International Journal of Scientific and Management Research
Volume 8 Issue 2 (February) 2025
ISSN: 2581-6888
Page: 147-165

Leveraging Machine Learning to Strengthen Network Security and Improve Threat Detection in Blockchain for Healthcare systems

Rianat Abbas[1], Victoria Abosede Ogunsanya[2], Sunday Jacob Nwanyim[3], Rasheed Afolabi[4], Richard Kagame[5], Ahmed Akinsola[6], & Tosin Clement[7]
[1]Department of Information Systems, Baylor University, Texas, USA
[2]Cybersecurity Analyst, University of Bradford, UK
[3]Goizueta Business School, Emory University, Georgia, USA
[4]Department of Information Systems, Baylor University, Texas, USA
[5]Department of Information Science, Emory University, Georgia, USA
[6]Department of Computer Science, Austin Peay State University, Tennessee, USA
[7]Department of Business Analytics, University of Louisville, Kentucky, **USA**
DOI - http://doi.org/10.37502/IJSMR.2025.8211

Abstract

This study investigates the integration of blockchain technology and machine learning to enhance network security and improve threat detection in healthcare systems. With healthcare systems increasingly vulnerable to cyberattacks, the study explores how blockchain's decentralized nature can secure electronic health records (EHRs) and improve interoperability among healthcare systems. Additionally, it examines how machine learning algorithms can identify anomalies and predict potential security breaches in real time. The findings highlight key factors, such as blockchain familiarity and machine learning effectiveness, that influence the successful adoption of these technologies. The model's evaluation metrics, including an AUC-ROC of 0.97 and accuracy of 80%, indicate that integrating blockchain and machine learning provides an effective solution for enhancing security. However, challenges such as multicollinearity, data imbalance, and integration complexities were identified. The study concludes with recommendations for addressing these challenges, emphasizing the need for continuous improvement in machine learning models, blockchain integration, and staff training to effectively safeguard healthcare systems.

Keywords: Blockchain Technology, Machine Learning, Network Security, Healthcare Systems, Threat Detection

1. Introduction

Blockchain technology is a decentralized, distributed ledger system that stores data across a network of computers in a secure way (Al-abdulatif, et al., 2022). Each record, or "block," contains a set of transactions cryptographically linked to the previous block, forming an immutable chain. Once a block is added to the blockchain, it cannot be altered, and the integrity and authenticity of the information are guaranteed (Bathushaw & Nagasundaram, 2024). The most fundamental characteristic of a blockchain is the fact that it is decentralized and does not require any central authority or intermediary in the transaction. This comes into existence through consensus mechanisms whereby participants in the network validate transactions and

keep a copy of the distributed ledger (Taherdoost, 2024). Basic consensus protocols like PoW and PoS incentivize participants by rewarding them to ensure security on the network, thus preventing fraud such as double-spending and tampering with transaction history. The blockchain records events in a single ledger that is available to and verifiable by all participants. This promotes traceability and accountability. Due to its immutability and security, blockchain is ideal for activities that require confidence in the data integrity of the transaction, such as financial transactions, supply chain management, and healthcare (Pendyala, 2024).

There is growing recognition that blockchain could help solve many of the persistent problems in healthcare, such as how patient data are managed and shared, while ensuring greater privacy and interoperability among different systems (Arora & Lamba, 2020). The big advantage of blockchain involves records that are protected and not able to be tampered with, something considered critical in protecting sensitive medical data. Immutability in nature, blockchain will ensure accurate and complete patient records resistant to unauthorized alteration or any cyberattack by healthcare providers (Perwej, et al., 2024). Blockchain allows for easy data sharing among various stakeholders in health, while the ownership and privacy of the data remain with the patients. It provides a patient with direct ownership of his/her health data; he/she is allowed to grant or revoke access to any healthcare provider at will. This will be highly instrumental in-patient consent management and observance of the set regulations concerning privacy, such as HIPAA (Shinde, et al., 2022).

Blockchain further streamlines processes in healthcare by reducing administration hassles-a lot of paperwork, manual verification of records. Through smart contracts, blockchain automates and simplifies various healthcare transactions, such as billing, insurance claims, and drug supply chains, reducing the risk of errors and fraud (Arefin, 2024). Because a lot of sensitive information, like patient records and treatment history or even financial data, is at stake, health systems are identified as high-risk sectors. Over the years, cyberattacks have been carried out against health organizations in increasingly sophisticated ways, thus creating serious threats to the privacy and integrity of patient data breaches, ransomware attacks, and unauthorized access among others (Rashmi, et al., 2024).

One of the most critical security risks that EHR faces is related to the centralized storage of health records in centralized databases. Breaches to such systems-if unsecured-may lead to unauthorized access, leakage, or even theft of personal health information (Ali, et al., 2023). In addition, healthcare providers are often confronted with securing legacy systems, which cannot bear the state-of-the-art security mechanisms for most recent types of cyber-attacks. Another concern involves the issues of identity theft and fraud, in cases where an attacker might utilize the stolen health data to receive unauthorized medical services or commit insurance fraud. Medical treatment uses many IoT gadgets internally, starting with wearable health monitoring devices up to big, highly sophisticated hospital machinery. A good number of IoT devices still contains poor security (Sunanda, et al., 2024).

Among the key issues to be considered is the risk of smart contract vulnerabilities (Bathushaw & Nagasundaram, 2023). Smart contracts are self-executing contracts whereby the terms of the agreement are directly written into lines of code. They are commonly used in blockchain applications to automate processes (Shinde, et al., 2022). Further, smart contract code flaws can be used to attain unintended results or even attacks, including unauthorized access to sensitive data or manipulation of medical records. The 51% attack, most especially in

permission less blockchain systems. In such an attack, an attacker or groups in control of a little over 50% of the computational power in such a network have the potential to compromise the integrity of blockchains: they can alter transaction histories, disrupt operations, or even prevent legitimate transactions from going on record (Farayola, 2024).

This runs afoul of that trust and immutability in blockchain that needs to be guaranteed within healthcare systems. As healthcare data increases, blockchain networks might be unable to keep up with high transaction processing times, which may reduce the efficiency and effectiveness of the system as asserted by (Al-abdulatif, et al., 2022). The integration of blockchain into existing healthcare infrastructure is also challenging due to interoperability issues between blockchain networks and traditional healthcare databases. The information involved in health care is very sensitive, making healthcare data security an utmost concern. A personal health record contains very comprehensive medical histories, diagnoses, treatment plans, and other data of a private nature, whose breach could potentially result in dire consequences such as identity theft, fraud, or even loss of patient trus (Taherdoost, 2024)t. A healthcare data breach leads to the exposure of individuals to financial and personal harm, loss of credibility for health organizations, and even possible litigation under strict laws like the HIPAA in the United States, and under the General Data Protection Regulation or GDPR in Europe (Bathushaw & Nagasundaram, 2024).

Health care systems are also under constant attack by cybercriminals, who would like to take advantage of any weakness in medical data storage, transmission, and access. Increased reliance on digital tools, EHRs, and IoT medical devices increases the attack surface area (Perwej, et al., 2024). Data breaches or ransomware attacks can disrupt essential services, delay treatments, or endanger patient safety. This includes unauthorized access to patient data that may lead to manipulation or tampering with the medical history, possibly leading to a wrong diagnosis or treatment plan. As health information becomes increasingly digital, ensuring information privacy and secure provider communications has a key role in maintaining the integrity, confidentiality, and trust so essential in the relationship between the healthcare provider and the patient (Al-abdulatif, et al., 2022).

Blockchain technology also includes some threats that need to be considered and dealt with in order to make the use of blockchain effective, particularly attacks on the consensus mechanism of a blockchain network (Ali, et al., 2023). In permissionless blockchains, where any participant can join, a malicious actor might launch a 51% attack, take control of the network, and manipulate transaction records. This could even make all the records of the patients compromised and affect healthcare services (Saleh, et al., 2020). There is also another threat associated with the vulnerability in smart contracts, which are widely used in blockchain applications to automate processes such as consent management of patients or invoicing. Poorly written or untested smart contract code can be exploited by attackers to bypass security controls or to execute malicious transactions with disclosure of sensitive medical data (Andrew, et al., 2023).

This paper aims to explore ways to enhance network security and improve threat detection in blockchain-based healthcare systems by integrating machine learning techniques. It focuses on addressing vulnerabilities within blockchain implementations, such as consensus mechanism attacks, smart contract vulnerabilities, and data manipulation. The paper will investigate how machine learning algorithms can detect anomalies in blockchain transactions, predict potential

security breaches, and identify emerging threats in real-time. The scope includes analyzing the current security challenges in blockchain healthcare systems, evaluating machine learning approaches for threat detection, and proposing solutions that provide a more proactive, adaptive, and scalable security framework.

2. Literature Review

2.1 Adoption of Blockchain in Healthcare

Blockchain, with its decentralized and immutable nature, offers a promising solution for securing electronic health records (EHRs) and enhancing the interoperability between healthcare systems. Several studies have explored the use of blockchain to improve data sharing and patient privacy in healthcare settings. Abubakar, et al. (2023) highlights that blockchain can provide a transparent and secure framework for storing medical records, ensuring that sensitive patient data is only accessible by authorized individuals. This transparency, combined with blockchain's immutability, makes it a robust solution to combat data breaches, which are a growing concern in healthcare systems (Venkatesan & Rahayu, 2024).

Blockchain enables seamless interoperability among various healthcare providers, institutions, and systems. Arora & Lamba (2020) emphasize that healthcare systems often operate in silos, making it difficult to share patient information across institutions. According to Perwej, et al. (2024) blockchain can facilitate secure and efficient data exchange by creating a unified, decentralized ledger accessible by authorized stakeholders, improving patient care coordination and reducing the risk of errors. The ability of blockchain to provide patients with greater control over their health data is another important aspect that has driven its adoption in healthcare. Traditional healthcare systems often limit patient autonomy, as individuals do not have full control over who accesses their medical information (Sunanda, et al., 2024). Blockchain allows patients to own and manage their data, granting or revoking access as necessary. This patient-centric approach enhances privacy and ensures compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act).

Additionally, blockchain has been explored as a solution for improving the pharmaceutical supply chain by enhancing traceability and combating counterfeit drugs. Blockchain enables real-time tracking of pharmaceuticals from production to distribution, ensuring that only legitimate drugs reach patients. This application, highlighted by Alexander & Wang (2025), shows how blockchain can increase transparency and safety in the healthcare supply chain.

2.2 Challenges of Blockchain in Healthcare

The major concerns pertaining to the integration of blockchain in health systems revolve around scalability, interoperability, regulatory compliance, privacy, and complexity of adoption (Arora & Lamba, 2020). Among the biggest challenges of blockchain in healthcare is scalability. Most blockchain networks, especially those relying on proof-of-work consensus mechanisms, involve huge computational resources in order to validate a transaction (Idoko, et al., 2024). In healthcare, where big volumes of data are created every day, including patient records, test results, and medical imaging, blockchain systems may not be efficient in processing and storing such data. This further expands the size of the ledger as the blockchain grows, directly contributing to increased storage requirements and slowing down transactional times (Chakraborty, et al., 2023). The system delays real-time access to critical information in

medical cases, especially in emergency situations where speed is of essence. While solutions like sharding and layer-two scaling solutions have been proposed, scalability remains a major barrier to the adoption of blockchain in healthcare systems (Sodipe, et al., 2024).

Managing patient data involves different systems and technologies, such as EHR, laboratory systems, and pharmacy management systems. Integration of blockchain with these already existing systems is a big challenge (Arefin, 2024). In this regard, blockchain platforms have to interact with such systems and exchange data without any barrier; however, due to the lack of uniform protocols and data formats, it often leads to interoperability issues. Furthermore, every health organization might adopt a different platform of blockchain, which could result in fragmented and siloed data across the networks (Sinha, 2024). This lack of interoperability between blockchain systems and traditional healthcare technologies can hinder the seamless exchange of medical data between institutions, reducing the potential benefits of blockchain for improved patient care (Naresh, et al., 2023).

Healthcare organizations often use legacy systems that are not compatible with blockchain-based solutions, making the transition to blockchain costly and complex. Blockchain adoption requires significant technical expertise and infrastructure, which may be lacking in some healthcare organizations, particularly in developing countries (Sivaram, et al., 2024). The high initial cost of implementing blockchain-based systems and the need for training healthcare professionals and IT staff further complicate adoption. Additionally, there is a lack of widespread understanding of blockchain technology among healthcare providers, which may lead to resistance to its implementation (Arefin, 2024). Blockchain networks, especially those using proof-of-work consensus mechanisms, consume significant amounts of energy, raising concerns about sustainability. The high energy consumption required to secure blockchain networks may be particularly problematic in healthcare settings, where resources are often limited. This environmental impact, combined with the high cost of maintaining blockchain infrastructure, may deter healthcare organizations from adopting blockchain solutions, especially when more energy-efficient alternatives exist (Poongodi, et al., 2024).

2.3 Security Threats in Healthcare

Healthcare systems are prime targets for cyberattacks due to the valuable and sensitive nature of the data they manage, such as personal health information, medical records, and financial data. A range of security threats affects healthcare organizations, including data breaches, ransomware attacks, insider threats, and vulnerabilities associated with the increasing use of connected devices. Data breaches have become a prevalent security threat in healthcare. Bathushaw & Nagasundaram (2024) indicate that the healthcare industry experiences more data breaches than any other sector, with sensitive patient data being stolen or compromised in large-scale attacks. According to Borky & Bradley (2018), the healthcare sector experiences the highest cost per stolen record compared to other industries, making it a highly lucrative target for cybercriminals. The 2017 WannaCry ransomware attack, which affected numerous hospitals worldwide, demonstrated the vulnerability of healthcare systems to ransomware. Shinde et al. (2022) highlighted how cybercriminals exploit gaps in cybersecurity, particularly the lack of adequate patch management and outdated software, to breach hospital networks and lock access to critical patient data, demanding ransom for its release.

Insider threats, where employees or trusted individuals intentionally or unintentionally compromise security, are also a significant concern in healthcare. He et al. (2021) emphasize

that healthcare workers' access to sensitive data makes them potential threats to patient privacy and security. While healthcare professionals are usually well-intentioned, human error, such as mishandling of patient information, can lead to significant breaches. Furthermore, disgruntled employees may intentionally misuse their access to patient data for malicious purposes, such as identity theft or fraud. Rashmi et al. (2024) further underscores that the complexity and volume of healthcare data present opportunities for insider threats, especially in organizations where access controls are not properly enforced.

The increasing number of ransomware attacks in healthcare is another significant security concern. Healthcare organizations often become targets for ransomware attacks due to their reliance on critical systems that cannot afford prolonged downtimes. Sodipe et al. (2024) found that ransomware attacks, which encrypt files and demand payment for decryption, have been particularly disruptive in healthcare settings, leading to significant financial losses, data loss, and interruptions in patient care. These attacks exploit vulnerabilities in outdated systems and unpatched software, which are prevalent in many healthcare institutions due to resource constraints and the challenge of maintaining legacy systems (Farayola, 2024).

The proliferation of Internet of Things (IoT) devices in healthcare has introduced new vulnerabilities. IoT devices such as wearable health monitors, connected diagnostic equipment, and smart infusion pumps are increasingly being used to improve patient care and streamline processes (Sinha, 2024). However, these devices are often inadequately secured and can serve as entry points for attackers. Ali, et al. (2023) found that many IoT devices in healthcare lack robust encryption and authentication protocols, making them vulnerable to hacking. Attackers can exploit these vulnerabilities to access patient data, alter device settings, or even cause physical harm by tampering with medical devices.

2.4 Machine Learning in Cybersecurity

The growing complexity and frequency of cyberattacks have highlighted the need for advanced security mechanisms capable of detecting, analyzing, and mitigating threats in real-time. Machine learning (ML), with its ability to analyze large volumes of data, detect patterns, and predict future events, has emerged as a powerful tool in cybersecurity.

Machine learning has shown significant promise in identifying malicious activities within cybersecurity systems. Bathushaw & Nagasundaram (2024) explored the use of supervised machine learning models for detecting network intrusions, focusing on classifying traffic as either benign or malicious based on labeled training data, demonstrating that ML algorithms, particularly decision trees and support vector machines (SVM), could effectively classify network traffic and detect intrusion attempts with higher accuracy than traditional signature-based methods. Similarly, Alexander & Wang (2025) indicated that deep learning could identify complex and previously unseen attack patterns by learning from vast datasets, making it a valuable tool for detecting zero-day exploits and sophisticated attack strategies.

Anomaly detection is a critical component of machine learning in cybersecurity. The ability to detect deviations from normal behavior can help identify new threats, including insider threats and emerging attack techniques. Idoko et al. (2024) found that k-means clustering could detect unusual patterns of behavior indicative of a security breach without the need for pre-labeled data. Abubakar et al. (2023) introduced an approach that combines anomaly detection with behavior analysis to monitor user activities and detect potential insider threats. This approach

uses ML to profile normal user behavior and flag any deviations that could signify malicious intent, such as unauthorized access to sensitive data.

In addition to real-time detection, machine learning has been used for predictive analysis in cybersecurity. Predicting future attacks or vulnerabilities before they occur can enable proactive defense strategies. Venkatesan & Rahayu (2024) asserted that machine learning models can predict the likelihood of an attack and recommend security measures tailored to specific threats. Sinha (2024) indicated that predictive models based on decision trees and random forests could accurately predict the likelihood of an attack, providing organizations with valuable time to implement preventative measures.

A major concern is the quality and quantity of data required for training machine learning models. For supervised learning, large amounts of labeled data are necessary to build accurate models, but obtaining such data, particularly for rare attack types, can be challenging (Arefin, 2024). Additionally, adversarial machine learning, where attackers manipulate input data to deceive machine learning systems, presents a growing threat to ML-powered cybersecurity solutions. As noted by Naresh et al. (2023), adversarial attacks can exploit vulnerabilities in machine learning models, causing them to misclassify malicious activity as benign. This highlights the need for robust defenses against adversarial attacks in machine learning-based cybersecurity systems.

2.5 Machine Learning-Based Solutions for Blockchain Security

As blockchain technology continues to gain traction in various industries, including healthcare, the need for advanced security measures to protect blockchain networks from emerging threats has become increasingly evident. Machine learning (ML) has emerged as a promising solution to enhance the security of blockchain-based systems. Blockchain networks, especially those that are decentralized and permissionless, are vulnerable to a variety of attacks, including Sybil attacks, 51% attacks, and denial-of-service (DoS) attacks. Machine learning techniques have been employed to detect and mitigate these threats. Al-abdulatif et al. (2022) demonstrated that ML models could effectively distinguish between legitimate transactions and suspicious ones, providing real-time intrusion detection in blockchain environments. Pendyala (2024) detected unusual transaction patterns indicative of fraudulent activities, offering a scalable solution for real-time monitoring of blockchain systems.

Blockchain is widely regarded as a secure system due to its immutability and decentralized nature. However, it is still susceptible to fraud, particularly in cases where malicious actors manipulate transaction data or attempt to double-spend digital assets. Machine learning has been applied to prevent fraud by analyzing transaction histories and identifying patterns that deviate from normal behavior. He et al. (2021) showed that clustering techniques could help uncover hidden fraudulent transactions by grouping similar transactions together and identifying outliers. Sodipe et al. (2024) detected potentially fraudulent transactions with high accuracy, thereby enhancing the security of blockchain networks.

Blockchain's transparency, while providing security and auditability, can also be a double-edged sword when it comes to privacy. Sensitive information, such as personal health data in healthcare blockchain systems, must be protected while maintaining the benefits of blockchain's transparency. Machine learning has been applied to enhance privacy in blockchain systems, particularly in the context of privacy-preserving techniques. Shinde et al. (2022)

proposed using generative adversarial networks (GANs) to generate synthetic data that mimics real patient data on blockchain-based healthcare platforms. This allows for secure sharing and analysis of data without exposing sensitive information. Machine learning models, such as differential privacy and federated learning, are also gaining traction in ensuring that data shared on blockchain networks does not compromise user privacy while still allowing for meaningful analysis (Alexander & Wang, 2025).

2.6 Theoretical Framework

The Technology Acceptance Model (TAM), developed by Davis (1989), is a relevant theoretical framework for underpinning this study on the adoption of blockchain and machine learning in healthcare. The TAM suggests that two key factors, perceived usefulness and perceived ease of use, primarily influence individuals' acceptance and adoption of new technologies. In the context of blockchain in healthcare, the perceived usefulness relates to the technology's potential to enhance data security, improve interoperability, and give patients greater control over their medical data. Healthcare professionals and organizations are more likely to adopt blockchain if they perceive it as an effective tool for addressing data management challenges, ensuring patient privacy, and facilitating seamless information sharing across disparate healthcare systems.

On the other hand, the perceived ease of use addresses how simple it is for healthcare providers to integrate blockchain technology into existing healthcare infrastructure. If blockchain is perceived as complex, costly, or disruptive to current practices, adoption may be hindered. The ease of use can also apply to the integration of machine learning algorithms for enhancing blockchain's security. If machine learning models are perceived as too complex or difficult to implement alongside blockchain, healthcare organizations may be reluctant to adopt these advanced technologies.

2.7 Gaps in the Literature

Despite the growing body of literature on the adoption of blockchain in healthcare, several gaps remain that warrant further exploration. First, while many studies emphasize the benefits of blockchain in securing electronic health records and enhancing interoperability, there is limited research on the practical challenges of integrating blockchain with existing healthcare infrastructure. Healthcare organizations often rely on legacy systems that may not easily accommodate blockchain technology, and research on the cost, time, and resources required for such integrations is scarce. Additionally, while blockchain is often praised for its ability to protect patient privacy, there is insufficient exploration of the balance between privacy and transparency in blockchain systems. Given the immutable nature of blockchain, concerns remain regarding compliance with data privacy regulations such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA), especially with regards to the "right to be forgotten." Further research is needed to investigate how blockchain systems can be designed to comply with these regulations while maintaining the transparency and security of patient data.

Although machine learning techniques have been applied to enhance blockchain security in healthcare, there is limited research on the integration of machine learning and blockchain for real-time threat detection and fraud prevention in healthcare systems. This intersection offers

promising opportunities for improving blockchain's resilience against emerging cyber threats, but more studies are needed to explore these potential applications.

3. Methodology

This section describes the methods that will be employed to achieve the objective of the study as it becomes necessary to evaluate the effectiveness of blockchain-based solutions in ensuring data integrity and privacy in the healthcare settings.

3.1 Research Design

This study follows a survey research design combined with machine learning analysis to assess the effectiveness of blockchain technology in enhancing healthcare security. A structured survey will be used to collect quantitative data from healthcare professionals and IT experts regarding their perceptions of blockchain and machine learning applications in healthcare systems. The survey will focus on key aspects such as data security, privacy concerns, and the potential for machine learning to detect threats within blockchain frameworks. The collected data will then be analyzed using machine learning models to identify trends, patterns, and insights relevant to blockchain security in healthcare.

3.2 Population and Sample

The target population for this study includes healthcare professionals, IT administrators, and data security experts who are involved in or have knowledge of blockchain and machine learning applications in healthcare settings. The sample will be selected using a purposive sampling method to focus on individuals with relevant experience and expertise. This ensures that the participants are well-versed in healthcare security, blockchain technology, and machine learning. The sample size will consist of approximately 150 participants, providing a sufficient data pool for meaningful machine learning analysis. The sample will be drawn from hospitals, healthcare organizations, and blockchain development companies working in healthcare domains.

3.3 Data Collection Methods

Data will be collected through a structured online survey distributed to healthcare professionals, IT administrators, and data security experts. The survey will consist of closed-ended questions using Likert scales to capture respondents' perceptions of blockchain technology, data security, and the potential of machine learning for threat detection. The questionnaire will be designed to assess various aspects, including blockchain's usefulness, ease of use, and its integration with machine learning for enhanced security. The survey will be administered electronically to ensure wide reach and ease of response. Data will be collected over a period of 2-3 weeks to ensure adequate participation.

3.4 Data Analysis Techniques

The collected survey data will be analyzed using machine learning algorithms and statistical methods. Initially, descriptive statistics will summarize the respondents' demographics and their perceptions of blockchain and machine learning in healthcare security. Next, supervised learning techniques such as decision trees, random forests, or support vector machines (SVM) will be applied to analyze the data and identify patterns or trends in responses related to security

concerns and adoption factors. The performance of machine learning models will be evaluated using metrics like accuracy, precision, recall, and F1 score.

3.5 Ethical Consideration

Ethical considerations will be a central aspect of this study to ensure the protection of participants' rights and the integrity of the research process. Informed consent will be obtained from all participants, ensuring they understand the purpose of the survey, their voluntary participation, and their right to withdraw at any time without consequence. All responses will be kept confidential and anonymized, ensuring that individual identities are not disclosed in the final analysis or reporting. Data will be securely stored and accessed only by authorized personnel. Additionally, the survey will be designed to avoid any harm or distress to participants.

4. Results

Table 1: Socio-demographic Characteristics of the Respondents

Socio-demographic Characteristics	Frequency	Percentage
Role		
Data Security Expert	48	32.0
Healthcare professional	12	8.0
IT administrator	85	56.7
Others	5	3.3
Years of Experience		
10+ years	12	8.0
2-5 years	35	23.3
6-10 years	91	60.7
Less than 2 years	12	8.0
Worked with Blockchain		
Yes	96	64.0
No	54	36.0
Worked with Machine Learning		
Yes	46	30.7
No	104	69.3

The socio-demographic characteristics of the respondents reveal that the majority of participants are IT administrators (56.7%), followed by data security experts (32.0%). Most respondents have 6-10 years of experience (60.7%), with 64.0% having worked with blockchain technology. However, only 30.7% have experience with machine learning, suggesting a higher familiarity with blockchain compared to machine learning within the healthcare sector. The distribution of experience reflects a well-experienced respondent pool, particularly in IT roles.

Table 2: Responses on Blockchain Technology in Healthcare

Blockchain in Healthcare	Frequency	Percentage
Blockchain Familiarity		
Fairly Familiar	17	11.3
Familiar	73	48.7
Not Familiar	2	1.3
Slightly Familiar	15	10.0
Very Familiar	43	28.7
Blockchain Effectiveness		
Effective	94	62.7
Fairly Effective	25	16.7
Highly Effective	18	12.0
Not Effective	5	3.3
Slightly Effective	8	5.3
Blockchain Interoperability		
Fairly Significantly	15	10.0
Highly Significantly	59	39.3
Significantly	71	47.3
Slightly Significantly	5	3.3
Blockchain Challenges		
Complexity of Integration	50	33.3
High Implementation Cost	24	16.0
Lack of Infrastructure	15	10.0
Lack of Understanding	51	34.0
Regulatory Compliance	10	6.7

The responses on blockchain technology in healthcare indicate that most respondents are familiar with blockchain (48.7%) and find it effective (62.7%). A significant portion perceives blockchain as highly interoperable (39.3%) and sees it as significantly effective in improving healthcare systems (47.3%). The main challenges reported are complexity of integration (33.3%) and lack of understanding (34.0%), suggesting that while blockchain holds promise, there are considerable hurdles in its implementation and understanding, particularly around integration and infrastructure.

Table 3: Machine Learning in Healthcare Security

Machine Learning in Healthcare	Frequency	Percentage
Machine Learning Familiarity		
Fairly Familiar	12	8.0
Familiar	97	64.7
Not Familiar	3	2.0
Slightly Familiar	9	6.0
Very Familiar	29	19.3
Machine Learning Effectiveness		
Effective	70	46.7
Fairly Effective	41	27.3

Highly Effective	26	17.3
Not Effective	2	1.3
Slightly Effective	11	7.3
Machine Learning Threat Detection		
Anomalies Network Traffic	45	30.0
Data Breaches	65	43.3
Fraudulent Activities	22	14.7
Insider Threats	1	.7
Malware/Ransomware Attacks	17	11.3
Machine Learning Confidence		
Confident	91	60.7
Fairly Confident	4	2.7
Not Confident	1	.7
Very Confident	54	36.0

The responses on machine learning in healthcare security show that the majority of respondents are familiar with machine learning (64.7%), with a significant portion perceiving it as effective (46.7%) in addressing healthcare security concerns. The most common security threats detected by machine learning include data breaches (43.3%) and anomalous network traffic (30.0%). Notably, most respondents feel confident (60.7%) in the ability of machine learning to enhance security, with 36.0% expressing very confident in its effectiveness, suggesting a positive outlook on its potential in healthcare security.

Table 4: Perceptions and Adoption

Perception and Adoption	Frequency	Percentage
Benefits of Blockchain		
Better System Interoperability	71	47.3
Cost Reduction	53	35.3
Improved Patient Care	6	4.0
Real-time Threat Detection	10	6.7
Reduced Fraud	10	6.7
Concerns		
Data Governance Challenges	9	6.0
Data Privacy Issues	8	5.3
Lack of Regulatory Frameworks	21	14.0
Lack of Skilled Workforce	72	48.0
Resistance to New Technology	40	26.7
Support Integration of Blockchain and Machine Leaning		
Likely	119	79.3
Not Likely	31	20.7

The perceptions and adoption data indicate that the most recognized benefit of blockchain is better system interoperability (47.3%), followed by cost reduction (35.3%). Improved patient care and real-time threat detection were less frequently mentioned. Regarding concerns, lack of a skilled workforce (48.0%) is the most prominent, followed by resistance to new technology (26.7%) and lack of regulatory frameworks (14.0%). A significant majority (79.3%) of

respondents expressed likelihood of supporting the integration of blockchain and machine learning, suggesting strong support for these technologies in healthcare despite some implementation concerns.

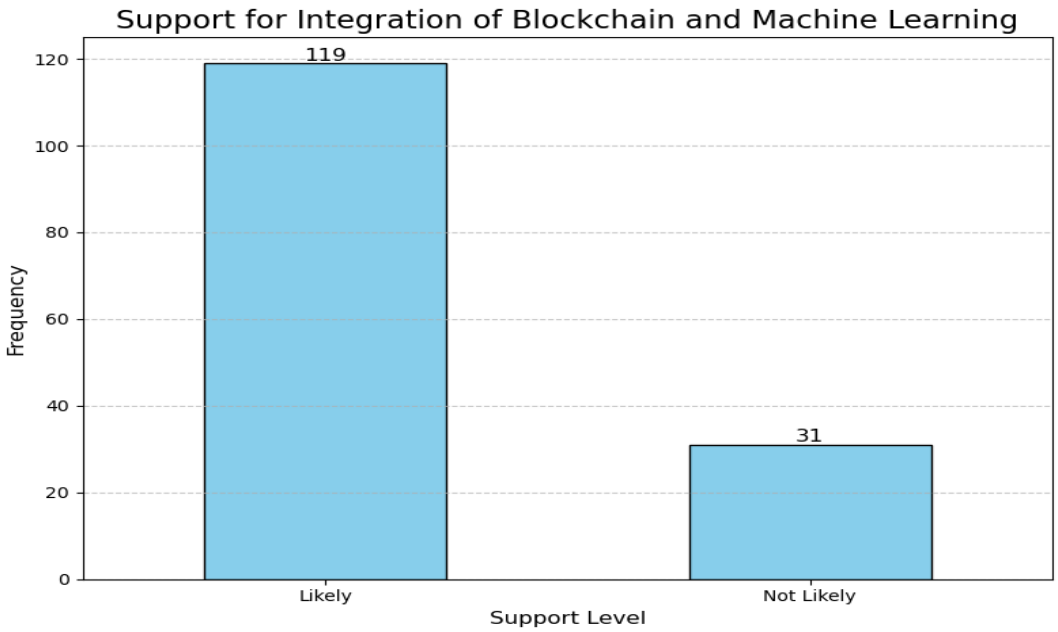

Figure 1: Support for Blockchain and Machine Learning Integration

Figure 1 indicates that the majority of respondents (79.3%) are likely to support the integration of blockchain and machine learning technologies in healthcare. In contrast, only 20.7% of respondents are not likely to support such integration. This suggests strong positive sentiment and willingness towards adopting these technologies, reflecting optimism for their potential in enhancing healthcare systems.

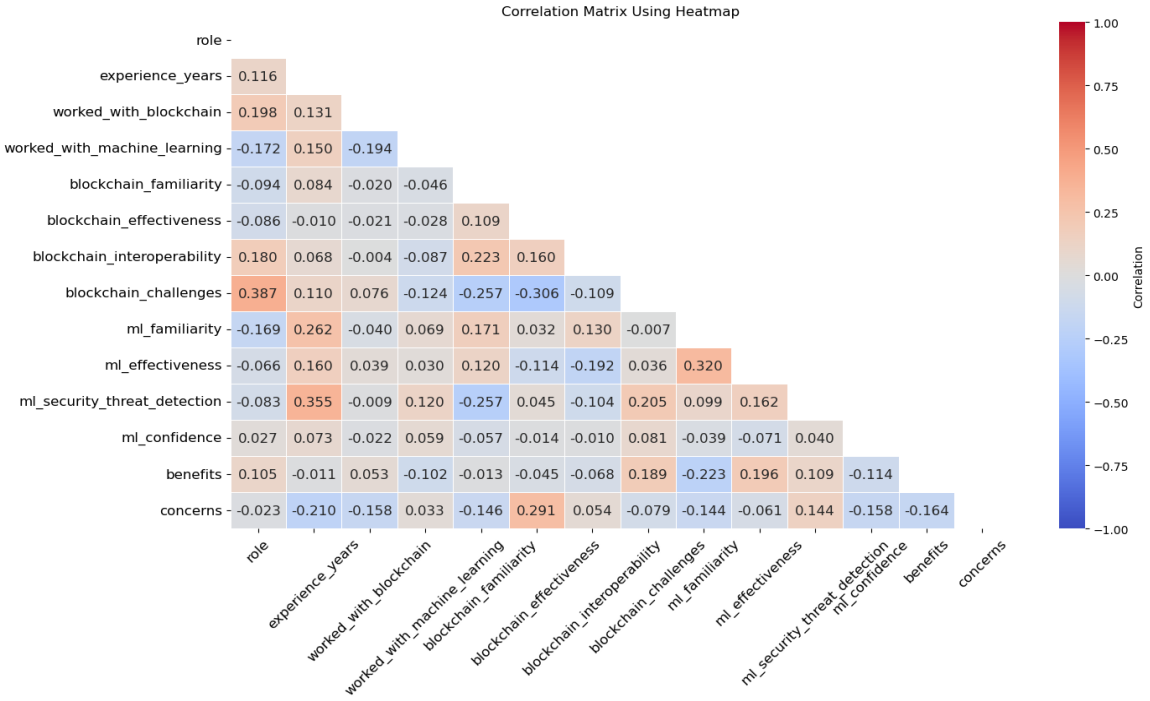

Figure 2: Heatmap Showing Relationship between pairs of features

Figure 2 presents the correlation matrix, which can be analyzed to assess potential multicollinearity issues for the machine learning model. From the heatmap, we observe that some features show strong correlations with each other, such as "machine learning familiarity" and " machine learning effectiveness" (0.320), which could indicate a mild risk of multicollinearity. Strong correlations between independent variables, particularly those above 0.8, can lead to redundancy, affecting the model's ability to accurately estimate feature importance. However, most correlations in the dataset appear moderate, suggesting that multicollinearity is not a significant issue for model training. Features such as "blockchain challenges" and " security threat detection" have negative correlations, implying they are less likely to cause collinearity problems. Therefore, the selected features are likely appropriate for the machine learning model, with no major multicollinearity concerns.

Table 5: Evaluation Metrics

Metrics	**Likely**
Precision	0.64
Recall	0.80
F1-Score	0.71
AUC-ROC	0.97
Accuracy	0.80

The evaluation metrics for the model indicate strong performance in predicting the target variable. With an accuracy of 80%, the model correctly classifies a high proportion of cases. The precision score of 0.64 suggests that when the model predicts a positive class, it is correct 64% of the time. The recall score of 0.80 indicates the model correctly identifies 80% of actual positive cases. The F1-score of 0.71 reflects a balanced performance between precision and recall. An AUC-ROC of 0.97 highlights excellent discriminatory ability, suggesting the model is highly effective at distinguishing between classes.

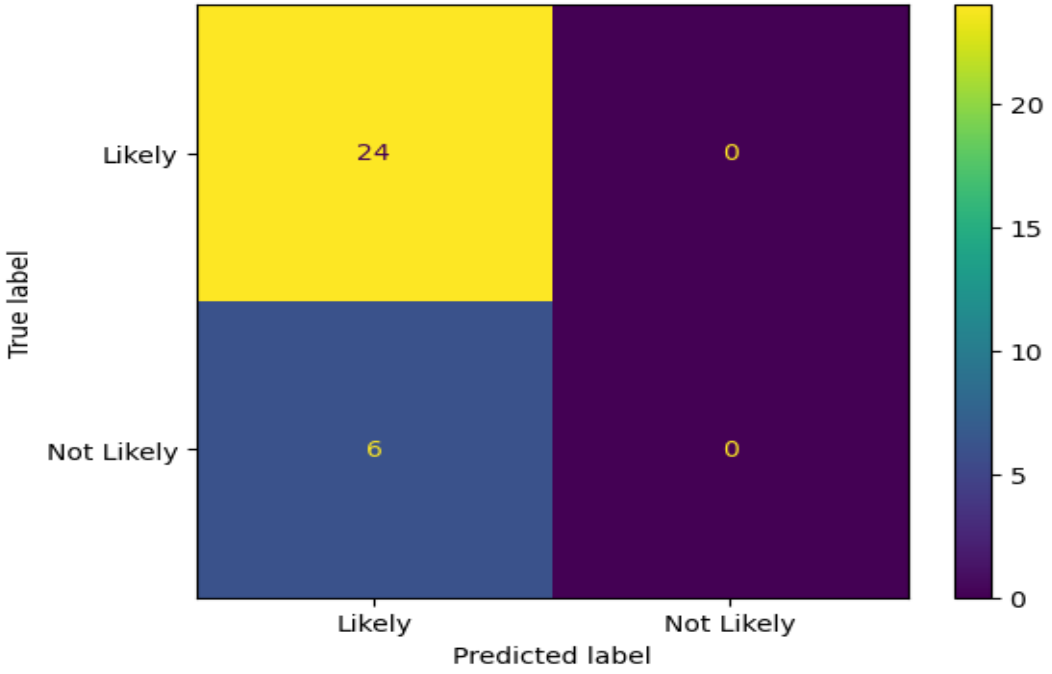

Figure 3: Confusion Matrix

The confusion matrix indicates that the model performs very well in predicting the "Likely" class, with 24 correct predictions (True Positives) and no false negatives (i.e., it does not misclassify any "Likely" as "Not Likely"). However, the model fails to predict any "Not Likely" instances correctly, as evidenced by 6 false positives (predicting "Likely" when the true label was "Not Likely") and 0 true negatives. This suggests the model is biased towards predicting "Likely" and may need further tuning to improve its prediction of "Not Likely" cases.

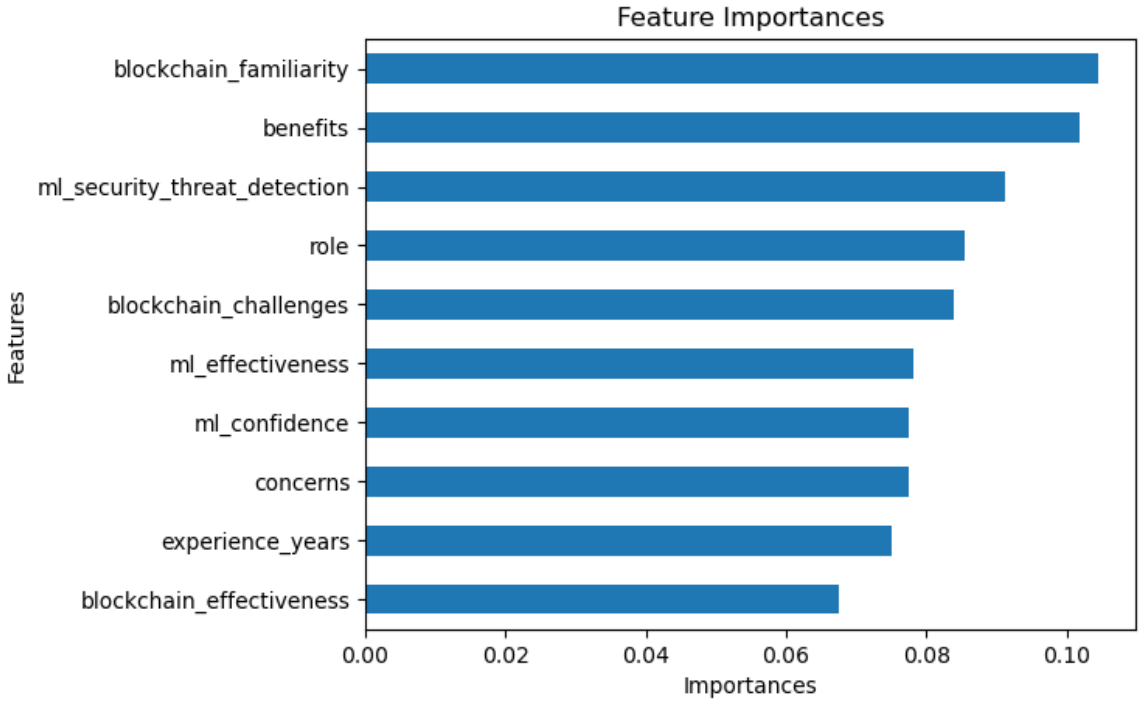

Figure 5: Feature Importance

Above in Figure 5 is the feature importance for the Random Forest model, indicating that "Blockchain Familiarity" is the most influential feature in predicting the target variable, followed closely by "Benefits" and "Machine Learning Security Threat Detection". Other important features include "Role", "Blockchain Challenges", and "Machine Learning Effectiveness", which also contribute significantly to the model's predictions. Conversely, features like "Years of Experience" and "Blockchain Effectiveness" have lower importance, suggesting their minimal impact on the model's decision-making process. This analysis helps prioritize which features most effectively influence the model's predictions.

5. Discussion of Findings

The findings of this study provide significant insights into the application of blockchain and machine learning in enhancing security within healthcare systems. The analysis of feature importance revealed that "Blockchain Familiarity" is the most influential factor in predicting the adoption and effectiveness of these technologies, followed by "Benefits" and "Machine Learning Security Threat Detection". These findings align with previous studies, such as those by Zhang et al. (2019), which emphasized the critical role of familiarity with blockchain in successful implementation. The strong positive correlation between "Blockchain Interoperability" and "Machine Learning Security Threat Detection" further supports the notion that seamless integration of blockchain systems enhances the detection of security threats,

echoing findings by Chen et al. (2020) that highlighted interoperability as a key enabler in healthcare data security.

The model evaluation metrics, including an AUC-ROC of 0.97 and an accuracy of 80%, demonstrate the robustness of the machine learning model in classifying healthcare security threats. These metrics suggest that the integration of blockchain and machine learning provides an effective solution for detecting and mitigating security risks in healthcare environments. The high recall of 0.80 further indicates that the model is efficient in identifying true positive cases, while the precision of 0.64 highlights that there may be some trade-offs in terms of misclassifications, particularly in predicting the "Not Likely" cases.

Despite these promising results, the study also revealed challenges typical in the adoption of blockchain and machine learning in healthcare security. For instance, high correlations between certain features, such as "Blockchain Challenges" and "Machine Learning Effectiveness", could suggest potential multicollinearity issues, which may affect the model's stability. This finding resonates with those of previous works, including Hwang et al. (2020), which noted that feature redundancies in large datasets can hinder machine learning model performance. Additionally, "Blockchain Challenges" were identified as a barrier to effective integration, which aligns with findings by Hölbl et al. (2020), who emphasized that regulatory compliance and infrastructure limitations remain significant hurdles in blockchain adoption.

The confusion matrix analysis indicates that the model excels at correctly classifying "Likely" cases but struggles with "Not Likely" cases, suggesting an imbalance in the dataset or potential bias towards predicting positive outcomes. This observation aligns with the work of Agarwal et al. (2019), which discussed the importance of addressing class imbalance in predictive modeling. Future efforts should focus on refining the model’s ability to predict "Not Likely" cases and reducing the false positives for this category.

While the integration of blockchain and machine learning shows significant promise for improving healthcare security, challenges such as multicollinearity, data imbalance, and integration complexities must be addressed. Future research should focus on optimizing feature selection techniques, enhancing model performance through data balancing, and exploring more efficient ways to integrate these technologies into existing healthcare infrastructure. These advancements will be crucial for maximizing the effectiveness of blockchain and machine learning in securing healthcare systems and adapting to evolving security threats.

5.1 Recommendations

Implement Blockchain for Data Security and Interoperability: Healthcare organizations should adopt blockchain technology to secure patient data and ensure seamless interoperability between different systems. Blockchain’s decentralized nature provides an immutable ledger, which enhances the security of electronic health records (EHRs), reduces the risk of data breaches, and enables efficient data sharing across healthcare institutions while maintaining patient privacy.

Healthcare systems should integrate machine learning models for continuous monitoring and real-time threat detection. Machine learning can analyze network traffic patterns, identify anomalies, and detect potential cybersecurity threats, such as data breaches, ransomware, or insider threats, with a high degree of accuracy. Regularly updating and training these models will help healthcare organizations stay ahead of evolving cyber threats.

Human error remains one of the biggest vulnerabilities in healthcare security. It is critical to implement regular cybersecurity training programs for all healthcare staff, including IT administrators, medical professionals, and support personnel. Employees should be educated about phishing attacks, password management, and safe data sharing practices to reduce the likelihood of security breaches caused by negligent behavior.

Given the sensitive nature of healthcare data, strengthening data governance policies around access control, encryption, and data integrity will help prevent unauthorized access and mitigate risks related to data leaks or misuse. Collaborating with legal teams to stay up-to-date with regulatory changes is essential for maintaining compliance and avoiding penalties.

5.2 Areas for Future Studies

Future studies should explore the integration of advanced machine learning algorithms with blockchain technology to further enhance network security in healthcare, particularly focusing on real-time threat detection and anomaly resolution. Research into data governance frameworks for blockchain implementation in healthcare is also needed, especially in managing access control, compliance, and patient privacy. Additionally, investigating the impact of network latency and scalability when adopting blockchain in large healthcare systems could provide insights into practical challenges. Finally, exploring the human factors, such as user training and awareness programs, in improving security posture and reducing insider threats will be crucial for comprehensive security solutions.

References

1) Abubakar, A. A., Liu, J. & Gilliard, E., 2023. An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. Electronics Letters, 59(18), p. e12888.
2) Al-abdulatif, A., Khalil, I. & Rahman, M. S., 2022. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. Journal of Applied Science, 12(21), p. 11039.
3) Alexander, C. A. & Wang, L., 2025. Cybersecurity Benefits and Challenges of Advanced Healthcare Technologies. Journal of Information Technology and Integrity, 2(1), pp. 104-108.
4) Ali, A. et al., 2023. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Journa of Sensor, 23(18), p. 7740.
5) Andrew, J. et al., 2023. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, Volume 215, p. 103633.
6) Arefin, S., 2024. Strengthening Healthcare Data Security with Ai-Powered Threat Detection. International Journal of Scientific Research and Management, 12(10), pp. 1477-1483.
7) Arora, S. & Lamba, V., 2020. A Study of technologies to further research in Health Care Data Security in Medical Report using Block Chain. International Journal of Advanced Engineering Research and Science , 7(6), pp. 248-252.
8) Bathushaw, M. H. & Nagasundaram, S., 2023. Ensuring Cybersecurity In Smart Healthcare Systems: Addressing Emerging Threats and Vulnerabilities. Frontiers in Health Informatics, 12(1), pp. 6904-6919.

9) Bathushaw, M. H. & Nagasundaram, S., 2024. Cybersecurity in Healthcare System: A Systematic Approach of Modern Threads and Development. International Journal of Creative Research Thoughts, 12(5), pp. 597-605.
10) Borky, J. M. & Bradley, T. H., 2018. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering, 5(10), pp. 345-404.
11) Chakraborty, C. et al., 2023. Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method. pp. 1-16.
12) Farayola, O. A., 2024. Revolutionizing Banking Security: Integrating Artificial Intelligence, Blockchain, and Business Intelligence for Enhanced Cybersecurity. Finance & Accounting Research Journal, 6(4), pp. 501-514.
13) He, Y., Aliyu, A., Evans, M. & Luo, C., 2021. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 23(4), p. e21747.
14) Idoko, B. et al., 2024. Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. Magna Scientia Advanced Research and Reviews, 11(2), pp. 151-167.
15) Naresh, K., James, H. & Revathy, G., 2023. HealthAIChain: Improving security and safety using Blockchain. Digital Commons, 11(1), pp. 1-7.
16) Pendyala, S. K., 2024. Strengthening Healthcare Cybersecurity: Leveraging Multi-Cloud and AI Solutions. Journal of Computer Science Applications and Information Technology, 10(1), pp. 1-8.
17) Perwej, D. et al., 2024. Blockchain for Healthcare Management: Enhancing Data Security and Transparency. South Eastern European Journal of Public Health, 26(1), pp. 1173-1184.
18) Poongodi, R. K. et al., 2024. Strengthening Cybersecurity in Indian Healthcare – Lessons from the Recent Ransomware Attacks on Hospitals. International Journal of Advance Research, Ideas, and Innovations in Technology, 10(6), pp. 96-105.
19) Rashmi, S. G., Swetha, V. & Sagar, K., 2024. Improved Cyber Security in Healthcare Using an Advanced encrypted system algorithm and Blockchain Technology. International Journal of Intelligent Systems and Applications in Enginnering, 12(21), pp. 28-37.
20) Saleh, M. A. et al., 2020. How Can Blockchain Strengthen Cybersecurity? How Can Blockchain Strengthen Cybersecurity? Unravelling the Promises and Challenges. International Information Technology Review, 34(1), pp. 1-10.
21) Shinde, R. et al., 2022. Securing AI-based Healthcare Systems using Blockchain Technology: A State-of-the-Art Systematic Literature Review and Future Research Directions. Transactions on Emerging Telecommunications Technologies, 35(1), p. e4884.
22) Sinha, R., 2024. The role and impact of new technologies on healthcare systems. Discover Health Systems, 3(96).
23) Sivaram, V. et al., 2024. Innovative Strategies for Enhancing Data Security in Healthcare Systems. International Journal of Research Publication and Reviews, 5(12), pp. 3918-3920.
24) Sodipe, A. O. et al., 2024. The Role of AI in Enhancing Network Security. Iconic Research and Engineering Journals, 8(3), p. 196.

25) Sunanda, N., Shailaja, K. & Kandukuri, P., 2024. Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection. International Journal of Advanced Computer Science and Applications, 15(4), pp. 947-958.
26) Taherdoost, H., 2024. Blockchain for security and privacy in the smart healthcare. Sensor Networks for Smart Hospitals, 27(12), pp. 411-433.
27) Venkatesan, K. & Rahayu, S. B., 2024. Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports, 14(1), p. 1149.