Journal of Information Systems Engineering and Management
2025, 10(32s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

An Exploratory Study on Securing Lives with Blockchain and AI: Advanced Systems for Pacemaker Malfunction Detection and Heart Attack Prevention

Ms. P. Subashree1, A. Hemaranjanee2, S. Jaya Kirtana3, HUANG XIBIN4
[1] *Assistant Professor, Department of Management Studies,M.O.P. Vaishnav College for Women (Autonomous)*
[2] *Business Analyst – Propel Technology Solutions*
[3]*Key Accounts Manager – Zomato*
[4]*Faculty of Education Shinawatra University*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Pacemakers are life-saving devices designed to protect patients from heart-related complications. However, their effectiveness is often compromised by vulnerabilities such as manufacturing defects and the risk of unauthorized access, leading to significant safety concerns. Numerous legal cases highlight the devastating impact of pacemaker malfunctions, where flaws in manufacturing or hacking attempts have resulted in severe health consequences and loss of life, underscoring the urgency of addressing these issues. This research explores integrating Blockchain and AI technologies to tackle these critical challenges. Blockchain offers a tamper-proof system to enhance production transparency, ensuring accountability and reducing the likelihood of defects, while also establishing a secure framework to protect pacemakers from data breaches and unauthorized manipulation. Furthermore, the study delves into the root causes of pacemaker malfunctions linked to production flaws and proposes targeted solutions to mitigate these risks. By leveraging AI's predictive capabilities alongside Blockchain's immutable record-keeping, this research aims to develop a comprehensive framework that enhances the safety and reliability of pacemakers, contributing to secure, efficient, and trustworthy healthcare technologies.

Keywords: Blockchain in Healthcare, AI in Medical Devices, Pacemaker Failure Prevention, Pacemaker Hacking Risks, Heart Attack Prevention, Medical Device Reliability.

INTRODUCTION

The heart is a vital organ that ensures the proper functioning of the human body by carrying oxygenated blood and supplying it to all the other vital organs through the blood vessels. Hence, it's always crucial to understand the various complications associated with the heart and its responses on a case-to-case basis, the major medical devices implanted in the human body concerning heart-related issues include Pacemakers, Stents, etc.

Daily, on average, the heart beats between the range of 60 - 100 BPM, these are analyzed based on the level of physical activity of an individual. The average adult human has 5 liters of blood in their body. The process of pumping the blood needs to be executed smoothly to supply to other organs, if any obstruction or blockage is found in the path, it leads to shortness of breath, even it can cause immediate death or create other heart-related ailments.

The increase in the heart attack rate in recent times has the spotlight; it should be addressed not only to prevent but also to secure people from dying, this can be achieved with the help of technology. The technology is used to find the reasons behind heart attacks and provide insights into improved diagnostics. The various reasons are obesity, Irregular sleeping patterns, blockage in the path of the blood flow to the heart, increased cortisol level, no physical activity, and Improper diet patterns, it's also necessary to analyze the medical history of an individual. Additionally, Chronic anxiety, poor eating habits, a lack of exercise, habitual smoking, and hereditary predisposition are all contributing causes.

A pacemaker is a small electronic device operated with a battery that helps to regulate heart rhythm and prevent slow heartbeats. Bradycardia: It is a condition where the heart beats less than 60 BPM. If the heart beat rate goes less than 60, it creates major shortness of breath and leads to the death of the person.

Table 1: Death Rates Due to Heart Attacks in India

Year	Death Rates Due to Heart Attacks in India
2018	25,764
2019	28,005
2020	28,680
2021	28,449
2022	32,410

Sources: indiastat.com

The rising death counts alarms each and everyone to take care of one's own health especially in India, as indicated by data from 2018 to 2022, have had a greater impact in recent years, regardless of age, underscoring the critical need for cutting-edge cardiovascular health management measures. Nowadays, people in their 20s and 30s are at risk, emphasizing the value of early detection and preventative healthcare practices.

Heart Attack is medically termed as Myocardial infarction – the blockage occurs due to the formation of blood clots in the blood vessels that create obstruction as well prevent the heart muscle from getting enough oxygen, resulting in cardiac tissue damage or necrosis.

Signs for Pacemaker Implantation:

- Chest pain is a sign, ensures a pacemaker should be implanted.
- An irregular pulse.
- Palpitations in the heart.
- Breathing difficulties.
- Bradycardia: It is a condition where the heart beats less than 60 BPM.
- Lightheadedness or dizziness, nausea, or fainting.
- Swelling in your legs, ankles, and stomach.

A pacemaker can majorly treat the following ailments:

- Certain heart arrhythmias are irregularities in the heart's regular rhythm.
- Electrical system disturbances in your heart, like heart blockages.
- Heart attack.
- Heart attack history.

TYPES OF PACEMAKERS:

- **Single Chamber Pacemaker:** The pacemaker is structured, it has a single wire that is connected to the right atrium or right ventricle of the heart, its main functionality is to send electrical signals to the lower right chamber of the heart.

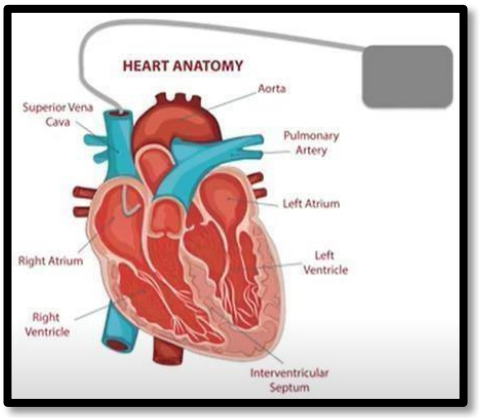

Figure 1: Single Chamber Pacemaker

- **Dual Chamber Pacemaker:** The pacemaker is structured, it has two wires that are attached to the right

atrium and right ventricle of the heart.

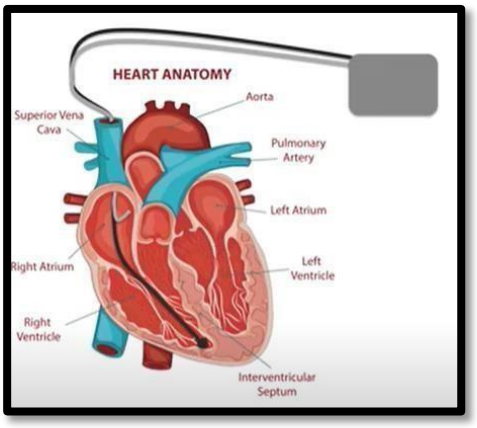

Figure 2: Dual Chamber Pacemaker

- **Biventricular Pacemaker:** The pacemaker is structured, it has three wires, out of which two leads connects to the lower chamber and one to the upper chamber of the heart. This pacemaker is otherwise known as CRT [Cardiac Resynchronization Therapy].

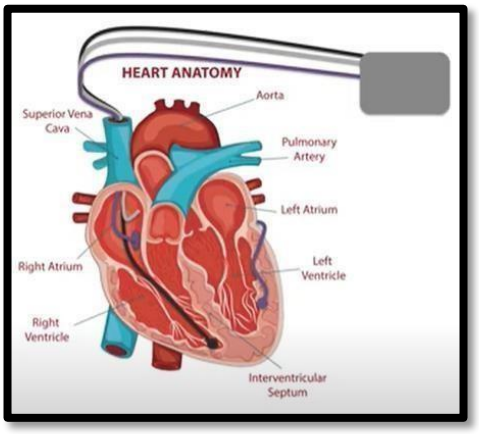

Figure 3: Biventricular Pacemaker

- **Leadless Pacemaker:** The leadless pacemaker doesn't possess leads, it has only the pulse generator to send the electrical impulses by making direct contact with the heart muscle. The leadless pacemaker should be implanted using a catheter-based technique.

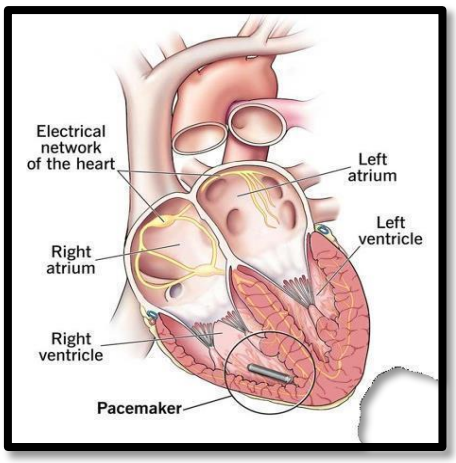

Figure 4: Leadless Pacemaker

The goal of this study is to address a critical issue that has surfaced in recent years: guaranteeing the effectiveness and safety of pacemakers in a population that is becoming more and more vulnerable. As technology develops, it is

essential to apply cutting-edge strategies like blockchain and artificial intelligence (AI) to improve pacemaker systems' dependability and security.

BLOCKCHAIN: THE UNBREAKABLE SHIELD FOR DATA SECURITY

Blockchain technology enables secure and tamper-proof transaction recording through a decentralized network of computers. A high level of security and openness is ensured by ensuring that data is stored in a way that precludes retrospective changes.

Every record, called a "block," contains a set of transactions or information, and these blocks are joined in a chronological "chain," making an unchangeable sequence. Blockchain technology uses consensus processes to verify and approve transactions rather than depending on a central authority.

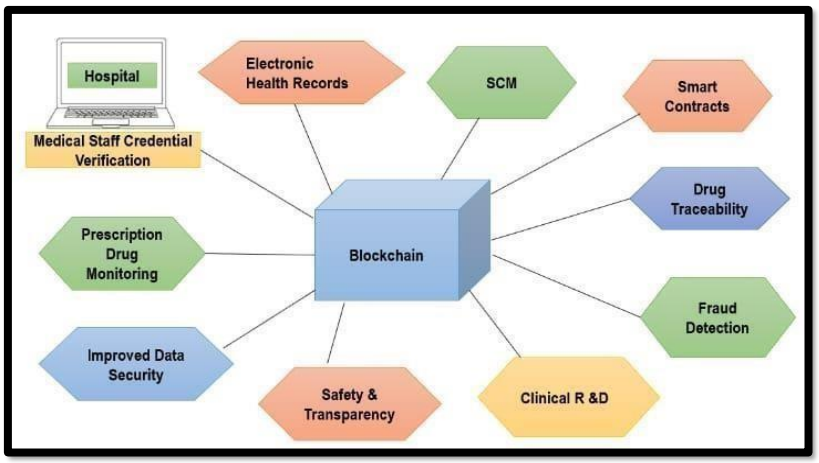

Figure 5: Blockchain in Healthcare

BLOCKCHAIN ESSENTIALS: WHAT MAKES IT SECURE & POWERFUL?

- Data Protection - Blockchain uses powerful cryptographic hash algorithms to protect digital documents, It's a decentralized system.
- Open Visibility.
- Distributed Control
- Records can't be altered once the data is entered into the block.
- Transaction Speed is high in Blockchain.
- Better Traceability and tracking of Information.

BLOCKCHAIN ENHANCING PACEMAKER'S SECURITY AND MEDICAL RELIABILITY:

- Real-time monitoring of patient's pacemaker data by storing heart rate, battery condition, and device performance in a decentralized system.
- Preventing Heart Attacks by analyzing the data and prescribing preventive measures. Blockchain technology can connect data from various wearable devices, such as pacemakers, to understand the patient's cardiac health and prevent heart attacks.
- Ensuring Patient Privacy and the patient gain control over their health data. Patients using decentralized systems can allow or remove access only to the authorized parties, and it can also be accessed by the doctor and the hospital to which the patient is associated.
- Blockchain is also used to manage the device and indicates terms of Repair, replacement, or any warranty issues in the pacemaker to provide security, safety, and peace of mind to the patient.

ARTIFICIAL INTELLIGENCE (AI):

Artificial intelligence (AI) is critical for improving pacemaker failure diagnosis and heart

attack prevention because it analyses and provides insights into the heart's functioning and early detection of

dangers in the heart. AI algorithms integrated with ML and Data analytics play a major role in studying the huge volume of trained datasets and provide an immediate solution by analyzing the situation of a patient on a case-to-case basis. AI can process all the data provided by the pacemaker and indicate the current health state of the patient.

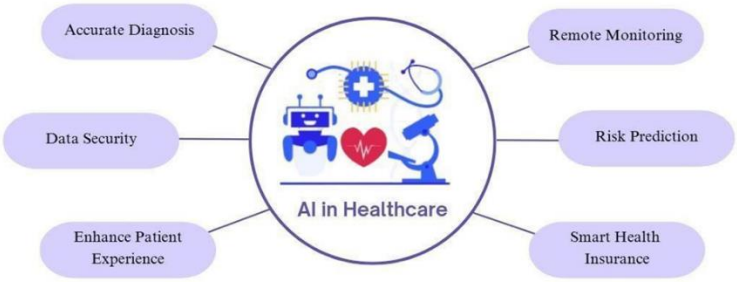

Figure 6: AI in Healthcare

AI REVOLUTIONIZING PACEMAKER MONITORING AND HEART ATTACK PREVENTION:

- Continuous Monitoring of heart conditions, including heart rate and heart rhythm, and also detect various abnormalities like arrhythmias, bradycardia, or tachycardia.
- AI can scan many data sources, including pacemaker data, fitness trackers, and EHRs, to identify risk factors for heart attacks and to provide better solutions.
- The stress levels are also measured by analyzing the data, if the stress increases, the palpitations will be created among the patients.
- AI-powered devices can provide real-time notifications to healthcare practitioners if pacemaker malfunctions or a patient's heart data indicates distress (e.g. Irregular heartbeat or low battery). This allows for prompt intervention before the issue escalates.
- Early Warning Systems in AI-powered devices can identify changes in the heart's electrical rhythms and anticipate the onset of a heart attack hours or days ahead. Early detection allows for prompt actions, such as adjusting pacemaker settings or providing drugs for better patient care.

BLOCKCHAIN AND AI INTEGRATION IN PACEMAKER:

The integration of Blockchain and AI work to enable secure, decentralized data exchange, allowing healthcare providers to share information while maintaining patient privacy. AI enhances its diagnostic capabilities through continuous learning, while blockchain ensures transparent and tamper-proof data storage. This combination supports real-time health monitoring, instant alerts, and the protection of critical medical records, ultimately improving patient safety and making healthcare systems more efficient.

OBJECTIVES OF THE STUDY:

- To analyze the use of Blockchain in developing a tamper-proof system to safeguard pacemaker data from unauthorized access and prevent data breaches.
- To develop AI-based predictive models for pacemaker malfunctions, identify manufacturing defects, and propose solutions to improve device reliability before deployment.

REVIEW OF LITERATURE:

1. Suliat Toyosi Jimoh and Shaymaa S Al-junior [1] examined the various cybersecurity risks faced by patients implanted with pacemakers, this study focuses on vulnerabilities like unauthorized access and data breaches due to advancements in wireless technology, where people have used it in appropriate form. Using the WUSTL-EHMS2020 dataset, the researcher applied ML models including—Support Vector Machines (SVM) and Gradient Boosting Machines (GBM)—to predict threats. GBM outperformed SVM, achieving 95.1% accuracy, 99.6% precision, 94.9% recall, and a 76.3% F1 score. The study ensures integrating GBM into security frameworks acts as a breakthrough in the pacemaker with regular updates on the health-related

data and retraining all that information to enhance pacemaker cybersecurity and mitigate emerging threats.

2. Abdullah Saeed, Abdullah AlShafea, Foton A, and Abdulrahman Bin Saeed [2] analysed pacemaker-related difficulties such as battery malfunctions, battery depletion, lead displacements, and external interferences,

which can result in various conditions such as arrhythmias, disorientation, and even cardiac arrest. The traditional diagnostic techniques, such as ECG and other device interrogations, give useful information, but they frequently lack real-time detection and predictive accuracy, if it's not performed on time, they cause huge complications. AI and blockchain technologies provide promising real-time solutions. AI offers continuous monitoring of pacemaker function and patient data, gives insights about Heartbeat rate, and rhythm, and helps to detect new symptoms and speedier emergency actions. At the same time, blockchain provides safe transmission of data, and tamper-proof storage of medical records, improving transparency, and collaboration, and maintaining patient information confidentially.

3. Hira Zainab, Arbaz Haider Khan, Roman Khan, and Hafiz Khawar Hussain [3] present a detailed study on the advancement introduced in monitoring heart conditions enabled by AI and wearable technology. This study majorly covers the ECG patches and biosensorsoffer continuous monitoring and real-time data collecting, which aids in the early detection of heart diseases. AI- powered solutions, ML, and data analytics are known for their capacity to handle massive datasets, anticipate cardiovascular risks, and increase diagnostic accuracy. The research also explores ethical and regulatory challenges, such as data security, ownership, and biases in AI-driven decision-making. The study explores all the possible challenges and provides better solutions at the earliest for better patient care.

4. Abdulatif Abdullatif, Ibrahim Khalil, and Mohammad Saidur Rahman [4] describe the importance of utilizing blockchain and AI to improve the security of smart healthcare systems. Their work focuses on the vulnerabilities addressed in interconnected healthcare devices, which are vulnerable to malware, hardware, and network-based assaults. The study proposes a blockchain-based secured architecture system integrated with AI to counteract malware and network intrusions, focusing on scalability and data integrity attributes—decentralization, immutability, and transparency—which are highlighted as critical for securing patient data and mitigating privacy risks. The data breach may also lead to other complications since all the information is sensitive The researcher stresses the importance of predictive capabilities in

detecting cyber threats and safeguarding critical healthcare operations. The proposed architecture proves improved performance in the accuracy and dynamic analysis of Malware.

5. Farah Yasmin, Syed Muhammad Ismail Shah, Aisha Naeem, Syed Muhammad Shujauddin, Adina Jabeen, Sana Kazmi, Sarush Ahmed Siddiqui, Pankaj Kumar, Shiza Salman, Syed Adeel Hassan, Chandrashekhar Dasari, Ali Sanaullah Choudhry, Ahmad Mustafa, Sanchit Chawla, Hassan Mehmood Lak [5] analyzed the revolutionary role of AI in diagnosing and treating heart attacks. The study focuses on AI and Blockchain integration into cardiovascular medicine, namely its applications in early detection, risk prediction, and optimal clinical care. AI outperforms better than the traditional diagnostic methods for heart failure identification by achieving accuracy rates of over 85% using neural networks and ML algorithms. AI provides more sophisticated decision- making when using imaging modalities such as ECG and cardiac MRI.

6. Adrian Baranchuk, MD, Marwan M. Refaat, MD, Kristen K. Patton, MD, Mina K. Chung, MD, Kousik Krishnan, MD, Valentina Kutyifa, MD, PhD, Gaurav Upadhyay, MD, John D. Fisher, MD, Dhanunjaya R. Lakkireddy, MD [6], this study addressed the cybersecurity concerns connected with Cardiac Implantable Electronic Devices (CIEDs), which include pacemakers and defibrillators. The report exposes and ensures the weaknesses in these devices, such as unauthorized access, data manipulation, and rapid battery depletion lead to heart attacks. It emphasizes the importance of integrating cybersecurity measures from the design stage and maintaining robust post-market monitoring to address emerging threats. Recommendations from the study include firmware updates, secure lifecycle management, and collaborative efforts between manufacturers, healthcare providers, and regulatory agencies like the FDA. While no clinical incidents of malicious hacking have been reported yet, proactive measures are advocated to mitigate theoretical risks.

7. Izabela Rojek, Piotr Kotlarz, Mirosław Kozielski, Mieczysław Jagodzi´nski, and Zbyszko Królikowski [7] proposes an AI-driven strategy for heart attack prevention that focuses on early risk prediction using non-invasive medical imaging and patient data analysis. The study investigates and analyses several AI models, including logistic regression and random forest algorithms, to calculate customized heart attack probabilities. The study identified four main risk factors: heart rate, age, BMI, and cholesterol, emphasizing the relevance of modifiable variables in effective prevention methods. The study proposes AI to improve precision in preclinical care and predictive medicine. The potential for AI systems to streamline preventative care by allowing for tailored interventions and better resource allocation is highlighted.

RESEARCH GAP IDENTIFICATION:

The intersection of technology and medicine holds vast potential, but only if we address the gaps in innovation.

- **Vulnerabilities in Pacemaker Security: An Unaddressed Threat.**

Blockchain and AI technologies have been acknowledged for their separate potential to improve healthcare systems, but their combined application, particularly for pacemaker security and malfunction detection, is underexplored. For example, in Pooja Gupta vs. Max Super Speciality Hospital and Others (2017), the hospital and its cardiologist were accused of implanting a faulty pacemaker that caused the patient's death. The Punjab and Haryana High Court stated that this was not just severe medical negligence but also cheating, emphasizing the ethical and legal implications of such activities. Creating complete frameworks that incorporate Blockchain immutable ledger capabilities with AI predictive analytics could proactively detect and mitigate such problems, dramatically boosting the reliability and safety of pacemakers.

- **Understanding Pacemaker Malfunctions: Causes and Consequences:**

Existing literature offers few insights into the exact manufacturing flaws that cause pacemaker failures. A remarkable case reported in the BMC Cardiovascular Disorders journal described an 83-year-old male patient who developed chest pain and dyspnea as a result of automated reprogramming after pacemaker battery depletion, which led to pacemaker syndrome. This case mainly emphasizes the crucial need to detect the problems at the earliest stage and to provide the appropriate solution for repair or replacements should be done to avoid such disastrous clinical consequences. In-depth investigations are needed to categorize and analyze manufacturing defects. Such assessments are much needed for creating focused actions that improve device dependability and patient safety.

- **Accountability in Pacemaker Safety:**

The legal cases filed against the pacemaker emphasize the need and the scope for analysis. In most cases, it's because of battery depletion the patients die, and there arises ethical questions about device quality and transparency.

For example, in the aforementioned case of Pooja Gupta vs. Max Super Speciality Hospital and Others, the court addressed the ethical and legal implications of implanting an inferior pacemaker, highlighting the importance of accountability in such circumstances. However, case studies are

scarce on the legal and ethical aspects of pacemaker failures, particularly in terms of liability in cases of manufacturing flaws or insufficient security measures. Addressing this gap is critical for guiding policy development and providing clearer standards for manufacturer and healthcare provider duties. It not only includes ethical concerns it also shows the medical negligence of the doctor using the malfunctioned pacemaker worth Rs, 45000 instead of Rs.4,50,000. This creates a major panic situation among the patients who they can trust and consult for better solution.

- **The Perception Paradox: Patient Understanding of Pacemaker Risks and Benefits:**

Patients always concerned about the security of medical devices, such as pacemakers, are not widely documented. The patients are not educated on the reason for implantation, the working style and conditions of the pacemaker, and maintenance of the pacemaker. The perception of technology among the patients differs on a case-to-case basis, Blockchain and AI for minimizing these risks. Understanding patient's viewpoints is critical for building educational programs and instilling trust in sophisticated medical technologies. Addressing these research gaps is the foremost step to improve pacemaker safety, dependability, and ethical standards, ultimately leading to better patient outcomes in medical device developments.

RESEARCH DESIGN:

Table 2: Research Design

Sampling Method	Simple Random Sampling
Sampling Size	n(s) = 242
Data Collection Method	Self-administered survey questionnaires
Methodology	• Correlation Analysis • Regression Analysis • Chi-Square Analysis • Random Forest • Structural Equation Model(SEM)
Tools Used	• Microsoft Excel • SPSS • R Studio

CORRELATION ANALYSIS:

Covariance:

The covariance analysis is performed to analyze the relationship between the two variables namely Data Security and the Feature Enhances Data Security with Blockchain and AI. The covariance matrix provided the following insights,

Table 3: Covariance Matrix

	Data Security	Feature Enhances Data Security with Blockchain and AI
Data Security	1.74	0.85
Feature Enhances Data Security with Blockchain and AI	0.85	1.23

Interpretation:

The diagonal elements represented the variance value for the 2 variables as follows:

- 1.74 corresponds to the variance of Data Security.
- 1.23 represents the variance of Feature Enhances Data Security with Blockchain and AI.
- The off-diagonal value (0.85) represents the covariance between the two variables.
- The off-diagonal element of the covariance matrix, 0.85, represents the upward trend in Feature Enhances the Data Security with Blockchain and AI leads to the upward trend in Data Security. The positive covariance value signifies there is a direct relationship between the two variables taken under the study, indicating that improvements in blockchain and AI-driven security measures lead to an increase in overall data security.
- This positive association suggests that data security measures exhibit a corresponding upward trend as advancements in blockchain and AI security features increase. However, it is important to note that covariance, while indicative of directional movement, does not quantify the strength or reliability of this relationship.

Table 4: Correlation matrix

Correlations

		Features Enhances Blockchain and AI	DataSecurity
Features Enhances Blockchain and AI	Pearson Correlation	1	.584**
	Sig. (2-tailed)		.000
	N	242	242
DataSecurity	Pearson Correlation	.584**	1
	Sig. (2-tailed)	.000	
	N	242	242

**. Correlation is significant at the 0.01 level (2-tailed).

Table 5: Correlation with p-value:

	r	p
Data Security and Feature Enhances Data Security with Block Chain and AI	**0.584**	**<.001**

Interpretation:

The correlation coefficient between Feature Enhances Data Security with Blockchain and AI and Data Security is 0.584, indicating a moderate positive relationship. This shows that improvements in blockchain and AI-powered security procedures are linked to an increase in overall data security.

Additionally, the correlation is statistically significant at the 0.01 level ($p < 0.001$), indicating its reliability and limiting the possibility of random variation. While the positive correlation indicates a directional relationship between the two constructs, it does not imply a causal influence. To investigate the predictive impact and underlying links further, more statistical approaches, such as regression analysis, would be required.

LINEAR REGRESSION:

Table 6: Summary of Linear Regression Model Fit

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	N (Valid Cases)
1	0.58	0.34	0.34	1.07	242

Table 7: Coefficients of the Regression Model

Model	Unstandardized Coefficients	Standardized Coefficients	Standard Error	t	p	95% Confidence Interval for B	
	B	Beta				Lower Bound	Upper Bound
(Constant)	**1.93**		0.14	13.39	<.001	1.65	2.22
Feature Enhances Data Security with Blockchain and AI	**0.69**	0.58	0.06	11.15	<.001	0.57	0.82

Interpretation:

A linear regression analysis was conducted to examine the relationship between *Feature Enhances Data Security with Blockchain and AI* and *Data Security*. The model indicates that 34.11% of the variance in Data Security can be explained by enhancements in blockchain and AI-driven security mechanisms ($R^2 = 0.34$), suggesting a meaningful association between these factors.

The regression equation derived from the analysis is:

Data Security=1.93+0.69· Feature Enhances Data Security with Blockchain and AI {Data Security} = 1.93 + 0.69 {Feature Enhances Data Security with Blockchain and AI} Data Security=1.93+0.69·Feature Enhances Data Security with Blockchain and AI.

This means that when no enhancements in blockchain and AI security features are present, the baseline level of *Data Security* is estimated at 1.93. Additionally, for every one-unit increase in *Feature Enhances Data Security with Blockchain and AI*, *Data Security* is expected to improve by 0.69 units, reinforcing the idea that advancements in these technologies contribute positively to data protection.

The standardized coefficient (Beta = 0.58) further supports this, indicating that *Feature Enhances Data Security with Blockchain and AI* has a moderate-to-strong influence on *Data Security*.

The model results are statistically significant, with a t-value of 11.15 and a p-value of < 0.001, confirming that the observed relationship is unlikely to be due to random variation.

Furthermore, the 95% confidence interval for B ranges from 0.57 to 0.82, ensuring the reliability of this estimate. Since this interval does not include zero, it strengthens the evidence that blockchain and AI enhancements contribute to improving data security.

These findings highlight the role of emerging technologies in strengthening data security frameworks. The results suggest that as organizations continue to adopt blockchain and AI-driven security enhancements, overall data protection measures are likely to improve.

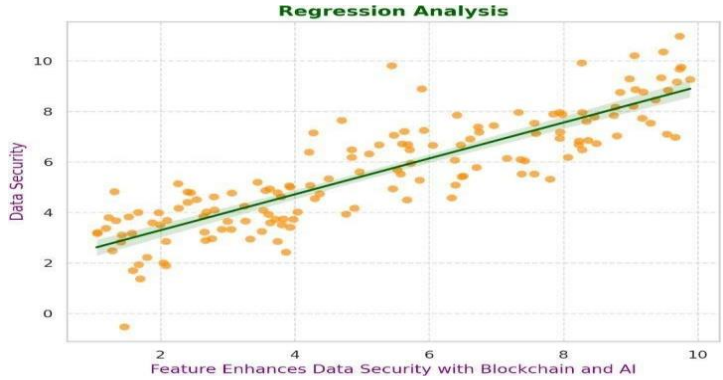

Figure 7: Graphical Representation of Regression Analysis

The scatter plot visualizes the relationship between Feature Enhances Data Security with Blockchain and AI and Data Security. The regression line, displayed in dark green, indicates a positive linear trend, suggesting that improvements in blockchain and AI-driven security features are associated with an increase in overall data security.

The alignment of residuals along the fitted line suggests a reasonably well-fitted model, reinforcing the statistical significance of the observed relationship.

CHI-SQUARE ANALYSIS:

The Chi-Square Analysis is performed to find the association between the variables. Here, we have chosen two variables for this analysis, namely, 'Factors that motivate to prioritize the AI model' and 'Challenges in using AI for Pacemaker Malfunction.'

Table 8: Factors Motivating the Prioritization of AI Models

	Observed	Expected N	Residual
Real – time Montioring	66	60.5	5.5
Early Failure Predictions	59	60.5	-1.5
Improved Diagnostics	40	60.5	-20.5
Manufacturing Defect	77	60.5	16.5
Total	242		

Table 9: Challenges in using AI for Pacemaker Malfunction Detection

	Observed	Expected N	Residual
Data Availability	63	60.5	2.5
Accuracy of Predictions	79	60.5	18.5
Cost of Implementation	58	60.5	-2.5
Ethical Concerns	42	60.5	-18.5
Total	242		

Table 10: Chi-Square Test Results

	Factor that motivate to Prioritize AI Model	Challenges in using AI for Pacemaker Malfunction Detection
Chi-Square	11.983	11.521
df	3	3
Asymp. Sig.	0.007	0.009

Interpretation:

A Chi-Square test of independence was used to investigate the relationship between parameters influencing AI model prioritizing and difficulty in detecting pacemaker malfunctions. The findings show that the relationship between these variables is statistically significant.

The Chi-Square statistic for factors motivating AI model priority was 11.983, with three degrees of freedom (df = 3) and a p-value of 0.007. This shows that the observed variations between expected and actual frequencies are unlikely to be due to chance, revealing a significant link between these motivational elements and AI adoption.

Similarly, for the issues of applying AI for pacemaker dysfunction, the Chi-Square statistic was 11.521, with 3 degrees of freedom (df = 3) and a p-value of 0.009.

The findings suggest a statistically significant link between these problems and AI adoption for identifying pacemaker faults. The null hypothesis is rejected since both p-values are less than the customary 0.05 threshold, indicating that the response distribution across categories is not random. The residual values showed the differences between observed frequency and expected frequencies, with considerable deviations in categories like "Improved Diagnostics" (-20.5) and "Ethical Concerns" (-18.5), suggesting places where actual responses deviated significantly from expected observations. These findings highlight the importance of the positives and drawbacks of AI adoption in medical applications.

The results reveal that while AI-powered systems provide more benefits such as real-time monitoring, and identifying the manufacturing problem, concerns about cost, accuracy, and ethical implications. Future studies can

be performed on addressing these issues to improve AI implementation is important in healthcare sectors and the services provided by the various industries associated.

RANDOM FOREST:

Table 11: Summary of the Model

Type of random forest	Classification
Number of trees	1000
No. of variables tried at each split	3
OOB estimate of error rate	3.46%

Table 12: Confusion Matrix

	Early Failure Predictions	Improved Diagnostics	Manufacturing Defect	Real-time Monitoring	Class Error
Early Failure Predictions	14	26	3	27	0.80000000
Improved Diagnostics	11	20	15	9	0.63636364
Manufacturing Defect	3	733	23586	5	0.03045998
Real-time Monitoring	8	7	1	74	0.1777778

Table 13: Mean Decrease Accuracy & Mean Decrease Gini

	Early Failure Predictions	Improved Diagnostics	Manufacturing Defect	Real-time Monitoring	Mean Decrease Accuracy	Mean Decrease Gini
Age Group	19.93484	19.93484	11.663641	34.62936	116.5497	3111.400
Concern for Medical Device Security	27.62201	22.542648	110.7063	90.15293	111.2184	4656.053
Trust in AI & Blockchain	2.20667	18.005760	108.7515	41.53989	109.1797	3250.524
Familiarity with Blockchain & AI	11.42563	8.931293	106.9118	35.67040	107.0202	3206.757

Interpretation:

The Random Forest classification model was trained on a balanced dataset with 1000 decision trees and a feature selection parameter of mtry = 3. The Out-of-Bag (OOB) error rate was observed to be 3.38%, indicating robust classification performance.

The confusion matrix highlights the strengths and weaknesses of the model. The Manufacturing Defect category possesses the highest predictive accuracy (23,603 correctly classified instances), whereas the other factors such as the Early Failure Predictions category showed the highest classification error (77.14% misclassification rate).

Feature importance analysis, measured through Mean Decrease in Accuracy, revealed that Concern for Medical Device Security was the most influential predictor (114.98 accuracy impact), followed by Trust in AI & Blockchain (110.69) and Familiarity with AI & Blockchain (102.14). This suggests that patient security concerns and trust in AI-driven technologies significantly impact predictive performance.

These results emphasize the model's high accuracy in identifying manufacturing defects while highlighting the need for further refinement in distinguishing early failure cases. Future work may focus on feature engineering or hyperparameter optimization to improve classification in misclassified categories.

STRUCTURAL EQUATION MODELING (SEM):

Structural Equation Modeling (SEM) is an advanced statistical technique used to analyze and understand the complex relationships between variables. SEM combines factor analysis and regression modeling to test hypotheses about their direct and indirect relationships among observed (measured) and latent (unobserved) variables.

Table 14: Summary of the Model

Estimator	DWLS
Optimization method	NLMINB
Number of model parameters	10

Number of observations	242

Table 15: Model Test User Model

Test statistic	0.056
Degrees of freedom	1
P-value (Chi-square)	0.812

Table 16: Model Test Baseline Model

Test statistic	11.241
Degrees of freedom	1
P-value (Chi-square)	0.001

Table 17: User Model vs Baseline Model

Comparative Fit Index (CFI)	1.000
Tucker-Lewis Index (TLI)	1.092

Table 18: Root Mean Square Error of Approximation

RMSEA	0.000
90 Percent confidence interval - lower	0.000
90 Percent confidence interval - upper	0.106
P-value H_0: RMSEA <= 0.050	0.860
P-value H_0: RMSEA >= 0.080	0.088

Table 19: Standardized Root Mean Square Residual

SRMR	0.000

Table 20: Parameter Estimates

Parameterization	Delta
Standard errors	Standard
Information	Expected
Information saturated (h1) model	Unstructured

Table 21: Regressions

	Estimate	Std.Err	z-value	P(>|z|)	Std.lv	Std.all
Security.Concern.Level ~ Fmlrty.wt.B.AI	-0.035	0.053	-0.671	0.502	-0.035	-0.049
Trust.in.AI.Blockchain ~ Scrty.Cncrn.Lv	0.222	0.066	3.369	0.001	0.222	0.222

Table 22: Thresholds

	Estimate	Std.Err	z-value	P(>|z|)	Std.lv	Std.all
Scrty.Cncrn.L|1	-1.954	0.244	-8.011	0.000	-1.954	-1.951
Scrty.Cncrn.L|2	-1.355	0.235	-5.755	0.000	-1.355	-1.353
Scrty.Cncrn.L|3	-0.974	0.229	-4.251	0.000	-0.974	-0.973
Scrty.Cncrn.L|4	-0.006	0.212	-0.028	0.977	-0.006	-0.006
Trst.n.AI.B|1	-1.567	0.185	-8.488	0.000	-1.567	-1.567
Trst.n.AI.B|2	-1.069	0.168	-6.360	0.000	-1.069	-1.069
Trst.n.AI.B|3	-0.137	0.167	-0.817	0.414	-0.137	-0.137
Trst.n.AI.B|4	0.699	0.165	4.231	0.000	0.699	0.699

Table 23: Variances

	Estimate	Std.Err	z-value	P(>|z|)	Std.lv	Std.all
Security.Concern.Level	1.000				1.000	0.998
Trust.in.AI.Blockchain	0.951				0.951	0.951

Table 24: R – Square

	Estimate
Security.Concern.Level	0.002
Trust.in.AI.Blockchain	0.049

Interpretation:

The variables used for SEM analysis are familiarity with Blockchain & AI, security concerns, and trust in AI-enhanced medical devices. The analysis is performed with 242 responses from our target audience.

Model Fit:

The results show it is an excellent model fit: CFI = 1.000, TLI = 1.092, and RMSEA = 0.000, with a p-value of 0.812 from the chi-square test, confirming that the proposed model adequately represents the observed data.

HYPOTHESIS TESTING & KEY FINDINGS:

1. The effect of familiarity with Blockchain & AI on security concerns:

The regression analysis shows a non-significant effect ($\beta = -0.035$, $p = 0.502$), suggesting that prior familiarity with these technologies does not strongly influence the level of concern regarding medical device security.

2. The impact of security concerns on trust in AI & Blockchain-based medical devices:

A significant positive relationship was found ($\beta = 0.222$, $p = 0.001$), indicating that individuals with higher security concerns exhibit moderate trust in AI and Blockchain-integrated medical technologies.

The R^2 value for trust in AI & Blockchain-based medical devices is 0.049, suggesting that security concerns explain approximately 4.9% of the variance in trust levels, indicating that other factors

(such as perceived benefits, regulatory assurances, or usability) may also contribute to trust formation.

The findings highlight that while familiarity with technology does not necessarily reduce security concerns, these concerns significantly influence trust in AI & Blockchain-enabled medical devices. If someone is more concerned about security, they are less likely to trust these technologies. This underscores the importance of addressing security risks and transparency in medical technology adoption strategies.

FINDINGS AND IMPLICATIONS:

- The research aims to analyze the use of Blockchain and AI Integration in Pacemakers, its impact level on improvising data security, and the pacemaker malfunction detection at the earlier stage by sending simultaneous reports on the health condition of the patients implanted with Pacemakers.
- The study suggests there is a positive association, data security measures exhibit a corresponding upward trend as advancements in blockchain and AI security features increase, it acts as a catalyst for achieving a high-level tamper-proof system, improved data security, safety, and transparency in terms of sharing the patient's data with the respective hospitals, and helps in monitoring the patient's health condition more efficiently to provide better care.
- The Chi-Square Analysis shows there is a strong association between the Factors that motivate to prioritize the AI model and the challenges in using AI for Pacemaker Malfunction.
- The Random Forest methodology provides insights by analyzing various factors such as Manufacturing defects, Real-time Monitoring, Improved Diagnostics, and Early Failure Prediction. The concern for Medical device security acts as the influential predictor in predicting the AI Model priority. The AI model can easily prioritize and identify the Manufacturing Defect accurately since the system is trained with all the possible defects rather than other factors.
- Organizations developing AI-driven healthcare solutions should prioritize security features to build user confidence and align their models with real-world concerns. Strengthening security can enhance adoption, reliability, and overall trust in AI for medical applications.

- The other findings of the study include the patients implanted with a pacemaker have sleep disturbances, and they can't handle the roller coaster of emotions simultaneously, In a few cases where the pacemakers have not been implanted properly, patients face Physical pain in the chest or Discomfort.
- The study also addressed the major complications faced by the patient, Battery Depletion and Pacemaker Generator failure, the patient should be educated on the device, the surgical methodology, the life span of the device, diet constraints, the physical activity, and the regular monitoring of the Pacemaker, if these measures and precautions are taken properly heart attacks can be prevented and saving the lives of the patients.

SUGGESTIONS:

Based on the findings, several key recommendations emerge for improving pacemaker reliability, security, and patient confidence in AI- and Blockchain-integrated medical technologies:

1. Developing a Blockchain-Based Tamper-Proof Ledger:

A decentralized system can track every stage of a pacemaker's lifecycle, from manufacturing to real-time performance monitoring. This would eliminate data manipulation risks, making device failures traceable and reducing legal ambiguities in accountability.

2. Implementing AI-Driven Predictive Maintenance Models ensures patient safety:

The integration of AI-powered algorithms in pacemakers provides better patient care by detecting not only battery depletion but also system failure, and hardware defects to give indications to nearby healthcare providers.

3. Strengthening Regulatory Frameworks for Device Security and to secure the lives of the patient:

The medical regulatory bodies must enforce strict rules on compliance standards, ensuring the manufacturers to incorporate AI-based diagnostics and Blockchain-driven security layers before getting device approval for manufacturing.

4. Enhancing Patient Awareness and Trust to use Technology:

Patients are not aware of the security risks associated with medical devices. Even User-friendly mobile applications should be introduced, and the patients should be educated on monitoring their health condition, receiving alerts, and securely communicating with healthcare providers. Additionally, public awareness campaigns should be conducted and educate patients on both AI and Blockchain to safeguard personal health data from cyber threats.

5. Integrating Blockchain with Cloud-Based Monitoring Systems:

A real-time, cloud-integrated Blockchain system would allow only authorized healthcare professionals to monitor the performance of the pacemaker securely, ensuring immediate intervention if an anomaly is detected in the device.

CONCLUSION:

The rise in Blockchain and AI technology leads to enormous upgrades in health care. The future of healthcare is undoubtedly digital, incorporating Medical codes to understand the History of the patient, AI for detecting malfunctions and improvise diagnostics in the pacemaker, Blockchain for providing tamper-proof systems and highly secured platforms to access patients' data for prescribing drugs, maintaining Electronic Health Records (EHR) and early identification of new symptoms in the Patient's body. The recent increased Heart attack rate captures the spotlight and creates a need to understand the reason for heart attacks and to provide better solutions.

Our research study significantly shows that the integration of technology in the Pacemaker has a positive impact on providing better patient care, highly secured data transmission, detecting unusual behavior in patients, and early indication of changes in health conditions to concerned hospitals and doctors to prevent Heart Attacks and secure the lives of the people. The other findings of the study show the challenges faced by the patient pre and post-implantation of the pacemaker. The initiative needs to be taken by the Medical Association to create awareness, educate on Heart attack, its symptoms, and awareness among all age groups to regain control over health.

FURTHER RESEARCH AGENDA:

The integration of AI and Blockchain in healthcare is advancing rapidly, yet critical gaps remain in ensuring the safety, security, and reliability of pacemakers. With the increasing number of reported pacemaker malfunctions—whether due to manufacturing defects, cyber threats, or system failures—it is crucial to explore innovative solutions that not only enhance device security but also improve patient trust and adoption.

This study is significant for several reasons:

Addressing Security Vulnerabilities: Cybersecurity threats to medical devices are rising, and Blockchain presents an opportunity to create tamper-proof security layers for protecting patient data and device integrity.

Enhancing Predictive Capabilities: AI-driven predictive models can identify potential malfunctions before they become life-threatening, ensuring proactive intervention.

Regulatory and Ethical Considerations: The legal cases analyzed in this research highlight accountability gaps in pacemaker manufacturing and healthcare delivery, underscoring the need for transparent tracking mechanisms using Blockchain.

Bridging the Trust Deficit: The study's results on patient familiarity with AI and Blockchain versus their level of trust in these technologies provide valuable insights for future adoption strategies.

This research is not just theoretical but has direct implications for device manufacturers, healthcare providers, regulators, and policymakers who seek to develop safer and more reliable medical technologies.

REFERENCES:

[1] Suliat Toyosi Jimoh and Shaymaa S Al-juboori. (2024). Cyber-Securing Medical Devices Using Machine Learning: A Case Study of Pacemaker, *Journal of Informatics and Web Engineering*, 3(3), pp. 271-289.

[2] Abdullah Saeed, Abdullah AlShafea, Foton A, Abdulrahman Bin Saeed. (2023). Pacemaker Malfunction in a Patient with Congestive Heart Failure and Hypertension.

[3] Hira Zainab, Arbaz Haider Khan, Roman Khan, Hafiz Khawar Hussain. (2024). Integration of AI and Wearable Devices for Continuous Cardiac Health Monitoring, *International Journal of Multidisciplinary Sciences and Arts* E-ISSN: 2962-1658 Volume 3, Number 4.

[4] Abdulatif Alabdulatif, Ibrahim Khalil, and Mohammad Saidur Rahman. (2022). Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis.

[5] Farah Yasmin, Syed Muhammad Ismail Shah, Aisha Naeem, Syed Muhammad Shujauddin, Adina Jabeen, Sana Kazmi, Sarush Ahmed Siddiqui, Pankaj Kumar, Shiza Salman, Syed Adeel Hassan, Chandrashekhar Dasari, Ali Sanaullah Choudhry, Ahmad Mustafa, Sanchit Chawla, Hassan Mehmood Lak. (2021). Artificial intelligence in the diagnosis and detection of heart failure: the past, present, and future, *IMR Press*, Vol. 22(4), 1095-1113.

[6] Adrian Baranchuk, MD, Marwan M. Refaat, MD, Kristen K. Patton, MD, Mina K. Chung, MD, Kousik Krishnan, MD, Valentina Kutyifa, MD, PhD, Gaurav Upadhyay, MD, John

[7] D. Fisher, MD, Dhanunjaya R. Lakkireddy, MD. (2018). Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know? *American College of Cardiology Foundation*, Vol. 71, NO. 11.

[8] Izabela Rojek , Piotr Kotlarz , Mirosław Kozielski , Mieczysław Jagodzi´nski and Zbyszko Królikowski. (2024).Development of AI-Based Prediction of Heart Attack Risk as an Element of Preventive Medicine, *Medical Applications of Artificial Intelligence*.

[9] Julián Palacios-Rubio, Juan José González-Ferrer, Nicasio Pérez-Castellano. (2019). "Advanced pacing algorithms resembling device malfunction: A comprehensive review," *REC: CardioClinics*, Volume 54, Issue 2.

[10] Nicola Schulz, Klaus Puschel and Elisabeth E. Turk. (2009). Fatal complications of pacemaker and implantable cardioverter defibrillator implantation: medical malpractice? *European Association for Cardio-Thoracic Surgery*.

[11] Min Kim, Younghyun, Seng ChanYou, Hyung-Deuk Park, Sang-Soo Lee, Tae-Hoon Kim, HeeTaeYu, Eue-Keun Choi, Hyoung-Seob Park, Junbeom Park, Young Soo Lee, Ki-Woon Kang, Jaemin Shim, Jung-Hoon Sung, Il-Young Oh, Jong Sung Park, Boyoung Joung. (2022). Artificial intelligence predicts clinically relevant atrial high-rate episodes in patients with cardiac implantable electronic devices", *Sci Rep* 12, 37.

[12] Allison Gibson, Geethapriya Thamilarasu. (2020). Protect Your Pacemaker: Blockchain- based Authentication and Consented Authorization for Implanted Medical Devices", *Procedia Computer Science*, Volume 171, 2020.

[13] Hamed Taherdoost. (2023). Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives", *MDPI, Sci*.