# AI AND BLOCKCHAIN ROLE IN FRAUD DETECTION IN AN INSURANCE CLAIMS: A QUALITATIVE STUDY AT CARE HEALTH INSURANCE

Dissertation Submitted to


**The IIHMR University, Jaipur**

for the partial fulfillment for the award of the degree of

Master of Business Administration (MBA)

in

**Hospital and Health Management**

by

**Mrudula Vikas Borkar**

Under the Supervision and Guidance of

**Dr. Sandipta Chakraborty**

**2025**

care HEALTH INSURANCE

BEST HEALTH INSURANCE COMPANY IN RURAL SECTOR | CLAIMS SERVICE LEADER OF THE YEAR
INDIA INSURANCE SUMMIT & AWARDS 2024

# CERTIFICATE

This is to certify that **Mrudula Vikas Borkar,** in partial fulfillment of the requirements for the award of the degree of MBA (Hospital and Health Management) from the IIHMR University, Jaipur, has successfully completed her internship at Care Health Insurance Ltd. during Mar 10 - May 31, 2025.

Place: Gurgaon
Date: 05/06/2025

Dr Pankaj Vats
Manager- Medical Claims
Care Health Insurance Ltd.

IIHMR UNIVERSITY

# CERTIFICATE

This is to certify that dissertation titled "**AI and Blockchain role in Fraud Detection in an insurance claims: A Qualitative Study at Care Health Insurance** " is a record of the research work undertaken by Mrudula Vikas Borkar in a partial fulfillment of the requirements for the award of the degree of **MBA (Hospital and Health Management)** from the IIHMR University, Jaipur under my guidance and supervision and her approach to the research study has been sincere, scientific and analytical.

Faculty Guide: Dr. Sandipta Chakraborty

Place: IIHMR University, Jaipur

Date: 16.06.2025

School Dean: Dr. Sanjay Gupta

Place: IIHMR University, Jaipur

Date: 16.06.2025

## DECLARATION BY STUDENT

I hereby declare that this dissertation titled "**AI And Blockchain Role in Fraud Detection in Insurance Claims: A Qualitative Study at Care Health Insurance"** is the Bonafide record of my original research work. I declare that it has not been submitted to any other university or institution for the award of any degree or diploma. Information derived from the published or unpublished work of others has been duly acknowledged in the text.

(Signature)

Name of Student Mrudula Borkar.

Date 16/6/25

**ACKNOWLEDGEMENT**

Those who assisted me during the completion of my dissertation, "AI And Blockchain Role in Fraud Detection in Insurance Claims: A Qualitative Study at Care Health Insurance," I am eternally grateful to them and their support. First things first: My gratitude goes to Care Health Insurance and Dr. for their help. I am grateful to Pankaj Vats (Manager- Medical Claims) for allowing me to conduct this research within their organization. The department's staff, particularly those in Investigation, Claims, IT, and Audit, were instrumental in providing valuable insights and experiences that helped shape the study.

The Indian Institute of Health Management Research (IIHMR), Jaipur has been instrumental in creating an academic environment that fosters research and inquiry. I appreciate their efforts greatly. A special thanks goes out to Dr,Sandipta Chakraborty, for his invaluable guidance, regular feedback and help me improve my direction and quality of work.

My thanks go out to my friends and colleagues, particularly Mr. Hari Harsh, Dr. Rahul Mewara, Dr. Aishwarya Pundir for being a source of inspiration, motivation, and thoughtful counsel throughout this endeavour.

Finally, I want to acknowledge and thank my family for their endless love, emotional support, and faith in me. They have been the most effective support for me during this academic journey. This work relied heavily on the collective efforts, collaboration, and support of those mentioned. All of them are truly my utmost priority.' Thank you all.

**Abstract**

**Title:**

AI and Blockchain Role in Fraud Detection in Insurance Claims: A Qualitative Study at Care Health Insurance

**Author Name:**

Mrudula Vikas Borkar

**Advisor Name:**

Dr. Sandipta Chakraborty

**Keywords:**

Insurance Fraud, Fraud Detection, Artificial Intelligence, Blockchain, Health Insurance, Qualitative Study, Stakeholder Perceptions, Care Health Insurance.

**Background:**

The insurance sector is a highly susceptible field to fraud, which can result in substantial losses, operational inefficiencies, and premium increases. It is becoming more common to observe that traditional fraud detection methods, which frequently involve rule-based systems and manual interventions, are inadequate in detecting sophisticated fraudulent activities and managing large amounts of claims data with efficiency. By utilizing AI and Blockchain, fraud detection can be revolutionized through the development of automated, data-driven analytical capabilities and unambiguous transaction records. Having an understanding of the practical use and viewpoints of stakeholders regarding these technologies in any given organizational setting is essential for adoption.

**Objective:**

This study intends to investigate the fraud detection methods currently used at Care Health Insurance, pinpoint the current obstacles and constraints as seen by important internal stakeholders, and evaluate the possible function, perceived advantages, and obstacles related to the incorporation of AI and Blockchain technologies to improve fraud detection procedures inside the company.

**Methodology:**

A qualitative, exploratory research design was employed in this study conducted at Care Health Insurance. Data was collected through in-depth semi-structured interviews with eight key stakeholders from important departments, including the Fraud Control Unit (FCU), Information Technology (IT), Claims, and Audit. This method enabled the acquisition of valuable, specific information.... By systematically examining the interview transcripts, they were able to identify and analyze recurring patterns and themes that are relevant to their research objectives and questions.

**Results/Findings:**

As per the findings, Care Health Insurance has implemented a fraud detection system that relies heavily on its internal claims management process's basic rule-based flagging, as well as rigorous manual scrutiny and its staff'. Fraud can manifest in different ways, including charging higher fees, receiving inflated billings, being absent from hospitals, not reporting pre-existing conditions, and challenges with validating medical records. Departments have identified significant issues with manual processes, the lack of real-time data analysis capabilities, insufficient integration of data from multiple sources, and the increasing sophistication of fraudster. These issues are also evident across departments. For stakeholders, AI offers great potential for advanced data analysis and complex pattern recognition tasks, as well as predictive risk scoring undoing tasks such as identifying anomalous billing patterns and validating documents. The primary objective of blockchain technology is to establish dependable, unalterable, and transparent records of claim transactions, which in turn improves document reliability, reduces manual verification,and enhances trust. Despite this, other significant barriers to the utilization of these technologies included an expensive initial investment, significant IT infrastructure upgrades, difficulties connecting new technologies to older systems, the need for specialized expertise and training, and concerns about AI explainability and regulatory compliance. However, they were not the only limitations.

**Conclusions:**

The research indicates that Care Health Insurance's fraud detection processes are under increasing pressure. AI and Blockchain have a clear scope to improve fraud management through more efficacy, efficiency or proactive approach. A strategic approach that addresses the identified technical, financial, and organizational challenges is essential for integrating

these technologies. The research suggests that a phased adoption, targeting specific high-impact use cases and supported by investment in data infrastructure and workforce upskilling, would be the most advantageous approach. Care Health Insurance can shift towards a more secure and advanced fraud detection system by adopting this approach.

**CONTENT**

**Abstract…….1**

**Acknowledgement…….……...3**

**Abbreviations……....5**

**Introduction…….....8**

**Literature Review……...……11**

**Methodology ……...…23**

**Data Analysis and Result……..…… 26**

**Discussion …….…..34**

**References……...……37**

**Table of figures**

**Summary of the literature……..23**

**Information of the participants……..26**

**Codes and themes of fcu department…….27**

**Codes and themes of IT department……...30**

**Codes and themes of claims department……31**

**Codes and themes of audit department……..33**

# CHAPTER 1: INTRODUCTION

## 1.1 Background of the Study

The insurance industry, created to shield us from the uncertainties of life, is still shrouded in a persistent shadow: deception. It's not only financial damage but also a subtle chipping away at the foundations of the industry. Policyholders experience the same effects as policyholder, with premiums rising and claims management becoming slow and inefficient. In health insurance, the intricate nature of medical procedures and billing procedures can unwittingly provide opportunities for individuals to take advantage of these systems. The use of tools like software with specific rules to indicate suspicious activity and dedicated adjusters, investigators, and auditors scouring claims has been a battleground for insurance companies for years. Although these techniques are effective, the situation is changing. Why? Increasing numbers of claims mean that those who are deceiving investigators are becoming more sophisticated and creative in their methods. Consequently, these customary methods are starting to show signs of ageing, occasionally encountering new opportunities or getting stuck in the details. Changes in challenges are just as likely to result in solutions. The ongoing digital revolution has brought together potent new partners, including Artificial Intelligence (AI) and Blockchain technology, which are generating significant interest. Consider AI as a super-smart analyst, learning at an astonishing speed from vast amounts of data to spot subtle red flags and predict potential fraud. While Blockchain is frequently connected to digital currencies, it possesses a genuine edge in producing highly secure, unalterable data. The transparency and anonymity that Blockchain provides can make it possible to record the entire process of a claim, from filing to payout. Care Health Insurance, a prominent health insurance company in India, is the focus of this study. The question at hand is not just about AI and Blockchain; we also want to know how they could actually function within this particular company. How does Care Health Insurance currently combat fraud? What are the daily challenges and difficulties that their teams encounter? What is the prevailing opinion of the people in the field, such as managers, IT specialists, claims processors, and fraud controllers regarding AI and Blockchain? Technology's effectiveness hinges on its ability to address the needs of its users and solve problems. This study will provide a practical and precise depiction of the current state, as well as potential opportunities by conversing with these key individuals.

### 1.2 Statement of Problem

Even with all the hard work and dedication put into it, Care Health Insurance still faces a persistent and expensive reality that is not being completely stopped. Despite their worth, the methods used to detect fraud are under increasing pressure. Often, they become caught up in the constantly shifting tactics of fraudsters and find it difficult to handle the multitude of claims that require verification every day. This indicates that Care Health Insurance must investigate, and potentially adopt more advanced technological solutions.

How would Care Health Insurance integrate AI and Blockchain into their existing operations, given the potential benefits for fraud detection? What specific problems could they possibly resolve? Are there any significant difficulties that need to be addressed when starting them? I mean, what do people who use these systems think they are worth using? And why? The purpose of this investigation is to uncover the specifics of these questions, delving into their potential relevance in the context of AI and Blockchain-based fraud detection within this particular firm

### 1.4 Research Questions

This study is essentially a quest to find answers to some key questions:

1. What fraud detection mechanisms are currently implemented at Care Health Insurance?
2. What are the existing challenges in fraud detection as perceived by stakeholders at Care Health Insurance?
3. How can AI and Blockchain be integrated to enhance fraud detection mechanisms at Care Health Insurance?
4. What are the potential barriers to implementing AI and Blockchain in fraud detection at Care Health Insurance?

### 1.5 Research Objectives

To get to the heart of those questions, this dissertation has set out to achieve a few key things:

1. To investigate the current fraud detection strategies, tools, and everyday processes currently up and running at Care Health Insurance.
2. To pinpoint the limitations, snags, and challenges that the teams at Care Health Insurance see in their existing ways of detecting fraud.
3. To explore what AI and Blockchain could genuinely offer in tackling those fraud-related problems and boosting detection within Care Health Insurance.
4. To understand how the key people at Care Health Insurance – those who would be

working with these new technologies – feel about the benefits, the practicality, and any potential hurdles of adopting AI and Blockchain for fraud management.
5. Ultimately, to offer some practical, well-grounded suggestions on how Care Health Insurance could make its fraud detection even stronger, possibly by carefully and thoughtfully bringing AI and Blockchain into the mix.

### 1.6 Significance of the Study

Why does this research matter? Well, for Care Health Insurance. The expectation is that the outcomes will present some highly beneficial, practical suggestions from their own teams.... It's about examining their effective fraud detection methods, identify potential weaknesses, and use AI and Blockchain to aid them. Some important decisions regarding investing in new technology, improving processes, and assisting teams in developing new skills could be determined by this.
The Indian health insurance industry could benefit from the lessons learned from this study.. Care Health Insurance's new tech challenges and perspectives may resonate with other businesses in the same circumstances.... The objective is to broaden the already established understanding of how to practically confront fraud with the aid of cutting-edge technology.

The aim of this research is to provide a qualitative and practical perspective on AI and Blockchain in specific fields like healthcare insurance. It must be approached from an academic standpoint.? The goal is to demonstrate the perception of these technologies among those who would use them, particularly in India, where each one has its own unique circumstances. Furthermore, it emphasizes the importance of conversing with individuals and analyzing their experiences to determine the effective interplay between technology, individuals, and processes.

### 1.7 Scope and Limitations of the Study

- This study zooms in specifically on Care Health Insurance. Looking at their internal ways of doing things and how their employees see the issue of health insurance claims fraud.
- When we talk about AI and Blockchain, it's mainly about how they could be used to spot and stop fraudulent health insurance claims.
- The information gathered comes directly from conversations with people working in the Fraud Control Unit (FCU), the IT department, the Claims team, and the Audit team at Care Health Insurance.

- I’ve chosen to go for depth over breadth – meaning we've used a qualitative approach to get rich, detailed understanding rather than broad, statistical numbers.

## CHAPTER 2: REVIEW OF LITERATURE

The chapter provides a thorough analysis of the literature that is currently pertinent to the subject of insurance fraud, with particular attention to Artificial Fraud.

The detection and mitigation of it using AI and Blockchain technologies. The objective is to provide a theoretical and empirical basis for the present study, contextualize the research problem within existing knowledge, identify emerging trends, and identify the specific gaps that this dissertation intends to close. It will be a review of the nature and effect.

The intersection between insurance fraud and traditional detection mechanisms, the rise of AI and Blockchain as anti-fraud tools, their integrated potential, and other factors.

A particular arrangement of these technologies within the Indian insurance industry.

This review will also provide a conceptual framework for the study.

**1. Insurance fraud** is the deliberate deception of an insurance company or agent for the purpose of illicit financial gain (Barlybayev et al., 2021; Coalition Against Insurance Fraud, n.d.). At any point in the insurance lifecycle, such as application, underwriting and claims processing, it can happen. But this is a form of misleading. Attacked by policyholders, third-party claimants, medical practitioners, insurance agents, or organized crime scenes. The extent of insurance fraud is extensive and affects all types of businesses- Health, automobile, property, life, and workers' compensation insurance.

Insurance fraud results in staggering financial losses of tens of billions or trillions each year across different sectors and nations (Accenture, 2023; FRISS, 2020).

The losses are not only taken by insurance companies but also pass on to consumers through heightened premiums. Apart from direct monetary costs, insurance deception damages consumer confidence, maroons the insurance industry, and may even finance other illegal activities. Fraud is a factor in the rising costs of healthcare, which make services more expensive and difficult to obtain (National Health Care Anti-Fraud Association, n.d.).

### 2. How Much Damage Does Insurance Fraud Cause To People?

The monetary consequences of insurance deception are substantial, but the accuracy of statistics is often difficult to determine because these practices are usually conducted in

secrecy. Estimates indicate that fraud accounts for a significant portion of total claims expenses worldwide, amounting to billions of dollars annually (Coalition Against Insurance Fraud, n.d.; Insurance Europe, 2021). The U.S. economy spends over $40 billion annually on non-health insurance fraud, with an average of $400 per incident according to the FBI.

An extra $700 in premiums per family was issued by the FBI.

Gee & Button (2015) estimated that fraud and errors lead to 7.29% of global health expenditure being lost due to healthcare fraud.

**3. The diverse models of Health Insurance Frauds and their schemes.**

Various actors in the healthcare industry are responsible for health insurance fraud, which can be seen in multiple ways:

- Billing of unretained services: Providers may submit claims for treatments, consultations, or tests that were not performed. It can encompass a variety of items and complete imaginary patient experiences.
- The act of upselling services or procedures results in providers charging for services that are more expensive than what was charged. A brief overview of the billing process for a complete office visit is provided by some individuals- Consultation occurred.
- Separate charges are applied to services that are typically bundled under one billing code to maximize reimbursement.
- Misrepresenting a patient's diagnosis to justify non-medical procedures such as surgeries or tests.
- Using the identity and insurance details of an authentic policyholder to falsely claim for services provided or not given by another individual.
- Billing medical services that are not necessarily due to the patient's actual medical condition is prohibited.
- The referral of patients to providers who receive payment or benefits for referring them can result in kickbacks being given. Specialized professionals, laboratories, or for prescribing specific medications are frequently the cause of overuse or atypical treatment.
- Examples of prescription drug fraud are physicians prescribing unnecessary medications, pharmacies billing prescriptions that are not filled, and brand-name billing while others forgetting them. These cases are common.
- Patient-Side Fraud: Patients may conceal pre-existing conditions, exaggerate symptoms to receive disability benefits, or collude with healthcare providers to make false claims.

**4. The limitations of conventional Fraud Detection Systems.?**

- In the past, insurance firms have utilized diverse strategies to identify and prevent fraud. Numerous insurers utilize automated systems that use predefined business rules and algorithms to analyze claims data. The guidelines are commonly founded on recognized fraud warnings, including inconsistencies in information submitted, claims from providers with a history of suspicion, and unusually high levels or rates of fraud. The billing process is based on standard procedures or a rapid succession of claims from varying parties (Phua et al, 2005). Injuries that surpass specific monetary boundaries or those related. Certain therapies might receive automatic review notifications.
- 2.3.2. Manual scrutiny and adjudication are crucial when it comes to claims adjusters and processors. Participation in initial appraisal of assertions. Their experience and intuition are often used to detect anomalies or suspicious elements that automated systems may not be able to identify. This. Manual scrutiny entails the review of claim forms, supporting documentation (such as medical reports, bills, diagnostic results), and cross-referencing information.
- Most major insurance companies have a dedicated SIU or FCU. What are these units? Specialists are employed in these units. Experts in the field of investigation, typically those with experience in law enforcement or accounting. Their investigations involve complex or valuable suspicious claims, and they are highly detailed. The scope of this may involve conducting field tests, conducting interviews with claimants and providers, monitoring, and cooperating with law enforcement agencies (KPMG, 2016).
- Post-payment audits of providers are frequently conducted to uncover any potential data that could be used for analysis or discovery. Patterns of inflated prices or fraudulent practices). The use of basic data mining techniques can be employed to analyze historical claims data and identify patterns and anomalies that could indicate systemic fraud.
- In the face of modern fraud challenges, traditional methods are limited in their effectiveness. This is a cautionary tale:
- Detection is often difficult due to the reactive nature of the organism. "After" An untrue accusation has been made. Recovering lost funds is a costly and difficult task.
- Scalability and Efficiency are important factors in manual review processes, which can lead to time and labor intensive work. Intensive and insufficient to manage the rising volume of claims, leading to delays and potential oversights.

- Eradicating new and intricate fraud is not possible with rule-based systems, which are constructed from past fraud patterns. Identifying novel, advanced or complex deceptions is difficult for them to accomplish. Methods that deviate from established standards. Fraudsters are capable of comprehending and avoiding these regulations.
- Automated rule-based systems have a high incidence of false positives, which are legitimate claims that are wrongly flagged as suspicious. This wastes valuable investigator time and can lead to unnecessary scrutiny of genuine claimants, which could negatively impact customer relations (Viaene et al, 2005).
- An organization's data is frequently fragmented into multiple legacy systems, such as policy administration, claims, and underwriting, resulting in a lack of holistic perspective. It is challenging to obtain a comprehensive view of an entity due to the absence of integrated data. The provider or policyholder's past and connections, preventing the exposure of fraudulent activities such as collusive or syndicated fraud.
- The conventional approaches are generally inadequate at forecasting future fraudulent acts or identifying potential fraud trends in advance.

**5. Artificial Intelligence (AI) for Fraud Detection.**

What are the fundamental techniques used in AI?

AI is a broad area of computer science that involves the development of systems that can perform tasks that typically require human intelligence, such as learning. The field also includes cognitive functions and artificial intelligence. Language comprehension, reasoning, problem-solving techniques.' A few AI sub-fields and techniques are crucial for fraud detection.

- The field of Machine Learning (ML) is a subfield of AI that allows systems to learn from data without being programmed. ML algorithms detect patterns in past data to make predictions or decisions about new, unseen data.
- Supervised learning is used to train models on labelled data, which contains information about both fraudulent and non-fraudulent instances. Common algorithms include Logistic. The use of Regression, SVM, Decision Trees, Random Forests and Neural Networks.
- Models can detect patterns and anomalies in unlabelled data through unsupervised learning. By using clustering techniques like k-means or the Local Outlier Factor to detect

anomalies, it is possible to identify fraudulent claims or behaviours. These methods are widely used in statistical analysis.

- Semi-Supervised Learning employs a blend of labelled and unlabelled data, which can be advantageous when labelling all data is either expensive or unmanageable.
- Deep Learning is a type of machine learning that employs multi-layered neural networks to learn complex representations from vast data sets. This is the primary focus of this discipline. This technology has demonstrated remarkable proficiency in various domains, including image recognition and natural language usage Processing.
- Natural Language Processing (NLP) enables computers to understand and process information. Derive meaning from human language. NLP is a technique used to extract text from claim forms, medical reports, adjuster notes, and customer communications in insurance. Identify pertinent data and identify potential fraud warning signs.
- Uses statistical algorithms and ML methods to analyze current and historical facts to create forecasts for unknown or future events, such as the probability of a statement being deceitful.
- Network analysis (Link Analysis) involves the visualization and evaluation of linkages among different sources. A range of entities, such as claimants, providers, addresses, and bank accounts, can be employed to detect clandestine connections and fraudulent schemes.

6. Abdallah, Maarof, & Zainal (2016) and Joudicelli et al. (2015) have demonstrated **significant benefits in the application of AI in insurance fraud detection** (as seen in Figure 1) and 2), respectively).

- AI can now identify subtle, intricate, and non-obvious patterns that could be used to fraudulently commit crimes. Detection impossible for humans or traditional rule-making systems.
- Real-Time Fraud Scoring: With AI, each claim can be flagged and prioritized accordingly, ensuring fraud is not a concern.
- Effort increases can be achieved by optimizing AI models to decrease false positives and enable investigators to focus on highly suspicious claims.
- The detection of new fraud schemes can be achieved using machine learning models, especially those that utilize deep learning. Identifying new and evolving fraud tactics is easier with unsupervised learning or adaptive techniques rather than static rule-based systems.

- AI can automate repetitive tasks such as processing claims and screening for fraud, which could free up human resources for more efficient process-based work.Complex investigative work.
- By identifying fraudulent claims quickly, AI can streamline the review process and enhance efficiency. Addressing authentic grievances, boosting customer satisfaction.
- Employing NLP methods enables insurers to extract beneficial information from unedited data, such as adjuster notes, medical reports and social media. Key indicators for fraud detection are frequently present in these documents.

7. While the **benefits of using AI for fraud detection** are compelling, there are still some obstacles to be overcome:

- High-quality, clean and well-labeled historical data is necessary for training AI models, particularly in the field of deep learning. The use of data silos, inconsistent formats of information (such as MSCI or SAS), and missing data can all impact model performance.
- The complexity of understanding advanced AI models, such as deep neural networks, is a challenge that often arises due to their black box nature. Reasoning behind their predictions. This deficiency in transparency can pose challenges for the concerned individuals.?
- Adherence to regulatory requirements and the justification of actions taken based on AI-generated notifications. Adding new AI platforms to existing core insurance systems can be both expensive and technically challenging, especially when compared to outdated systems.
- The cost of implementation and talent: Investing in AI technology, infrastructure, and recruiting skilled data scientists and AI professionals can be expensive at first.
- Artificial intelligence models that are trained on biased historical data may perpetuate or even be fair. Increase existing prejudices, resulting in unjust consequences for specific groups of policyholders or providers.
- The methods used by fraudulent individuals remain evolving. The effectiveness of AI models against new fraud is dependent on regular monitoring, training, and updating Schemes.
- Regulatory and ethical concerns include questions of data privacy, the ethical use of AI in decision-making, and compliance with local data protection laws or GDPR.

**8. The use of Blockchain Technology for Fraud Prevention and Detection.**

Fundamentals of Blockchain Technology.

Blockchain is a digital ledger that is distributed, decentralized and can be modified.

Nakamoto (2008) emphasized the importance of transactions being secure and transparent.

A "chain" is formed by grouping transactions into distinct blocks, with key features associated with each block.

Include:

• Decentralization is achieved by distributing the ledger across a network of computers, eliminating the need for single-point storage locations.

• Transactions on the blockchain are untainted once they have been verified and recorded on our system. The network is highly susceptible to manipulation and deletion, which ensures the record's integrity and permanence.

• While public, private, or consortium blockchains may offer varying levels of privacy, transactions are typically disclosed to authorized participants. However Fostering transparency and auditability.

• Using cryptographic techniques like hashing and digital signatures to protect the blockchain, transactions on the network are made secure.

• Self-executing contracts that incorporate smart contract principles, where the terms of the agreement between buyer and seller are written in lines or stored in code throughout a distributed, decentralized blockchain network, there are agreements contained within it. They activate automatically when specific conditions are met.

**9. The utilization of Blockchain to Combat Insurance Fraud.?**

In the insurance industry, there are many innovative ways to use blockchain technology to combat fraud (Gatteschi et al., 2018; EY, 2019):

• Secure claims submission and processing by storing and using Claims data.?

Documents such as bills and medical records can be stored on a blockchain to provide dependable evidence for insurers, claimants, and providers.

• Effective identity verification can be achieved through blockchain technology, which can reduce the risk of identity theft and fraudulent policy applications for providers and customers. Verification-only credentials can be stored for later use. Shared with authorization and securely on the blockchain.

• The use of an immutable ledger, which is shared among relevant parties, can help prevent duplicate claims and ensure the identification and prevention of duplicate submissions.

• Smart contracts enable the automated verification and processing of specific claims.

For example, if a policyholder's verifiable health events, such as hospitalizations, are securely stored on a blockchain by reputable parties. A smart contract with a source (like e.g. london hospital) may automatically trigger claim processing and payout, provided that all conditions are met.

• Ensuring data integrity for supporting documents has been enhanced by storing cryptographic hashes of high quality. A blockchain facilitates the verification of the authenticity and legitimacy of medical records, lab reports, and repair bills by making it more challenging to submit documents that are not genuine or counterfeit. Additionally,

• Ensure transparency in the audit trail created by blockchain, which can be instrumental in investigations and regulatory actions/Compliance.

**10. How does Blockchain Technology help to combat fraud?**

• Accurate and unbiased information is fostered through shared, unchanging records in the insurance industry.

• The use of cryptographic security and immutability is crucial for ensuring the protection of data against unauthorised alteration.

• Smart contracts and simplified verification processes can significantly decrease manual effort and processing times through operational inefficiencies.

• Accurately and transparently record transactions through history.'

• The inherent transparency and ease of tampering with blockchain records can serve as a deterrent to potential fraudsters.

**11. Issues with Blockchain for Insurance?**

• Blockchain platforms may be scalable and perform poorly in terms of performance.

High-volume insurance businesses could encounter issues with transaction throughput and speed.

• Ensure that blockchain solutions can integrate with existing legacy IT systems and other blockchain networks, as well as ensure interoperability between the two networks.

Significant challenge.

• The regulatory and legal framework surrounding smart contracts and blockchain-based records is still evolving in various regions. Greater acceptance necessitates greater clarity regarding regulations.

• Developing, operating and maintaining blockchain solutions necessitates specialized skills and can involve significant upfront costs.

• Although blockchains can improve security, they also enhance privacy and confidentiality.

Whether public or private, blockchains are utilized to store confidential personal information such as birth and death details. Raises privacy concerns.

Common solutions include off-chain storage of the relevant data, using only hashes or referencing on-demand, or applying more sophisticated cryptographic techniques such as zero-knowledge proofs.

• The absence of industry-specific standards for data formats and governance models can hinder the adoption of consortium blockchains.

• Energy consumption is a notable characteristic of Proof-of-Work blockchains, which are highly efficient in this regard.

The use of energy is not a new phenomenon, but consensus mechanisms with higher energy efficiency (such as Proof-of-Stake) are becoming more common.

**12. Robust Fraud Detection Through Integration of AI and Blockchain: Synergies.**

The integration of AI and Blockchain offers a potent framework for developing additional digital capabilities.'".

Effortful and resilient fraud detection systems. Several significant complements exist between these technologies:

Blockchain can provide AI algorithms with reliable, non-manipulating data for their trustworthiness. The accuracy and reliability of fraud predictions can be enhanced by training AI models with high-integrity data (Salah et al, 2019).

• Blockchain data can be analyzed by AI, which has the capability to do so.

A blockchain can be used to gather data on transactions in order to identify fraudulent activities, anomalies or collusive networks that may not be detectable through simple queries.

• The use of AI can enhance smart contracts by adding an intelligence layer.

To illustrate, an AI model could be trained to assess the risk of a claim on the blockchain and then trigger underlying rules through recurrent execution of some kind of smart contract.

Variable responses to the risk score, such as receiving an immediate payment for low-risk and indicating for high-risk reviews.

• The use of blockchain could enable decentralized AI marketplaces that are secure and transparent, enabling insurers to utilize their own fraud detection algorithms.

• Providing a transparent and unchangeable record of AI decision parameters and outcomes through blockchain recording could help address the "black box" issue of regulatory compliance.

**13. The Indian insurance context of AI and Blockchain for Fraud Detection.**

Indian insurance industry, which has a high potential for growth. The use of AI and Blockchain presents a compelling scenario due to the challenges associated with fraud, as well as digital penetration. The extent and type of Insurance Fraud in India: Insurance fraud is a recognized problem in the country.India is especially at risk with health and motor insurance. Typical examples include the falsification of documents, false claims, misleading statements by policyholders, and provider-based fraud such as unnecessary procedures or overbilling for services not provided.

(IRDAI, various reports; PwC, 2018). It is challenging to obtain clear consolidated figures, however The Indian insurance industry's estimates suggest significant losses. Various reports, articles, and reporting from leading Indian financial news organizations (e.g, EY, KPMG, Deloitte, PwC) on the insurance industry in India. IRDAI has been actively supporting technological advancements in the insurance sector, with a focus on regulatory changes and digital initiatives.

Improving efficiency and customer service.

The purpose of initiatives such as the Insurance Information Bureau (IIB) is to establish data repositories that can be utilized for fraud detection. A foundation digital infrastructure has been established through the government's "Digital India" campaign and the India Stack.

Secure data exchange.

The ABDM, which is designed to create a national digital health ecosystem, has particular significance for health insurance and may leverage blockchain for security and consent management. Impaired data for AI-based health insights and fraud prevention, governed by robust privacy regulations.

• The adoption of AI and artificial intelligence in various fields is on the rise among insurance companies in India, with chatbots playing a significant role, along with fraud processing, underwriting risk assessments (Claims), and claims processing automation.

The task of detecting and stopping criminal activity (NASSCOM, 2021; FICCI & BCG, 2020) is assigned to the following missions: Several Insurtech startups in India are creating AI-based fraud detection solutions. What is the purpose of this development?

Analyses, predictive modelling, and anomaly detection for the Indian market.

• In India, the use of Blockchain in insurance companies is not as advanced as AI, but it is becoming more prevalent.

Industry consortia and individual insurers are exploring Blockchain for applications such as KYC, claims processing, and fraud mitigation (e.g., Bajaj Allianz's Travel Ezee), with discussions and pilot projects in progress. Working groups have been established by IRDAI to examine the regulatory aspects and implications of Blockchain Technology.

**14. Contextual Implications and Prospects in India.**

• Despite the growth in data generation, issues arise with data availability and quality. Why?

Strong AI models' development may be impeded by factors such as quality, standardization among different healthcare providers and accessibility.

• In urban and rural India, the lack of digital literacy or infrastructure access may impede the equitable implementation and reach of technology-driven initiatives.

Solutions.

• The complexity and expense of integrating modern AI and Blockchain platforms is compounded by the fact that many established insurers still rely on outdated IT systems.

• In India, there is a gap in the workforce for IT professionals, but there are still opportunities for those with expertise in AI/data science and Blockchain development.

• Regulatory adaptation is essential for innovation and adoption, which requires a distinct regulatory framework from IRDAI and other organizations to address data privacy, AI ethics, and blockchain-based records and smart contracts. Additionally, it must ensure the legality of these developments.

• Building trust and awareness among stakeholders, including insurance companies, is a crucial aspect of the strategy.

It is crucial for customers and providers to be aware of the advantages or safety of these new technologies.

**15. Stakeholder perspectives and Technology adoption frameworks.**

Success in implementing new technologies such as AI and Blockchain depends on the perceptions and acceptance of those who will use them or be affected by them. Frameworks like Davis (1989) and Venkatesh et al. (2003) (UTAUT model) provide guidance for understanding factors that affect user acceptance through Technology Adoption Models (TAM). The models usually concentrate on factors such as what is a positive or negative outcome.

User perception of ease of use and usefulness (the degree to which a user believes that using X would enhance their job performance) both measure levels.

The use of AI and Blockchain in insurance fraud detection raises questions for claims managers, investigators, IT workers, and auditors about the dependability, precision, level of effort, degree of safety, as well as potential ramifications on their job responsibilities and job security.

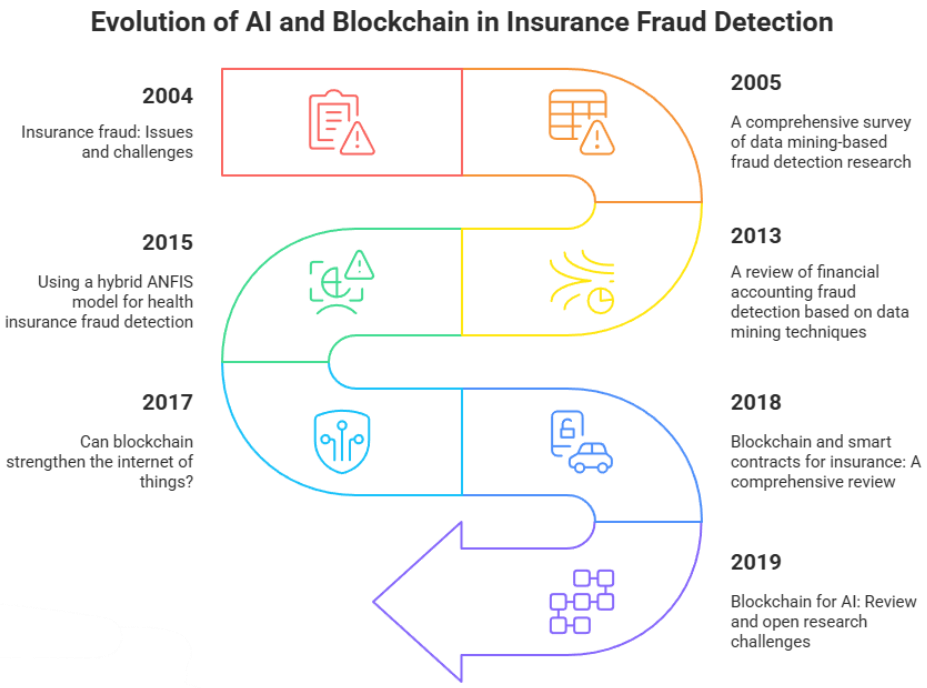
Organizational various factors, including guidance and encouragement from superiors or staff members; resources (training), training, and effective leadership.

Successful adoption and resistance reduction can be achieved through the use of change management strategies (Gagnon et al, 2016).

Understanding these human and organizational.

Implementation strategies based on dynamics require significant involvement.

Summary of Literature




## CHAPTER 3: METHODOLOGY

### 3.1 Introduction

This chapter thoroughly describes the methodological framework used for this dissertation. The primary goal of this research is to examine the existing fraud detection mechanisms at Care Health Insurance, recognize potential obstacles in detecting fraud, and evaluate the potential role of AI and Blockchain technologies. To achieve these objectives, it was decided that a qualitative research paradigm would be the most effective approach. The research design, rationale for its selection, the site of study, characteristics of the study sample group, sampling method, data collection methods, comprehensive analysis plan and ethical considerations.

## 3.2 Research Design

This study is qualitative.' The. An exploratory research design was employed in particular. The study's design is appropriate as it seeks to gain deep understanding and perspectives on complex phenomena, such as current fraud detection practices, associated challenges, and stakeholder attitudes towards new technologies like AI and Blockchain, within the context of Care Health Insurance. When the issue is not well-defined or understood, exploratory research can provide flexibility and generate new insights from the data. Its aim is to comprehend the 'how' and -why' of these practices and perceptions, rather than quantifying their frequencies or relationships.

## 3.3 Research Questions

1. What fraud detection mechanisms are currently implemented at Care Health Insurance?
2. What are the existing challenges in fraud detection as perceived by stakeholders at Care Health Insurance?
3. How can AI and Blockchain be integrated to enhance fraud detection mechanisms at Care Health Insurance?
4. What are the potential barriers to implementing AI and Blockchain in fraud detection at Care Health Insurance?

## 3.4 Study Setting and Timeline

The study was conducted at Care Health Insurance, a prominent health insurance provider in India. The primary data collection phase was conducted over a period of approximately four weeks, between 10th march 2025 and Access to participants was facilitated through official channels within the organization, following appropriate approvals.

## 3.5 Study Population and Sampling

Study Population: Care Health Insurance's target group included workers who were directly involved in claims processing, fraud detection, IT systems management related to these processes, and internal audit functions.

Sample Size: In-depth interviews were conducted with eight subjects for the study.... The initial narrative targeted a small number of individuals, but the quantity and quality of data obtained from these eight informants, which encompassed the main departments involved, was considered adequate to achieve data saturation for the key areas of interest in this trial.

However, the method of purposive sampling was employed. The selection process considered individuals with specialized roles, extensive experience (such as managers, senior managers or leads), and personal knowledge relevant to the research questions. The use of non-probability sampling enabled individuals to provide valuable and relevant data on fraud detection processes, challenges, and perspectives on AI and Blockchain

The primary method for collecting data was through semi-structured, in-depth interviews (IDIs). This approach was chosen because it has the structure of an "interview guide" that covers all the major areas, but also allows for additional exploration and opportunities to explore emergent themes while still maintaining a sense of what is to come.

The eight participants were each interviewed for just one purpose.

All interviews were conducted in real-time within the departments of each participant who worked for Care Health Insurance, enabling participants to observe contextual clues. Each interview lasted for an average of 20-30 minutes.

The participants' responses were recorded in detailed contemporaneous notes during each interview, with their answers included. In order to ensure a complete and precise record of the interview, these notes were reviewed immediately after each interview. No audio recordings were made.

3.7 Data Analysis Plan: Thematic Analysis

By utilizing the same systematic approach as Braun and Clarke (2006, 2012), we were able to analyse qualitative data from interview transcripts using thematic analysis, which was considered both flexible in its use and effective in uncovering patterns (themes) within rich qualitative information. It was an iterative process that involved the following distinct phases:

1. Familiarization with the Data: The first step involved transcribing all audio interviews accurately.. After analyzing the transcripts, they also listened to the audio recordings and read them repeatedly. This intense training was designed to provide a full understanding of the dataset and to record initial ideas as well as areas that could be covered.
2. Generating Initial Codes: Through systematic reading of the transcripts, early codes were assigned to segments of text that matched relevant research questions, ranging from brief words to lengthy sentences. The process was rigorous and thorough. The term code refers to a label that represents the essence of. Data-driven and deductively informed the process, resulting in codes being derived from the participants' narratives.

3. Searching for Themes: Once we had coded all the transcripts, the focus shifted to uncovering wider themes or general meanings.
4. Reviewing Themes: Two-level review was conducted for the potential themes.
5. Defining and Naming Themes: Once a well-defined group of topics was determined, they were all carefully defined and articulated in terms of their scopes or core meanings as well as how they relate to the overall plot of the data..
6. Producing the Report: The concluding segment entailed picking convincing and informative quotes from the contenders to validate each theme and sub-theme.

## CHAPTER 4: RESULTS AND FINDINGS

The chapter presents the empirical outcomes of semi-structured interviews conducted with eight key stakeholders from the Fraud Control Unit (FCU), IT, Claims, and Audit departments at Care Health Insurance.

The study involved eight participants holding managerial and senior-level positions within their respective departments. The purposive sampling method ensured that the selected individuals possessed deep domain knowledge and experience relevant to the research questions. The distribution of participants across the departments is as follows:

| Participant ID | Designation | Department | Gender |
|---|---|---|---|
| P1 | Manager- Fruad detetction | FCU(Fraud control unit) | Female |
| P2 | Senior Manager- Fruad detection | FCU(Fraud control unit) | Female |
| P3 | Manager- IT | IT department | Female |
| P4 | Senior manager – IT | IT department | Male |
| P5 | Manager- claims (Team lead) | Claims department | Male |

| | | | |
|---|---|---|---|
| P6 | Senior manager-claims | Claims department | Male |
| P7 | Team lead audit | Audit department | Male |
| P8 | Senior auditor | Audit department | Female |

### 1) Findings from the Fraud Control Unit (FCU)

Members of staff from the Fraud Control Unit (FCU) characterized their group as 'the main investigative unit of the firm' and were responsible for undertaking a deep analysis of claims flagged as suspicious by the Claims and Audit teams. They combine on-site fieldwork with a focus on data-driven analysis. 'Tariff fraud,' false bills, patient fraud (bogus hospitalization), non-disclosure of pre-existing conditions, and collusive fraud where patients and providers work together were all examples of the most common types of frauds mentioned by them.

They assert that the identification of red flags involves examining unusual high costs for uncomplicated procedures, short hospital stays with significant expenses, and suspicious patterns from particular hospitals. This is where the investigation begins. When the FCU identifies a claim as highly suspicious, it initiates an extensive investigation that involves visiting hospitals, conducting interviews with patients and doctors, and collecting physical evidence. The sheer amount of claims is a significant obstacle to keeping up.' According to them, the lack of real-time analysis and integrated technology results in them being reactive, which means that fraud can be investigated only after payment has been made. FCU officials expressed strong optimism that artificial intelligence could aid in identifying intricate patterns and scoring claims for fraud risk, while Blockchain would provide a means of preserving the authenticity of evidence by creating enduring records of all claims/documents.

Table 4.1 (shows codes and themes of FCU department)

| **Codes** | **Themes** | **Quotable Quotes (Participant)** |
|---|---|---|

| | | |
|---|---|---|
| Investigative Focus, Field Investigation, Ground-Level Work, Data-driven Role | FCU Role & Methodology | "My job is to really dig deep into suspicious claims... We're the people on the ground, getting solid proof of fraud..." (Manager FCU) |
| Tariff Fraud, Exaggerated Bills, Collusive Fraud, Hospital Fabrication | Types of Fraud Encountered | "Besides the usual stuff, I often see 'collusive fraud,' where patients and providers work together to cheat the insurance company." (Senior Manager FCU) |
| Red Flag Indicators, Hospital Reputation Check, Past Claim Analysis | Fraud Detection Techniques | "We look for stories that don't add up... and we also check the hospital's reputation and past claims." (Manager FCU) |
| High Caseload, Reactive Approach, Lack of Real-time Analysis | Challenges in Fraud Control | "The biggest problem is that we're always reacting. We often find out about fraud after it's already happened..." (Senior Manager FCU) |
| AI for Pattern Detection, AI for Predictive Analytics | Potential of AI | "Imagine AI systems that can instantly go through massive amounts of claim data to find really complicated fraud patterns that we'd probably miss by hand." (Manager FCU) |

| | | |
|---|---|---|
| Blockchain for Immutable Records, Enhanced Evidence Trustworthiness | Potential of Blockchain | "Blockchain has huge potential for making a record of all claim-related transactions that absolutely cannot be tampered with..." (Manager FCU) |

**2) Findings from the IT Department**

Participants from IT stated that they were responsible for handling the core technology used in all aspects of the claims process. According to them, the current fraud detection system is a fundamental rule-based element of their customized claims management system, which primarily flags minor issues such as duplicate claims or claims exceeding. The detection of fraud is impeded by significant technical obstacles, as they have highlighted. The most significant difficulty identified by both IT managers is the inability to perform real-time analysis, which implies that the system is reactive and analyzes past data instead of current transactions.

They also mentioned that the widespread disorganization of company data in unconnected, scattered systems poses a significant challenge for advanced fraud detection. The current infrastructure's ability to support advanced technologies was questioned, as it required significant upgrades and resource allocation for the implementation of AI and Blockchain. This was not a straightforward solution. Key issues included expensive costs, the need to hire or train experts in AI and Blockchain, and challenges associated with integrating new platforms into existing systems, making sure that AI is explainable—and ultimately complying with regulatory bodies.

Table 4.2 (shows codes and themes of IT department)

| **Codes** | **Themes** | **Quotable Quotes (Participant)** |
|---|---|---|
| Basic Rule-based Fraud Detection, Custom Claims Management System | Current Technology & Tools | "For basic fraud detection, we use a set of fixed business rules within that system. ...it's not very dynamic." (Senior IT Manager) |
| Lack of Real-time Analysis, Data Silos, Data Integration Challenge, Legacy System Limitations | Systemic Challenges & Limitations | "One of the biggest problems is that we can't do real-time analysis... Another challenge is that our data is scattered everywhere..." (IT Manager) |
| System Not AI/Blockchain Ready, Complex Implementation | Barriers to Adopting New Technology | "Our older systems aren't really set up to connect directly with AI and blockchain. ...It's not just a matter of 'plugging in' these advanced technologies." (Senior IT Manager) |
| High Implementation Cost, Skill Gap, Data Migration Difficulty | Barriers to Adopting New Technology | "Putting AI and blockchain into action would bring several challenges. First, it would cost a lot... Second, we'd need to hire or train a lot of people..." (IT Manager) |
| AI Explainability Issue, Regulatory Compliance Challenges | Barriers to Adopting New Technology | "There's also the problem of 'explainability' with AI... making sure we follow all the 'regulatory compliance' rules with new technologies is always a hurdle." (IT Manager) |

### 3) Findings from the Claims Department

The Claims department is the primary component of fraud detection. Why? Their primary duty is to handle the initial processing and adjudication of all incoming claims, which involves checking for policyholder eligibility, verifying document accuracy, and conducting a medical examination to determine if treatment was justified and necessary. Their approach heavily relies on basic system rules, as well as the "human touch" and experience of claims handler/medical team to detect suspicious activity. According to the Senior Claims Manager, fraud is primarily caused by hand-wiping and being vigilant.

This manual process is directly connected to the difficulties they confront. The presence of "false positives," where authentic claims are highlighted and scrutinized, necessitates a significant amount time and effort. The examiners documented a comprehensive inventory of warning signs they employ, such as costly surgeries for minor colds and pharmacy bill serial number variations, or when patients' vitals appear normal but treatment is for invasive disease. Additionally, they emphasized that "unplanned hospitals" are vulnerable to being used for fraudulent purposes. The department presently lacks AI-integrated tools to automate the intricate verification processes and depends solely on human judgment to detect abnormalities.

Table no. 4.3 (shows codes and themes of claims department)

| **Codes** | **Themes** | **Quotable Quotes (Participant)** |
|---|---|---|
| Initial Claim Screening, Medical Necessity Review, Suspicious Claim Flagging | Current Fraud Detection Processes | "Our process starts when we get the claim documents... a medical team reviews the claim... Any claims that look suspicious get flagged for a deeper look." (Claims Manager) |
| Red Flag: High Claim Amount, Red Flag: Short Stay, High Bill | Fraud Detection Techniques | "We have a list of warning signs we look for. These include things like super high claim amounts for common |

| | | |
|---|---|---|
| | | procedures, very short hospital stays with big bills..." (Claims Manager) |
| Medical Inconsistency, Single Stretched ICP, Provider Vulnerability | Prevalent Fraud Typologies | "We often find that 'unprepared hospitals are more prone to fraud,' especially... primary care hospitals... because they're easier to use for inflated bills and fake treatments." (Senior Claims Manager) |
| Manual Vigilance, Reliance on Human Experience, Lack of Smart Tools | Current Technology & Tools | "For fraud, though, it's mostly about us being vigilant by hand. We don't have any fancy software that can automatically spot complex fraud patterns." (Senior Claims Manager) |
| Challenge: False Positives | Systemic Challenges & Limitations | "We often get 'false positives' where a claim looks suspicious but ends up being real after we spend a lot of time checking it out." (Senior Claims Manager) |

**4) Findings from the Audit Team**

The Audit team is regarded as a crucial "second layer" of support in the fraud detection process, conducting both pre- and post-payment audits to ensure compliance and detect any violations. To identify fraudulent activities, they conduct a thorough analysis of claim records, paperwork, and financial information. Specific irregularities, such as division of services, conversions to more expensive methods, and claims from providers with suspiciously high average claim costs, are scrutinized by them.

The Audit team follows a manual approach like the other departments. According to the Audit Lead, they primarily go through claim documents manually and analyze data using simple Excel spreadsheets. However, this manual method is disputed by the "huge number of claims" and the constant intelligence of fraudsters. They pointed out that distinguishing between a genuine mistake and actual fraud is incredibly difficult due to the subjective nature of most people.

The Audit team participants were enthusiastic about and comprehended the potential of new technologies.. The use of AI may enhance their ability to identify peculiarities and patterns in massive datasets. Blockchain was a topic of great optimism for the Auditor, who believed it could revolutionize the industry by creating an undeniable record of all transactions.

Table 4.4 (shows codes and themes of audit department)

| **Codes** | **Themes** | **Quotable Quotes (Participant)** |
|---|---|---|
| Ensuring Compliance, Pre- and Post-payment Audits | Current Fraud Detection Processes | "Basically, my main job when we audit insurance claims is to make sure everything's on the up and up. ...We do audits before and after payments to keep things tight." (Audit Lead) |
| Upcoding, Unbundling, Provider Outlier Behavior | Prevalent Fraud Typologies | "Besides the usual stuff like inflated bills and unneeded treatments, I also watch out for 'upcoding' – that's when they charge for a more expensive service than what was actually done." (Senior Auditor) |
| High Claim Volume, Sophisticated Fraudsters, Distinguishing Error vs. Fraud, Reactive Fraud Detection | Systemic Challenges & Limitations | "The sheer number of claims is a huge headache... It's also hard to tell if something is just a genuine mistake or actual fraud – that takes a lot of judgment |

| | | |
|---|---|---|
| | | from experienced people." (Audit Lead) |
| AI for Anomaly/Pattern Detection | Perceived Potential of AI | "Yes, I've heard quite a bit about them, especially how AI could help us find weird things and patterns..." (Senior Auditor) |
| Blockchain for Audit Reliability, Anti-falsification, Document Authentication | Perceived Potential of Blockchain | "Definitely. Blockchain could change everything for us. It would create a record that simply couldn't be denied... Being able to prove that lab reports and other key documents are real would also be a massive help..." (Senior Auditor) |

## CHAPTER 5: DISCUSSION

### 5.1 Introduction

The chapter focuses on the qualitative interviews conducted with stakeholders at Care Health Insurance and provides a detailed analysis of the findings. In keeping with the literature reviewed in Chapter 2, it analyzes the current methods of fraud detection, the operational difficulties, and the opinions of stakeholders regarding Artificial Intelligence (AI) and Blockchain as potential means for better fraud identification.

Inquiries made by stakeholders were examined in A System Under Pressure. Among the issues identified in the study were:

The magnitude of operations is too large for manual verification to meet. Why? Finesse in Real-Time analytics can increase financial exposure by detecting the majority of fraud after payouts.

Problems with data integration arise when claims data is dispersed throughout systems and not centralized.

Coordination networks have become sophisticated techniques for exploiting blind spots in systems.

People consistently highlighted the "reactive" aspect of detection among their respondents. The inability to report suspicious claims at the entry-level results in resource-intensive investigations after damage is caused.

5.4. Ideas Concerning The Integration of AI and Blockchain.

5.4.1. The estimated value of AI is envisioned by advocates as a revolutionary means of automating and enhancing fraud detection. Identified capabilities include: Pattern identification in large datasets

• Automated anomaly detection. Claims are assessed for their predictive value through a risk assessment process. Obtaining duplicate GST numbers, lab results and billing methods. The move away from rule-based detection and towards AI-led pattern recognition could help tackle the burgeoning nature of fraud. Sharma & Panigrahi (2013) argue that this is consistent with the observation of AI's ability to detect subtle patterns and learn from past ones. Training neural networks on integrated datasets could enable the detection of collusion across provider networks.

5.4.2. Considered the potential of Blockchain Blockchain in providing documents with greater transparency, security, and immutability. Potential applications were mentioned by the participants, including:. Hospitalization-related time-stamped records. The examination and confirmation of medical records, such as lab reports, Make arrangements for audit trails and commentaries of claim reviewers. This is consistent with the work of Gatteschi et al. (2018) and Salah fm. (2019), who highlight the benefits of Blockchain in elevating confidence in data exchange and improving document origination. The use of Blockchain can enable the development of AI applications, as it facilitates decentralized access and safeguards against alterations.

5.4.3. While discussing the potential benefits of AI and Blockchain synergy, stakeholders frequently identified them as distinct but implied their complementary applications. Data is crucial for AI; Blockchain ensures the authenticity of structured information and provides assurance. Without the worry of tampered input, AI models can verify patterns by using Blockchain-stored lab reports as their source code. According to Salah et al. (2019), the "mutually reinforced architecture" involves AI controlling intelligence and Blockchain providing trust. 5.5. Stakeholders were receptive to the implementation obstacles, but

optimistic.: Technical challenges arise in legacy systems due to their lack of APIs or the ability to integrate AI tools. Cleaning and training models with slaloed data systems is challenging. High upfront costs are associated with hardware, software, and consulting services. •. There is a scarcity of internal talent in AI, machine learning, and blockchain development. Risks to Regulatory Issues: Compliance with IRDAI rules, data privacy laws and making the AI models understandable. The challenges identified are rooted in the concerns raised by industry reports from NASSCOM and policy studies concerning digital health infrastructure at a national level.

**5.6 Research Questions Answered**

1. **What mechanisms currently exist?** A mix of system-generated alerts and manual review; no advanced analytics or Blockchain.
2. **What are the key challenges?** High claim load, fragmented data, lack of real-time response, and rising fraud sophistication.
3. **How can AI and Blockchain help?** AI offers automation and intelligence; Blockchain ensures data transparency and trust. Together, they enable proactive, trustworthy fraud detection.
4. **What are the barriers?** Financial, infrastructural, skill-related, and regulatory challenges.

**5.7 Implications of the Study**

5.7.1. Context-Specific Variations of Technology Adoption Frameworks (TAM, UTAUT): This study adds context context specific variables such as regulatory clarity, infrastructural readiness, and domain specific training gaps to the framework. Additionally, it presents a practical interpretation of how AI and Blockchain are perceived in practice.

5.7.2. The Practical Implications for Care Health Insurance. Start pilot projects in document verification using artificial intelligence (AI). Utilize Blockchain to safeguard valuable medical records. Develop internal training programs and cross-functional tech implementation tems

5.7.3. Industry Implications Findings can be used to replicate for other Indian insurers.__ It is necessary to have shared data platforms, upskilling initiatives, and regulatory sandboxes. Using blockchain-led registers and AI-based anomaly detection engines could help standardize fraud mitigation across the industry**.**

### 5.8 Strengths and Limitations

**Strengths:**

- Detailed qualitative insights are present across all departments
- Technology innovation based on application
- An inclusive perception of Indian health insurance for context-sensitive purposes

**Limitations:**

- The small sample size limits the ability to make generalizations.
- Participant perceptions provide subjective information.
- The study's recommendations may be weakened by technological advancements

REFERENCES

1. Barlybayev, A., Sharipov, K., Sarsembayeva, L., & Abdisattar, G. (2021). Insurance Fraud: A Bibliometric Analysis. *Risks*, 9(10), 183.
2. Coalition Against Insurance Fraud. (n.d.). *Stats and Facts*. Retrieved from [Insert URL]
3. Accenture. (2023). *Combating Insurance Fraud with AI*. [User to find specific report title and URL]
4. FRISS. (2021). *Insurance Fraud Report*. [User to find specific report title and URL]
5. National Health Care Anti-Fraud Association (NHCAA). (n.d.). *The Challenge of Health Care Fraud*. Retrieved from [Insert URL]
6. FBI. (n.d.). *Insurance Fraud*. Retrieved from [Insert URL for FBI page on insurance fraud]
7. Gee, J., & Button, M. (2015). *The financial cost of healthcare fraud: a global estimate*. Palgrave Macmillan.
8. Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint cs/0509079*.
9. Viaene, S., & Dedene, G. (2004). Insurance fraud: Issues and challenges. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 29(2), 313-333.
10. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical

Science*, 17(3), 235-255.
11. Sharma, R., & Panigrahi, P. K. (2013). A review of financial accounting fraud detection based on data mining techniques. *Journal of Money Laundering Control*, 16(2), 129-150.
12. KPMG. (2019). *Fraud Risk Management – The C-suite challenge*. [User to verify title and find URL]
13. Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., & Goudarzi, M. (2015). Using a hybrid ANFIS model for health insurance fraud detection. *Journal of Medical Systems*, 39(9), 94.
14. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90-113.
15. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.
16. Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, 19(4), 68-72.
17. Deloitte. (2019). *Blockchain in insurance: From theory to reality*. [User to find specific report title and URL]
18. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: A an_extensive_review. *Future Internet*, 10(2), 7.
19. Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access*, 7, 10127-10149.
20. PwC. (2020). *Fighting fraud with AI and machine learning in the financial services industry*. [User to find specific report title and URL]
21. IRDAI. (Various Years). *Annual Reports*. Insurance Regulatory and Development Authority of India. [User to cite specific reports used]
22. NASSCOM. (2021). *AI adoption in India: The journey ahead*. [User to find specific relevant NASSCOM report on AI/BFSI]
23. FICCI & BCG. (2022). *India Insurtech Landscape and Trends*. [User to verify title and find URL or source]
24. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
25. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of

information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.
26. Gagnon, M. P., Nsangou, É. R., Payne-Gagnon, J., Grenier, S., & Gauthier, S. (2016). Barriers and facilitators to implementing electronic prescription: a systematic review of systematic reviews. *Journal of the American Medical Informatics Association*, 23(5), 1016-1026.
27. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.
28. Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 57–71). American Psychological Association.
29. Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage publications.
30. Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Sage publications.
31. Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education Limited.