EVALUATING CURRENT AND EMERGING TECHNOLOGIES IN FRAUD PREVENTION FOR HOTEL FINANCIAL SYSTEMS

AFRICA UNIVERSITY
A UNITED METHODIST-RELATED UNIVERSITY

2025

AFRICA UNIVERSITY

(A United Methodist-Related Institution)

EVALUATING CURRENT AND EMERGING TECHNOLOGIES IN FRAUD PREVENTION FOR HOTEL FINANCIAL SYSTEMS

BY

TAKUNDA JEFFREY LIMBANI KATUNGA

A DISSERTATION/THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELORS IN COMPUTER SCIENCE IN THE FACULTY OF

COLLEGE OF ENGENEERING AND APPLIED SCIENCES.

2025

Abstract

This study investigates how well current and new fraud prevention technology works in hotel accounting systems. It also identifies the leading difficulties and makes practical recommendations in an effort to improve fraud control in the hotels. As the hospitality sector faces a threat from financial fraud, hotels need to protect their income using supply chain solutions. This is because fraudsters are exploiting the hospitality industry's complex nature and many firms offer security. The study employs a mixed-method approach that includes insights from questionnaire responses and interviews. The document review has also ensured better clarity on existing fraud prevention practices and technologies being used to mitigate fraud in hotels. Many hotels are adopting fraud detection technology, the findings reveal. The study also lays out some vulnerability like slow response rates for detecting threats real-time, difficulties in integration with pre-existing finance systems, and inconsistency in observance to security policies by employees in the hotels, among others. New technologies like blockchain, AI fraud detection and biometric identification are also considered relevant to fraud prevention in hotels. The high prices and rules are making the use of the method hard and limited. Research indicates all-encompassing training of personnel and efficient enforcement of security measures, as well as embedding end-to-end fraud prevention frameworks in the hotel system should be totally integrated and transparent. The research incresearly utility of custom cyber insurance as well as the importance of basically enhancing existing offline fraud prevention.

Keywords: fraud prevention, hotel financial systems, cybersecurity, artificial intelligence, blockchain, hospitality industry

Declaration

I, Takunda Jeffrey Limbani Katunga declare that this dissertation is my original work except where sources have been cited and acknowledged. The work has never been submitted, nor will it ever be submitted to another university for the award of a degree. This was done with the close supervision of my supervisor.

Takunda Jeffrey Limbani Katunga	Tkatunga (28/03/25)
Student's Full Name	Student's Signature (Date)
…….	…….....
Supervisor's Full Name	Supervisor's Signature (Date)

Copyright

No part of this dissertation may be reproduced, stored in any retrieval system, or transmitted in any form or by any means for scholarly purposes without the prior written permission of the author or of Africa University on behalf of the author.

Acknowledgements

I sincerely thank my supervisor for all the help she has given throughout my work. I managed to complete the research with the help of all constructive feedback. I would also like to thank the Africa University staff, especially the College of Engineering and Applied Sciences, for the resources and academic environment essential for my research. A special thank you goes to the participants of this study. Their insights and experiences have significantly influenced this research. In the end, my family and friends deserve special mention for their constant support, motivation and patience throughout this journey. My greatest strength has come from their encouragement.

Dedication

I dedicate this dissertation to my Mother, Spiwe Masendu, whose unconditional support and belief in my abilities have always been the driving forces of my hope and own belief, she has fought tooth and nail to make sure I come out on top, as the best possible man I can be. This is also dedicated to my Step Father, Alex Siyavora, who has always seen and encouraged the champion in me and who has been my mother's rock and support in all that she does. My have always been ready to make the sacrifices needed for me to continue in my academic journey and life in general. My friends and mentors have also been instrumental in the shaping of my academic journey.

List of Acronyms and Abbreviations

2FA – Two-Factor Authentication

AI – Artificial Intelligence

AML – Anti-Money Laundering

API – Application Programming Interface

CCTV – Closed-Circuit Television

CNP – Card-Not-Present (transactions)

CVV – Card Verification Value

DLP – Data Loss Prevention

EMV – Europay, Mastercard, and Visa (chip card technology)

ERP – Enterprise Resource Planning

KYC – Know Your Customer

ML – Machine Learning

NFC – Near Field Communication

OTP – One-Time Password

PCI DSS – Payment Card Industry Data Security Standard

POS – Point of Sale

RBAC – Role-Based Access Control

RFID – Radio Frequency Identification

ROI – Return on Investment

TLS – Transport Layer Security

TPM – Trusted Platform Module

VAPT – Vulnerability Assessment and Penetration Testing

Definition of Key Terms

Artificial Intelligence (AI) in Fraud Detection – Artificial intelligence technology uses algorithms to analyze data for transaction activities to identify any suspicious financial transactions.

Blockchain for Fraud Prevention – Blockchain is a decentralized technology that is used to keep financial transactions safe and decreased fraud.

Biometric Authentication – Biometric authentication, which has various applications in mobile banking, means authenticating your identity using your fingerprints, facial recognition or retina scans.

End-to-End Encryption (E2EE) – The security that encrypts the financial data that the sending party wants to send which is kept encrypted until it reaches the receiving party. No third-party intermediary anywhere in between will ever have access to the data.

Cloud-Based Fraud Prevention – Cloud-based fraud prevention enables security experts to monitor, investigate and prevent fraud in real time on the cloud.

Tokenized Payment Systems – A tokenized payment system is a method of payment processing that replaces credit card information with a token.

Zero-Trust Security Model – Zero-trust security model refers to an approach to cybersecurity in which the identity of every user of the system is strictly verified, irrespective of whether they are within the network of the organization or outside it.

Financial Fraud – The intentional act of deception with the goal of financial gain, often by theft, fraud, or manipulation of financial transactions.

Internal Fraud – Internal fraud constitutes fraudulent activities carried out by personnel or insiders of a company. For instance, it can be done through unauthorized fund transfers, payroll fraud, or falsifying financial records.

External Fraud – External fraud occurs when fraud by customers or vendors like a phishing and credit card fraud happens that target a hotel's financial systems.

Identity Theft – The wrongful acquisition of identification information, the use of which in whole or in part is fraudulent

Contents

CHAPTER 1: INTRODUCTION

1.1 Introduction

For several years now, the hospitality industry has continued to acknowledge the need to protect its finances from fraud. This corresponds with similar developments made in other fields of business. Hotels would make use of security equipment and methods such as safe deposits, cameras and guard men for safety purposes. This was before the development and recognition of more sophisticated fraudulent threats. Today the industry has transitioned into a digital era. Cyber security in the area of financial transactions and hotel finances at large has become extremely critical. This is specifically crucial due to numerous cases of fraud in hotel financial systems. The cases range from staff stealing from their institutions to hacking by outsiders. What used to be a problem only at physical levels is now faced by hotels even in their digital interfaces.

Hotels' financial transactions and systems have been secured within the industry by applying already existing and some up and coming technologies in order to deal with fraud. As a result of strides made in the industry and on-going improvements, this dissertation is going to assess the current and the new emerging technologies that are being utilized by some organizations, together with those that some institutions are currently considering. This will add to the literature and methods of how hotels can better ensure robust cyber security for themselves. The researcher makes use of thorough analysis of methods and a variety of industry perspectives to propose what could be more secure frameworks against fraud in hotel finances.

1.2 Background to the Study

Digitalization in almost all aspects has been significantly embraced by the hospitality industry, mainly hotels. They seek to simplify their booking, check-in, checkout and financial processes to improve efficiency, enhance customer satisfaction and for the ease of doing business for their employees. However, this digital change has also opened up doors to more complicated forms of fraud. Unauthorized transactions, data breaches and internal embezzlement are now threatening both the financial stability and the reputations of organizations.

The traditional, mostly physical methods of preventing fraud within hotels are essentially ineffective against modern cyber-attacks. In response to these new and creative threats, hotels are employing more sophisticated technologies in order to protect themselves. These technologies and methods include but are not limited to; artificial intelligence (AI), blockchain

and multi-factor authentication (MFA). Specialized AI systems can review transaction information in real time and can identify irregular patterns according to its set parameters to flag what seems like fraudulent activity. The blockchain provides a tamper-proof, detailed ledger for transactions. Furthermore, MFA strengthens user-access controls by requiring multiple types of authentication from a user before one can access sensitive information or complete transactions.

Employee-related internal theft creates a unique and hard-to-solve occurrence of fraud where employees manipulate payment systems or generate fictitious invoices. These employees are authorized to access the financial systems of the hotels, making it harder to trace them and their activity. However, there have been proposed methods and technologies to combat these internal and external threats, which is what the researcher seeks to study and uncover in detail.

1.3 Statement of the Problem

The hotel industry, in particular, is constantly confronted with an increasing challenge of securing its financial systems against fraud. Today's digitalized world and having made the same improvements in the hospitality industry, has made them more open to sophisticated cyber-attacks and in-house fraud. Many hotels lack the capabilities to cope with modern-day fraud complexities, which may result in significant loses of money and damage to their brand images.

Fraudulent activities that are conducted through cyber activity from outside the organizations like unauthorized transactions and information breaches take advantage of the weaknesses that are present in digital payment systems and financial databases: this then leads to a loss in trust by clients on sensitive financial information namely, their banking and card details. Internal employee fraud including things such as payment manipulations or misappropriation of funds create a long-standing threat that is often hard to trace. Through the use of legitimate credentials for financial system access, employees can exploit internal controls' weak points resulting into heavy financial damages which are often uncovered a long time after damage is already done.

These are the main problems with current efforts for preventing hotel fraud that each have various dimensions and their own complexities. It is necessary to look closely at how existing

technologies can be combined with the new and be used more effectively to prevent external as well as internal fraud in hotel financial systems.

1.4 Research Objectives

1. To evaluate the effectiveness of current fraud prevention technologies in hotel financial systems.

2. To identify challenges faced by hotels in implementing fraud prevention technologies.

3. To propose recommendations for enhancing fraud prevention strategies in the hospitality industry.

1.5 Research Questions

1. To what extent are current fraud prevention technologies in hotel financial systems effective and how do they fall short?

2. What are the key challenges that hotels face in implementing fraud detection systems?

3. What are some effective existing and emerging technologies that hotels can utilize for fraud prevention?

1.6 Assumptions/Hypotheses

This study assumes that hotels that are taking part in this research have already implemented, or are in the process of implementing some form of fraud prevention technologies within their financial systems to protect both from internal and external fraud. It is also assumed that the departments that deal with hotel finances and the individual IT professionals involved possess enough knowledge and consciousness about current as well as emerging fraud prevention technologies. In addition, it presumes that participants will provide truthful and factually accurate answers in surveys and interviews that genuinely reflect on their experience and

personal with fraud prevention technology. Lastly, it is presumed that the data collected through surveys, interviews, and analysis respectively, will be relevant to and representative of the wider hospitality industry.

The first hypothesis is that current fraud prevention technologies significantly reduce the incidence of fraud in hotel financial operations compared to traditional measures of protection. Another hypothesis is that hotels encounter serious challenges like high costs, technical complexity, resistance to change from their users when seeing to adopt and integrate these technologies as well. Also, there can be increased effectiveness of existing fraud control measures by addressing concerns from relevant individuals and making suggestions according to particular requirements of the hospitality industry. The last assumption is that by understanding and minimizing these difficulties, hotels can have an improved utilization of the current and developing systems in order to prevent fraud, thus leading to better financial security.

1.7 Significance of the Study

This study is highly significant in improving financial safety within the hospitality industry, but more specifically, in hotels. With much more sophisticated fraud being carried out in all sectors more frequently than ever before. By analysing how effective current fraud prevention technologies are, this research examines them thoroughly to determine their strengths and weaknesses. For hotels to prevent both internal and external fraud, this comprehension is crucial for a hotel's smoother functionality as well as reputation among clients who need to be assured of their safety.

Another important part of this research revolves around identifying the main difficulties experienced by hotels while adopting fraud prevention cybersecurity technologies. Hotels often face such major obstacles as high costs, technical complexities; as well as employee resistance to change in their systems. This research will identify these challenges so that it can provide specific recommendations for overcoming them. The latter may facilitate better and wider adoption of these advanced security measures hence improving overall security posture in the

hospitality industry. To facilitate the smooth integration of these technologies, it is necessary to shed light on these implementation issues.

Policymakers and hotel administrators will find the results of this study highly valuable. Through evidence-based understanding of the effectiveness and challenges related to fraud prevention, this research can enlighten strategic decision-making processes and policy making. This will enable the hotels to make more informed decisions about investing in and integrating these technologies thus leading to stronger security frameworks. Policymakers can then develop regulations and guidelines that support hotels in their security efforts based on the nuanced understanding of fraud prevention in the hospitality industry that comes from such a study.

Again, this investigation will make a significant contribution to academic knowledge by filling in some gaps in the existing literature on fraud prevention in the hospitality industry. The study will provide a strong basis for future studies. It is through exploring both practical and theoretical aspects that the research will enable us realize on how such technologies can be effective in manipulating hotel financial systems. This scholarly input is important for creating new frameworks and models that can then be modified and tested in future investigations.

The main outcome of this research will result to actionable recommendations which aim at improving fraud prevention strategies within the hospitality industry. These recommendations shall be based on empirical data and insights from hotel finance and IT professionals. By giving pragmatic solutions that are designed to meet specific needs as well as conditions of the hospitability sector, this paper provides valuable guidance to all stakeholders involved with efforts of preventing fraudulent activities. With its pragmatic approach, these suggestions guarantee their theoretical foundation as well as practicality.

1.8 Delimitation of the Study

The primary concern of this research is examining the efficacy of technologies designed to avert fraud in hotel financial systems within the context of the hospitality industry. It will mainly look at hotels that have already used protective measures and are planning to incorporate more sophisticated financial security systems. The focus will be on hotels as

opposed to other sub-sectors in the broad framework of the hospitality industry including; travel agencies, lodges, restaurants and varied services firms.

1.9 Limitation of the Study

The scope and findings of this study may be limited by several factors. First, depending on hotel professionals' self-reports may create response bias or inaccuracies. Second, the sample size and representativeness of the hotels surveyed may influence the results, making them applicable only to a few hotels within the hospitality industry, thus limiting its generalizability across the entire sector. Thirdly, given that technology changes rapidly as well as cybersecurity; it is important to note that fraud prevention technologies can have different impacts at any given time. This study gives a picture of current practices and perceptions in relation to this subject during one point in history because it might not be relevant tomorrow.

CHAPTER 2 REVIEW OF RELATED LITERATURE

Chapter 2.1: Introduction

The contemporary hospitality industry necessitates financial system management as a means of sustainable operations and keeping trust with stakeholders. As hotels try to maintain profitability and guard against fraud, the uptake of new technologies has proven imperative. This part consists of an overview of the literature on fraud in the hotel sector and assesses how different cutting-edge technologies help to fight fraud. By incorporating state-of-the-art security protocols, utilizing digital solutions, and cultivating a proactive corporate mindset, hotels can well handle ever-changing risks from criminals.

Chapter 2.2: Theoretical Framework

Fraudulence is a major challenge in the hospitality industry, resulting in regulatory penalties, customer compensation and investigation expenses besides other financial losses. Hospitality sector fraud generally divides into two main categories: internal and external frauds. External ones consist of cyber-enabled crimes, consumer deception and supplier scams. Cyber-enabled one focuses on stealing intellectual property as well as client data while deceptive activities within an organization like making false refunds, discounts or payments are considered as customer fraud whereas the creation of fake expenditures or overpricing organizations is known as supplier fraud. Internal Fraud also referred to occupational fraud, involves cooperation among insiders who manipulate books of accounts so that they can embezzle

funds. For instance, it can happen when an account clerk falsifies correspondences approved by his/her supervisor (account supervisor), whereby the chief accountant produces forged and genuine notes to enable smoothening things up for all involved parties. This case study highlights the importance of strong measures against fraud while at the same time ensuring that no form of unauthorized access is allowed. Falsification of financial records constitutes a common sort of false activities practiced by people in hotel finance systems. Employees may manipulate financial statements to hide their embezzlement acts, thus making it hard for routine audits to uncover discrepancies. When several personnel are involved in approving transactions, it serves as a way of hiding fraudulent actions and poor internal controls and oversight mechanisms which contribute further to fraud's rampantness (Alemar, 2024).

Hotels have been adopting sophisticated cybersecurity measures to fight these different forms of frauds. Sensitive financial information can be secured through data encryption. Additional security is provided if two-factor authentication (2FA) is implemented so that even if login credentials have been compromised unauthorized access would be minimized (Kassem, 2024). By verifying transaction authenticity and raising red flags for examination, automated invoice matching systems accompanied by digital authorization forms actually enhance accuracy and compliance regarding such transactions thereby curtailing fraud. Emerging technologies like contactless check-in systems and digital authorization forms are crucial in boosting fraud prevention efforts. This includes meeting guests' expectations for ease of use, integrating with high-level anti-fraud mechanisms to protect guest data and transactions.

For example, solutions such as the Canary Contactless Check-In represent excellence in terms of infrastructure which is PCI Compliant and robust fraud algorithms for seamless interaction with guests (Alemar, 2024). Comprehensive employee training and effective communication are also important to consolidate measures on fraud control. They need to be empowered as front-liners against fraud by teaching employees how to detect and report potentially illegal activities thus fostering a vigilant organizational culture (Horng et al., 2018).

Hotels can significantly improve their ability to prevent fraudulence, protect their financial systems as well as retain customer confidence by embracing these state-of-the-art technologies

while building an active organizational culture. Both financial integrity and secure guest experiences during the entire stay would be ensured through this integrated approach.

Chapter 2.3: Relevance of the Theoretical Framework to the Study

The theoretical framework provides a comprehensive analysis of various types of fraud within the hospitality sector and the technological measures employed to prevent them. Technological advancements in tourism and hospitality are reshaping traditional practices and enhancing operational efficiencies. Innovations such as iPad check-in systems and integration of local cultural elements elevate guest experiences and strengthen internal controls against financial risks (Horng, Tsai, & Hu, 2018). Technologies like Near-Field Communication (NFC), Global Positioning System (GPS), and Virtual Reality (VR) enable seamless navigation, immersive experiences, and personalized services, which not only attract tech-savvy travellers but also empower hotels with real-time data for informed decision-making and robust fraud detection capabilities (Gençer & Mil, 2018).

Hotels confront external threats such as cyber-enabled fraud and industrial espionage by implementing data encryption and robust access controls (Alemar, 2024). Two-factor authentication further enhances security by adding layers of verification, mitigating risks from both internal and external actors. Comprehensive security monitoring systems detect and mitigate suspicious activities promptly, including monitoring online reviews and ad spend patterns to pre-empt reputation damage or financial losses (Özkan & Duran, 2018). Vendor fraud, particularly in smaller hotels, is mitigated through automated invoice matching systems and thorough vendor due diligence. Modern point-of-sale systems equipped with fraud detection capabilities address internal threats like skimming and inventory theft. Manager approvals for transactions and inventory monitoring via security cameras reinforce internal controls and deter fraudulent activities (Kassem, 2024).

To mitigate the risk of fraud, hotels are increasingly turning to technological solutions that enhance the security and integrity of financial systems. Implementing secure data encryption and stringent access controls ensures that sensitive financial information is protected from unauthorized access. Transitioning from paper-based to digital authorization forms and automated invoice matching systems enhances accuracy and compliance (Alemar, 2024). These technologies verify the authenticity of transactions and flag discrepancies for further

investigation. Incorporating two-factor authentication (2FA) for accessing financial systems adds an additional layer of security. This measure ensures that even if login credentials are compromised, unauthorized access is still prevented (Kassem, 2024).

Utilizing real-time monitoring systems and advanced fraud detection algorithms helps identify suspicious activities promptly. These systems analyse transaction patterns and alert management to potential fraud, enabling swift action to mitigate losses. Conducting regular security audits to review internal controls and employee training programs helps in identifying vulnerabilities and educating staff on best practices for fraud prevention (Özkan & Duran, 2018). Training employees to recognize and report suspicious activities is crucial for maintaining a secure financial environment (Horng, Tsai, & Hu, 2018).

Emerging technologies like contactless check-in systems and digital authorization forms are crucial in boosting fraud prevention efforts. This includes meeting guests' expectations for ease of use, integrating with high-level anti-fraud mechanisms to protect guest data and transactions.

For example, solutions such as the Canary Contactless Check-In represent excellence in terms of infrastructure which is PCI Compliant and robust fraud algorithms for seamless interaction with guests (Alemar, 2024). Comprehensive employee training and effective communication are also important to consolidate measures on fraud control. They need to be empowered as front-liners against fraud by teaching employees how to detect and report potentially illegal activities thus fostering a vigilant organizational culture (Horng et al., 2018).

Hotels can significantly improve their ability to prevent fraudulence, protect their financial systems as well as retain customer confidence by embracing these state-of-the-art technologies while building an active organizational culture. Both financial integrity and secure guest experiences during the entire stay would be ensured through this integrated approach.

Chapter 2 Summary:

The chapter defined the overall effect of dishonesty on hospitality business, and assessed how effective the current and emerging technologies can help in preventing it. It gives an overview

of various kinds of frauds external or internal and shows countermeasure technology used. In order to preserve the trustworthiness of their financial systems and uphold guest faithfulness, hotels should use advanced technologies, promote proactive culture within organizational framework among its employees and conduct all-encompassing training programs for staff. The chapter stresses that continuous innovation is vital in outpacing changing threats rather than being complacent with existing security measures.

Chapter 3 - Methodology

3.1 Introduction

This chapter outlines the research methodology to be used in evaluating the current and emerging technologies in fraud prevention of hotel financial systems. It consists of research design, population and sampling, data collection instruments, data collection procedure, analysis and organization of data as well as ethics. These components give a structure to the study ensuring that the researcher's findings are reliable and valid.

3.2 Research Design

The methodological approach employed in this study is mixed a methods design, using both qualitative and quantitative designs to gain a comprehensive understanding of the problem of fraud and how it is and may be minimized and prevented by anti-fraud technologies in hotel financial systems. The qualitative part of the research will be done through industry experts' interviews while the quantitative part will involve surveys carried out on financial controllers and managers. This double barrel approach ensures that it will capture insights at micro level as well as general trends, therefore enriching the overall analysis.

3.3 Population and Sampling

Financial controllers and IT personnel in different hotels of various areas are the select sample group for this study. A purposive sampling method is employed to choose respondents with experience and relevant knowledge on hotel financial systems and their fraud prevention technologies. This would allow the researcher accurate and usable data.

3.4 Data Collection Instruments

The study utilises three main instruments for gathering primary data, which are; a questionnaire, interview guide and document reviews. The survey questionnaire targets the quantitative collection of data, interviews and document analysis will target the qualitative

collection of data. These all together form the mixed methods approach of data collection instruments for this study.

3.5 Data Collection Procedure

In order to collect data, the process is combined into a system with a mixed methods approach of data collection. First, an online survey questionnaire is to be sent to a sample of the relevant individuals, which consists of the information technology department of a hotel and anyone else involved in the setting up and maintenance of its cyber-security in the area of finances. Participants are expected to email back their completed surveys. In order to obtain high response rates, reminders are to be sent out in case of any non-responses whatsoever in this initial process. Secondly, another select group of individuals are to be interviewed either face-to-face or via video conferencing for detailed information. Each interview taking between ten to twenty minutes in order to respect the people's time and to also keep them engaged. Document reviews to be collected online and from the participant hotels themselves, of industry standards and approaches would be another method of data collection, it would give insight into best practices and why they work as well as an idea of the improvements that could be made.

3.6 Analysis and Organization of Data

Several steps are to be taken in the data analysis process. Statistical software is to be used in order to analyse quantitative data collected from the survey, with descriptive statistics such as frequencies and percentages used to summarize the information it will streamline the process of identifying similarities and differences in participants' responses. Correlation and regression analysis are inferential statistics that help explore relationships between variables drawn from responses. With thematic analysis, qualitative data from the interview transcripts is to be analysed by coding ideas and methods in the responses, this then simplifies identifying repetitive themes and patterns concerning how fraud prevention technology has been put into use and its impacts thereof in this case.

3.7 Ethical Considerations

For the sake of conducting a fair and acceptable study, the researcher has thought about and considered multiple ethical points of view. One consideration and point of action is that all participants are given an informed consent form explaining the purpose of the study, their rights as well as the confidentiality of their responses before the research commences. There is also prior consent before one can participate in the survey or interview. Another is that participants'

identities should remain anonymous and confidential; data must be securely stored and only accessible to the researcher. In addition, there must not be any reports or publications resultant from this study containing any disclosure of participant identities. Most important is the fact that participation in this study is entirely voluntary and any subjects' withdrawals will be accepted as they are by the researcher and not result in any consequences for the subjects.

3.8 Summary

This chapter gives a detailed description of the procedure that is to be employed to examine the facts of current and emerging technologies for fraud prevention in hotels. It systematically blends both qualitative and quantitative methods in its execution. The research design, target population, sampling technique, data collection instruments used, method of collecting data, analysis and presentation of data and ethical issues were all well explained to guarantee objectivity and dependability of the study results.

CHAPTER 4 DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

In this chapter the researcher's data collected has been presented, analysed, and interpreted to meet respective objectives in this chapter. This report shall meet in these earlier chapters.

This chapter starts with a brief overview of the data collection process that was selected and implemented. The chapter also highlights the methods that were used in order to gather both quantitative as well as qualitative data in this mixed-methods approach.

The research utilized questionnaires, participant interviews, and existing related documents for review in order to gain well-rounded insights into fraud prevention technologies in the financial systems of hotels. Before the data collection, all participants gave their consent. The quantitative data, which came mostly from the questionnaire responses, are presented in detail in charts, tables and other statistical summaries. The data from the interviews has been analysed through thematic analysis. As a result, patterns, challenges, and emerging trends are noted in the fraud preventions with the document analysis.

4.2 Sample Profile

This section of the study provides a complete overview of the sample profile that was used in the study. The section includes an analysis of the participant response rate, this ensures that the data collected by the researcher is representative of the relevant key stakeholders in the Zimbabwean hospitality industry for this study. Since this study focuses on fraud prevention technologies for hotel financial systems, the sample was carefully selected so that it included professionals that are directly involved in both the managing as well as securing of financial transactions within the hospitality industry, hotels especially.

The researcher sought input from a diverse group of hotel industry professionals. The first of those that were selected were Information Technology managers and system administrators, those people who are responsible for implementing, managing, and securing accounting and financial systems in general. Another sample of participants that was selected were cybersecurity specialists, who are involved and specialize in detecting and preventing any and all fraud attempts on company digital platforms. The next group of participants considered and included were finance managers and accounting personnel, which are a group of people who conduct as well as oversee financial transactions and detect irregularities. Hotel operations managers, who have a role that involves ensuring that compliance with fraud prevention policies is met by their hotel and personnel. The last participants that were involved and engaged were a number of fraud prevention consultants, who were picked because they provide external expertise on improving security measures in financial transactions and would most probably have experienced a number of fraud incidents with their clients. These participants were targeted and engaged in order to gain an in-depth understanding of the current and emerging fraud prevention technologies in Zimbabwean hotels and the hospitality industry at large. The responses received provided great insight into how businesses in the hospitality industry, especially hotels protect their financial systems. The researcher gained insight into the effectiveness of existing fraud prevention measures as well as the challenges that these key stakeholders face in implementation.

4.2.1 Response Rate Analysis

A total of 80 professionals were invited to participate in the study by the researcher. They were invited to take part in the study through a consent form, which detailed the goal of the study and the matter of confidentiality, as well as the fact that they reserve the right to be a part of the study or to pull out at any time. Through a combination of questionnaires and structured

interviews the professionals gave their own first hand insight on the matter of fraud prevention systems in the hospitality area. The research aimed to maximize participation by reaching out to individuals from different hotel sizes and in different roles of operation, ensuring a broad perspective on fraud prevention, from those who implement to those that face the effects of that implementation. The response rate was then analysed in order to assess the level of engagement among the targeted participants. The breakdown of all responses and non-responders is presented in Table 1 below.

Table 1: Response Rate Analysis

Category	**Invited to Participate**	**Responded**	**Completed Responses**	**Response Rate (%)**	**Completion Rate (%)**
Questionnaires Sent	60	49	41	81.66%	68.33%
Interviews Requested	30	17	15	56.66%	50%
Total	90	66	56	73.33%	62.22%

From the total of 90 targeted participants, 66 participants responded. This was representative of an overall response rate of 73.33%. However, not all the responses were fully completed by those that participated; only 56 responses (62.22%) were fully usable for the researcher's data analysis. The researcher distributed 60 questionnaires, where finance, IT, and cybersecurity professionals in various hotels were targeted. From those 60, 49 individuals responded, which gave a response rate of 81.66%. However, it turned out that 8 of these responses were incomplete, leaving 41 fully usable responses, which gave a complete response rate of 68.33% for the questionnaires alone. A total of 30 structured interviews were requested with professionals in the fraud prevention space, these individuals being, mostly, consultants for other businesses. The researcher manages to have 17 interviews granted, which gave a response rate of 56.66%. 15 of these 17 interviews were fully completed by recording and transcription. This, in total gave a 50% completion rate. While the response rate was relatively strong. The

researcher found that a number of factors which challenged participation affected the research. Time constraints were the first big issue. A number of the participants, particularly IT managers and finance professionals, mentioned that heavy workloads and tight deadlines were a reason for not participating at all, as well as not completing the questionnaire or attending scheduled interviews. A number of confidentiality concerns were raised. Some respondents were hesitant to disclose detailed fraud prevention measures. They feared that such information could be sensitive for their organizations. The participants also withheld some information on fraud incidents that occurred within their organizations, for reasons of not exposing their company vulnerabilities, as well as the fact that some these incidents were still under investigation. Another problem the researcher ran into were corporate approvals. Several of the targeted respondents required approval from hotel management, some from their head offices, in order to participate. In some cases, permission was denied due to internal policies, and in some other cases, permission took very long to receive.

Some of the participants had a very limited awareness of fraud prevention technologies, within their own companies and just in general. Some small and medium-sized hotels had limited to no exposure when it came to existing and advanced fraud prevention technologies. This made participants at these hotels reluctant to engage in detailed discussions, or to even participate at all. Despite the challenges faced, the overall response rate of 73.33% was sufficient for insight and robust data analysis. The diversity in responses provided valuable insights. The effectiveness, challenges, and potential improvements of fraud prevention technologies within Zimbabwe's hotel industry were all exposed and laid out. The 62.22% completion rate is considered acceptable for research in the field of hospitality and cybersecurity. In these fields confidentiality concerns as well as workload constraints often impact people's participation. The broad range of participants across a number of different hotel sizes and multiple job roles ensures that the findings are well-representative of the entire industry. The response rate analysis confirms that the reliability and relevance of the collected data. The next section (4.2.2) will further analyse the demographic profile of the respondents. It will examine factors such as the sizes of hotels, participant's job roles, and their years of experience. These are factors which are critical for understanding the effectiveness of fraud prevention technologies in their different settings.

4.2.2 Sample Demographic Characteristics

This part of the study focuses on how and who contributed to this study and all those involved. The research was aimed at people in the hotel sector involved in financial security and fraud prevention. They included IT personnel, cybersecurity professionals, finance officers, and hotel managers responsible for hotel fraud detection and prevention in Zimbabwean hotels. The researcher collected data from 66 respondents who either filled questionnaires or were interviewed. The respondents were made of a wide variety of professionals from small, medium, and large hotels operating in Zimbabwe. The breakdown of the respondents by job title, hotel size, and years of working in the hotel industry.

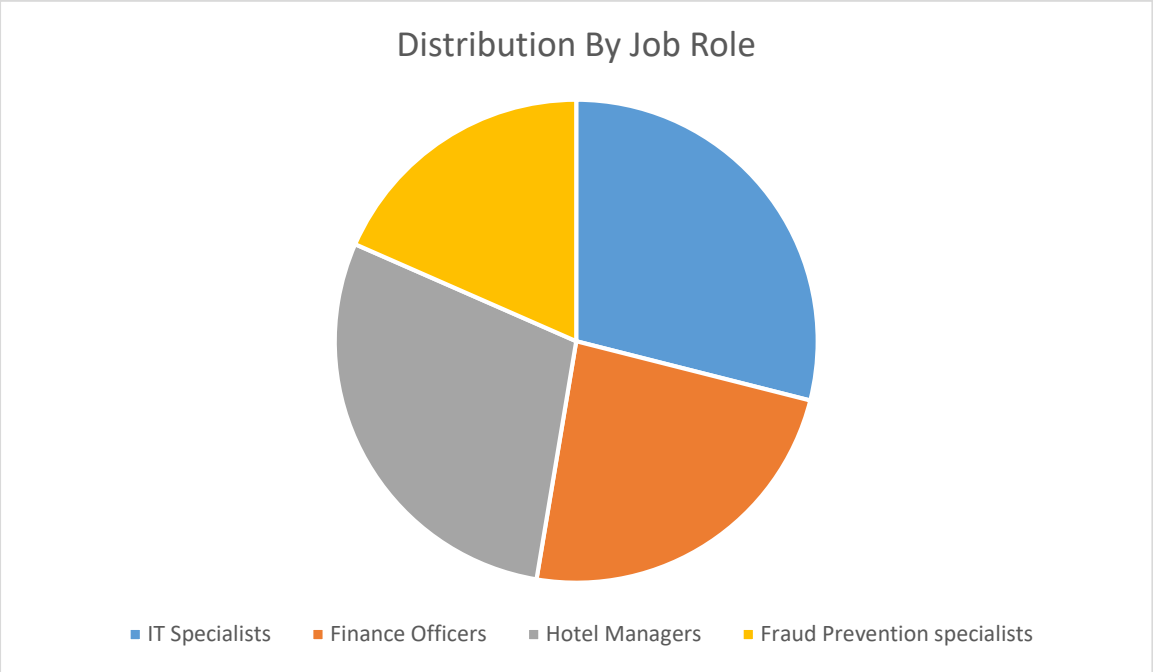
4.2.2.1 Respondents' Distribution by Job Role

The research was directed towards those who worked in hotels to set up, maintain and secure financial systems. As presented in table 2 below, job role-wise distribution of the respondents.

Table 2: Respondents' Distribution by Job Role

Job Role	Number of Respondents	Percentage (%)
IT Specialists (Hotel IT Administrators, Cybersecurity Officers)	22	33.33%
Finance Officers (Accountants, Auditors, Revenue Managers)	18	27.27%
Hotel Managers (General Managers, Operations Managers)	14	21.21%
Fraud Prevention Specialists (Risk Analysts, Compliance Officers)	12	18.18%
Total	66	100%

Pie Chart 1:



The majority of respondents (33.33%) were IT specialists. They are important respondents as they implement and maintain fraud prevention technology in organizations. Almost a third of respondents belonged to a specific category, finance officer; they are accountants and auditors directly involved in fraud detection. The dataset included hotel managers, who accounted for 21.21% of the sample, due to the fact that they supervise financial and operational decision-making of their hotels. The sample also included those specialists, like risk analysts and compliance officers, that will implement policies so that fraud will be reduced, as they will understand what the regulatory frameworks are that can help alleviate fraud, or at least prevent its incidence. In other words, fraud prevention specialists make up 18.18% of the sample.

4.2.2.2 Respondents' Distribution by Hotel Size

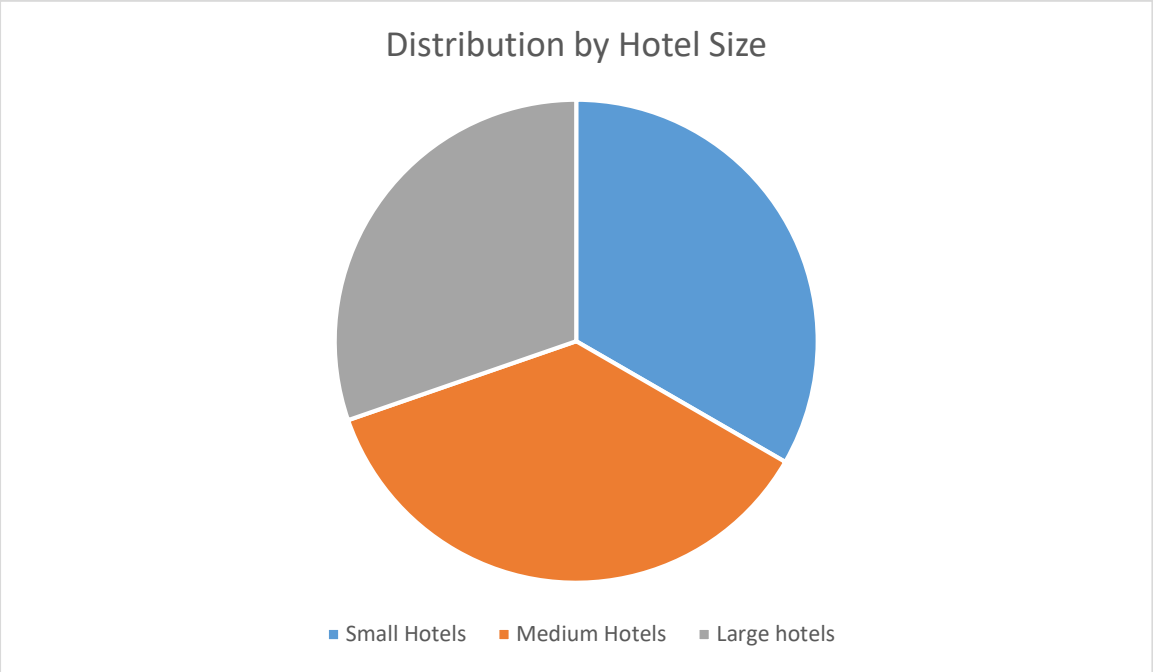
The study included respondents from hotels with different sizes to get a balanced view. Table 3 below shows the distribution of respondents as per the size of the hotel they are working for and the pie chart visualizes the hotels' distribution.

Table 3: Respondents' Distribution by Hotel Size

Hotel Size	Number of Respondents	Percentage (%)
Small Hotels (Less than 50 rooms)	22	33.33%

Medium Hotels (50–150 rooms)	24	36.36%
Large Hotels (Above 150 rooms)	20	30.30%
Total	66	100%

Pie Chart 2:



According to the results, medium hotels (36.36%) were the most represented sample, followed by small and large hotels 33.33% and 30.30% respectively. This means medium-sized hotels in Zimbabwe are most likely more involved in fraud prevention due to their requirement of scalable security which is affordable and effective.

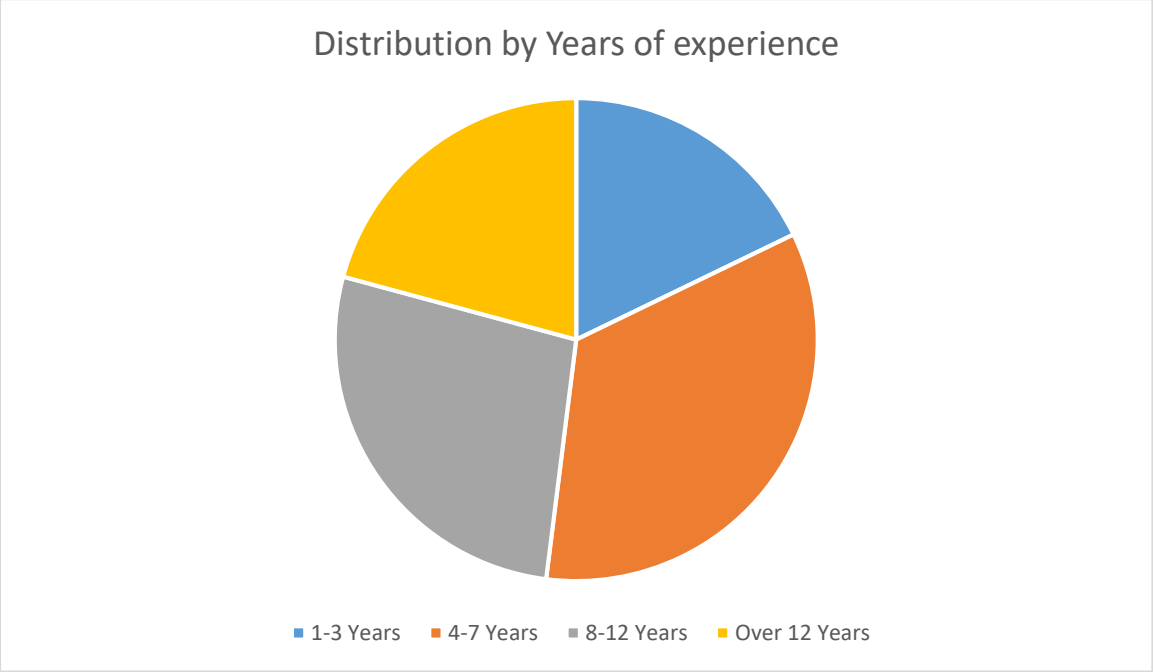
4.2.2.3 Respondents' Distribution by Years of Experience

The years of experience of the respondents in the hospitality industry were also considered because level of experience often affects the awareness of items related to financial fraud and fraud prevention measures. Table 4 shows how the respondents are distributed according to their experience in the industry and the pie chart below visualizes the information further.

Table 4: Respondents' Distribution by Years of Experience

Years of Experience	Number of Respondents	Percentage (%)
1-3 Years	12	18.18%
4-7 Years	23	34.84%
8-12 Years	17	25.75%
Over 12 Years	14	21.21%
Total	66	100%

Pie Chart 3:



According to the findings, the highest range (34.84) of the surveyed population experienced 4 to 7 years of experience in the hospitality sector. A good percentage (25.75%) has experience of 8 to 12 years which indicates good knowledge of hotel finances and fraud detection strategies. Additionally, a small number of respondents (18.18% experienced 1-3 years) are new at the hospitality sector bringing fresher insights on fraud prevention technology. The balance of 21.21% had above 12 years of experience on their belts and gave their expert opinions on fraud prevention practices over time.

The representation of key personnel in the fraud prevention function of hotels in Zimbabwe is well covered. Most of the respondents were IT experts and finance officers whose roles directly relate to ensuring financial transaction security and fraud detection technologies. The participants came from small, medium, and large hotels, giving a wide angle of industry perspective. Also, there are different levels of experience so that we have those who have just joined the industry and those who have worked for long enough to help with the study.

4.3 Findings

This section of the study looks into the findings from the research questionnaires and interviews with the key personnel who are responsible for fraud management in hotel financial systems. The responses gathered provide useful insight on efficiency of existing technology to combat fraud, the issue faces in using them and what can be improved upon to counter frauds in hotel industry. Many hotels have means of detecting and preventing fraud. However, impacts on frauds occur because such means do not take effect due to finances, technology and human-related scenarios. Many respondents noted that fraud is still an issue with their hotels' financial systems, with incidents including employees perpetrating fraud, and cybercriminals attacking weak security structures. We noted that fraudsters constantly tweak their techniques, which calls for fraud prevention strategies that can outsmart them, and never become obsolete. According to financial managers and IT staff of various hotels, although the hotel industry has adopted fraud prevention technology, various other technologies have been adopted in silos. Many fraud detection systems work in silos rather than being embedded into larger financial management systems thereby losing out on efficiency. Also, the study mentions that the emerging technologies -like blockchain financial security, AI fraud detection, biometric authentication, etc.- are good solutions but they are not used widely because of their high costs, complexity and regulatory ambiguity.

4.3.1 Prevalence and Nature of Financial Fraud in Hotels

Fraud schemes in hotel financial systems were reported as widespread and prevalent, with respondents giving an account of numerous fraudulent cases in their establishments. Many establishments reported various types of fraud. Internal employee fraud was reported the most. Other frauds included credit card fraud, refund fraud, invoicing fraud, identity theft and phishing-related cyber fraud. Internal employee fraud was very common as financial staff were regularly found misusing their access to hotel accounting and transaction systems.

Several interviewees spoke of incidents where staff had altered financial records, generated duplicate refunds and changed invoices to steal money that wasn't immediately noticed. According to the finance director of one hotel, "In one instance, an accounts clerk made numerous refunds to the same external bank account citing guest cancellations." "It took weeks to see. The internal checks didn't give us any real-time alerts," she said. As per another controller, "An employee realized that even changing an invoice number on a transaction enabled them to draw out a few bucks and not raise an alarm Signal. As a result, this became thousands of dollars in time went unnoticed." These two cases demonstrate how fraudsters can exploit gaps in financial oversight, particularly in hotels that still rely on manual processes for financial record-keeping. Another concern mentioned quite a bit is credit card fraud, particularly in hotels with no real-time verification and transaction monitoring. A lot of respondents said fraudsters used stolen or cloned credit cards to book stays and make payments. Hotels faced losses due to a reason that transactions were not flagged fraudulent unless banks or credit card companies didn't initiate chargebacks. There was one incident, a guest booked an expensive suite and paid in full via credit card," explained one IT manager. We got a chargeback notification a few days after checkout from the bank as the transaction was fraud. It was too late to recover the loss as the guest had checked out by then." The other big issue was fake refunds. This was particularly rampant in hotels that didn't have stringent authorization practices for refunds. Certain employees exploited manual refund systems to reroute funds into their own or their accomplices' personal accounts. A hotel finance admin said "Refunds are processed as per a supervisor's verbal approval. Some employees discovered creating fake refund transactions could be done easily and disguising them as real guest refunds. Also, hackers intercepting credit card payments or accessing the credit card information of guests at certain hotels, resulting in cyber fraud and phishing attacks were a threat. One example came from an IT Security expert who said, "We had an incident where an employee clicked on a phishing email that looked like it was from the payment processor. An employee clicked on a phishing email which came from a reputed payment provider. The hacker had access to our system and was trying to alter payment details to divert payments. Either through negligence or lack of awareness, staff becomes an easy target to external frauds.

4.3.2 Effectiveness of Current Fraud Prevention Technologies

Most hotels have fraud prevention technology in place. However, it does not mean that all these technologies are created equal, and substantial, noticeable differences can exist based on budget, staff training, system integration, as well as technology level.

Hotels that have invested in multi-factor authentication (MFA), and biometric authentication, AI-powered fraud detection, as well as encrypted payment processing have reported fewer fraud incidents as compared to hotels relying on traditional security measures. Especially, fingerprint scanning to access hotel's system is particularly strong in preventing unauthorized access and employee impersonation fraud.

A financial security expert said, “There was a significant decrease in unauthorized login access and password sharing after using biometric authentication. Biometrics differ from passwords because they cannot be easily shared or stolen. But as responses highlighted, many fraud prevention tools don’t work seamlessly, but in a silo, and not entirely within the hotel’s financial system. Some hotels use separate fraud detection software that flags suspicious behaviours after they have already taken place instead of preventing them from happening in the first place. An IT administrator stated that their fraud detection software flags the transaction as fraudulent, but only afterward. By the time we investigate, the damage has already been done.” This means that real-time fraud detection mechanisms which stop transactions before completion will allow to allow better financial security. Additionally, alert fatigue was a recurring problem. Some hotels noticed that fraud detection systems created too many false positives leading to the employees ignoring or dismissing security alerts. According to a finance manager, “We have so many alerts that staff takes them lightly only. Actually fraud attempt gets unnoticed sometimes because of alerts. Another big worry was the flaw in legacy financial management systems. Many hotels rely on age-old software lacking modern encryption protocols and fraud detection features, making it easy for fraudsters to cheat. Some IT managers noted that their older financial management software posed issues integrating with more advanced security tools to prevent fraud.

4.3.3 Challenges in Implementing Fraud Prevention Technologies

Cited challenges in the implementation of fraud prevention technologies were budget constraints, change resistance, cybersecurity personnel shortages and incompatibility with existing security and IT systems. Small and mid-sized hotels were especially tight on budget

as management believes that guest experience is more important than cybersecurity. A financial controller from a large hotel said: “Fraud prevention systems are expensive. Management sees them as non-revenue-generating systems.” We only deal with security after facing a major fraud that hurts us. Another big problem was the resistance to fraud prevention measures. Some staff bypass security as multi-factor authentication and strict app login policy is inconvenient for them. One officer from the IT admitted, “Even after enforcing strict login requirements, some employees share credentials for convenience.”

4.3.4 Suggested Measures to Improve Fraud Prevention

Respondents proposed using AI for fraud detection, blockchain for transactions, enhanced training, and stricter enforcement to prevent fraud. One suggestion that popped up quite a bit was to get fraud detection powered by AI. This would help automatically spot weird patterns in transactions in real-time. Moreover, regular training workshops on cybersecurity were suggested so that the officials recognize when fraud is taking place and have an understanding of compliance. Finally, some were in favour of stricter regulation from the industry as they believe that fraud prevention set by the government would help hotels upgrade their financial security.

4.3.5 Findings from Document Reviews

In addition to using data from questionnaires and interviews, a detailed document review was conducted. A review of academic papers, industry reports, guidelines relating to cybersecurity, and case studies of financial fraud in the hospitality industry. These publications offered insights into previous trends and instances of fraud, along with assessments of existing and new technologies for preventing fraud.

4.3.5.1 The Growing Threat of Financial Fraud in Hotel Systems

Numerous papers point out the rising sophistication of financial fraud in the hospitality sector as a result of cybercriminal innovations and weaknesses in legacy financial frameworks. The Hospitality Financial and Technology Professionals (HFTP) revealed in a report that “hotels are still one of the most targeted sectors for financial fraud,” imported. “I have a high number of transactions, a high number of card-not-present transactions, and a high reliance on out-of-date security systems.” According to interview responses, older financial management systems

in hotels are not encrypted, have no fraud detection and are therefore become a victim of financial fraud. Academic research also shows that the financial losses that were realized due to fraud in hospitality. According to a study published in the International Journal of Hospitality and Tourism Administration, it is stated that financial fraud causes a loss in revenue of about 5% yearly for hotels and even more for small and medium hotels (Smith & Kaur, 2022), which is a significant amount lost. This supports the responses from the researcher's questionnaire where the financial controllers admitted that the losses from fraud had adverse effects on profitability.

4.3.5.2 Common Types of Fraud in Hotel Financial Systems

Hotel fraud is categorized into many types of fraud in the reviewed literature. Examples include internal fraud, payment fraud, invoice fraud, and loyalty fraud. As per a white paper by PwC's Hospitality and Fraud Division, almost 60% of the financial fraud in hotels is internal fraud. Fraudsters usually commit this kind of fraud using falsified supplier invoices, they also make use of unauthorized refunds, and cash skimming (PwC, 2023). Hotels that offer limited or inadequate oversight over financial statements and auditing procedures are at an elevated risk of internal fraud, concluded the PwC study. A case study by Marriott International reveals that a front desk manager reportedly tried to create fake refunds in the records to channel funds into his personal account (Marriott Case, 2021). This coincidence of responses with hotel IT managers in the interviews is interesting, as they speak about refund fraud often going undetected due to no multi-level approvals for transactions. Therefore, they were also recommended by many interviewees that the automation of refunds' approval with AI activity verification can safeguard from this fraudulent activity (Marriott Case Report, 2021).

4.3.5.3 Evaluation of Current Fraud Prevention Technologies

The literature review highlights the effectiveness of fraud prevention technologies on financial systems of hotels. The Cybersecurity and Infrastructure Security Agency report (CISA) for 2022 findings suggest that typical hotel groups are armed with the basics of fraud detection technology, however, most hotels do not enjoy the benefit of real-time fraud monitoring. As the report indicates, further, the entire hotel and gaming sector are behind the "8-ball" lagging behind more progressive industries in being early adopters of AI-based security solutions. The report states.

Hospitality is behind banking and retail industries in fraud detection because its use of machine learning and real-time transaction monitoring tools is relatively delayed (CISA, 2022).

The survey data confirms this statement as numerous hotels reported using outdated fraud detection software with rule-based functionalities, which is not a real-time anomaly detection tool.

The above findings were further corroborated by Nguyen and Patel in 2023 where they find hotels using machine learning based fraud detection solutions witnessed reduction in incidence of financial frauds by 45% in two year period (Journal of Financial Security and Fraud Prevention). According to the study, up-to-date fraud detection tools, especially those relying on AI, have a greater accuracy in detecting fraud when they are compared to traditional legacy rule-based systems. Nevertheless, as highlighted in conversations with hotel financial controllers as well as the IT professionals who liaise with them, the cost of AI-based fraud detection is a major problem when it comes to requesting approval for them, not to mention the actual implementation.

4.3.5.4 Challenges in Implementing Fraud Prevention Strategies

The review of the documents supports the findings of the questionnaires as well as the interviews on known barriers to fraud prevention implementation. A comprehensive study carried out by Deloitte's Hospitality Risk Advisory Team (2022) identified various challenges and barriers. These included cost challenges, aged financial infrastructure, and untrained cyber experts. The study noted the fact that many hotels are still using old financial management software that does not have real-time fraud detection capabilities. The process of then upgrading these systems requires considerable financial investment, which is usually deprioritized for enhancements to guest experience" (Deloitte, 2022).

This finding closely mirrors the inputs from the financial managers who often cited fraud prevention being a secondary priority to guest service and revenue-generating initiatives. These initiatives are seen as costly and ones that will not bring about a profit so they are treated as unimportant.

The document reviews also highlight employee resistance to fraud prevention technology as a challenge. According to a Global Hospitality Security Forum report, roughly a third of hotels reported that staff bypass security. This occurs most often, due to general inconvenience and lack of awareness regarding fraud (GHSF, 2022). IT managers interviewed for this study share

that some employees often find it irritating to have multi-factor authentication and other security steps, so they bypass security, they do not exactly see its necessity.

4.3.5.5 Emerging Technologies and Future Trends in Fraud Prevention

The literature reviewed also presents the new technologies to prevent fraud which can supplement hotels' current issues. A recent report issued by the Cybersecurity Research Division of IBM (2023) mentions that transaction security through blockchain and behavioural analytics through AI can be the next fraud prevention technology for the hotels. The study explains that.

According to IBM (2023), blockchain technology decentralises the process of verifying transactions. This significantly reduces the chances of invoice frauds and refunds or financial data theft.

Biometric verification could potentially be the key to securing all hotel financial transactions, say industry reports. According to Kaspersky Labs' 2023 Hospitality Cybersecurity Report, organizations that adopted biometric authentication saw fraud incidents reduced by as much as 70%. The report states.

Security measures like facial recognition and finger ID help organizations defend more against financial fraud from both external as well as internal sources. They eliminate the risks of thieves stealing and hacking passwords to gain access. (Kaspersky, 2023)

As noted in several hotel IT professionals' interviews, using biometric authentication would prevent unauthorized financial transactions.

4.3.5.6 Summary of Document Review Findings

The findings from the document review provide substantial corroboration to what was ascertained from both the survey and interview data. It indicates that the challenge of financial fraud persists in the hospitality industry because of outdated physical security systems, there is also the risk of internal fraud, as well as the insufficient adoption of technology. The implementation of crime-prevention technologies such as AI and blockchain has been hampered due to cost constraints, lack of technical know-how, and push-back from the hotel employees.

In conclusion, the literature proves that that the hotels must upgrade the fraud prevention methods in place, especially by incorporating tools that detect fraud in real time and enhancing

cyber security awareness amongst their staff. According to multiple reports, the future of fraud prevention for financial systems in hotels lies in automation, AI-enabled analytics and multi-layered security.

CHAPTER 5 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary, conclusions and recommendations relating to the findings of the research on the evaluation of current and affirmative technology to prevent a fraud on hotel financial system. This chapter summarizes the study findings, objectives and application of the results in the hotel industry for fraud prevention.

The study sought to evaluate the effectiveness of current fraud prevention technologies in hotel financial systems and the challenges facing hotels in implementing these technologies. Further, the study will propose recommendations to enhance fraud prevention strategies for the hospitality industry. The use of interviews, questionnaires and document reviews in this research helped in the extensive collection of data on fraud prevention technologies.

The research shows significant findings regarding the fraud prevention practices among hotels including the types of fraud prevention technologies in use, the effectiveness of their systems, and the challenges faced by hotels for technology integration and maintenance. Also, various emerging technologies were discovered along with recommendations to improve existing technologies. This will bring out the key findings, conclusion from analysis, key implications for the industry, and recommendations for hotel to strengthen fraud prevention efforts. Through fulfilling the research objectives and summarising the findings, this chapter provides both theoretical and practical contributions to the prevention strategies of frauds in hotel financial systems and how they can be enhanced for efficiency and secure for future use. The chapter will conclude with areas of future study that can be taken to further examine research on fraud prevention innovations and their uses in the hotel industry.

5.2 Discussion

This chapter discusses the investigation's findings based on responses to the questionnaires and interviews and review of the key documents obtained during the study. This discussion aims to realise the effectiveness of existing fraud prevention technologies in the financial

system of hotels, what difficulties hotels are facing while implementing these systems and how growing technologies can be used for fraud prevention in the hospitality industry.

A key objective of this study is to assess how effective the fraud prevention technologies used in hotel financial systems actually are. According to the findings, there is technology to counter fraud in hotel financial systems. However, this technology does not fully meet the requirements of the hotel operations. Majority of the surveyed hotels employ basic fraud prevention methods such as user's rights management and complex password. However, many respondents stated that while these are must-haves, they alone do not provide a good fraud prevention mechanism. For example, many respondents spoke of layering security, such as limiting access to financial information but added that such measures are often not enough to deal with the risks of insiders or colluding employees.

A recurrent theme that surfaced within the interviews is the difficulty of adopting fraud-prevention systems due to human errors. A hotel IT professional said, "We do have access control. But there is always a chance for employees to get through the access controls, especially where collusion is concerned." So, as we say technology can help, technology does help. But collusion or malicious insiders is where the big risk lies. For instance, employees colluding to manipulate financial records – that's very possible. Though the systems can dome a good job of blocking unauthorized access from the outside, they are less effective in spotting fraud from within—especially when trusted employees are involved.

Other mentioned technologies included biometric authentication and AI-driven fraud detection, as well as additional more complex controls. Though these technologies have gained popularity this year, they have been reported to be used on a very sporadic basis due to implementation costs and lack of compatibility. We have probes for AI but it needs investment is what one hotel manager said. It is not implemented yet. It shows a key hindrance faced by lots of hotels especially those which have less budget. The cost of implementation of such fraud prevention technology is higher than its benefits especially in short operations.

The second research objective sought to find out what challenges hotels face when using fraud prevention technologies. The study revealed many problems that hinder effective implementation and utilization of these systems. One of the main issues respondents pointed to was the cost of setting up and running fraud systems. These issues were particularly noticeable in the case of smaller hotels or those short of funds. Several respondents indicated that the initial price tag to obtain high-tech systems, along with costs of updates and training,

made it difficult for their systems to be deployed on a wider scale. One participant said, “The cost of upgrading to better systems is too prohibitive for smaller hotels to handle, and that is a critical impediment to fraud prevention technologies’ growth.”

Another major challenge was the lack of integration between different financial systems. A lot of hotels use multiple software for different purposes such as booking, POS terminal, accounting, etc. But it doesn’t communicate seamlessly, making it harder for fraud prevention technologies to penetrate these areas. One IT manager said, “We have multiple systems. But, they aren’t synched up to our fraud detection systems. So, this leads to inefficiencies and increases fraud potential.” When systems aren’t integrated, they don’t exchange information. Consequently, this leads to situations where data isn’t available for fraud detection systems.

Many also said that staff training was lacking and a challenge. Many hotels found it hard to guarantee staff were trained to use fraud prevention technologies effectively, even if these systems were installed. Staff were often not aware of how to detect and respond to potential fraudulent activities, respondents said. According to a respondent, “We have training on the operation of the technology, but we don’t focus on fraud prevention and the spotting of suspicious behaviour on the part of employees.” This sort of comment would suggest that while the tech may have fraud-detection capability, it can’t benefit the company if employees are not trained adequately.

A lot of discussion is also devoted to whether these technologies are capable of helping hotels prevent fraud. The study shows growing interest in using technologies like artificial intelligence (AI), machine learning (ML), and blockchain to improve fraud detection systems that are currently in use.

Tools that detect fraud using AI were mentioned. They leverage machine learning algorithms to detect anomalies by analysing large sets of data. Most of the respondents felt positive about the potential of using AI to find frauds. "I think AI can detect patterns in transaction data that we can't see. This will allow us to detect fraud early," said one hotel IT specialist. "These technologies are especially good for big hotels with lots of transactions." They will also be able to flag suspicious activities in real-time. Nonetheless there were concerns about the high cost of these systems and the technical know-how to manage them. An option to improve financial safety of hotels is blockchain technology, experts discussed the possibility. Essence of Blockchain Technology: Most of the cryptocurrencies used blockchain technology for their working. Hotel manager further said, “Blockchain is a system that creates a clear and tamper-

proof record of financial transactions so that the activity cannot take place under the radar." Although this technology sounds good, the hospitality sector is not currently adopting it as hotel staff don't know to what extent it could be useful. Further, it has a complex reputation.

Even though there is excitement for these new technologies, respondents have barriers to their adoption. There is a cost barrier to using new technologies, as some require costly investments, which are not feasible for many small hotels. There is also a lack of knowledge and expertise among hotel staff to evaluate and implement these technologies effectively. According to a finance director, 'We are open to new technologies, but we don't have technical skills to evaluate those or integrate them with our existing financial systems'.

To sum up, this research conclusion shows that many of the fraud technologies currently available are generally used because they provide a certain level of protection but would not be successfully able to protect the hotel from internal fraud. The successful implementation of fraud detection technologies in the hotel sector is severely affected by constraints relating to cost, system integration and staff training. Despite this, there is much interest in new technologies like AI and blockchain that could improve fraud prevention strategies. The adoption of these technologies will depend on overcoming existing barriers such as cost and technical expertise. Their potential to transform fraud prevention practices in hotels is evident and is taken note of by many individuals.

5.3 Conclusions

This study looks into the impact of hotel finance system fraud technologies. It assesses current technologies available for fraud-proofing and the challenges facing hotels. Finally, it tries to suggest measures that the hospitality industry can take to fraud-proof their system. Conclusions have been drawn based on the information gotten through the questionnaire, interview and document review.

5.3.1 Effectiveness of Current Fraud Prevention Technologies

According to this research, most hotels now use fraud prevention technology. However, the fraud prevention technology is not fully capable of preventing a more sophisticated type of fraud. More importantly, this type of fraud is internal. The research result highlights that a high percentage of hotels are using user rights management systems and password protection, which is essential but not comprehensive enough. Many hotels are not using more advanced technologies like biometrics and AI-driven fraud detection because they are too costly and cannot easily be integrated into existing financial systems. Moreover, fraud prevention systems

are seen as ineffective for human error or collusion between employees. One participant noted that “Insider fraud remains a major risk and current technology cannot address this issue.” This seems to suggest that while technology can help reduce fraud from outsiders, it cannot help manage fraud from insiders. This is a major gap in the fraud prevention systems of many hotels.

5.3.2 Challenges in Implementing Fraud Prevention Technologies

Research indicates that financial constraints, system integration challenges, and insufficient staff training are the main barriers to implementing fraud prevention technologies in the hospitality industry. In the case of many hotels, especially small ones, the cost of adoption of advanced fraud prevention technologies becomes a big hurdle. Many answered that application of advanced fraud detecting tools is not possible for hotels as their first cost on top of maintenance cost and training cost is quite high. IT Manager of a hotel said, “Smaller hotels have financial limitations that stop them from investing in advanced fraud detection systems, making them susceptible to threats.”

Numerous hotels face difficulties in integrating their POS systems, booking engine and accounting software with each other. Owing to this lack of integration they cannot share data and monitor payments in real-time. The lack of integration between fraud prevention technologies inhibits a complete perspective of financial data, making it useless in the end. An IT professional noted that we have fraud detection tools. But they don’t work well because of the lack of integration with other systems.

The insufficient training of personnel was another major challenge identified in the research. Many hotels did put in place essential disaster prevention systems but, because the staff is not trained they are not utilizing these solutions to their maximum or not recognizing fraud. A participant stated, “Staff may not be fully launch on fraud detection and as a result may miss the signs.” Thus, it shows that the human element is still very much in play with the system. Without enough training and awareness, employees cannot act as an added layer of protection against fraud, thus lessening the impact of tech measures.

5.3.3 Emerging Technologies and Future Potential

The hotel industry has reportedly regarded the importance of emerging technology like AI and blockchain in fraud prevention which is also an ethical issue being faced by the industry. Machine learning algorithms that AI runs, can be used to identify strange transaction patterns. These strange transaction patterns help in identification of frauds and more. According to one response, AI could track millions upon millions of data and abnormal discrepancies could easily be tracked by using these tools. However, they are still in early stages of adoption owing to price, complexity, and difference in technical requirements of a typical hotel and the products.

Another promising technology is blockchain, which clients are using for transparency and integrity in financial transactions. Hotels could create a tamper-proof record of financial transactions using blockchain, thus mitigating fraud risk. Nevertheless, it was noted that blockchain technology was underutilized in the hospitality industry, which was confirmed by the absence of knowledge on how to leverage this technology for financial transactions of hotels.

These technologies appear promising, but the findings trace a slow rate of adoption. This is particularly the case for small hotels, which often do not have the means to invest. According to one respondent, smaller hotels are unable to use fraud prevention technologies due to their high costs and thus, lag behind larger hotels.

5.3.4 Insider Fraud and Its Challenges

The study concluded that insider fraud remains a major threat to hotels and that current technicalities do not always do just about that. Findings of the study indicate several hotels are enforcing access control systems and various layers of security, which limit accessibility to the financial system but employees, due to their position of trust, often circumnavigate it. Fraud involving employees colluding with outsiders or manipulating financial info continues to be a problem, several respondents noted.

Given this, fraud prevention can’t be limited to plugging access holes and creating technical control measures. Many believed that employees should be more vigilant as the solution to the crime alongside increased transparency and internal audits. One of the hotel managers quoted “Frauds prevention is not only about technology but also infusing a culture of honesty and integrity among the staff.” This reinforces the idea that technology is only a solution to frauds while it is essential to steer a fraud-free environment at the hotel.

5.3.5 Recommendations for Improvement

One must draw several recommendations from the research to improve fraud-prevention mechanisms in the hospitality sector. To start, hotels, especially small ones, should invest in AI and blockchain to reap large scale benefits in fraud prevention and mitigation. Although, these technologies require a significant investment at first; they can help reduce the risk of fraud in the latter.

The second measure is hotels enhancing the integration of the hotel's financial system to ensure data flows seamlessly to enable real-time monitoring. Fraud detection tools will work better due to the presence of integrated systems which quite accurately help in the detection of fraud due to an overview.

Staff training and education for fraud prevention is essential. Hotels should train their staff on fraud detection and prevention tools. As one respondent said, "Staff training would also not happen just once; it would be ongoing."

This research conclusion indicates schemes to reduce hotel financial fraud through technology have potential, yet this is a major challenge for the accommodation sector. To enhance the effectiveness of fraud prevention, it is important for the industry to deal with these challenges such as cost element for installation of advanced technologies etc. New technologies such as AI and blockchain can help in fraud preventions. The constraints of cost and expertise implementation act as hurdle in this process. As the hospitality industry continues to evolve, it will be critical for hotels to stay abreast of technological advancements and adopt more comprehensive fraud prevention strategies.

5.4 Implications

Results of this study are important for the hospitality industry with regard to improving fraud prevention, improving the integration of systems. Furthermore, ensuring that employee is capable of carrying out secure monetary transactions. The research shows the fraud prevention challenges in the hotel sector that can be adopted to enhance future practices, policies, and technology implementations.

5.4.1 Impact on Hotel Financial Systems and Operational Efficiency

One of the key implications of this study is the use of fraud prevention technologies enhancing the overall operational efficiency of the financial systems of hotels. The results show that the

use of present technologies reduces certain risks, but there are still limitations in dealing with sophisticated fraud committed by, in particular, internal fraud. As indicated in the research, fraud prevention systems based on user rights and passwords fail to cope with frauds by insider systems that are devastating on hotel financial systems and stability.

According to the results, hotel managers and IT people would benefit from investing in more sophisticated fraud detection systems.

According to the IT Times article, fraud detection and operational efficiency will be significantly enhanced through the use of powerful technologies like artificial intelligence (AI), machine learning and blockchain. Such technologies will enable analysis of large data sets in real-time and identification of any anomalies which existing systems do not currently detect. But, despite these advantages, the research shows that the costs associated with the implementation of such systems continue to serve as a major barrier for many hotels, especially smaller hotels.

The implication here is twofold. To begin with, the hotels must re-strategize their budgets to accommodate long-term investments in fraud prevention tools which are capable of improving the effectiveness and efficiency of their payments systems. Secondly, it is important for hotels to consider affordable options or hybrid solutions that combine new technology with old systems to lessen the cost of a total replacement.

5.4.2 Employee Training and Internal Culture

Another important implication of this study is that hotel employees need to be trained and encouraged to create a transparent environment and be accountable. Results show that fraud prevention technologies are necessary but not enough to tackle the issue. Many of the respondents mentioned that human errors and collusion of employees contribute greatly to fraud and cannot be resolved entirely with technology.

Clearly, hotels must start staff training on fraud each time they hire or promote. Employees need training not only in fraud detection systems, but also in possible fraud schemes. For instance, financial manipulation and misappropriation of funds that are not readily detected by fraud detection systems must be highlighted. All personnel such as front desk agents, those in accounting, managerial staff etc. all capable of gaining access to financial systems must be

trained. Having all staff members aware of fraud risks can serve as an extra layer of protection against internal and external fraudsters.

Additionally, it's important to create an internal culture of integrity. One interviewee pointed out that a culture where employees can report odd behaviour is essential to preventing fraud. Shaping the culture may mean changing hotel policies to reflect transparency, transparency, and the rewarding of whistle-blowers who expose misdeeds.

5.4.3 Technological Integration and System Compatibility

The study has a great implication that systems must be integrated on the technological platform within the hotel financial systems. A key hurdle to effective fraud prevention is the lack of integration of various financial and operational systems. Point-of-sale (POS) systems, booking engines, and accounting software are often not connected, creating data silos which prevent real-time fraud detection and end-to-end transaction tracking.

Incorporating valuable financial and operational data from systems like point-of-sale, booking, and accounting will make fraud detection more effective. In other words, hotels should buy systems that merge different kinds of software into one platform for payments. Better system integration will allow fraud detections tools to check the data as it happens, identify possible frauds early on, and instantly notify the management.

Moreover, if the financial systems are integrated with fraud detection systems, both the audit will become more simple and the chances of human error that allow fraud to occur will go down. Hoteliers must realize that the cost of fully integrated systems is nothing compared to their benefits. A fully integrated system provides long-term security with operational efficiency and financial integrity.

5.4.4 Industry-Wide Collaboration and Knowledge Sharing

The results of the study noted that the hospitality industry could gain through better cooperation and sharing of knowledge on fraud. For the access to the resources needed to install sophisticated fraud prevention systems, many respondents remarked that small hotels, in particular, struggle. This shows there is need to share information on the latest fraud prevention techniques and technologies across the industry.

To fix this, networks of hospitality and industry associations can play a proactive role in facilitating information sharing and implementation help to small hotels. Group actions can

take many forms. The industry can create common systems for fraud identification, offer discounts on tech adoption, training for teams, etc. By using common resources and sharing common practices, the hotels in the industry can work together to prevent financial fraud.

5.4.5 Legal and Regulatory Implications

This research implies a need to develop stronger legal and regulatory frameworks in the hospitality industry to effectively combat financial fraud. Some hotels may have internal fraud prevention measures in place; however, the external regulations and standards are often inadequate or poorly enforced. The study found that numerous hotels were not in full compliance with industry standards and best practices for fraud, which may have led to fraud and financial loss.

Tougher rules in hotel industry like clearer guidelines to prevent fraud, more strict enforcement of these rules will provide hotels with the necessary structure to prevent financial fraud. Also, regulatory bodies can provide hotels with guidance on adopting new technology to outsmart or prevent fraud. If hotels are told to follow these regulations then hotels would benefit from additional security. In addition, customers may also trust the hotel more.

To sum up, this study shows how fraud prevention in hotels is not simple. It is, in fact, quite complex. Technologies used for fraud prevention are important but addressing other challenges like cost, integration to other systems, training of employees and internal culture are equally important. The hotels should invest in advanced technologies, merge their financial systems, and cultivate a culture of transparency and accountability. Also, bigger companies spending more on fraud-related tech and systems integration, better employee support and training and altering their internal culture can help.

5.5 Recommendations

This study suggests various recommendations for fraud prevention in the financial system of the hotel. In this regard, the recommendations involve reducing impediments for hotels on implementing fraud preventative technologies and enhancing the effectiveness of technologies already in use as well as recommending the adoption of newest technologies and best practices for combating fraud in the hospitality industry.

5.5.1 Adoption of Advanced Fraud Prevention Technologies

A recommendation ensuing from this study is the greater use of more advanced fraud prevention technology. The study found that hotels do have a few basic fraud-stopping items, like password protection and user rights management. In actual fact these technologies often fail to detect more sophisticated fraud techniques. This is especially true of fraud from internal staff. In order to prevent fraud, hotels should ensure that they have advanced technologies like artificial intelligence (AI), machine learning, and blockchain to help combat fraud in real time as these have proven useful in detecting and preventing fraud.

AI and machine learning algorithms can examine extensive amounts of financial data to discover anomalies or patterns that suggest dishonest practices, they can handle a bigger workload than the average human being. These technologies can learn from past data. This improves their ability to detect potential fraud over time because there are now patterns available to them. AI can identify unusual transaction types, such as too many refunds or odd transactions. This may be tough for humans to identify manually. Moreover, machine learning can get better at detection over time as fraudsters thwart detection methods by coming up with new tactics.

Fraud prevention could also benefit from blockchain technology. Its decentralized and transparent nature can provide an unchangeable ledger of all transactions, making it hard for con artists to interfere with economic records. Hotels can implement blockchain technology in their financial systems, allowing customers to be confident that nothing is wrong with their financial transactions. Blockchain technology also offers great potential in fraud prevention. Its decentralized and transparent nature can provide an immutable record of all transactions, making it difficult for fraudsters to manipulate or alter financial records. By implementing blockchain technology, hotels can ensure the integrity of their financial systems and provide customers with greater confidence in the accuracy of their transactions.

5.5.2 Strengthening System Integration

A major suggestion that come out of the research is the need for better system integration with hotel finance systems. Many hotels, especially small hotels, still use separate software systems

for their POS systems, reservation systems, and accounting. The integration between these systems are lacking so data silos are created which hinders monitoring and detection in real time.

Hotels must prioritize adopting software that integrates financial, operational and customer data to address this problem. When tools by various departments don't provide the same information, fraud can be detected sooner. Integrated systems can allow for better cross-checking and detect fraud sooner. If for example there is an integrated system, the hotel management can use the same data for the POS system and the reservation system. This is to easily detect possible fraud like overbilling or discounting that is not authorized.

Moreover, the efficiency of financial reporting and auditing can be improved with an integrated system. When it comes to integrated systems, rather than manually reconciling data from many systems as is the standard. What can be done is that hotel managers can access real-time reports giving them a complete picture of the transactions which are happening.

As a result of this change this can lower audit time and improve financial transparency overall, thus lowering the chances of fraud occurring.

5.5.3 Comprehensive Employee Training Programs

It is also recommended that employee training for employee fraud prevention be adequately undertaken.

The study found that many fraud prevention technologies do not work because of human error, ignorance or collusion by the employees. A training of the employees who interact with the financial systems will be equally essential to prevent this fraud. All hotel staff from front desk to accounting staff, managers and supervisors will need this training, so that every level will be updated in every department, not just IT staff.

In-house employee training programs should involve educating staff about fraud, which can take various forms, such as financial manipulation, theft, and internal collusion. Training should cover the application of fraud prevention technologies. Employees must understand how to use multi-factor authentication, user access controls, and real-time fraud detection technologies, among others. In addition, there should be a culture where employees can report

suspicious activities without fear of retaliation. To encourage whistleblowers, hotels should implement clear reporting protocols to foster a culture of integrity and accountability.

Along with training, hotels should also keep their staff updated regularly on the latest fraud risks as well as the fraud prevention technology. Running regular workshops or webinars for the staff can keep them equipped to deal with financial frauds.

5.5.4 Strengthening Internal Controls and Audit Procedures

Results of this study also necessitate strengthening controls and audit processes in hotel finance systems. When you don't have strong internal controls, fraud is likely. For example, there could be a breakdown in the segregation of duties. To prevent this from occurring, hotels must devote duly documented internal control policies to the segregation of financial dealings.

For example, hotels should separate the functions of employees who initiate transactions, authorize payments, and reconcile records. To lessen the risk of internal fraud, an individual's ability to bypass control and manipulate financial data must be made more difficult. Also, the hotels should make use of regular internal audits to monitor the efficiency of fraud prevention techniques and unveil any possibly weak links in the setups.

To augment the controls, hotels should require employer monitoring in the financial system. Hotels should monitor employee activity in financial systems as an important Internal Control activity. This could involve tracking user login attempts, monitoring transaction histories, and generating real-time alerts for any suspicious activities. By keeping a continual watch on employee conduct, hotels can detect fraudulent behaviour before it causes great loss.

5.5.5 Enhanced Collaboration within the Industry

An important recommendation from this research is a broader collaboration. Many smaller hotels are unable to afford advanced fraud prevention technology, nor have the technical know-how to use this. To deal with this, Knowledge sharing and the provision of resources for smaller businesses can be facilitated by associations and hospitality networks. Working together helps hotels, technology suppliers, and regulatory organizations share shared practices to come up with affordable anti scam solutions.

In other words, industry associations and hospitality networks may also create sharing platforms to provide hotels access to fraud prevention tools at lower rates. In addition, hotels can work to bring about common industry standards for fraud prevention so that all hotels follow the same best practices and technology requirements. Collaboration of this nature can also lead to the development of open-source fraud detection tools which may help smaller hotels to access high-end technologies at no cost.

5.5.6 Regulatory Framework and Legal Support

Lastly, the study indicates that improved regulatory frameworks as well as legal support are crucial to enhancing fraud prevention in the hotel industry. The study reveals that many hotels have a low compliance rate with their industry standards concerning fraud prevention and thus, they remain vulnerable to fraud. Thus, it is vital that the government and the industry regulator set out proper operational standards for fraud prevention compliance in hotels.

Hotels should be mandated to include basic fraud detection regulations, such as secure payment processing and employee background checks, as part of their operational licenses. Moreover, we should put a law in place that enhances transparency of finance and require hotels to disclose fraud information. Authorities should impose strict regulations and provide legal support to ensure that hotels protect the integrity of their financial systems.

To sum up, the recommendations in this part are useful in order to fraud prevention in the hotel industry. By utilizing technology, hotels can incorporate their financial systems and train employees about various frauds that may be encountered. The hotels must put in place internal controls to enhance fraud prevention. In addition, fraud cannot be prevented in isolation. The industry must collaborate in a high-level manner to discuss challenges, issues, and the way forward. Stronger regulations must be checked which can work in a hotel's benefit.

The recommendations take care of the problems that we found. Besides, they are all quite feasible. Therefore, the industry has to start taking these recommendations seriously in order to protect themselves.

5.6 Suggestions for Further Research

This research has provided meaningful and needed insights into the effectiveness of current fraud prevention technologies in the financial systems of hotels. This study has also opened up

several doors for future exploration. Given the constantly changing nature of the hospitality industry and the rapid pace at which new technologies and means of fraudulent activities are being developed, it means that continued research is needed so that hotels may be able to refine existing strategies and explore newer solutions. To a large degree, several key areas warrant further attention, building on the findings of this study. Multiple key areas of this topic of study require further attention. These areas would build on that which was already uncovered in this study. One such important area for future research lies in exploring the impact that emerging technologies will have in these hotels. Blockchain is an example of such technologies, as well as artificial intelligence (AI), areas such as machine learning, and biometric security systems, because their impact has not yet had time to be fully been seen and studied. Even though this study has acknowledged the potential of these preventative technologies, there is very limited to no empirical evidence when it comes to their practical implementation and long-term effectiveness within hotel environments because they just have not been allowed the necessary time yet. Therefore, more case studies could provide valuable knowledge into how these technologies are being integrated into hotel financial systems. Further research could also lay out the challenges faced during adoption of these technologies. What is most important and is to be taken serious note of are the real-world outcomes after an acceptable time period of implementation. As an Example, blockchain' s decentralized and tamper-proof nature is often seen and cited as advantageous for fraud prevention. There is very little research on how blockchain can be applied to hotel transactions or for it to be integrated with existing financial systems in this sector. Exploring all of these aspects would allow a deeper dive for insights into the future potential of blockchain and other advanced technologies in preventing fraud within these hotels.

In addition, the integration of a mix of these technologies to create a more robust fraud prevention strategy could be an important avenue for future research. Research could focus on how hotels can combine technologies like AI for fraud detection with blockchain for secure transactions or biometric verification for identity management, to create a comprehensive and secure financial system. By examining real-world examples of hotels that have adopted integrated solutions, future research could identify best practices and the challenges that come with integrating these technologies into legacy systems. Another promising area for further research is the role of human factors in financial fraud prevention. While this study focused heavily on technological solutions, many instances of fraud are not solely due to weaknesses in technology but also due to human behaviour. For example, internal fraud may occur when

employees intentionally manipulate systems or fail to follow proper procedures, either out of negligence or for personal gain. Understanding the psychological and behavioural aspects of fraud is essential for developing more holistic fraud prevention strategies that include not only technology but also a focus on human behaviour.

Studies could examine how employee engagement, ethics, and job satisfaction influence the outcomes of fraud prevention. We have to understand how organizational culture, management practices and employee training can enhance or hamper the effectiveness of fraud prevention efforts. It could be helpful to study employee attitudes and awareness about fraud and fraud awareness programs. Moreover, investigating the influence of departmental silos, whereby various hotel departments (e.g., finance, IT, and human resources) do not communicate or cooperate with one another, could reveal further weak points in fraud detection and prevention. Training programs play a prominent role in preventing fraud. However, not much research has been conducted as to what sort of training best suits various hotel employees at every level. Future studies can find out which training method (online, in-person, or game-based learning) is the best and how it can be customized as per the role in the hotel. Research could explore how different roles such as front desk, accounting and IT require different types of fraud prevention training and whether these role-specific training programs are more effective in reducing fraud incidents. One of the crucial areas for future research work is the cybersecurity and fraud areas. As hotels are adopting more digital means of payment and loyalty programs, cyber security is an important factor in preventing fraud. Research can look on how hotels can better integrate cybersecurity into their fraud prevention. This may involve assessment of how premium encryptions technologies, secured payment gateways and multi - factor authentication mechanisms are coming into use for protection of sensitive data and prevention of unauthorized access. In addition, the research should also look into the role hotels IT departments play in keeping these cybersecurity systems up to date, and whether that challenges them in ensuring fraud prevention measures are effective over time. Further investigations into the financial consequences of fraud could seek to estimate the losses caused by fraud across various hotel categories. Independent hotels may be more susceptible to financial loss due to fraud than larger hotels, which have the resources to implement sophisticated fraud prevention technologies. Future studies can explore the financial impact of fraud and analyse the subsequent implications across hotel categories (small, medium and large). This data will offer more precise details that can help a hotel make key decisions regarding fraud investment choice. If the fraud is understood to impact profitability of various hotels, then fraud prevention

could be developed based on types of hotels. Cost-benefit analysis of various fraud technology is an option to pursue for future research. Although many types of fraud prevention technologies are available, hotels must examine the costs to implement these technologies, which include costs for initial setup, ongoing maintenance as well as training of the hotel staff. Researching the ROI from adopting fraud prevention methods will be beneficial for hotels that are often on a budget and don't want to leave themselves opened to fraud. If hotel managers could identify the technologies that produce the greatest net financial gain, in relation to the cost of implementing the technology, then they would be better positioned to prevent fraud. Longitudinal studies that examine how fraud prevention systems fare over time would also be beneficial. This research gave great insights into fraud prevention, but fraudsters are innovative, and what works today will not work tomorrow. It is recommended that future research focus on studies that examine the long-term outcomes and evolution of fraud over time. We may carry out longitudinal studies of hotels that set up specific fraud prevention systems to observe whether these will remain useful in the long run and how they can be modified as frauds evolve. Finally, hotel fraud prevention strategies are influenced by factors outside of the hotel's control and would therefore warrant further research. Further analysis could explore how regulatory shifts, such as new data privacy rules or accounting standards, impact the uptake and efficiency of fraud controls in hotels. Also, it would be useful to know how fraud could become more common in the hotel industry after a global recession. Or after more cases of fraud on online booking sites. And, how hotels could revise their prevention activities in response to this increase in fraud.

To conclude, this study has contributed significantly to fraud prevention in the hotel financial system. However, many avenues for research are possible. Future researches should observe emerging technologies, human factors affecting fraud prevention, cyber security combined with fraud detection systems, and the financial impacts of fraud on hotels. These issues will be studied, so the hotel industry can be guided on how to build more effective, resilient and adaptive fraud prevention strategies.

References

1. Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer, Mulatu Fekadu Zerihun, Polly Mashigo, Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry, Heliyon, Volume 10, Issue 1

2. 2024 Mutanda, Bronson & Maireva, Chrispen. (2023). TOWARDS A CYBER RESILIENT BANKING SYSTEM: EFFECTIVENESS OF CYBER FRAUD RISK MANAGEMENT STRATEGIES ADOPTED BY COMMERCIAL BANKS IN ZIMBABus. STUDIES AND SCIENTIFIC RESEARCHES ECONOMICS EDITION. 37. 54-69. 10.29358/sceco.v0i37.544.

3. Maphosa, Vusumuzi. (2024). An overview of cybersecurity in Zimbabwe's financial services sector. F1000Research. 12. 1251. 10.12688/f1000research.132823.2. Cybersecurity: An Overview." Journal of Banking Innovation, 20(2), 55-70.

4. Zimbabwe Banking Association. (2022). "Annual Report on Cybersecurity Practices in the Zimbabwean Banking Sector."

5. Reserve Bank of Zimbabwe. (2022). "Guidelines on Cybersecurity Standards for Financial Institutions."

6. Alhassan, I., Adam, I., & Afriyie, S. (2022). Fraud detection and prevention in the hospitality industry: A review of emerging technologies. *International Journal of Hospitality and Tourism Management, 5*(3), 67-89.
7. Chawla, K., & Mukherjee, P. (2021). The role of artificial intelligence in financial fraud detection: Challenges and opportunities. *Journal of Financial Crime, 28*(2), 315-332.
8. Fadiya, O. O., & Idowu, E. A. (2020). Cybersecurity threats in the hotel industry: A critical review. *Journal of Cybersecurity Research, 12*(1), 56-75.

9. Ho, L. T., & Yang, L. (2019). Financial fraud in the hospitality sector: A comparative study of risk factors in developing and developed economies. *Tourism Economics, 25*(6), 1-18.
10. Okonkwo, R. N., & Nduka, C. O. (2021). Financial fraud detection in hotels: An analysis of biometric security and blockchain applications. *Journal of Hospitality Financial Management, 19*(4), 278-295.
11. Button, M. (2020). *Financial crime and fraud prevention in the digital age.* Routledge.
12. Singleton, T. W., & Singleton, A. J. (2017). *Fraud auditing and forensic accounting.* Wiley.
13. Wells, J. T. (2018). *Corporate fraud handbook: Prevention and detection.* Wiley.
14. Accenture. (2022). *Fraud detection and prevention: Emerging trends in financial security for the hospitality industry.* Retrieved from www.accenture.com
15. Deloitte. (2021). *AI-driven fraud detection in the hospitality sector: Enhancing financial security.* Retrieved from www2.deloitte.com
16. PwC. (2020). *Global economic crime and fraud survey: Hospitality and tourism insights.* Retrieved from www.pwc.com
17. World Economic Forum. (2021). *How blockchain technology can revolutionize fraud prevention in financial systems.* Retrieved from www.weforum.org
18. U.S. Department of Justice. (2020). *Cybercrime and financial fraud: Trends and prevention strategies in the travel and hospitality industry.* Retrieved from www.justice.gov
19. National Institute of Standards and Technology (NIST). (2019). *Guidelines for financial fraud detection and mitigation.* Retrieved from www.nist.gov
20. Marriott International. (2019). *Lessons learned from the data breach: Strengthening fraud detection in hotel financial systems.* Internal security report.
21. Kaspersky Lab. (2021). *Fraud in the hospitality industry: How cybercriminals target hotel financial transactions.* Retrieved from www.kaspersky.com

Appendix I: AUREC Approval Letter

"Investing in Africa's future"

AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60026/61611 Fax: (+263 20) 61785 Website: www.africau.edu

Ref: AU 3420/24 21 August, 2024

TAKUNDA KATUNGA
C/O Africa University
Box 1320
MUTARE

RE: Evaluating Current and Emerging Technologies in Fraud Prevention for Hotel Financial Systems

Thank you for the above-titled proposal that you submitted to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following.

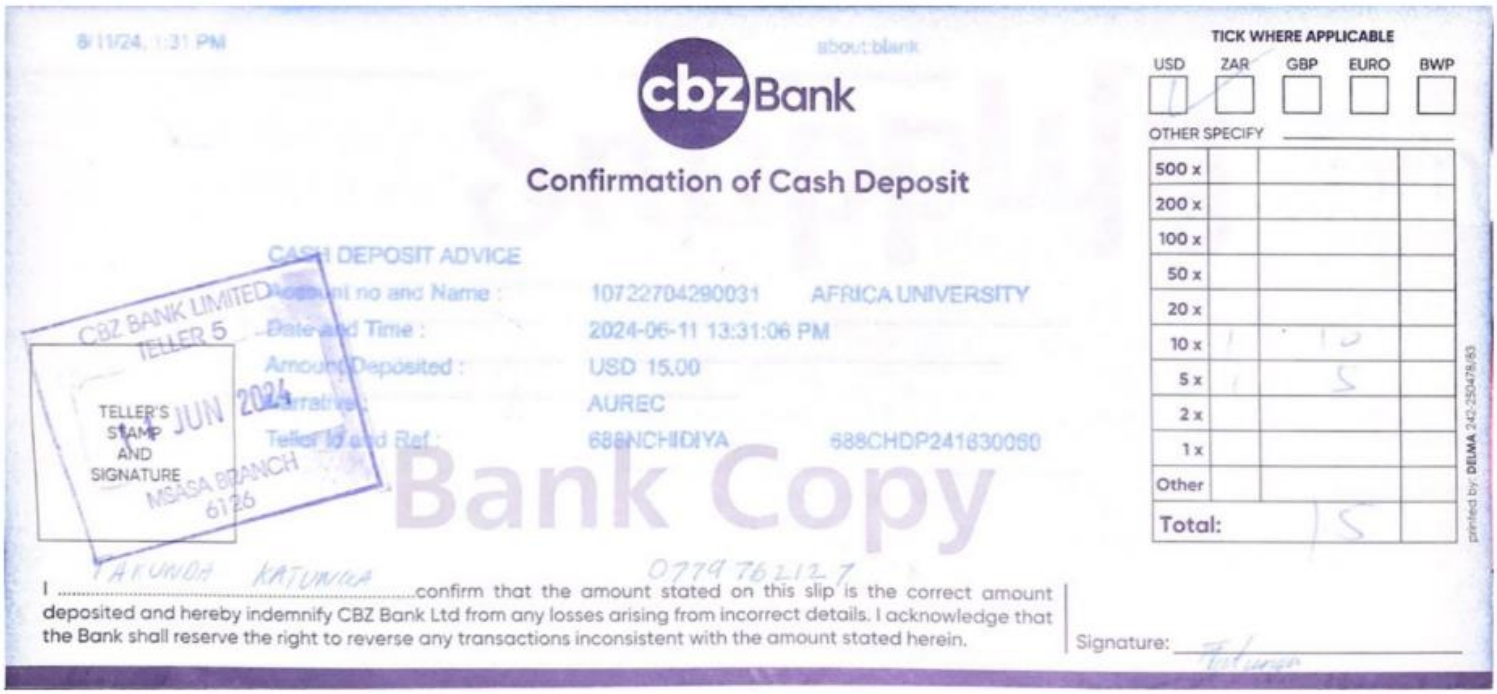
a) Research proposal

- **APPROVAL NUMBER** AUREC 3420/24
  This number should be used on all correspondences, consent forms, and appropriate documents.
- **AUREC MEETING DATE** NA
- **APPROVAL DATE** August 21, 2024
- **EXPIRATION DATE** August 21, 2025
- **TYPE OF MEETING**: Expedited
  After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems concerning subject safety must be reported to AUREC within 3 working days on the standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.

Yours Faithfully

MARY CHINZOU
ASSISTANT RESEARCH OFFICER: FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE

Appendix II: AUREC Proof of Payment



8/11/24, 1:31 PM about:blank

cbz Bank

Confirmation of Cash Deposit

CBZ BANK LIMITED TELLER 5

TELLER'S STAMP AND SIGNATURE JUN 2024 MSASA BRANCH 6126

CASH DEPOSIT ADVICE

Account no and Name : 10722704290031 AFRICA UNIVERSITY

Date and Time : 2024-06-11 13:31:06 PM

Amount Deposited : USD 15.00

Narrative : AUREC

Teller Id and Ref : 688NCHIDIYA 688CHDP241630060

Bank Copy

TAFUNDA KATUNGA 0779761127

I .....confirm that the amount stated on this slip is the correct amount deposited and hereby indemnify CBZ Bank Ltd from any losses arising from incorrect details. I acknowledge that the Bank shall reserve the right to reverse any transactions inconsistent with the amount stated herein.

Signature: .....

TICK WHERE APPLICABLE

USD	ZAR	GBP	EURO	BWP
☐	☑	☐	☐	☐

OTHER SPECIFY .....

500 x			
200 x			
100 x			
50 x			
20 x			
10 x	1	10	
5 x	1	5	
2 x			
1 x			
Other			
Total:		15	

printed by DELMA 242-250478/83

Appendix III: Letter for Data Collection Permission

Holiday Inn Harare
Cnr Samora Machel Av/Fifth Street.P. O. Box 7, Harare, Zimbabwe
T: +263 (242) 251 200-14, 795 611/291 F: +263 (242) 795 630/251 215
Email:reservations@holidayinnharare.co.zw
www.holidayinn.com

Holiday Inn
AN IHG HOTEL

26 June 2023

To Whom it may concern

Ref:Dissertation Research approval

This letter confirms that Takunda Katunga of Africa University is permitted to conduct his dissertation research at the Holiday Inn Harare Hotel. We support Takunda's academic endeavours and are pleased to facilitate his study within our premises.

For any further details please do conduct the undersigned.

Yours sincerely
For and behalf of Holiday Inn Harare

FP
Machel Zingoma
Human Resources Manager

HOLIDAY INN HARARE
26 JUN 2024
CNR S MACHEL AVE FIFTH ST.
P. O. BOX 7, HARARE
TEL

This hotel is operated by African Sun Limited under license from InterContinental Hotels Group.

Appendix IV: Informed Consent

Consent Form for Participation in Research Study

Title of Study: Evaluating Current and Emerging Technologies in Fraud Prevention for Hotel Financial Systems

Researcher: Takunda Jeffrey Limbani Katunga

Institution: Africa University

Contact Information: katungat@africau.edu, +263781177438

Purpose of the Study: This study aims to assess how effective current and emerging fraud prevention technologies are within hotel financial systems. Additionally, it seeks to understand the challenges associated with implementing these technologies and to recommend strategies for improvement.

Participation Details: If you decide to participate, you will be asked to fill out a questionnaire and or participate in a brief interview. Completing the questionnaire will take approximately 5 minutes, and the interview will take about the same amount of time. Your input is vital to achieving the goals of this research.

Confidentiality: Your responses will remain strictly confidential and will only be used for academic purposes. All data will be anonymized, and no personally identifying information will be included in the final report or any related publications.

Voluntary Participation: Your participation is completely voluntary. You are free to skip any question or withdraw from the study at any time without any negative consequences.

Risks and Benefits: There are no expected risks involved in participating in this study. While there are no direct benefits to you, the information you provide may contribute to enhanced fraud prevention measures in the hospitality sector.

Consent: By signing below, you confirm that you have read and understood this consent form, agree to participate voluntarily, and acknowledge your right to withdraw at any point without penalty.

Participant's Signature: _____Date: _____

Researcher's Signature: _____Date: _____

Appendix V: Questionnaire

Dissertation Questionnaire

Section 1: Background Information

1. What is your role in the hotel industry?

2. How many years of experience do you have in this field?

3. What is the size of your hotel? (e.g., small, medium, large)

4. Which financial systems does your hotel use?

Section 2: Current Technologies

5. Which fraud prevention technologies are implemented in your hotel

_____
_____
_____
_____
_____
_____

6. How effective are these technologies in preventing fraud? (Rate 1-5: 1 = Not effective, 5 = Highly effective)

_____

7. Has your hotel experienced a reduction in fraud incidents since adopting these technologies? (Yes/No)

_____

If yes, by approximately what percentage? _____%

Section 3: Fraud Prevention Methods

8. What non-technological methods does your hotel use to prevent fraud?

_____
_____
_____
_____
_____
_____
_____

9. How effective do you find these methods in preventing fraud? (Rate 1-5: 1 = Not effective, 5 = Highly effective)

_____
_____
_____
_____
_____

Section 4: Challenges

10. What challenges has your hotel encountered with fraud prevention technologies?

_____
_____
_____
_____
_____

11. How frequently do technical issues occur with these technologies?

_____
_____
_____
_____
_____

Section 5: Recommendations

12. Are you aware of any emerging fraud prevention technologies? (Yes/No)- If yes, please specify:

_____
_____
_____
_____
_____

13. What measures do you think could improve fraud prevention in hotels? (Select all that apply)-
    [ ] Advanced technologies
    [ ] Improved system integration
    [ ] Enhanced staff training
    [ ] Stronger industry regulations

    [ ] Other (please specify): _____

14. What additional resources or support would assist your hotel in strengthening fraud prevention efforts?

_____
_____
_____
_____
_____
_____

Thank you for participating. Your feedback is essential to this research.

Appendix V: Interview questions

Interview Questions

1. What fraud prevention technologies does your hotel currently use in its financial systems?

_____
_____
_____
_____

2. How would you assess the effectiveness of these technologies in preventing fraud?

_____
_____
_____
_____

3. Can you share examples where these systems either succeeded or failed to detect fraud?

_____
_____
_____
_____

4. What types of fraud are most frequently encountered in your hotel?

_____
_____
_____
_____

5. Besides technology, what other methods does your hotel employ to prevent fraud?

_____
_____

_____
_____

6. What challenges have you experienced when implementing fraud prevention technologies?

_____
_____
_____
_____

7. How do costs impact your hotel's decision to adopt fraud prevention systems?

_____
_____
_____
_____

8. What operational or technical issues have arisen during the integration of these technologies with existing systems?

_____
_____
_____
_____

9. How does staff training influence the success of your hotel's fraud prevention measures?

_____
_____
_____
_____

10. Are there any new or emerging fraud prevention technologies you think could benefit your hotel? If so, please describe them.

_____
_____
_____
_____

11. How effective do you think non-technological measures, such as policies or audits, are in preventing fraud?

_____
_____
_____
_____

12. What improvements would you recommend to enhance fraud prevention strategies in the hospitality industry?

_____
_____
_____
_____