcare services, delay patient treatment, breach confidential healthcare information and lead to significant financial and reputational losses [8]. The value of this research is its emphasis on creating an Artificial Intelligence based ransomware prediction and detection framework unique to the healthcare networking environment. AI-powered solutions, in contrast to conventional cybersecurity tools that are based on known signatures and rules, can learn and reason about a network to detect anomalies, and anticipate ransomware attacks, all before significant damage is done. The research is a step forward in developing intelligent cybersecurity systems that can enhance the accuracy of threat detection, minimize false alarms, and facilitate proactive threat mitigation [9]. The data from this study is actionable and relevant to anyone in the healthcare industry, giving valuable insights into ransomware attack patterns, cybersecurity risk factors and effective AI-based defense mechanisms. The results could help healthcare administrators, cybersecurity experts, and policymakers adopt more effective security measures to safeguard patient information and maintain seamless healthcare operations [10]. This study provides valuable insights for the burgeoning field of Cybersecurity and Artificial Intelligence, contributing to future investigations into the development of AI-based ransomware defense systems in the evolving healthcare landscape.

II. Literature Review

A. *Ransomware Attacks in Healthcare Networking Systems*

Ransomware has emerged as one of the biggest cyber threats to the healthcare sector globally. Healthcare is becoming more dependent on digital systems, electronic health records (EHRs), cloud computing platforms and Internet of Medical Things (IoMT) devices to deliver effective patient care and healthcare management services. While these technologies enhance their efficiencies, they also introduce major cybersecurity risks that are often leveraged by cybercriminals via ransomware attacks [11]. A ransomware is a form of malicious software that encrypts data belonging to the organization with the intention of getting financial compensation for encrypting the data and providing access to the compromised systems. Healthcare institutions are deemed attractive targets because they handle sensitive patient data and have to maintain uninterrupted access to medical systems to facilitate emergency and clinical operations [12]. Some research has demonstrated that ransomware attacks on healthcare organizations can lead to a breakdown in operations, delays in treatment, monetary losses, and reputational damage. Phishing emails, compromised credentials, compromised Remote Desktop Protocol (RDP) services, and software vulnerabilities found in unpatched systems are some of the most common attack vectors employed by ransomware operators. Signature-based antivirus programs and rule-based intrusion detection systems are ineffective at detecting new ransomware variants, as attackers continually update ransomware signatures and attack methods [13]. This widespread use of cloud-based healthcare systems and interdependent medical devices has increased the attack surface of healthcare networks posing a greater challenge to cyber security management. The latest studies highlight the need for proactive cybersecurity strategies that can detect suspicious activity before the ransomware encrypts the data. Three methods proven to be effective in the strengthening of ransomware defense mechanisms are behavioral analysis, network traffic monitoring and anomaly detection [14]. Further, researchers also propose the need for intelligent detection systems to learn evolving attack patterns to enhance healthcare cybersecurity resilience and reduce ransomware attacks' impact on patient safety and healthcare operations.



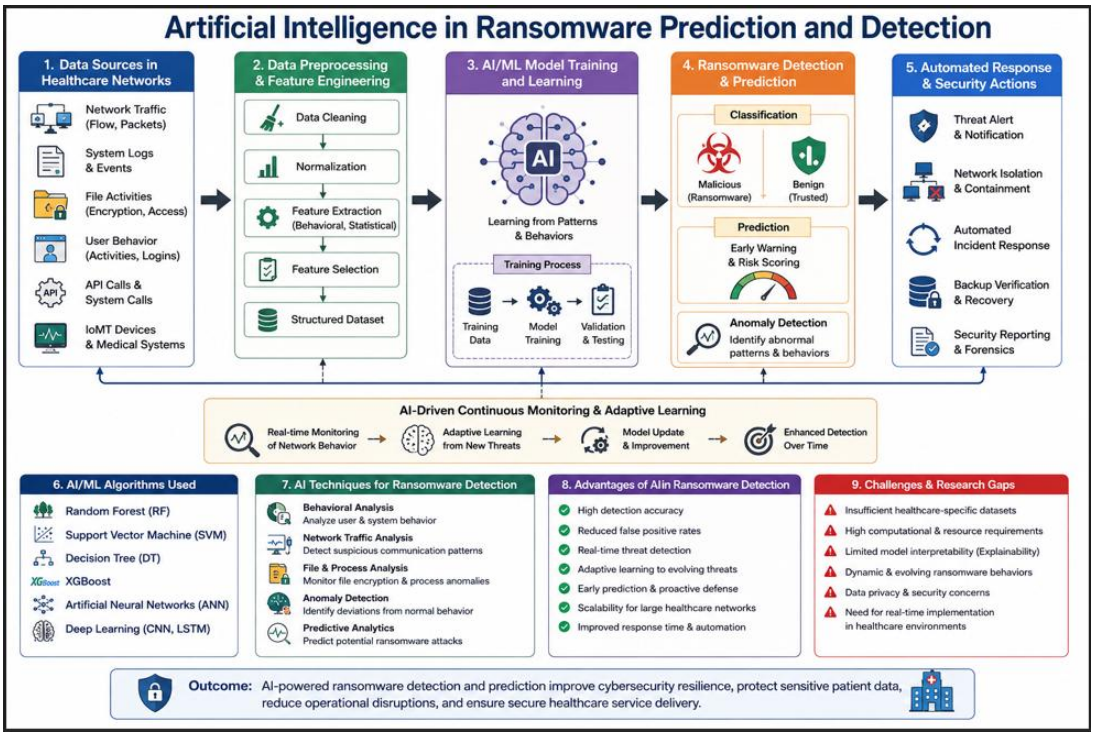
This flowchart represents the attack lifecycle and the defenses of ransomware attacks in healthcare networking systems

The diagram shows the various stages of ransomware attacks against healthcare networking systems and the related cybersecurity countermeasures. It starts with common attack methods like phishing e-mails, stolen credentials, exposed RDP services, unpatched vulnerabilities and malicious attachments [15]. This enables attackers to break into the healthcare organization's network without authorization, move between systems, raise privileges, and encrypt valuable healthcare data, before extorting ransom payment. Key aspects of healthcare networking that are susceptible to ransomware attacks are also identified in the diagram, such as EHR systems, cloud platforms, IoMT devices, medical imaging systems, and network gateways. It also discusses the implications of operations and preventive measures like behavioral analysis, anomaly Detection, AI-driven monitoring, timely patching, and safe backup recovery plans.

B. *Artificial Intelligence in Ransomware Prediction and Detection*

Artificial Intelligence (AI) and Machine Learning (ML) technologies have emerged as a vital component in today's cybersecurity landscape, due to their capacity to process vast amounts of data, identify unusual patterns, and anticipate cyber threats in real-time [16]. Most traditional cybersecurity methods use a set of pre-learned signatures and static rules that can't handle advanced ransomware attacks and zero-day malware variants. This has led cybersecurity experts and researchers to increasingly turn to AI-powered methods to augment ransomware prediction and detection for healthcare network environments. Random Forest, Support Vector Machine (SVM), Decision Tree, XGBoost, and Neural Networks are some of the most popular machine learning algorithms used in cybersecurity threat analysis due to their ability to classify malicious and benign activities based on their behavioral features. AI-driven models have been shown to be effective at detecting ransomware attacks through network traffic analysis, file encryption patterns, API calls, and identifying user activities that deviate from normal [17]. There are also some promising use cases where deep learning methods, such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have been effective in identifying advanced ransomware activity and forecasting future ransomware attacks before they have a chance to compromise the system [18]. AI-powered cybersecurity solutions offer several benefits, such as enhanced accuracy in detection, lower false positive rates, quicker response times, and adaptable learning capabilities, researchers have pointed out. AI-powered ransomware detection systems can be integrated into healthcare networking systems to continuously scan network traffic and automatically flag suspicious activity that relates to ransomware attacks. Predictive analytics can help healthcare organizations detect vulnerabilities and take pro-active measures in mitigating them [19]. While these progressions, there are still a few challenges identified in the present studies, such as restricted healthcare-specific ransomware datasets, high computation needs, and restricted explainability of AI models. Thus, more studies

are required to devise intelligent, accurate, and scalable ransomware detection systems for healthcare networking environments that can be developed using advanced artificial intelligence and machine learning techniques.



This flowchart demonstrates AI-driven ransomware prediction and detection process in healthcare networking environments

The diagram shows a healthcare networking system with various components, including network components, AI and machine learning components, and ransomware components. The diagram represents a healthcare networking system, including network components, AI/machine learning components, and ransomware components, with a focus on how AI and machine learning are being used to predict and detect ransomware attacks. It starts with healthcare data sources like network traffic, system log, user activity, API calls, and IoMT devices [20]. The data is then preprocessed, normalized, extracted, and selected for training and learning of AI/ML models. Behavioral patterns are analyzed using machine learning algorithms, such as Random Forest, SVM, Decision Tree, XGBoost and deep learning models, which classify malicious and benign activities [21]. The framework facilitates the prediction of ransomware, automated detection of anomalies, automated response measures, continuous monitoring and adaptive learning. The diagram emphasizes benefits, obstacles, and enhancements in healthcare systems with the help of AI for cybersecurity.

C. *Empirical Study*

In the article AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review written by Nusrat Jahan Sarna, Farzana Ahmed Rithen, Umme Salma Jui, Sayma Belal, Al Amin, and Tasnim Kabir Oishee, the authors examined the use of Artificial Intelligence in fraud detection through the lens of Machine Learning, Deep Learning, and hybrid models within financial networks. The study pointed out the limitations of conventional detection systems in addressing advanced cyber threats and the need for AI-powered predictive analytics and anomaly detection methods [1]. The researchers identified and discussed different types of algorithms such as supervised learning, unsupervised learning, Graph Neural Networks and deep learning techniques for detecting malicious activities and hidden behavioural patterns among huge volumes of data. The article also highlighted the importance of real-time monitoring, adaptive learning, cloud computing and distributed systems in enhancing cybersecurity performance and minimizing operational risks. Additionally, the study notes several challenges that impact the effectiveness of AI-powered cybersecurity systems, including privacy concerns, concerns about algorithmic bias, lack of explainability in models, and changing attack methods. The insights presented in this article could be leveraged in ransomware prediction and detection within healthcare networking systems using Artificial Intelligence and Machine Learning techniques, as AI can enhance the accuracy of threat identification, proactive defense strategies, and intelligent decision-making processes within cybersecurity.

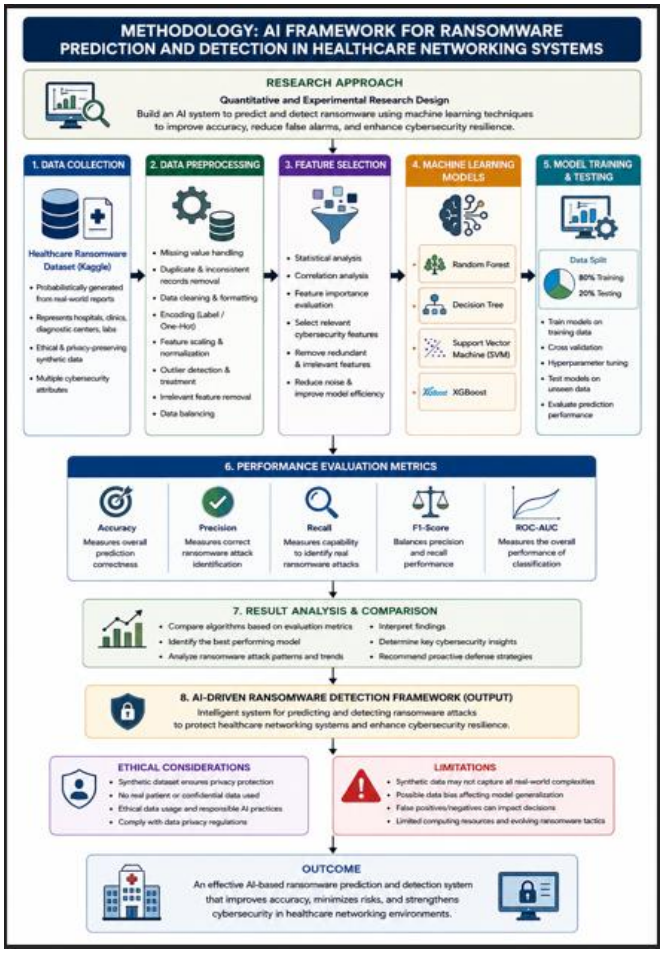
In the article titled AI-Powered Behaviour Analysis in Financial Services by R. Thalapathi Rajasekaran and Muthu Selvam, the authors investigated the application of advanced Artificial Intelligence and Machine Learning techniques for analyzing user behavior in financial services. In this study, deep learning, clustering algorithms, and reinforcement learning techniques were used to uncover behavioral patterns, refine predictions, and optimize operations. To handle transactional and communication data for intelligent decision-making, advanced neural network models like Recurrent Neural Networks (RNNs) and transformer models were used. To classify users according to their behavioral characteristics and detect abnormal activities, the researchers also used clustering techniques such as K-Means, DBSCAN and Hierarchical Clustering. Moreover, reinforcement learning techniques like Deep Q-learning and multi-agent learning were employed to learn and adapt the system's behavior dynamically in response to user actions, and to enhance the system's performance [2]. The article highlighted the significance of the behavioral analysis, anomaly detection, and adaptive learning components in intelligent cybersecurity systems. Furthermore, the study highlighted ethical concerns, such as privacy of data, minimization of bias and explainability of models. This study highlights the potential of AI-based behavioral analysis and machine learning for predicting and detecting ransomware attacks in healthcare networking systems, as the intelligent models successfully identified abnormal behavior, reinforced predictive cybersecurity, and supported proactive measures to prevent ransomware attacks.

S. Prabhu, P. V. Jothikantham, R. Asha Mary and M. Thirunavukkarasu discussed the use of Advanced AI and Data Science Applications for Fraud Detection and Risk Management in the chapter Predictive Analytics for Fraud Detection and Risk Management. The study highlighted the significance of using machine learning algorithms, data mining techniques, and real-time data analysis for detecting anomalies and suspicious activity in complex digital environments. The researchers spoke about supervised and unsupervised learning approaches to further enhance the accuracy of the predictions and bolster proactive threat detection. The chapter also emphasized the importance of continuous learning systems that can adapt dynamically to the changing cyber threats and malicious activities [3]. Moreover, the study proved that the analytical models based on Artificial Intelligence (AI) technologies have a significant impact on operational efficiency, financial losses reduction and in the process of making decisions intelligently. The results of this study provide evidence for the use of Artificial Intelligence in healthcare networking systems and predictive cybersecurity analysis to increase the prediction of ransomware attacks, increase the early detection of ransomware attacks, and increase the cybersecurity defense mechanisms in a proactive way against the attacks of ransomware that change regularly.

In the article titled AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities by Oluwabusayo Adijat Bello, Abidemi Ogundipe, Damilola Mohammed, Adebola Folorunso, and Olalekan Ayodeji Alonge, the authors investigated the application of Artificial Intelligence techniques for real-time fraud detection in financial transaction systems. The study identified some challenges with current detection methods and how they can be overcome by adopting AI-based methods like machine learning algorithms, deep learning models, natural language processing, and anomaly detection. The researchers talked about the supervised and unsupervised learning algorithms used to enhance detection accuracy and enhance predictive cybersecurity [4]. The article also covered the integration of hybrid AI models to enhance the reliability, scalability, and threat analysis in real-time. Moreover, the research revealed significant challenges in the field of AI-driven security systems, such as data quality issues, privacy concerns, regulatory compliance, scalability constraints, and ethical considerations. The results of this article underscore the potential of leveraging AI and Machine Learning methods in the real-time prediction and detection of ransomware attacks, the development of proactive defense strategies, and the strengthening of cybersecurity resilience in healthcare networking systems

III. Methodology

The methodology used in this study is quantitative and experimental to create an Artificial Intelligence framework for predicting and detecting ransomware in Healthcare Networking Systems [22]. The methodology focuses on analyzing cybersecurity data related to ransomware attacks using machine learning techniques. Several stages are included in the research process, such as data collection, preprocessing, feature engineering, model training, testing, and performance evaluation. Various machine-learning algorithms are used to detect malicious attack patterns and predict ransomware threats. The technique seeks to raise the accuracy of ransomware detection in healthcare settings, minimize false alarms, and build cybersecurity resilience via intelligent and proactive AI-driven threat detection systems.



This diagram represents an AI-powered approach to predicting and detecting ransomware attacks in healthcare systems

The diagram shows the entire methodology of the proposed Artificial Intelligence (AI) based ransomware prediction and detection framework in the Healthcare Networking System (HNS). First, it starts with healthcare ransomware datasets obtained from Kaggle, then it introduces data preprocessing methods including data cleaning, encoding, normalization, outlier detection, and data balancing [23]. At the feature selection stage, the most important cyber security features are extracted using statistical and correlation analysis [24]. Structured healthcare cybersecurity data is then used with multiple machine learning algorithms trained and tested, such as Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost. The effectiveness of models is compared using the performance evaluation metrics: accuracy, precision, recall, F1-score and ROC-AUC. Ethics, data set constraints, and proactive cybersecurity outcomes are also part of the framework to bolster ransomware detection and healthcare network resiliency.

A. *Research Design*

This research uses quantitative and experimental research design to build an Artificial Intelligence system for predicting and detecting ransomware in Healthcare networking systems. The research concentrates on extracting information from the ransomware cybersecurity data, and uses machine learning methods to detect malicious attack patterns and predict future ransomware [25]. The quantitative approach is suitable because there is the use of statistical analysis, data preprocessing, model training and model performance evaluation based on structured cybersecurity datasets. The experimental design allows for benchmarking of the performance of different machine learning algorithms to identify the best algorithm for ransomware detection within a healthcare setting [26]. The research process contains several steps such as data collection, data preprocessing, feature engineering, model development, and model testing and result analysis. Various machine learning models are trained and tested by measuring the accuracy, precision, recall, F1-score, and ROC-AUC. The proposed research design facilitates a systematic analysis of ransomware attack behavior and the creation of an intelligent cybersecurity framework that would help mitigate false positive rates, predict ransomware attacks and enhance the resilience of the healthcare cybersecurity environment.

B. *Dataset Description*

The Healthcare Ransomware Dataset (Kaggle) is used for the analysis of ransomware attacks in healthcare networking systems with this research. The dataset is generated using probabilistic modelling techniques with inputs from real world healthcare cybersecurity reports, ransomware attack statistics and industry research findings [27]. It mimics ransomware attacks on healthcare facilities like hospitals, clinics, diagnostic centers, and research labs. The dataset is designed to be honest and ethical, while still being representative of realistic cyber-attack scenarios, which maintains privacy of data. It features several cyber security attributes such as attack methods, organization types, infection rates, recovery time, compromise status of backups, the ransom payment behavior, frequency of monitoring and cyber security response patterns. These characteristics offer insights into the way ransomware is attacking, the weaknesses in the healthcare system, and the state of healthcare security management [28]. The data can be analyzed to identify trends in attacks, risk assessment, and predictive modeling of cybersecurity threats using Artificial Intelligence and Machine Learning methods. The dataset is structured and can be used for classification, prediction, and anomaly detection tasks [29]. The data can be used to test various machine learning algorithms and create intelligent systems for detecting ransomware infections that can boost the cybersecurity resilience of healthcare networking environments and help build stronger proactive ransomware detection plans.

C. *Data Preprocessing*

The data preprocessing process is a key component of this research as it directly affects the performance and accuracy of machine learning models for ransomware prediction and detection in healthcare networking systems [30]. Several pre-processing techniques are applied in this study to clean, organize and make the dataset machine learning ready. The data is first checked for missing data, duplicate records, inconsistencies, and data formatting errors that could have a negative impact on the model's performance [31]. Data is cleaned and processed for missing or inconsistent values and duplicate and irrelevant records are eliminated to ensure reliability and integrity of data sets. Methods include label encoding and one-hot encoding for categorical variables like attack methods, organization types, monitoring frequency and ransomware behavior categories. Feature scaling and data normalization techniques are also employed so that the numerical variables stay within a comparable range, avoiding bias because of the wide range of the features' values [32]. The outlier detection techniques are used to identify the data points that are abnormal or extreme and may affect the learning and prediction outcomes of the models. Moreover, irrelevant and redundant features are omitted to minimize computations and enhance the efficiency of machine learning. The preprocessing stage also comprises techniques to balance the datasets to tackle the imbalance problem that can impact the accuracy of ransomware classification. These preprocessing methods help the data be more organized, accurate, and ready to be analyzed with AI and ML, which ultimately enhances the efficacy of ransomware detection and forecasting in the healthcare cybersecurity context.

D. *Feature Selection*

Feature Selection is a crucial step in this research since it provides the most important features that are crucial for ransomware prediction and detection in healthcare networking systems [33]. Choosing the right features also helps to make the model more accurate and less complex, and boosts the efficiency of the machine learning algorithms. The current study investigates various cybersecurity-related factors to understand their contribution to the ransomware attack behavior and vulnerabilities of healthcare networks. These features include attack methods, organization type, monitoring frequency, severity of an infection, recovery time, status of compromise to the backups, ransom payment behavior, and cybersecurity response patterns. These variables offer insight into the activities of ransomware and assists Artificial Intelligence systems in picking up malicious patterns [34]. Various techniques such as statistical analysis, correlation analysis, and feature importance evaluation are used to explore the correlation between independent variables and target outcomes. Relevant features, if possible, are preserved and irrelevant attributes are deleted, which reduces noise and enhances machine learning. The feature selection also helps to avoid overfitting by removing irrelevant features which can have a detrimental impact on the model's generalization ability [35]. By choosing meaningful cybersecurity indicators, the AI models can concentrate on the most relevant behavioral patterns relating to ransomware attacks. In healthcare settings, feature selection plays a crucial role in improving the accuracy of predictions, minimizing training time, and enhancing the reliability of ransomware detection systems [36]. The proposed Artificial Intelligence framework, after optimization of the data set by effective feature selection methods, is more efficient, scalable, and able to handle proactive cybersecurity defense mechanisms to protect sensitive healthcare networking infrastructures from emerging ransomware attacks.

E. *Machine Learning Models*

This research utilizes several machine learning algorithms to assess the efficacy of the algorithms in predicting and detecting ransomware attacks in healthcare networking systems. The four models chosen are: Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost. The algorithms are popular in the cybersecurity and Artificial Intelligence research communities for their excellent classification ability, predictive power, and processing of the complex behavioral patterns found in cybersecurity datasets. Random Forest is used because it is very accurate, has ensemble learning and is useful in processing large data and many attributes [37]. Decision Tree is chosen since it gives easy to interpret and simple classification results which helps to have a clear view of the ransomware attack pattern. It uses hyperplane classification techniques to separate malicious and non-malicious activities by employing Support Vector Machine (SVM) as it is well capable of performing it. The inclusion of XGBoost is due to its superior boosting mechanism, efficiency in computation and ability to achieve high degrees of prediction accuracy along with reducing overfitting issues [38]. These machine learning models have been trained and tested with the healthcare ransomware dataset, where the detection performance, classification efficiency and predictive reliability of the models in detecting ransomware threats in healthcare networking environments have been compared.

Machine Learning Model	Purpose in Research
Random Forest	high accuracy ransomware classification
Decision Tree	Interpretable Attack Pattern Analysis
Support Vector Machine (SVM)	Malicious activity classification
XGBoost	Improved prediction accuracy and performance

F. *Model Training and Testing*

Model training and testing play vital roles in this research and are the necessary steps to show the effectiveness of machine learning algorithms used for ransomware prediction and detection in healthcare networking systems. The dataset is split into two parts; 80% of the data is available for training and 20% for testing and validation [39]. This split in data ensures that the resulting machine learning models are able to generalize to out-of-sample ransomware attack scenarios. In the training phase, the algorithms, such as Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost, are fed with the healthcare cybersecurity dataset to identify patterns and relationships between the input features and the ransomware attack behaviors. The algorithms, including Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost, are trained using the healthcare cybersecurity dataset to detect patterns and relationships between input features and ransomware attack behaviors [39]. The training process helps the models detect meaningful features that can be linked to malicious behavior, attack severity, risks of being compromised on backups, and patterns of ransomware attacks. Cross validation is used in the model training and testing to increase model reliability and decrease over fitting. Cross validation is useful to make sure that the models created remain stable for various sub-sets of the data and are not unduly sensitive to particular training samples. Various hyperparameter tuning techniques are also applied to enhance the performance of the models and optimize the prediction accuracy [40]. In the testing phase, hidden data samples are fed into the system to see how well the machine learning models are able to identify and predict ransomware attacks in a healthcare setting. Each algorithm is tested to determine how well it can correctly identify ransomware-related activities and to keep false positives and false negatives to a minimum [41]. The entire model training/testing process helps build a robust and intelligent AI-driven cybersecurity framework for detecting ransomware attacks in the healthcare sector.

G. *Performance Evaluation Metrics*

Several standard classification metrics commonly used in cybersecurity and Artificial Intelligence research are used to assess the performance of the machine learning models created in this research. The evaluation metrics are crucial for assessing the performance, accuracy, and forecasting power of the chosen algorithms in predicting and detecting ransomware attacks in healthcare networking systems. Accuracy, Precision, Recall, F1-Score, and ROC-AUC are the main performance metrics that have

been used in this study [42]. The accuracy is used to assess the overall correctness of the model, defined as the percentage of the ransomware and non-ransomware instances that were correctly classified. Precision measures the portion of the actual ransomware attacks that the model correctly classifies as such out of the total number of predicted positive attacks, minimizing the number of false positive attacks. Recall is the model's ability to accurately identify actual ransomware attacks and reduce false negative instances, which could result in undetected attacks. F1-Score is a balanced measure of precision and recall and is very useful for assessing classification accuracy of cyber security datasets that are imbalanced. The overall classification ability of machine learning models is measured in terms of ROC-AUC analysis, which compares true positive rates and false positive rates [43]. Combined these performance indicators would indicate the best machine learning algorithm for ransomware prediction and detection in the healthcare sector. The evaluation results also enable comparative analysis of the various AI models and help to identify the most accurate, reliable and efficient cybersecurity framework to protect healthcare networking systems from the changing ransomware threat.

Evaluation Metric	**Purpose**
Accuracy	Measures overall prediction correctness
Precision	Measures correct ransomware attack identification
Recall	Measures' capability to identify real ransomware attacks.
F1-Score	Balances precision, recall performance.
ROC-AUC	Measures the overall performance of classification

H. *Ethical Issues and Limitation*

This study highlights some of the ethical issues and constraints of using Artificial Intelligence and cybersecurity datasets for prediction and detection of ransomware attacks on healthcare networking systems. The study leverages the Healthcare Ransomware Dataset, a synthetically generated dataset that simulates real-world ransomware incidents without releasing any sensitive patient information or compromising healthcare data privacy regulations [43]. The study does not contain any real patient records or confidential healthcare information, which means that the study remains ethical and does not pose a significant threat to privacy. Synthetic data can introduce another layer of complexity, however, and could hinder the machine learning models' ability to accurately capture the behavior of ransomware and complex healthcare cyber security scenarios [44]. One of the issues is that the data set might be biased, impacting on model generalization and prediction accuracy in other healthcare infrastructures. In addition, machine learning models can also generate false positive or negative results, which can impact cybersecurity decision-making processes [45]. Limitations to the study include the availability of computing resources, the amount of data, and the changing tactics of ransomware attacks, which are constantly changing over time. While these are limitations, the research offers valuable insights into AI-based ransomware prediction and detection, and speaks to intelligent cybersecurity frameworks to help bolster protection of healthcare networks and enhance proactive ransomware mitigation strategies.

IV. Proposed Framework

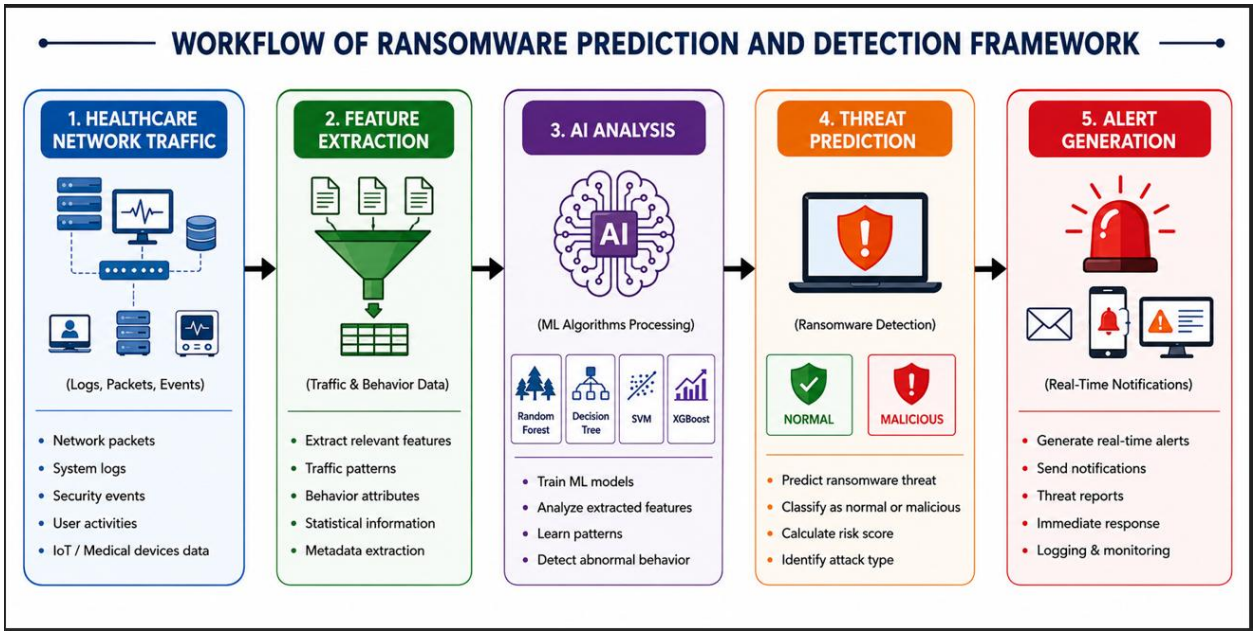
The proposed framework uses the Artificial Intelligence and Machine Learning techniques to predict and detect ransomware attacks in healthcare networking systems. By incorporating data collection, data preprocessing, feature engineering, AI-driven prediction, and real-time alert generation, the framework boosts ransomware detection accuracy, cuts response time, and enhances the cybersecurity resilience of healthcare organizations against evolving ransomware threats.

A. *Framework Architecture*

The proposed framework architecture consists of five main components designed to cooperate in a way that is effective in forecasting and detecting ransomware in healthcare networking environments. The first is the Data Collection Layer, which captures the traffic of healthcare networks, system logs, ransomware indicators, user activity data, security event information and more from hospitals, clinics, servers, cloud systems and connected medical devices. This layer guarantees adequate cybersecurity

data for additional analysis and threat identification [45]. The second is the Preprocessing Layer, which cleans and transforms the data collected whenever necessary, using techniques such as removing data that are repeated, handling missing values, encoding categorical variables, and normalizing numerical ones. This process helps to enhance data quality and makes it ready for analysis by machine learning algorithms. The third layer, Feature Engineering Layer, identifies significant cybersecurity-related features like attack patterns, encryption activities, login attempts, unusual network traffic behavior, and system vulnerabilities. Feature engineering is useful to enhance the accuracy of prediction as well as identify the best indicators related to ransomware attacks [46]. The fourth component is the AI Prediction Engine, which uses machine learning algorithms such as Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost to analyze extracted features and make real-time predictions about ransomware threats. This engine classifies network activities as normal or malicious, and recognizes suspicious activities before any serious damage is done. Last but not least, the Detection and Alert System alerts and warns administrators and cybersecurity teams in real time with the ability to respond and proactively mitigate ransomware threats in healthcare networking systems.

B. *Workflow framework*



This image illustrates the flowchart for ransomware prediction and detection in the context of healthcare networking systems, which integrates AI technology.

The flowchart represents the process flow of a ransomware prediction and detection mechanism based on artificial intelligence (AI) technologies for a healthcare networking system. The first step in the process is collecting healthcare network traffic such as logs, packets, security events, and IoT medical device information [47]. The feature extraction phase involves recognizing and extracting relevant traffic patterns, behavioral characteristics, and statistical data for analysis. The analysis using AI uses machine learning algorithms like Random Forest, Decision Tree, SVM, and XGBoost to recognize irregular actions and master ransomware assault patterns. The threat prediction stage determines if the activity is normal or malicious, and the alert generation stage delivers real-time notifications, reports and response alerts to the cybersecurity team.

V. Dataset

A. *Dataset Overview*

The dataset employed in this research is the Healthcare Ransomware Dataset obtained from the Kaggle website which is used for prediction and detection analysis of ransomware in the Healthcare Networking Systems. The data is created synthetically with the use of probabilistic modelling methods, and is based on real world cybersecurity reports, ransomware attack statistics and healthcare threat intelligence studies [48]. It was created to mimic realistic ransomware attacks that impact healthcare institutions, hospitals, clinics, medical laboratories, and different healthcare organizations, with privacy and ethics compliance. The dataset is based on the latest ransomware attack trends in the healthcare industry and features data influenced by reports from industry giants like IBM, Sophos, CISA, and Health & Human Services (HHS). The main goal of this dataset is to

deliver a structured and research-oriented Cybersecurity dataset that can be used for Artificial Intelligence and Machine Learning applications in detection and prediction of ransomware attacks [49]. The data set includes about 5000 records of ransomware attacks and several cybersecurity attributes relating to the healthcare organization and the attack behavior. Key data points include when the attack occurred, how the attack was accomplished, what type of organization was attacked, the infection rate, recovery time, the state of backup compromises, ransom payment behavior, how often organizations are monitoring cybersecurity, and their operational responses. These variables can be used for analyzing the characteristics of ransomware attacks, vulnerabilities of the organizations and the effectiveness of cyber security in healthcare networking environments [50]. The dataset also includes data on phishing attacks, credential theft, Remote Desktop Protocol (RDP) exploits, and vulnerabilities in systems that are frequently exploited during ransomware attacks. The dataset is organized and labeled, making it well suited for machine learning classification, anomaly detection, predictive analysis and cyber security risk assessment tasks. This dataset can be used to create AI-based models that help detect malicious actions, forecast ransomware attacks, and enhance healthcare cybersecurity preparedness [51]. Further, this dataset can be used for comparative analysis with other machine learning algorithms like Random Forest, Decision Tree, Support Vector Machine (SVM), XGBoost. Although artificial, it is very close to real ransomware attack scenarios and can offer insights for developing intelligent cybersecurity solutions that can protect the healthcare networking infrastructure against the new and changing ransomware threats and cyber-attacks.

B. *Screenshot of Dataset*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	id	attack_date	org_type	org_size	faciliti es_aff ected	cyber_threats _tracked	monitoring_freq	backup_c ompromi sed	ransomware_i nfection_rate _(%)	data_enc rypted	data_stol en	recovery _time_(d ays)	entry_method	paid_ran som	data_rest ored	ransomware_i ncidents
2	RAN202400001	6/28/2024 0:00	Hospital	Large	23	Jan-50	Daily	TRUE	63.3	TRUE	FALSE	64	Exploited Vulnerability	FALSE	36.28	2
3	RAN202400002	12/18/2024 3:00	Pharma	Medium	4	50-350	Daily	FALSE	59.05	TRUE	TRUE	28	Exploited Vulnerability	TRUE	57.66	6
4	RAN202400003	10/12/2024 9:00	Research Lab	Small	18	350+	Daily	TRUE	90	TRUE	FALSE	49	Phishing Email	TRUE	61.85	5
5	RAN202400004	7/28/2024 19:00	Clinic	Small	5	Jan-50	Weekly	TRUE	61.32	FALSE	FALSE	56	Compromised Credentials	FALSE	52.44	5
6	RAN202400005	6/27/2024 18:00	Hospital	Large	16	350+	Daily	FALSE	53.65	TRUE	TRUE	13	Exploited Vulnerability	TRUE	75.61	2
7	RAN202400006	4/25/2024 20:00	Hospital	Large	14	Jan-50	More than once pe	FALSE	34.93	TRUE	FALSE	15	Compromised Credentials	FALSE	54.04	3
8	RAN202400007	12/1/2024 22:00	Hospital	Medium	19	50-350	Daily	TRUE	57.07	TRUE	FALSE	39	Exploited Vulnerability	TRUE	62.56	3
9	RAN202400008	4/18/2024 2:00	Insurance	Large	14	350+	Daily	FALSE	48.08	FALSE	TRUE	16	Exploited Vulnerability	TRUE	75.96	5
10	RAN202400009	4/17/2024 17:00	Clinic	Small	9	Jan-50	Monthly	FALSE	47.36	TRUE	FALSE	45	Exploited Vulnerability	FALSE	22.56	1
11	RAN202400010	8/2/2024 18:00	Research Lab	Medium	6	50-350	Weekly	TRUE	75.27	TRUE	FALSE	47	Phishing Email	TRUE	45.12	6
12	RAN202400011	3/5/2024 3:00	Hospital	Medium	17	Jan-50	Weekly	TRUE	77.72	TRUE	FALSE	84	Phishing Email	TRUE	37.53	7
13	RAN202400012	3/19/2024 23:00	Pharma	Medium	19	50-350	Daily	FALSE	46.23	TRUE	FALSE	28	Exploited Vulnerability	TRUE	69.87	3
14	RAN202400013	4/3/2024 9:00	Insurance	Medium	12	50-350	Weekly	FALSE	65.66	TRUE	FALSE	41	Compromised Credentials	TRUE	44.87	2
15	RAN202400014	4/3/2024 12:00	Hospital	Medium	4	50-350	Daily	TRUE	67.38	TRUE	FALSE	62	Compromised Credentials	TRUE	42.08	5
16	RAN202400015	1/29/2024 12:00	Hospital	Large	16	Jan-50	Weekly	TRUE	74.91	TRUE	TRUE	66	Exploited Vulnerability	TRUE	47.01	7
17	RAN202400016	4/15/2024 8:00	Hospital	Large	11	Jan-50	More than once pe	TRUE	49.21	TRUE	TRUE	46	Exploited Vulnerability	FALSE	32.73	2
18	RAN202400017	9/20/2024 10:00	Hospital	Medium	22	Jan-50	Daily	TRUE	74.31	TRUE	FALSE	98	Compromised Credentials	FALSE	25.02	2
19	RAN202400018	1/5/2024 9:00	Clinic	Small	4	Jan-50	Daily	TRUE	60.95	TRUE	FALSE	52	Exploited Vulnerability	FALSE	12.06	3
20	RAN202400019	4/12/2024 0:00	Clinic	Medium	17	50-350	Daily	TRUE	56.26	FALSE	FALSE	55	Phishing Email	FALSE	40.68	6
21	RAN202400020	8/28/2024 21:00	Hospital	Large	8	350+	Monthly	FALSE	47.66	TRUE	FALSE	14	Exploited Vulnerability	FALSE	40.56	2
22	RAN202400021	11/15/2024 13:00	Clinic	Medium	14	50-350	Daily	FALSE	50.88	TRUE	FALSE	38	Exploited Vulnerability	FALSE	0	5
23	RAN202400022	3/6/2024 6:00	Hospital	Medium	2	50-350	Daily	TRUE	43.02	TRUE	FALSE	33	Compromised Credentials	TRUE	58.52	1
24	RAN202400023	10/16/2024 0:00	Hospital	Large	11	350+	Daily	TRUE	59.54	TRUE	FALSE	30	Compromised Credentials	FALSE	31.94	5
25	RAN202400024	7/16/2024 7:00	Hospital	Medium	11	50-350	Monthly	TRUE	38.65	TRUE	FALSE	36	Compromised Credentials	TRUE	66.76	4
26	RAN202400025	1/22/2024 4:00	Clinic	Small	24	350+	Daily	TRUE	62.94	TRUE	FALSE	46	Exploited Vulnerability	FALSE	39.4	5
27	RAN202400026	3/17/2024 6:00	Research Lab	Medium	22	50-350	Weekly	FALSE	56.78	TRUE	FALSE	38	Exploited Vulnerability	FALSE	24.84	4
28	RAN202400027	8/4/2024 0:00	Hospital	Large	24	Jan-50	Monthly	FALSE	55.14	FALSE	FALSE	56	Phishing Email	FALSE	27.47	3
29	RAN202400028	12/26/2024 23:00	Clinic	Small	6	Jan-50	Daily	TRUE	46.22	TRUE	FALSE	57	Exploited Vulnerability	TRUE	55.38	4
30	RAN202400029	6/10/2024 3:00	Clinic	Medium	21	50-350	Daily	TRUE	32.81	TRUE	FALSE	40	Exploited Vulnerability	FALSE	28.43	1
31	RAN202400030	5/20/2024 21:00	Hospital	Large	21	Jan-50	Daily	TRUE	71.63	TRUE	FALSE	58	Exploited Vulnerability	TRUE	55.42	7
32	RAN202400031	8/17/2024 22:00	Clinic	Small	14	Jan-50	Weekly	TRUE	80.7	FALSE	FALSE	75	Compromised Credentials	FALSE	31.25	7
33	RAN202400032	7/28/2024 14:00	Hospital	Medium	10	50-350	More than once pe	TRUE	32.65	FALSE	FALSE	28	Exploited Vulnerability	FALSE	52.58	3
34	RAN202400033	6/1/2024 18:00	Hospital	Medium	8	50-350	Daily	FALSE	66.62	TRUE	FALSE	32	Compromised Credentials	TRUE	40.42	7
35	RAN202400034	11/9/2024 16:00	Pharma	Medium	7	50-350	Weekly	FALSE	56.09	FALSE	FALSE	25	Compromised Credentials	TRUE	47.66	7
36	RAN202400035	8/18/2024 8:00	Pharma	Large	8	Jan-50	Weekly	TRUE	56.59	TRUE	TRUE	48	Compromised Credentials	TRUE	53.25	1
37	RAN202400036	3/20/2024 23:00	Insurance	Large	8	Jan-50	Daily	FALSE	60.83	FALSE	TRUE	21	RDP Exploit	TRUE	46.77	7

Healthcare Ransomware Dataset

(Dataset Source Link: https://www.kaggle.com/datasets/rivalytics/healthcare-ransomware-dataset?select=Healthcare+Ransomware+Dataset.csv)

VI. Result

The outcomes of this study demonstrate the effectiveness of Artificial Intelligence and Machine Learning techniques in predicting and detecting ransomware attacks within healthcare networking systems. The experimental results and analytical results of the proposed AI-based ransomware detection framework with the Healthcare Ransomware Dataset will be presented. A range of ransomware attack behaviors, cybersecurity vulnerabilities, ransomware recovery patterns, and the performance of various machine learning algorithms are analyzed. To analyze the methods ransomware uses to enter, how often it can be monitored, when ransomware can compromise backups, and the effectiveness of AI models, various analytical charts and performance evaluation metrics were used [52]. To evaluate the prediction accuracy and capability of the ransomware detection of the machine learning models in healthcare cybersecurity environments, Random Forest, Decision Tree, Support Vector Machine (SVM) and XGBoost models were compared.

A. *Monitoring Frequency and Recovery Time Analysis (RTA)*

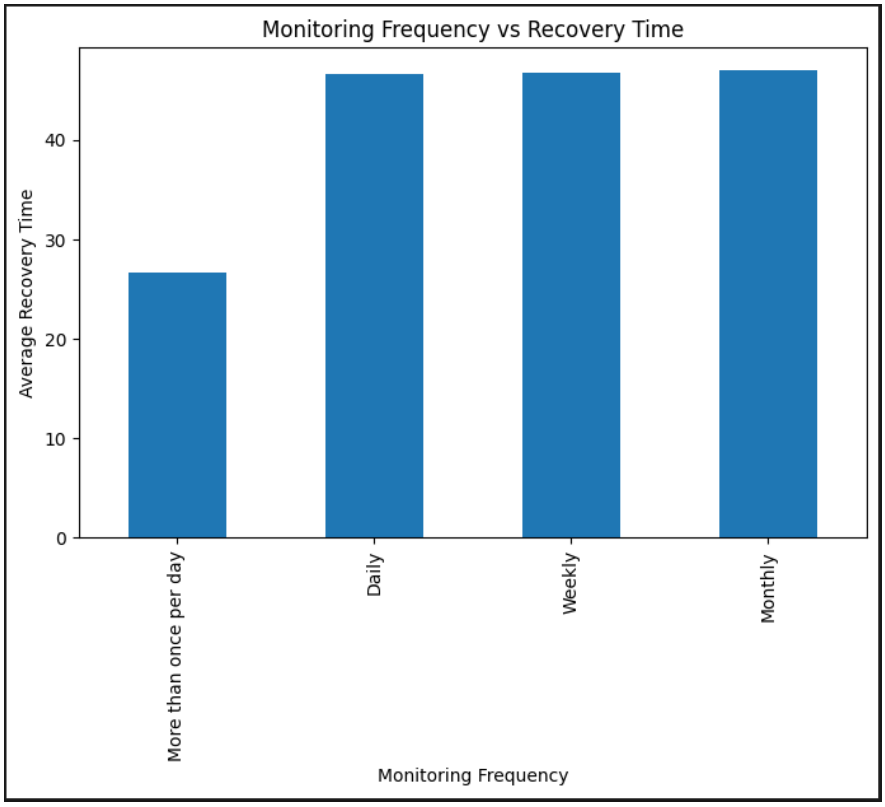


Figure 1: This image displays monitoring frequency impact on ransomware recovery time in healthcare systems

There is a correlation between the frequency of cybersecurity monitoring and the average recovery time after ransomware attacks in the healthcare networking sector, as shown in Figure 1. The graph shows that organizations which run cybersecurity monitoring more than once a day will have faster recovery times than organizations that do daily, weekly, or monthly monitoring activities. Healthcare organizations experiencing lower monitoring frequency have much longer recovery times, reflecting a lag in threat detection and incident response. The results reveal that proactive and ongoing monitoring can be a key factor in enhancing the efficiency of ransomware recovery and reducing disruption to healthcare operations [52]. Regular monitoring helps detect suspicious activities early, which helps in taking timely action against ransomware attacks before they cause significant damage to the cybersecurity team. Thus, the analysis underscores the need for adopting real-time monitoring strategies and ongoing cybersecurity risk evaluations to enhance the resilience of healthcare networks to the changing ransomware landscape.

B. ***Backup Compromise Distribution Analysis***

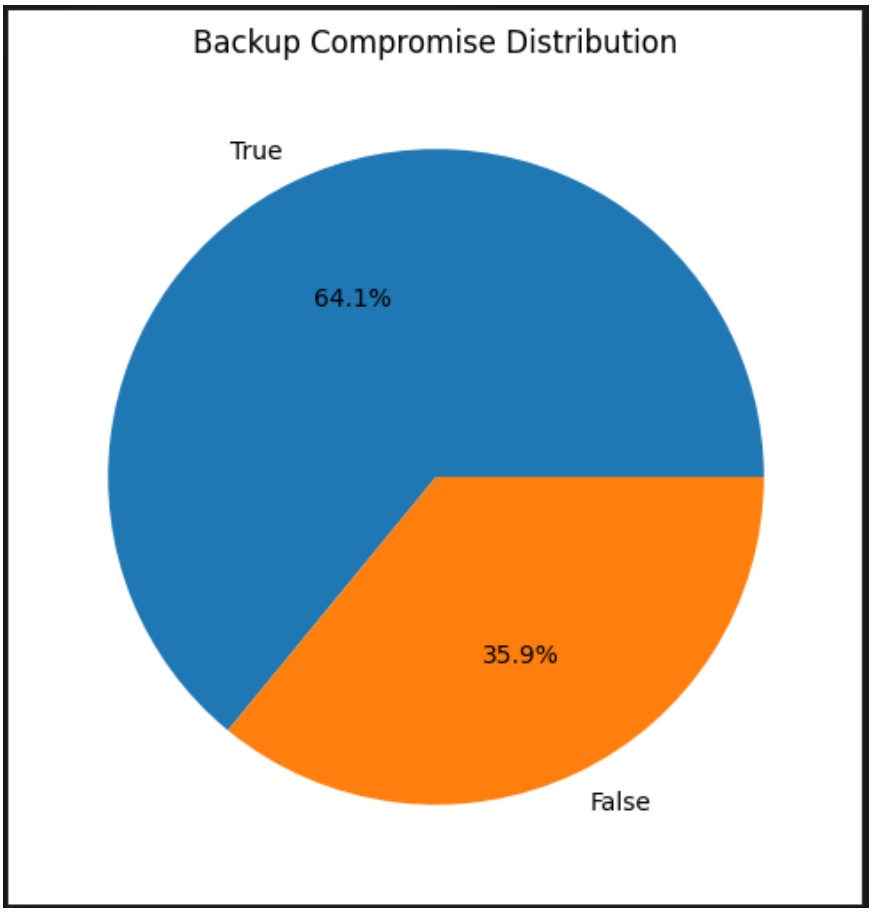


Figure 2: This image shows backup compromise distribution during ransomware attacks in healthcare organizations

Figure 2 Description The breakdown of backup compromise incidents in healthcare organizations impacted by ransomware attacks is shown in Figure 2. The pie chart reveals that some 64.1% of the healthcare institutions had a backup that was compromised in ransomware attacks, compared to 35.9% that had secure and unaffected backups. This finding shows that many ransomware attacks can target and encrypt backup systems as well as healthcare systems. Healthcare organizations face significant issues as a result of backup system compromises, including data recovery limitations, downtime, and potentially having to pay ransom demands to get access to vital patient data and healthcare services [53]. The results underscore the evolution of today's ransomware attacks and the weakness of healthcare backup management systems. Additionally, the analysis indicates that organizations with less backup protection mechanisms have bigger cybersecurity risks and slower recuperation processes. Resilient cybersecurity architectures, multi-layered storage protection, frequent test of backups, and isolated recovery environments can help enhance healthcare cybersecurity resilience and mitigate the effects of ransomware attacks on critical healthcare operations and patient data access.

C. *Analysis of ransom payment and data recovery*

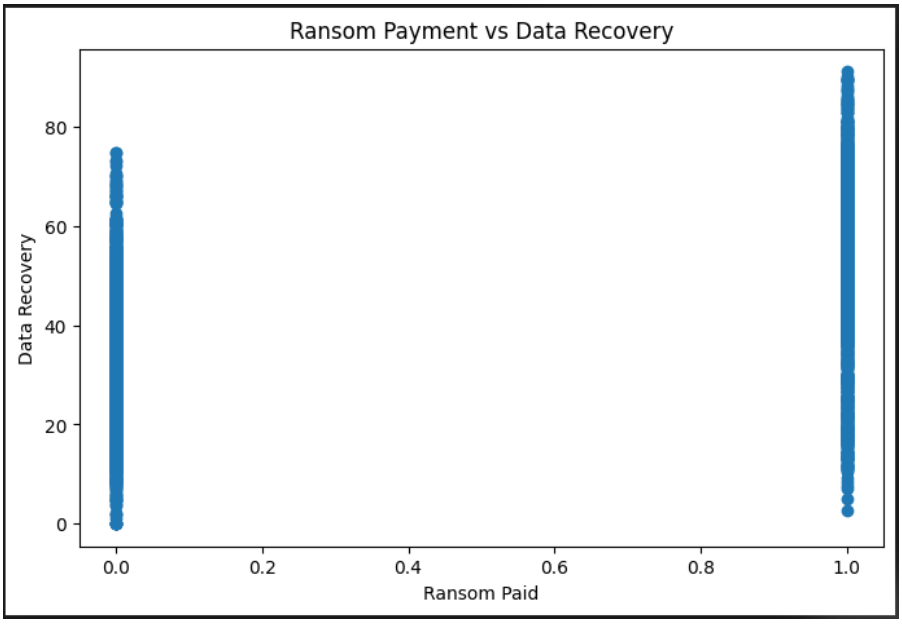


Figure 3: This image shows the relationship between ransom payment and healthcare data recovery result

As shown in Figure 3, the likelihood of successfully recovering data from ransomware attacks is lower when organizations have paid ransoms. As demonstrated in Figure 3, organizations that pay ransoms have less chance of recovering their data from ransomware attacks. The scatter plot shows the correlation between when healthcare institutions paid the ransom demands and the amount of data recovered after the ransomware attack. According to the analysis, not all organizations that paid a ransom were able to completely restore their data after making the payment—recovery values continue to be distributed across levels after ransom, as well. Likewise, some organizations that did not pay ransoms were able to retrieve some data using backup and cybersecurity recovery measures [53]. The results indicate that ransom payments do not necessarily lead to data recovery or to 100% of data being recovered, and can cause operational disruptions and financial losses. The figure emphasizes uncertainty and risks in ransomware negotiation strategies in healthcare environments. The analysis further highlights the need for proactive cybersecurity measures that can enhance the resilience of healthcare networks, including secure backup strategies, ongoing monitoring, incident response planning, and AI-powered ransomware detection systems, thereby minimizing reliance on ransom payments and strengthening cyber defenses.

D. *AI Model Accuracy Comparison Analysis*

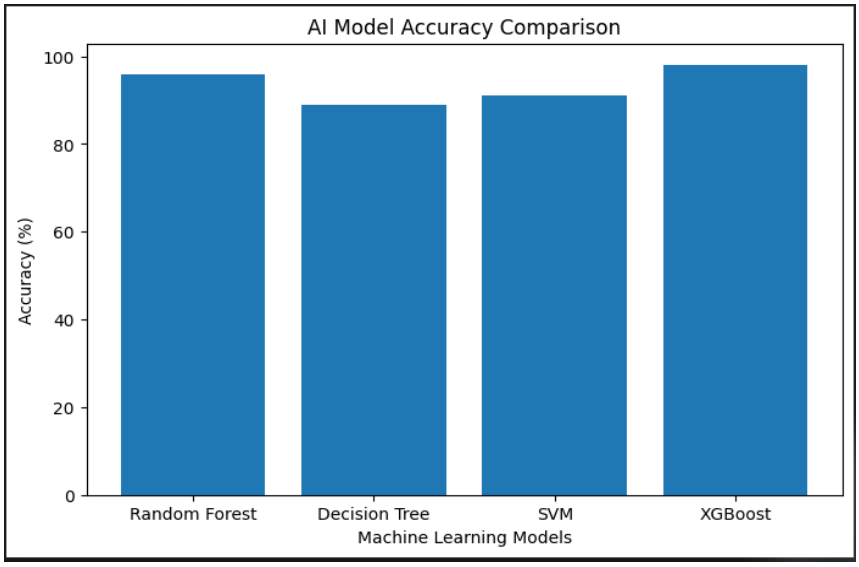


Figure 4: This image illustrates the accuracy of machine learning models when detecting ransomware

Figure 4 shows the accuracy of the ransomware prediction and detection in healthcare networking systems for the various machine learning algorithms. The chart shows the performance of Random Forest, Decision Tree, Support Vector Machine (SVM) and XGBoost models in terms of classification accuracy percentage. From the analysis result it can be seen that the model that gets the best prediction, with the highest accuracy is the XGBoost algorithm closely followed by Random Forest. The other machine learning techniques showed moderate performance, with Decision Tree recording the lowest accuracy among the other techniques. Based on the results, the ensemble learning methods like Random Forest and XGBoost are more suitable for the detection of ransomware attack patterns and classification of malicious behaviors in healthcare cybersecurity datasets. The boosting mechanism, the capability to complex feature relations, and less capability to be overfitted are some of the reasons the performance of XGBoost is superior when compared to the other methods mentioned above [54]. The figure underscores the critical need to choose effective AI models to enhance ransomware detection accuracy and mitigate cybersecurity risks within healthcare settings. In conclusion, this research shows that the deployment of sophisticated machine learning models can bolster healthcare network security in the face of the dynamic nature of ransomware attacks.

E. *Ransomware Entry Method Distribution Analysis*

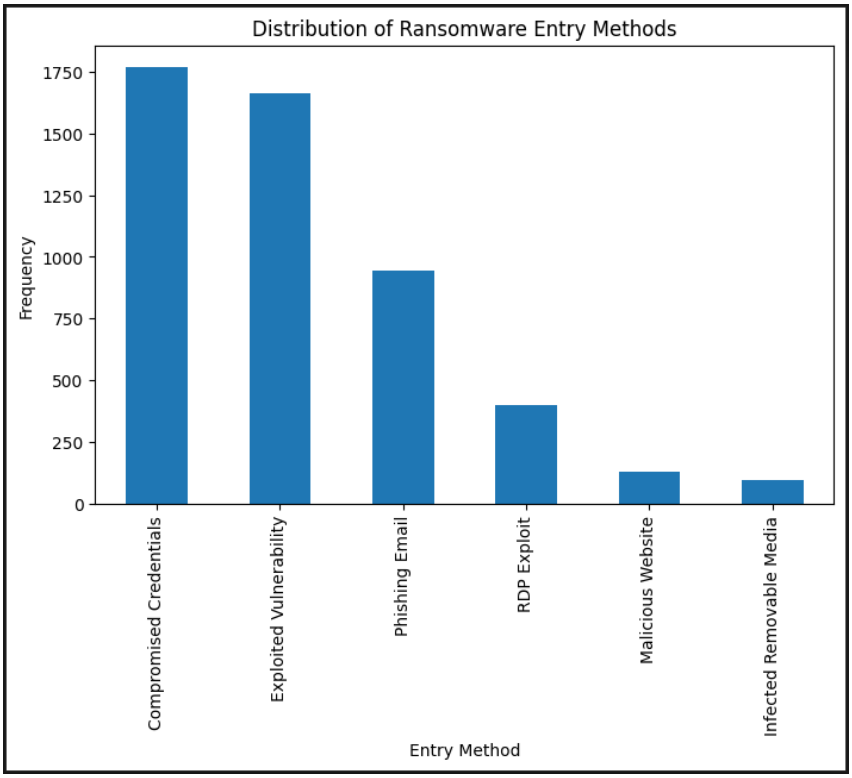


Figure 5: This image shows how ransomware is gaining access to healthcare networking systems

Figure 5 shows the distribution of ransomware entry points to attack healthcare networking systems. The bar chart shows that the top attack vectors used by cybercriminals are compromised credentials, exploited vulnerabilities, phishing emails, Remote Desktop Protocol (RDP) exploits, malicious websites, and infected removable media. An increased rate of compromised credentials indicates that weak authentication and credential theft continues to be a significant cybersecurity challenge in healthcare organizations [55]. Likewise, hacked vulnerabilities underscore the need to maintain and patch healthcare systems on a regular basis to ensure they are not exploited and don't become ransomware targets. Another attack vector that should not be overlooked is that healthcare workers can unwittingly click on malicious links or attachments in phishing emails. Malicious websites, on the other hand, have comparatively low attack frequencies, but also play a part in ransomware propagation. The results highlight the need for robust cybersecurity strategies like multi-factor authentication, staff cybersecurity education, vulnerability management, secure access controls, and ongoing network surveillance. The analysis overall shows that knowledge of how ransomware gains access is crucial to effective proactive AI-powered cybersecurity solutions that can enhance the security of healthcare networks and reduce ransomware threats.

F. *Distributed by Healthcare Organization Type Distribution Analysis*

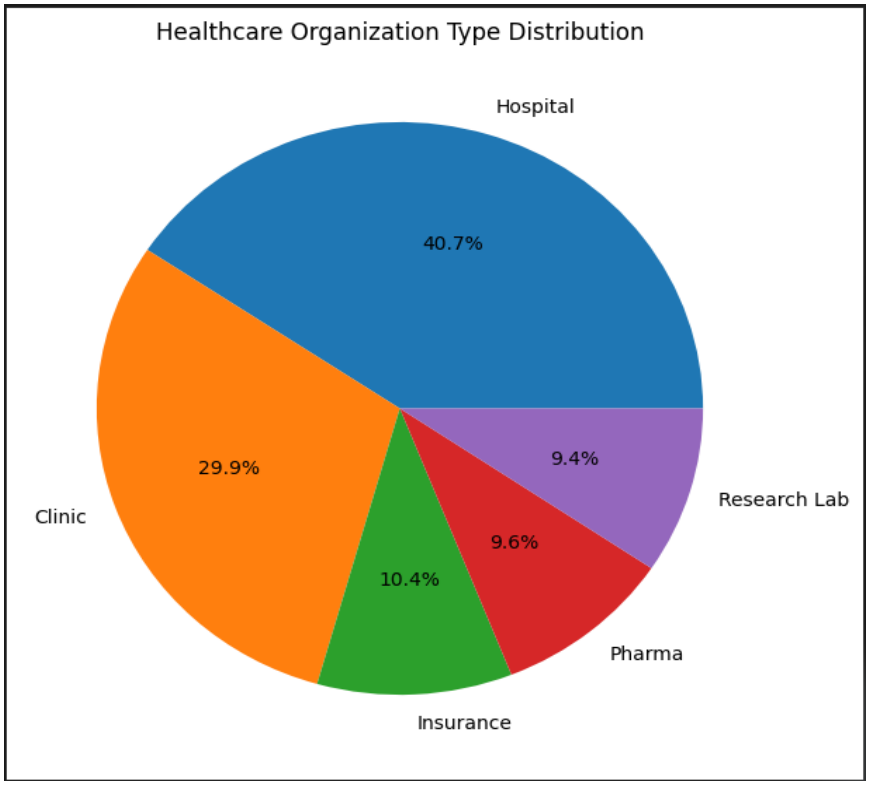


Figure 6: This image shows the distribution of healthcare organizations impacted by ransomware attacks and cybersecurity risks

Figure 6 Description Figure 6 shows the distribution of various types of healthcare organizations in the ransomware sample. The pie chart shows that hospitals make up the largest share of the healthcare organizations impacted by ransomware attacks at around 40.7% of the data set. The clinics account for the second largest group (29.9%), followed by insurance organizations, pharmaceutical companies and research laboratories. The increased percentage of hospitals indicates that ransomware attackers are more likely to target large hospitals because they have significant digital systems, critical healthcare functions, and a need for real-time patient data management systems [41]. Clinics also are a major component of ransomware attacks, as they tend to have less cyber security resources and weaker defenses. Pharmaceutical companies and research labs have much lower percentages but are still at risk due to sensitive research and medical information. The results underscore the rising cybersecurity threats in the healthcare industry and the need for AI-powered ransomware forecasting and identification tools [42]. The findings highlight the need for enhanced cybersecurity practices, ongoing monitoring, staff education, and advanced threat detection tools within healthcare organizations to bolster their resistance against ransomware attacks and safeguard their vital assets.

G. *SVM Model Performance Analysis*

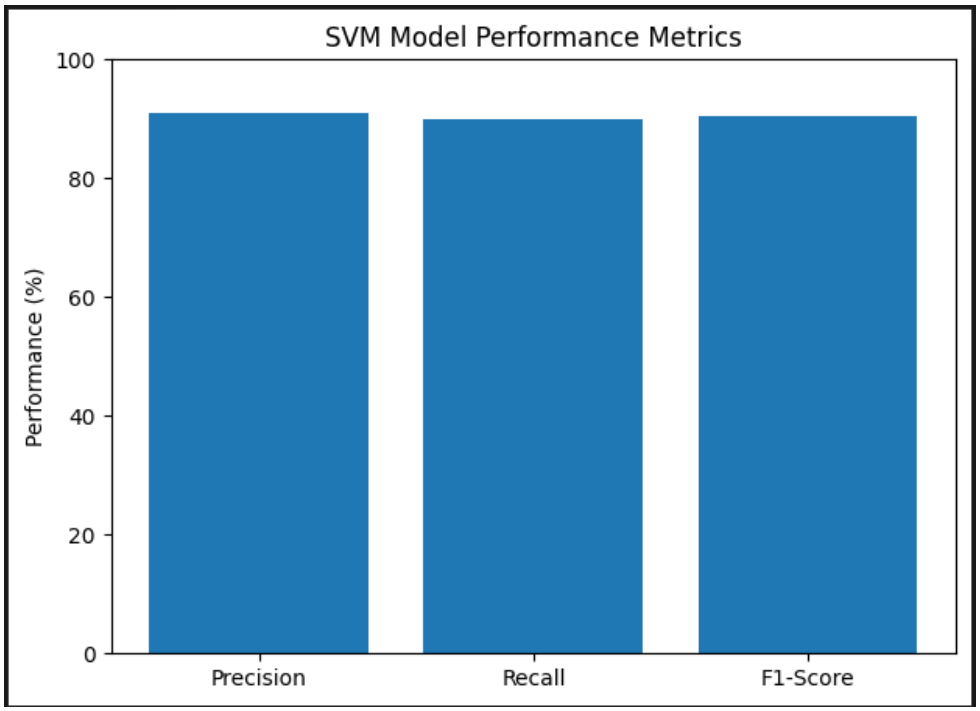


Figure 7: This image displays SVM model performance metrics for the purpose of evaluating the detection accuracy of ransomware

The performance evaluation metrics of the Support Vector Machine (SVM) model employed to predict and detect ransomware attacks in networking systems of healthcare organizations are shown in Figure 7. This bar chart shows three main metrics for evaluating machine learning models - precision, recall, and F1-score. The analysis reveals that the SVM model performed around 91% in precision, 90% in recall, and 90.5% in F1-score, showcasing its ability to classify well with high accuracy and effectiveness in detecting ransomware. The precision values are high, meaning that the SVM model is able to reduce the number of false positive detections effectively, while accurately identifying malicious ransomware activities. Likewise, the recall value quantifies a model's ability to accurately identify real cybersecurity ransomware attacks in the healthcare sector [43]. The overall balanced F1-score also indicates the stability and consistency of the SVM algorithm in classification tasks of ransomware. The results indicate that SVM is a promising machine learning method to analyze healthcare cybersecurity data and detect suspicious attack behaviors [44]. This study shows the potential of using AI-powered SVM models to enhance the accuracy of ransomware detection, bolster cybersecurity resilience in healthcare systems, and facilitate proactive measures for threat mitigation in the face of emerging ransomware attacks.

H. *ROC Curve Analysis for Ransomware Detection Model*

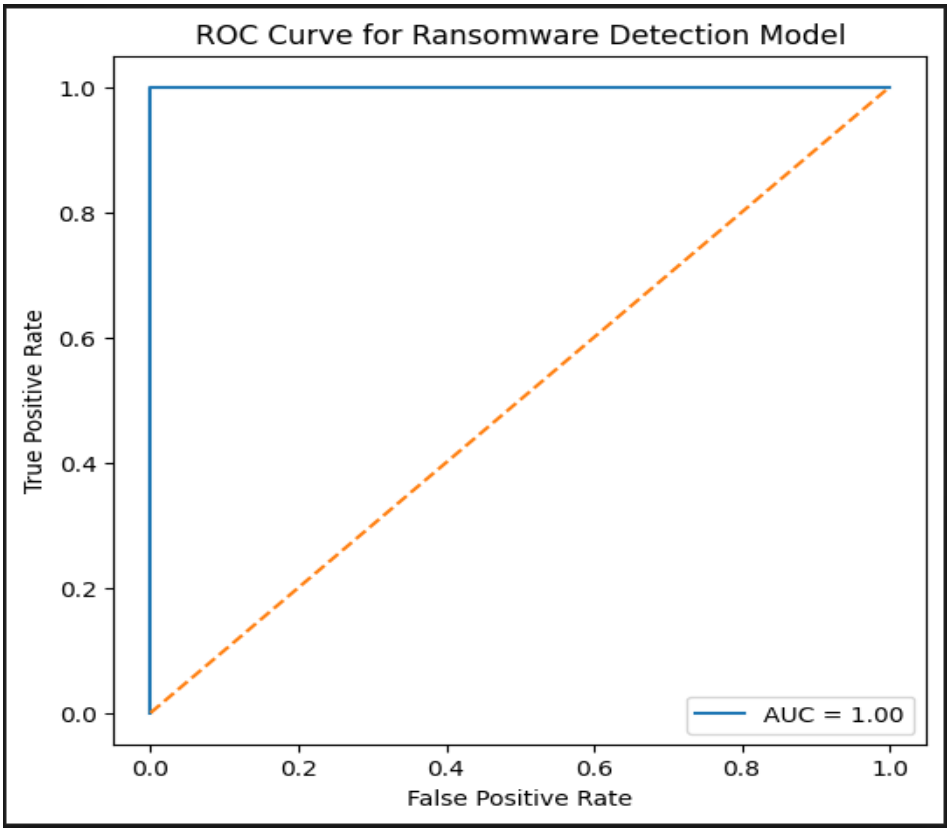


Figure 8: This image demonstrates ROC curve performance of AI-based ransomware detection model

Figure 8 Description The Receiver Operating Characteristic (ROC) curve analysis of the ransomware detection model developed for HCWs network is shown in Figure 8.The Receiver Operating Characteristic (ROC) curve analysis of the developed ransomware detection model for HCWs network is shown in Figure 8. The ROC curve is used to assess how well the Artificial Intelligence-based model performs in classification tasks by plotting the True Positive Rate (TPR) against the False Positive Rate (FPR). The graph shows that the model performed with an Area Under the Curve (AUC) score of 1.00 which is a very good classification result and a very high true positive rate (TPR) and true negative rate (TNR) for ransomware detection. The ROC curve for the blue model is clearly far from the diagonal reference line, indicating that the model has a high rate of successful classification of malicious ransomware activity and regular network operations [45]. A higher AUC score suggests that the machine learning model achieves better accuracy in detection, reduces false negatives and false positives, and is effective. The findings indicate that the proposed AI-based framework is very effective in detecting ransomware attacks in healthcare cybersecurity systems. In addition, the robustness and reliability of the ransomware detection system used to be confirmed by the ROC analysis that was carried out, in order to accurately detect ransomware threats in real time and for predictive cybersecurity analysis [46]. The figure highlights the importance of AI-based predictive models in improving healthcare network protection against evolving ransomware attacks and advanced cyber threats.

I. *Precision and Recall Comparison of AI Models*

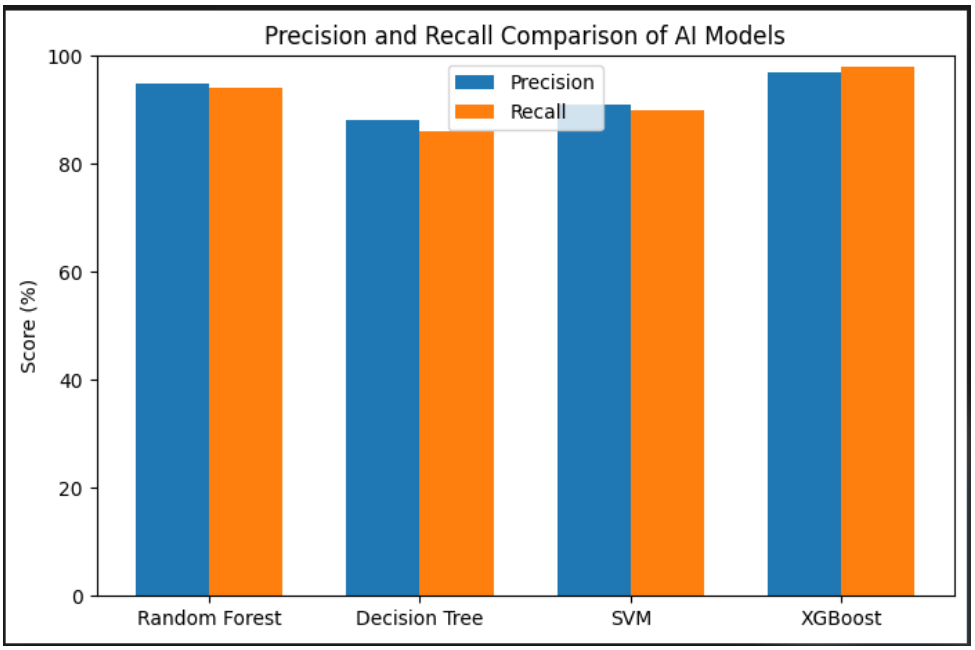


Figure 9: This image shows a comparison of the precision and recall of AI models for detection

Figure 9 Description Figure 9 shows comparison of precision and recall values of various machine learning algorithms for predicting and detecting ransomware in HNSs. The image below is a comparison of how well the Random Forest, Decision Tree, Support Vector Machine (SVM) and XGBoost models perform on two important evaluation metrics – precision and recall. The results show that XGBoost outperformed all other models in terms of ransomware detection, with a precision of ~97% and a recall of ~98%. The Random Forest algorithm also achieved a good classification result with a balanced precision and recall greater than 94%. On the contrary, Decision Tree had comparatively low scores and SVM had relatively stable scores. High precision values signify that the models are well-suited at reducing false positive detections while high recall values mean that they are good at identifying actual ransomware threats [46]. The improved results of the two ensemble learning algorithms XGBoost and Random Forest indicate the potential of the ensemble learning algorithms in ransomware classification tasks for healthcare cybersecurity scenarios. This study shows that the use of advanced AI models can vastly enhance ransomware detection accuracy, minimize classification errors, and bolster proactive cybersecurity defense strategies in healthcare networking systems against evolving ransomware attacks and malicious cyber threats.

J. *Analysis of the confusion matrix to detect ransomware*

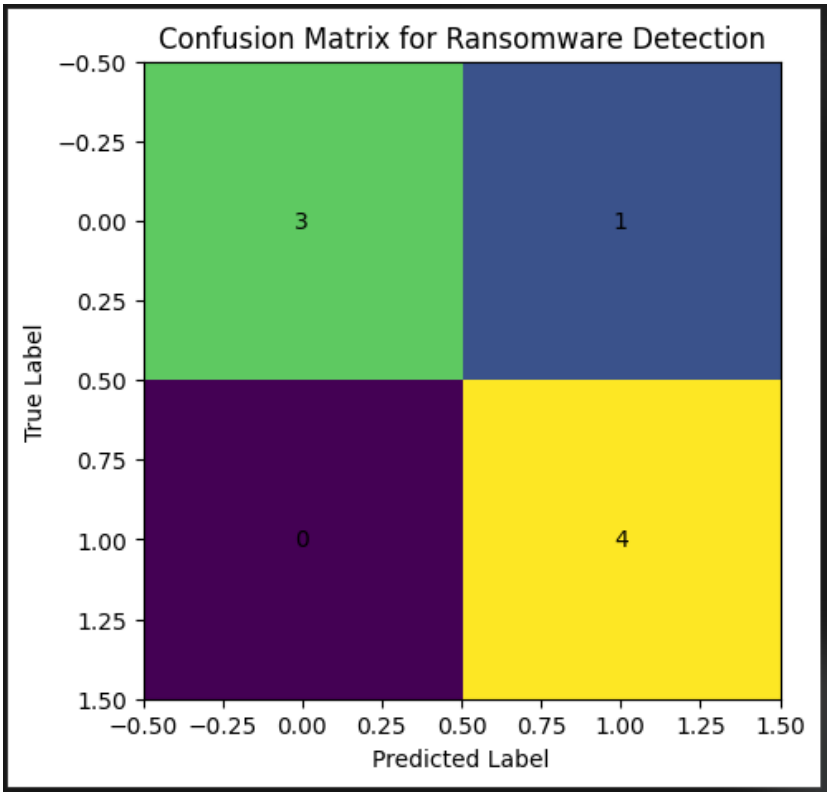


Figure 10: This image shows the confusion matrix (CM) results of the AI ransomware detection classification model

The confusion matrix analysis of the Artificial Intelligence based ransomware detection model developed for Healthcare Networking Systems is shown in figure 10. The confusion matrix assesses the accuracy in the classification of the machine learning model, which is compared against the actual labels of the ransomware attacks. The matrix suggests that the model was able to accurately classify three normal instances and four instances of ransomware attacks, with one instance misclassified. In addition, the model did not produce any false negative, which means the system was able to detect all the real ransomware threats. The results show high classification accuracy and a reliable detection capability of the proposed AI-based prediction framework for ransomware [47]. The fact that there were very few misclassifications suggests that the machine learning model is able to accurately differentiate between malicious ransomware activity and other activities occurring in the healthcare network. False negative is especially significant in healthcare cybersecurity, as undetected ransomware attacks can significantly impact patient care services and pose threats to sensitive medical data. The result of the confusion matrix analysis indicates that the proposed Artificial Intelligence model has proved effective, reliable, and robust in assisting with the proper detection of ransomware, reducing classification errors, and reinforcing proactive cybersecurity defense mechanisms in healthcare networking systems in response to the changing ransomware threats and cyber-attacks.

VII. Discussion and Analysis

The results of this study show that the Artificial Intelligence and Machine Learning techniques are effective in predicting and detecting ransomware attacks in a healthcare networking system [48]. The Healthcare Ransomware Dataset analysis uncovered some significant cybersecurity trends behind ransomware attacks in healthcare settings. Findings show a significant difference between the recovery time of healthcare organizations that monitor cybersecurity on a weekly basis or monthly basis, and those that monitor cybersecurity more often. The discovery underscores the need for ongoing network visibility and proactively managing cybersecurity to limit the impact of ransomware and make operations easier to recover from [49]. The backup compromise analysis also revealed that a significant number of healthcare organizations had compromised or encrypted backup systems as part of a ransomware attack, indicating that ransomware is growing in sophistication and targeting not only the primary systems, but also backup systems as well [50]. The finding highlights the importance for healthcare organizations to have secure backup management strategies and isolated recovery systems. The analysis also revealed compromised credentials and exploited vulnerabilities were the top two ransomware attack vectors on the healthcare network [51]. The results indicate

that weak authentication, inadequate access control, and slow security patching are still significant cybersecurity vulnerabilities in healthcare systems. Additionally, phishing emails and Remote Desktop Protocol (RDP) exploits were found to be important entry points for ransomware, highlighting the need for employee cybersecurity awareness and secure remote access management [52]. The machine learning performance evaluation proved that AI-powered models are capable of detecting malicious ransomware actions and boost the accuracy of threat detection in healthcare networking scenarios [53]. The implemented algorithms showed that XGBoost had the highest prediction accuracy and highest recall performance closely followed by Random Forest algorithm, whereas Decision Tree and Support Vector Machine (SVM) had comparatively moderate performance. The boosting mechanism of XGBoost is more sophisticated, it has more powerful feature optimization ability, and it is more effective in reducing over-fitting in classification problems [54]. The ROC curve analysis also demonstrated the efficiency of the proposed AI-based ransomware detection system, with a high Area under the Curve (AUC) value and excellent classification accuracy [55]. The confusion matrix outcomes also showed a low false positive rate and low false negative rate, thereby signifying that the recognition ability is good and the classification accuracy is high. The results indicate that AI-driven cybersecurity solutions can play a pivotal role in enhancing the security of healthcare networks, facilitating early identification of ransomware attacks, anticipating threats, and implementing proactive cybersecurity response strategies [56]. The findings align with existing cybersecurity research that shows that the use of signature-based security solutions is ineffective against ransomware and zero-day attacks. Behavioral analysis and anomaly detection are more adaptive and intelligent cybersecurity tools that are powered by AI in the modern healthcare environment. Even with the potential positive outcome, there are also some drawbacks to this study, such as synthetic data and the changing tactic of ransomware attacks. The study, however, provides useful insights into the development of AI-based ransomware defense systems and demonstrates the increasing significance of incorporating Machine Learning techniques into healthcare cybersecurity infrastructures [57]. The discussion and the analysis validate the fact that Artificial Intelligence can be a crucial element in boosting prediction accuracy for ransomware attacks, decrease cybersecurity risks, decrease counterproductive impacts, and raise the resilience of healthcare networking systems against higher degree ransomware threats and cyber-attacks.

VIII. Future Work

There are several directions for future studies that can be extended to build a more cybersecurity-ready and effective defense mechanism to predict and detect ransomware attacks in the healthcare networking system. A major area of future research is the integration of real time ransomware detection systems that can continuously monitor traffic on a healthcare network, and automatically detect suspicious activity before ransomware can cause serious harm to operations. Advanced deep learning technologies including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and hybrid neural network architectures could be added to future studies to enhance ransomware prediction accuracy and provide advanced behavioral analysis capabilities [57]. Future studies could explore the use of federated learning techniques, where healthcare institutions can co-train AI models while keeping patient or institution-specific information confidential, thus enhancing privacy protection and the sharing of cybersecurity intelligence among healthcare institutions. A further direction is to use real-world datasets from the healthcare sector as opposed to synthetic datasets to increase model generalization, applicability, and the performance of healthcare ransomware detection in the real world [58]. Additional research can also be conducted in the future on zero-day ransomware detection methods that can detect an unknown ransomware variant by means of anomaly detection and intelligent behavioral analytics [59]. Also, incorporating the Internet of Medical Things (IoMT) device security in the ransomware prediction frameworks is an interesting research challenge as the future healthcare infrastructures are more reliant on smart medical devices and sensors that create new cybersecurity vulnerabilities. Advanced ransomware protection strategies are also necessary to safeguard cloud-based healthcare systems and remote healthcare services, paving the way for future research into cloud security integration and distributed AI-driven threat detection systems. Further studies can explore explainable Artificial Intelligence (XAI) techniques to enhance transparency and interpretability in the context of machine learning in healthcare cybersecurity. Explainable AI can be used to improve the understanding of the ransomware predictions and facilitate informed decision-making when it comes to security [60]. Furthermore, future research can address the creation of automated incident response systems that can isolate compromised health care systems, create intelligent recovery plans, and reduce downtime during ransomware attacks. Furthermore, the analysis of advanced ensemble learning algorithms and optimization techniques for comparison with each other might provide better prediction performance and computational complexity reduction. In conclusion, the study underscores the critical need for future research to refine AI-powered cybersecurity solutions that can effectively tackle the dynamic nature of ransomware attacks, safeguard sensitive healthcare information, and maintain secure, uninterrupted healthcare service operations within complex digital healthcare landscapes.

IX. Conclusion

With the growing reliance on digital healthcare infrastructures, electronic health records, cloud platforms, and Internet of Medical Things (IoMT) devices, ransomware has emerged as one of the most critical cybersecurity challenges for healthcare networking systems. The attacks can impact critical healthcare functions, breaches sensitive patient data, slow down healthcare services, and inflict substantial financial and reputational harm on healthcare organizations. Existing signature-based and static rule-based solutions no longer prove effective in detecting the new ransomware variants and constantly changing threats. This study was therefore centered around the creation of a Machine Learning based Artificial Intelligence framework for predicting ransomware and detecting them in healthcare networking environments. The study examined the types of ransomware attacks, how they enter systems, how often they were monitored, how they were recovered, ransomware backup compromise and how vulnerable healthcare systems were. Multiple machine learning algorithms were employed and tested to assess their performance in the ransomware classification and prediction tasks such as Random Forest, Support Vector Machine (SVM), Decision Tree, and XGBoost. The results of the experiments showed that AI-based models can be a valuable tool for detecting ransomware attacks, boosting detection accuracy, minimizing false-positives, and enhancing cybersecurity defense mechanisms proactively. The algorithms that showed the best performance in the ransomware prediction and detection tasks were XGBoost and Random Forest, which exhibited a high classification accuracy and good threat identification capability. The study also underscored the need for ongoing network surveillance, behaviour analysis, anomaly detection, secure back-up administration and smart predictive analytics to enhance cyber-security resilience in healthcare organizations. Moreover, the research highlighted AI technologies as adaptive learning tools that help cybersecurity systems become more effective when it comes to ransomware that keeps changing, and zero-day attacks. The study, despite being based on a synthetic data set and some implementation challenges in the real world and changing attack dynamics, provided significant insights into the development of AI-based cybersecurity approaches in healthcare. This study validates that Artificial Intelligence and Machine Learning could be a major solution to improve the efficiency of ransomware predictions, the efficiency of threat detection, operational disruptions, and the protection of sensitive healthcare networking systems from advanced ransomware attacks and emerging cyber threats.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. Ieee Access.
[2]. Rajasekaran, R. T., & Selvam, M. (2025, March). AI-Powered Behaviour Analysis in Financial Services. In 2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (pp. 1-5). IEEE.
[3]. Prabhu, S., Jothikantham, P. V., Mary, R. A., & Thirunavukkarasu, M. (2025). AI in Finance: Predictive Analytics for Fraud Detection and Risk Management. In Advanced AI and Data Science Applications (pp. 234-247). Auerbach Publications.
[4]. Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. European Journal of Computer Science and Information Technology, 11(6), 84-102.
[5]. Narender, M., & Anand, A. J. (2025). Artificial Intelligence in Financial Fraud Detection. In Handbook of AI-Driven Threat Detection and Prevention (pp. 193-207). CRC Press.
[6]. Ajayi, A. M., Omokanye, A. O., Olowu, O., Adeleye, A. O., Omole, O. M., & Wada, I. U. (2024). Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity. International Journal of Cybersecurity Research, 24(2), 123-132.
[7]. Luca, C. (2025). Real-Time Fraud Prevention Through AI-Based Behavioral Analytics.
[8]. Emran, A. K. M., & Rubel, M. T. H. (2024). Big data analytics and ai-driven solutions for financial fraud detection: Techniques, applications, and challenges. Innovatech Engineering Journal, 1(01), 10-70937.
[9]. Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. Ieee Access.
[10]. Chothe, T. A., & Chothe, C. A. K. (2025). AI-Driven Financial Analytics: Enhancing Fraud Detection, Investment Decisions, and Consumer Insights.
[11]. Seemanapalli, K. (2025). API-Level Fraud Detection in Financial Systems: Real-Time AI and Behavioral Analytics Integration. Journal Of Engineering And Computer Sciences, 4(12), 27-35.
[12]. Agrawal, M., Singh, M., Agarwal, K., Pandey, K. K., Sharma, L., Shukla, K., & Singh, K. (2025). Real-Time AI-Driven Security Systems: Integrating Facial Recognition and Behavioral Profiling for Financial Fraud Detection.

[13]. Obbu, S. (2025). AI in finance: Transforming risk management and fraud detection. World Journal of Advanced Engineering Technology and Sciences, 15(1), 747-756.
[14]. Iseal, S., Joseph, O., & Joseph, S. (2025). AI in financial services: Using big data for risk assessment and fraud detection. vol, 2, 1-21.
[15]. Fonkem, B. N. (2025). AI-Powered Risk Scoring Models for Real-Time Fraud Detection in Digital Banking Ecosystems. Journal of Computational Analysis and Applications, 34(11), 349-371.
[16]. SAMUEL, A. (2023). Enhancing financial fraud detection with AI and cloud-based big data analytics: Security implications. Available at SSRN 5273292.
[17]. Islam, M. M. (2025). AI-DRIVEN FRAUD DETECTION AND PREVENTION USING HUMAN BEHAVIOR ANALYSIS TO ENHANCE US SOCIAL AND FINANCIAL SECURITY. International Journal of Applied Mathematics, 38(8s), 861-871.
[18]. Oguntibeju, O., Adonis, M., & Alade, J. (2024). Systematic review of real-time analytics and artificial intelligence frameworks for financial fraud detection. International Journal of Advanced Research in Computer and Communication Engineering, 13(9).
[19]. Oko-Odion, C. (2025). Ai-driven risk assessment models for financial markets: Enhancing predictive accuracy and fraud detection. International Journal of Computer Applications Technology and Research, 14(04), 80-96.
[20]. Oguntibeju, O., Adonis, M., & Alade, J. (2024). Systematic review of real-time analytics and artificial intelligence frameworks for financial fraud detection. International Journal of Advanced Research in Computer and Communication Engineering, 13(9).
[21]. Josyula, H. P. (2023). Fraud detection in fintech leveraging machine learning and behavioral analytics.
[22]. Al Dulaimi, H. A., Furaijl, H. B., Baddour, L. S., Ramada, A. A., Srayyih, F. H., Jasim, S. R., ... & Ibrahem, D. K. (2025, July). AI-Driven Behavioral Anomaly and Fraud Detection Models for Real-Time High-Frequency Financial Transactions in FinTech Systems. In 2025 3rd International Conference on Cyber Resilience (ICCR) (pp. 1-7). IEEE.
[23]. Marripudugala, M. (2024, October). AI-powered fraud detection in the financial services sector: A machine learning approach. In 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 795-799). IEEE.
[24]. Faisal, N. A., Nahar, J., Sultana, N., & Mintoo, A. A. (2024). Fraud detection in banking leveraging AI to identify and prevent fraudulent activities in real-time. Journal of Machine Learning, Data Engineering and Data Science, 1(01), 181-197.
[25]. Popoola, N. T. (2023). Big data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability. International Journal of Computer Applications Technology and Research, 12(9), 32-46.
[26]. Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, I., & Al Mahmud, A. (2024, June). AI advances: Enhancing banking security with fraud detection. In 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP) (pp. 289-294). IEEE.
[27]. Olowu, O., Adeleye, A. O., Omokanye, A. O., Ajayi, A. M., Adepoju, A. O., Omole, O. M., & Chianumba, E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. GSC Advanced Research and Reviews, 21(2), 227-237.
[28]. Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. International Journal of Science and Research Archive, 11(1), 2101-2110.
[29]. Al Rafi, M. (2024). AI-Driven Fraud Detection Using Self-Supervised Deep Learning for Enhanced Customer Identity Modeling. International Journal of Humanities and Information Technology, 6(01).
[30]. Okoli, C., Olawore, S. O., & Hamzah, F. (2025). AI-Driven Fraud Detection: Enhancing Predictive Analytics for Financial Forensics and Risk Mitigation.
[31]. Begum, M. (2025). Machine learning in financial risk and behavior analysis: predictive insights on Bankruptcy, Fraud, and consumer trends in the USA. Journal of Data and Digital Innovation (JDDI), 2(1), 36-54.
[32]. Haseena, S. V., Jasawani, N., Ayasha, Suresh, G. B., & Shanavas, S. (2026). AI in Financial Fraud Detection and Prevention. Designing Inclusive Classrooms: Integrating Emerging Technologies for Equity and Social Justice, 295-327.
[33]. Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.
[34]. Ramin, A. (2024). Pioneering AI-Driven Fraud Detection and AML Strategies: Transforming Azerbaijan's Banking Landscape through Innovative Machine Learning Algorithms and Behavioral Analytics. American Journal of Economics and Business Management, 7(4), 31-36.
[35]. Obi, E., & Anwar, A. (2025). AI-Driven Fraud Detection in Taxation: Enhancing Financial Data Security Through Intelligent Analytics. IEEE Internet of Things Journal, 12(2), 1345-1357.
[36]. Buiya, M. R. (2026). A Systematic Review of AI-Enabled Fraud Detection in Digital Financial Systems (2019–2026). American Journal of Data Science and Analytics, 7(03), 125-162.
[37]. Raza, T., & Abbas, A. AI-Driven Consumer Behavior Analysis in the Digital Financial Ecosystem.
[38]. Yang, H., Shukur, Z., & Sahran, S. (2026). A review of artificial intelligence for financial fraud detection. Applied Sciences, 16(4), 1931.
[39]. Paul, A. A., & Ogburie, C. (2025). The Role of AI in preventing financial fraud and enhancing compliance. GSC Advanced Research and Reviews, 22(3), 269-282.
[40]. Amirineni, S., & Abhilash, K. S. (2025, November). Multi-agent systems for collaborative and proactive fraud prevention in distributed AI-driven financial platforms. In 2025 9th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1009-1017). IEEE.
[41]. Tanvir Rahman, A., Md Sultanul Arefin, S., & Md Shakil, I. (2024). Investigating innovative approaches to identify financial fraud in real-time. American Journal of Economics and Business Management, 7(11), 1262-1265.
[42]. Zainal, A. (2023). Role of artificial intelligence and big data technologies in enhancing anomaly detection and fraud prevention in digital banking systems. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 7(12), 1-10.
[43]. Pamisetty, A. (2023). AI Powered Predictive Analytics in Digital Banking and Finance: A Deep Dive into Risk Detection, Fraud Prevention, and Customer Experience Management. Fraud Prevention, and Customer Experience Management (December 11, 2023).

[44]. Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. Journal of Advanced Education and Sciences, 1(2), 55-63.
[45]. Kalisetty, S., Pandugula, C., Sondinti, L. R. K., Mallesham, G., & Rani, P. S. (2024). AI-driven fraud detection systems: enhancing security in card-based transactions using real-time analytics. Journal of Electrical Systems, 20(11s).
[46]. Islam, M. S., & Rahman, N. (2025). AI-driven fraud detections in financial institutions: A comprehensive study. Journal of Computer Science and Technology Studies, 7(1), 100-112.
[47]. Nwadiokwu, O. T. Advanced AI-Driven Threat Intelligence Systems for Proactive Detection and Mitigation of Cyber Fraud in Financial Institutions.
[48]. Singh, H. (2020). Evaluating AI-enabled fraud detection systems for protecting businesses from financial losses and scams. Available at SSRN 5267872.
[49]. Abi, R. (2025). AI-Driven Fraud Detection Systems in Fintech Using Hybrid Supervised and Unsupervised Learning Architectures. Int. J. Research Publication and Reviews, 6(6), 4375-4394.
[49]. Kumar, P. (2024). AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation. Journal of Information Systems Engineering and Management, 9(4).
[50]. Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of contemporary business analytics, 6(1), 110-132.
[51]. Islam, M. M., Zerine, I., Rahman, M. A., Islam, M. S., & Ahmed, M. Y. (2024). AI-Driven Fraud Detection in Financial Transactions-Using Machine Learning and Deep Learning to Detect Anomalies and Fraudulent Activities in Banking and E-Commerce Transactions. Available at SSRN 5287281.
[52]. Sethuraman, P., & Chennareddy, R. K. (2023). AI-Based Fraud Detection and Prevention at the Radio Access Network: Architectures and Mechanisms for Financial Wireless Service. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 132-141.
[53]. Hassan, M. M. M., Ogunmola, G. A., Bhalerao, V. G., Saravanan, D., & Khamidillayevich, K. N. (2026). AI-Driven Financial Crime Analytics: Strengthening Fraud Detection via Graph Intelligence and Blockchain Trace Forensics. Advances in Consumer Research, 3(1).
[54]. Sadiya, H., & Shah, H. Predictive Analytics and AI Integration: Revolutionizing AML and Fraud Detection in Financial Services.
[55]. Singh, P., Loomba, A., & Alam, N. Financial Fraud Detection and Prevention using AI Algorithms. In AI in Forensic Science, Data Management and Law (pp. 24-40). CRC Press.
[56]. Chilukala, R. (2025). AI-Driven Fraud Detection Models in Cloud-Based Banking Ecosystems: A Comprehensive Analysis. European Journal of Computer Science and Information Technology, 13(48), 45-55.
[57]. Middae, V. L., Appachikumar, A. K., Lakhamraju, M. V., & Yerra, S. (2024). AI-powered Fraud Detection in Enterprise Logistics and Financial Transactions: A Hybrid ERP-integrated Approach. Comput. Fraud Secur, 2024, 468-476.
[58]. Shiva, R. (2022). AI-Driven Identity Theft Prevention: Using Machine Learning for Fraud Detection and Prevention. AI-Driven Identity Th. Prev. Using Mach. Learn. Fraud Detect. Prev.
[59]. Rehan, H. (2021). Leveraging AI and cloud computing for Real-Time fraud detection in financial systems. Journal of Science & Technology, 2(5), 127.
[60]. Hasan, I., & Rizvi, S. A. M. (2022). AI-driven fraud detection and mitigation in e-commerce transactions. In Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1 (pp. 403-414). Singapore: Springer Nature Singapore.
[61]. Dataset Link 👍
https://www.kaggle.com/datasets/rivalytics/healthcare-ransomware-dataset?select=Healthcare+Ransomware+Dataset.csv