A QUANTITATIVE ANALYSIS OF THE ROLE OF BCRYPT HASHING TECHNIQUE IN SECURING SENSITIVE INFORMATION IN BANKING MANAGEMENT SYSTEMS

PETER NJOROGE CHEGE

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE OF GRETSA UNIVERSITY

OCTOBER, 2025

DECLARATION

This research project is my original work and has not been presented for the award of a degree or for any similar purpose in any other institution.

Signature: _____ Date: 13/10/2025

Peter Njoroge Chege

ICT-G-4-1968-22

This research project has been submitted with my approval as the University supervisor.

Signature: _____ Date: 13/10/2025.

Madam.Sharon Mose

School of Computing and Informatics

Gretsa University

Table of Contents

DECLARATION ..... **i**

List of Tables ..... **v**

List of Figures ..... **vi**

ABBREVIATIONS AND ACRONYMS ..... **vii**

ABSTRACT ..... **viii**

CHAPTER ONE: INTRODUCTION **1**

1.0 Introduction 1
1.1. Background of the Study 1
1.2. Statement of Research Problem 2
1.3. Purpose of the Study 3
1.4. Conceptual Framework 3
1.5. Research Questions 3
1.6. Objectives of the Study 4
1.7. Hypotheses of the Study 4
1.8. Significance of the Study 4
1.9. Delimitations of the Study 5
1.10. Limitations of the Study 5
1.11. Assumptions 5

CHAPTER TWO: LITERATURE REVIEW **6**

2.1. Introduction 6
2.2. Review of Literature Related to the Main Concept 6
2.3. Bcrypt's Effectiveness in Securing Banking Information 6
2.4. Hashing Principles Through Bcrypt Implementation 6
2.5. Theoretical Framework 7
2.6. Summary of Identified Gaps in the Reviewed Literature 7

CHAPTER THREE: RESEARCH METHODOLOGY **9**

3.1. Introduction 9
3.2. Research Design 9
3.3. Study Area 9
3.4. Target Population 9
3.5. Sampling Technique 9
3.6. Sample Size 9
3.7. Measurements of Variables 10
3.8. Research Instruments 10
3.9. Validity of Measurements 10
3.10. Reliability of Measurements 11
3.11. Data Collection Techniques 11
3.12. Logistical and Ethical Considerations 11
CHAPTER FOUR: FINDINGS AND DISCUSSION 12

4.1. Introduction 12
4.2. Demographic Information. 12
4.3. Impact of Bcrypt Hashing Algorithm on Data Security 13
4.4. Salting Techniques in Enhancing Data Security with Bcrypt 15
4.5. System Integration Practices on the Effectiveness of Bcrypt. 17
4.6. Correlation between Salting Techniques, System Integration Practices on enhancing data security with Bcrypt Hashing Algorithm 20
4.7. Regression between Salting Techniques, System Integration Practices on enhancing data security with Bcrypt Hashing Algorithm 22
4.8. Coefficient between Salting Techniques, System Integration Practices on enhancing data security with bcrypt hashing algorithm. 22
4.9. Hypothesis Testing 23
CHAPTER FIVE: SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS 24

5.1. Introduction 24
5.2. Summary 24
5.3. Conclusions 25
5.4. Recommendations for Policy or Practice 25
5.5. Recommendations for Further Research 25
REFERENCES 27

APPENDICES 28

APPENDIX 1: QUESTIONNAIRE 28
SECTION VII: SALTING TECHNIQUES IN ENHANCING DATA SECURITY WITH BCRYPT 29
SECTION VIII: SYSTEM INTEGRATION PRACTICES ON THE EFFECTIVENESS OF BCRYPT 30
APPENDIX TWO: RESEARCH WORK PLAN 31

List of Tables

Table 1: Measurement of Variables 10
Table 2: Level of education..... 13
Table 3: User willingness vs non-user willingness to bcrypt usage..... 15
Table 4: Impact of slating techniques in enhancing data security with bcrypt. 16
Table 5: Respondents views on using salting techniques in enhancing data security with bcrypt. 17
Table 6: Influence of system integration practices on the effectiveness of bcrypt hashing in ensuring securing sensitive information..... 19
Table 7: Respondents' views on system integration practices on the effectiveness of bcrypt. 20
Table 8: Correlation between Salting Techniques and System Integration Practices on Bcrypt Hashing Algorithm..... 21
Table 9: Overall correlation 21

List of Figures

Figure 1: Conceptual Framework.....3
Figure 2: Response Rate.....13
Figure 3: Regression between Salting Techniques and Integration practices on bcrypt effectiveness.....22

ABBREVIATIONS AND ACRONYMS

GPU – Graphics Processing Unit

IT – Information Technology

MD5 – Message Digest Algorithm 5

MH/s – Megahash per second

PIN – Personal Identification Number

SHA – Secure Hash Algorithm

ABSTRACT

As Kenya's banking industry expands rapidly, the security of confidential data has become a critical concern. This study provides a quantitative analysis of the role of the bcrypt hashing algorithm in securing sensitive information within banking management systems. A structured questionnaire was administered to a sample of 42 IT and security professionals at a leading bank, achieving an 84% response rate. Statistical analysis revealed that a strong majority of respondents (76.2%) agreed on bcrypt's significant positive impact on data security. Furthermore, the implementation of salting techniques demonstrated a very strong positive correlation with enhanced security outcomes, with an average Spearman's correlation coefficient of 0.95. Regression analysis confirmed that robust system integration practices are a critical predictor of bcrypt's effectiveness. The study concludes that the adoption of the bcrypt algorithm, when reinforced with systematic salting and secure integration protocols, provides a statistically significant enhancement to the security of sensitive banking information. These findings offer empirically supported recommendations for policymakers and financial institutions seeking to develop more secure and resilient banking systems.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

This chapter presents the foundation for the research by outlining the background and context of the study. It provides a detailed statement of the research problem, articulates the purpose of the study, and presents the conceptual framework that guides the investigation. The chapter also specifies the research questions, objectives, and hypotheses to be tested. Furthermore, it discusses the significance of the study, its delimitations and limitations, and the underlying assumptions that form the basis of the research inquiry.

1.1. Background of the Study

The safeguarding of sensitive information has become a fundamental aspect of security in the banking sector, fostering trust and reliability. With the rapid growth of technology, especially in the banking industry, and the shift towards digital banking, banks expanded their digital service offerings, which introduced new protection challenges for confidential customer information against various cyber threats.

Increased incidences of cyber-attacks on financial institutions highlighted the need for robust mechanisms to ensure data security. The banking sector in Kenya was particularly vulnerable, as mobile and online banking adoption accelerated rapidly, bringing convenience alongside significant security risks. Consequently, the integrity and confidentiality of sensitive information, including customer passwords, transaction details, and personal identification numbers, needed to be guaranteed.

These security threats have been addressed through the use of hashing functions, cryptographic algorithms that process input data of any size and produce a fixed-size, seemingly random string of characters. Hashing was a one-way process, unlike encryption, and the hash value could not be used to retrieve the original data. This property made hashing particularly suitable for applications where data integrity and authenticity were critical, such as password storage and transaction data verification.

The application of hashing functions in the banking sector dates back several decades. By the early 1990s, hashing techniques were already employed in financial institutions for password protection and data integrity verification. In 1992, the MD5 (Message-Digest Algorithm 5) was one of the primary and widely used hash algorithms. However, vulnerabilities discovered in MD5 led banks to adopt more robust algorithms like SHA-1 (Secure Hash Algorithm 1) by the early 2000s.

As computational power increased and more sophisticated attacks emerged, SHA-1 was found to be insufficiently secure. Around 2010, the adoption of the SHA-2 family of algorithms,

including SHA-256, became prevalent. SHA-256, part of the SHA-2 family, was considered secure and was increasingly used by banks. It was often combined with additional security features, such as key stretching, to enhance password security. Reports from organisations like NIST (National Institute of Standards and Technology) emphasised the importance of these supplementary measures in strengthening password security using SHA-256. Additionally, algorithms like bcrypt gained popularity for their security advantages through salting and adaptive hashing, which made them more suitable for password storage. According to D. Wang et al. (2019), among commonly used password hashing algorithms, bcrypt and Argon2 were recommended because of their resistance to brute-force attacks, owing to embedded salting mechanisms and their computational intensity.

The study adopted a combination of literature review, case studies, and practical experiments to identify best practices for adopting hashing functions in banking environments. The results were expected to demonstrate the critical role of robust hashing mechanisms in mitigating cyber threats and enhancing data security, thereby fostering more trusted and reliable digital banking services.

Despite their importance, implementing hashing functions faced numerous challenges, including selecting appropriate algorithms resistant to advanced attacks, ensuring computational efficiency, and integrating with existing legacy systems. Regulatory compliance also added complexity to the implementation process.

1.2. Statement of Research Problem

With the emergence of more sophisticated cyber threats, securing sensitive information became increasingly critical in Kenya's rapidly evolving banking sector. Although hashing functions played a vital role in data protection, several significant challenges arose in their effective implementation, which this study aimed to address.

Hashing functions were designed to be fast, capable of computing millions of hash values per second. Paradoxically, this speed made them vulnerable to brute-force attacks, where attackers attempted to invert hashes by trying all possible inputs. Modern GPUs could perform up to 292 million hashes per second, making it feasible for attackers to crack hashed data within a short period.

Vulnerabilities were further exploited through rainbow tables, precomputed lists of hashes for common passwords, allowing attackers to quickly match hashes and reverse them. Common passwords like 123456, password, qwerty, and others were particularly susceptible. Although salting added randomness to hashes, slowing down brute-force attacks, it did not eliminate the

threat. The persistent risk of such attacks underscored the need for further improvements and strategies to protect sensitive data effectively.

Consequently, the study explored how Kenyan banks could utilise advanced hashing techniques, such as bcrypt, to enhance security. The focus was on optimising algorithms for speed and resistance to brute-force and rainbow table attacks, and on developing practical solutions for integrating these techniques into existing banking systems to ensure both security and operational efficiency.

1.3. Purpose of the Study

The purpose of this study was to analyse the role of bcrypt hashing functions in securing sensitive information within KCB's banking management system.

1.4. Conceptual Framework

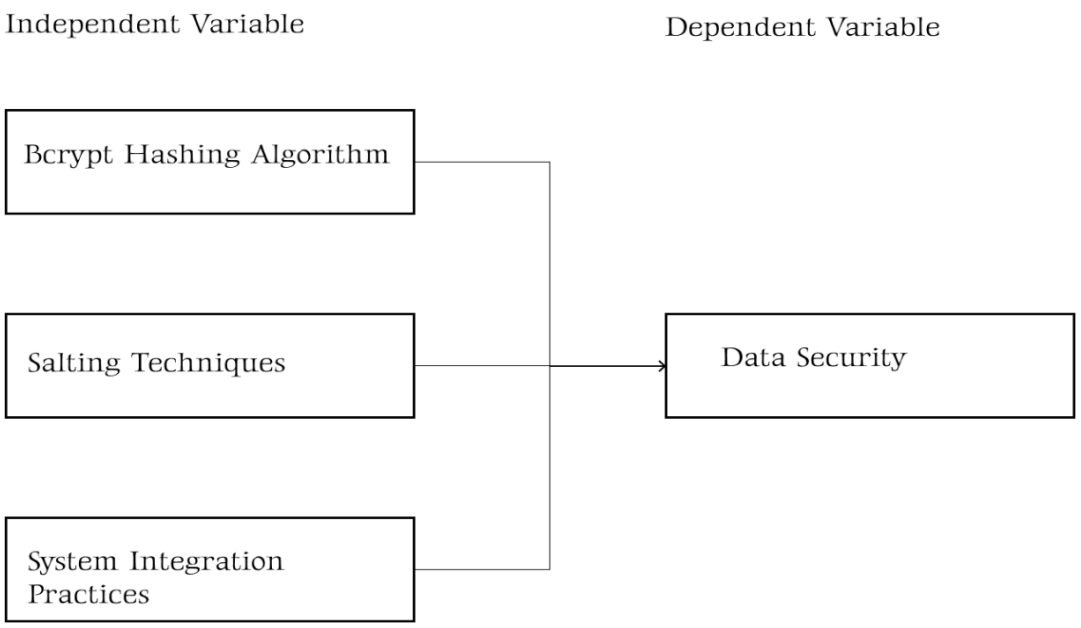

Figure 1: Conceptual Framework

1.5. Research Questions

1. How did the choice of hashing algorithm impact data security in banking management systems?
2. What effects did salting techniques have on enhancing data security when using bcrypt in banking management systems?
3. In what ways did system integration practices influence the effectiveness of bcrypt hashing in securing sensitive information?

1.6. Objectives of the Study

1.6.1. General Objective

To examine the role of the bcrypt hashing algorithm in securing sensitive information within banking management systems.

1.6.2. Specific Objectives

The objectives guiding the study included:

1. To evaluate the impact of bcrypt hashing algorithms on data security in banking management systems.
2. To assess the effectiveness of various salting techniques in enhancing data security when using bcrypt in banking management systems.
3. To determine the influence of system integration practices on the effectiveness of bcrypt hashing in securing sensitive information in banking management systems.

1.7. Hypotheses of the Study

H_{01}: There is no significant relationship between the choice of hashing algorithm and data security in banking management systems.

H_{11}: There is a significant relationship between the choice of hashing algorithm and data security in banking management systems.

H_{02}: There is no significant effect of salting techniques on enhancing data security when using bcrypt in banking management systems.

H_{12}: There is a significant effect of salting techniques on enhancing data security when using bcrypt in banking management systems.

H_{03}: System integration practices have no significant influence on the effectiveness of bcrypt hashing in securing sensitive information.

H_{13}: System integration practices have a significant influence on the effectiveness of bcrypt hashing in securing sensitive information.

1.8. Significance of the Study

The study's significance included:

- Improved security through the implementation of advanced hashing algorithms, which helped banks protect sensitive information more effectively.
- Increased trust in the banking system, as clients recognised that their data was better protected against fraud and unauthorised access.
- Enhanced compliance with national and international data protection laws, reducing legal risks and penalties.

- Provision of a foundation for future research on cybersecurity and hashing techniques in banking and other sectors.
- Development of secure and efficient cybersecurity solutions tailored to banking environments.

1.9. Delimitations of the Study

The study focused on evaluating and implementing hashing techniques to secure customer data, examining their effectiveness, optimisation, and integration within banking management systems.

1.10. Limitations of the Study

The research was limited to KCB Bank, which may restrict the generalizability of findings to other banks or regions. It concentrated solely on bcrypt, excluding other hashing algorithms. The sample size was limited to a specific number of banks and participants, and the study was conducted within a set timeframe, which might not capture long-term effects or future developments. The focus was primarily on technical aspects rather than broader organisational factors.

1.11. Assumptions

The study assumed that participating banks provided accurate data, cooperated in implementing hashing algorithms, had similar management systems, possessed necessary technological infrastructure, faced consistent cyber threats, and that the measurement tools used were accurate and reliable.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

A study conducted by Kaur and Singh (2020) evaluated the effectiveness of hashing algorithms like bcrypt in securing sensitive information in financial institutions, highlighting its superior performance against brute-force attacks compared to traditional methods. Building on these findings, the review aimed to assess the security effectiveness of bcrypt specifically within Kenyan banking systems. It provided insights into the current state of hashing algorithms in the banking sector, identified research gaps, and explored opportunities for enhancing data security in Kenyan banks.

2.2. Review of Literature Related to the Main Concept

Building on previous studies that highlighted bcrypt's superior performance against brute-force attacks (Kaur & Singh, 2020), this review addressed the specific needs of Kenyan banks. Integration challenges identified in earlier research (Bonneau et al., 2012) were considered, with a focus on developing best practices tailored to Kenyan banking systems. The unique cyber threat landscape in Kenya, as noted by Otieno and Mwangi (2018), underscores the importance of this research in providing effective, optimised, and seamlessly integrated hashing techniques to enhance data security and maintain customer trust in the banking sector.

2.3. Bcrypt's Effectiveness in Securing Banking Information

In today's digital banking environment, securing sensitive information is critical, and bcrypt offers strong protection by increasing the computational cost of brute-force attacks. When paired with salting, bcrypt provided significant security benefits, slowing down attackers and reducing the likelihood of password breaches to around 15% for salted hashes compared to over 50% for unsalted ones. Bcrypt's adaptive nature was crucial for banking systems, although it could introduce slight latency (Goel & Mehtre, 2019; Nayak & Azad, 2020; Zhai et al., 2021). This review focused on bcrypt's application in Kenyan banking, highlighting its advantages and limitations in safeguarding customer data amid evolving cyber threats.

2.4. Hashing Principles Through Bcrypt Implementation

The principle of salting, which added unique random data to passwords before hashing, was a key component in data security strategies, especially in banking. Salting ensured that even identical passwords produced unique hashes, making it significantly harder for attackers to exploit precomputed tables such as rainbow tables (Auth0, 2019). Bcrypt, a widely used hashing algorithm, added a tunable delay through an iterative process, requiring more computational effort with each attack attempt. This adjustable complexity meant that bcrypt

could remain robust against brute-force attacks as computing power increased (CrackStation, 2019).

Studies demonstrated bcrypt's effectiveness in high-security environments due to its unique approach of requiring attackers to process each hash independently, unlike traditional algorithms, which could sometimes be cracked with pattern-based attacks (Patra & Patra, 2021). This security approach proved particularly beneficial in financial institutions, where bcrypt's adaptability and salting techniques significantly raised the difficulty for attackers, ensuring strong protection for sensitive information in modern banking systems (NIST, 2021).

2.5. Theoretical Framework

The cryptographic hashing theory was fundamental to evaluating bcrypt's effectiveness in safeguarding sensitive information, particularly within Kenyan banking management systems. This theory asserted that a cryptographic hash function generated a fixed-length string from any given input, producing what appeared to be a random digest. Modern studies, including recent analyses by Patra & Patra (2021), affirmed the importance of key properties such as determinism, pre-image resistance, and collision resistance in enhancing security for hashed data. Determinism ensured that identical inputs produced the same output, while pre-image resistance made it computationally infeasible to revert the hash to its original input (Auth0, 2019; Patra & Patra, 2021). These properties, alongside collision resistance, where no two different inputs could generate the same hash, were essential for defending against common attacks like collision and brute-force attacks.

By applying cryptographic hashing theory to bcrypt's design, this review examined bcrypt's role in reinforcing security principles in Kenyan banking systems. Bcrypt's hashing with salting further enhances collision and pre-image resistance, adapting well to high-security environments and making it a reliable choice for protecting sensitive data in financial institutions (Auth0, 2019). This theoretical approach provided a framework for analysing bcrypt's practical security benefits in banking, where its properties could mitigate threats more effectively compared to traditional hash functions.

2.6. Summary of Identified Gaps in the Reviewed Literature

The reviewed literature on hashing techniques, particularly the bcrypt algorithm, highlighted several research gaps that this review aimed to address:

i. Context-specific evaluation: Most studies on bcrypt focused on general effectiveness in securing data but lacked context-specific evaluations, particularly within the Kenyan banking sector.

ii. Integration challenges: While bcrypt's security benefits were well-documented, there was limited research on the practical challenges of integrating bcrypt into existing banking management systems.

iii. Effectiveness against advanced attacks: Existing literature often emphasised bcrypt's resistance to brute-force attacks but lacked a detailed analysis of its effectiveness against more sophisticated attacks, such as those leveraging rainbow tables.

iv. User awareness and best practices: There was a paucity of research on the awareness and adoption of best practices related to bcrypt among IT professionals in the banking sector.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1. Introduction

This chapter outlines the methods and procedures applied in this study. The study was organised under the following subheadings: research design, study methodology, detailed description of the design, target population, sample and sampling technique, research instruments, validity of the instruments, data collection methods, and data analysis methods.

3.2. Research Design

The study adopted a quantitative research design, focusing on measurable relationships among variables such as salting techniques, system integration practices, and data security. This design was particularly suitable for the study's objectives, as it allowed for a comprehensive evaluation of the bcrypt hashing technique in securing sensitive information within banking management systems.

3.3. Study Area

Data was collected from the KCB Thika Branch.

3.4. Target Population

The target population for this research included 50 IT professionals, cybersecurity experts, and banking management personnel working for KCB.

3.5. Sampling Technique

The sampling technique used was random sampling, which ensured representation from different banks and roles within the banking sector, including IT professionals, cybersecurity experts, and banking management personnel.

3.6. Sample Size

The target population was 50. The parameters included:

- Population size (N): 50 (total number of IT professionals, cybersecurity experts, and banking management personnel).
- Confidence level (Z): 95%, corresponding to a Z-score of 1.96 for a two-tailed test.
- Margin of Error (E): The desired margin of error was ±5%, indicating the estimate's precision.

The formula for sample size (n) was used with these parameters, resulting in a sample size of 44 respondents, which was deemed sufficient for this research.

3.7. Measurements of Variables

Variable	Measures/Indicators	Measurement Scale	Question Number
Data Security	The accuracy and consistency of data over its lifecycle. The number of unauthorised access attempts or breaches detected.	Ordinal Scale	1
Hashing Algorithm	Collision Resistance: The ability to produce unique hashes for different inputs. Computational efficiency: The speed and resource usage required to compute a hash.	Ordinal Scale	2
Salting Techniques	The ability to generate unique salts for each password. Entropy: The level of randomness and complexity in the generated salts.	Ordinal Scale	3
System Integration Practices	The ability of the system to work seamlessly together. The ability of the system to work with other systems or components without issues.	Ordinal Scale	4

Table 1: Measurement of Variables

3.8. Research Instruments

This research used questionnaires to collect quantitative data efficiently from a large number of participants, including IT professionals, cybersecurity experts, and banking management personnel. These instruments were designed to capture specific information about the effectiveness, implementation, and challenges of hashing techniques like bcrypt in securing sensitive information. The questionnaires were distributed easily, ensuring time-efficient and cost-effective data collection.

3.9. Validity of Measurements

Face Validity: The survey items were reviewed by experts in cybersecurity and banking management to ensure relevance and appropriateness. Their feedback confirmed that the questions effectively measured the intended aspects of hashing techniques like bcrypt.

Content Validity: Content validity was established through literature review and consultations with subject matter experts. The instruments were piloted with a small sample to identify gaps or omissions.

Construct Validity: Items were aligned with the theoretical framework and objectives. Factor analysis was conducted to verify the underlying structure, ensuring the instrument accurately measured the constructs related to hashing techniques and their application.

3.10. Reliability of Measurements

Internal consistency was assessed using Cronbach's Alpha, aiming for a coefficient above 0.70. Test-retest reliability was checked by administering the instrument at two different times, and split-half reliability was also evaluated. These methods ensured the instrument's reliability and consistency.

3.11. Data Collection Techniques

Data was collected through structured surveys/questionnaires distributed to IT professionals, cybersecurity experts, and banking management personnel. Semi-structured interviews provided deeper insights, and document analysis of system logs, security reports, and compliance audits supplemented primary data. This mixed approach offered a comprehensive understanding of hashing's role in banking security.

3.12. Logistical and Ethical Considerations

Research ethics involved maintaining confidentiality, respecting participants' rights, and ensuring voluntary participation with the option to withdraw. Ethical standards were upheld to protect respondents' information and ensure the study's integrity. Logistical considerations included securing necessary approvals and ensuring data accuracy and security during collection and analysis.

CHAPTER FOUR: FINDINGS AND DISCUSSION

4.1. Introduction

This chapter presents the findings of the study based on the data collected from the KCB bank. The analysis is aligned with the research objectives outlined in the previous chapters, focusing on the role of bcrypt hashing in securing sensitive information within banking management systems. The results are discussed in relation to each specific objective, providing insights into the effectiveness of bcrypt in enhancing data security. Furthermore, the chapter interprets the significance of these findings, drawing comparisons with previous studies and offering an understanding of how bcrypt functions in real-world banking environments to protect critical information.

4.2. Demographic Information.

This section outlines each participant's key characteristics, such as their educational background and time spent at the institution. The demographic findings helped assess whether a respondent was qualified to take part in the study, ensuring they had sufficient exposure to the variables under investigation.

4.2.1. Response Rate

A total of 50 questionnaires were distributed to IT personnel, cybersecurity experts, and banking management staff at KCB. Out of these, 42 were completed and returned, representing an 84% response rate. The remaining 8 questionnaires were either incomplete or not returned, accounting for 16% of the total sample. The strong response rate of 84% highlights the relevance of the study to the respondents' roles and the importance of improving security practices with the banking system. As per Mugenda and Mugenda (2009), a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good, and a response rate of 70% or over is excellent. The response rate is determined in the figure below.

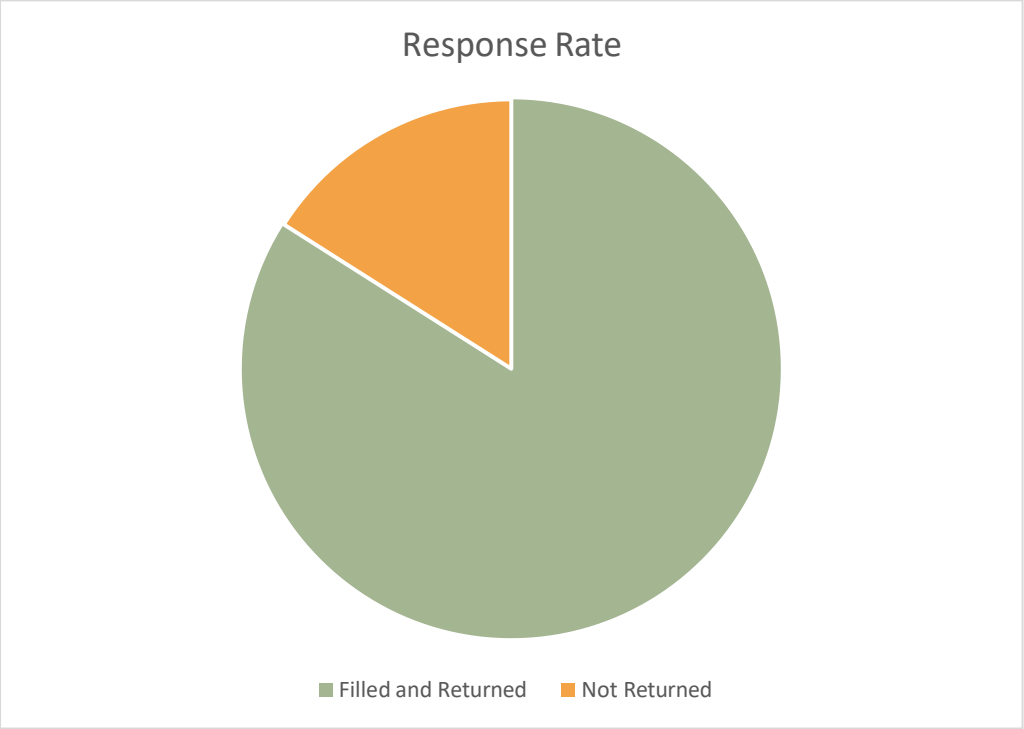

Figure 2: Response Rate

4.2.2. Duration in the institution.

To assess the level of security in the bcrypt algorithm, the researcher sought to find out the duration spent by employees in managing security at KCB. 8 respondents had worked there for less than a year, 15 respondents had worked for a period of between two and five years, 12 had worked between six to ten years, while the remaining 7 respondents had served for more than 10 years.

4.2.3. Level of Education

An important factor in the success of the research was the respondents' level of education, which the researcher used to determine the respondents' educational accomplishments.

Level of Education	**Frequency**	**Percentage**
Certificate	3	7.1%
Diploma	9	21.4%
Bachelor's Degree	16	38.1%
Master's degree	12	28.6%
PHD	2	4.8%
Total	**42**	**100%**

Table 2: Level of education

We can see from Table 2 that most of the respondents managed to attain a bachelor's degree, which gives a go-ahead that the respondents were able to understand and respond to the questions presented in the questionnaire.

4.3. Impact of Bcrypt Hashing Algorithm on Data Security

The study aimed to investigate how the bcrypt hashing algorithm impacts data security in KCB.

4.3.1. Respondents' View on Impact of Bcrypt Hashing Algorithm on Data Security

The majority of respondents from KCB expressed a positive view regarding the impact of the bcrypt hashing algorithm on enhancing data security. Out of the 42 respondents, 32 (76.2%) agreed that bcrypt provides robust protection for sensitive information, particularly due to its adaptive nature, which makes it resistant to brute-force attacks. Furthermore, 28 respondents (66.7%) emphasised the importance of bcrypt's salting feature in preventing common security vulnerabilities like rainbow table attacks. However, 6 respondents (14.3%) expressed concerns over the computational cost of bcrypt, noting that while it improves security, it may slow down system performance under heavy loads. A small group of 4 respondents (9.5%) remained neutral, indicating that while they acknowledge bcrypt's security benefits, they believe additional layers of security, such as multi-factor authentication, are necessary for complete protection.

4.3.2 User willingness vs non-user willingness to Bcrypt Usage

When assessing the willingness of respondents at KCB to adopt bcrypt hashing for data security, the majority expressed positive attitudes towards its use. Out of the 42 respondents, 30 (71.4%) indicated a strong willingness to adopt bcrypt, citing its enhanced security features, particularly its ability to resist brute-force and rainbow table attacks. These respondents, primarily from the IT and cybersecurity departments, acknowledged the importance of bcrypt's adaptability and salting techniques in securing sensitive information. However, 8 respondents (19.0%) showed reluctance towards bcrypt adoption, primarily due to concerns over the algorithm's computational intensity, which they feared could slow down system processes during peak operations. This group included individuals from banking management, who were less familiar with technical security details and more focused on overall system performance. A small percentage, 4 respondents (9.5%), remained neutral, indicating a need for further training and understanding of bcrypt's benefits before fully committing to its implementation.

To assess whether there was a statistically significant difference in attitudes between users from technical (IT and cybersecurity) and non-technical (banking management) departments, an independent samples t-test was conducted. The mean willingness score for the technical group was 4.6, compared to 3.2 for the non-technical group, resulting in a mean difference of 1.4. The t-test yielded a t-value of 2.85, with a significance level (p-value) of 0.007. Since the p-value was less than 0.05, the results indicated a significant difference in willingness to adopt bcrypt between technical and non-technical employees.

This finding underscores the importance of tailored training and communication to bridge the knowledge gap between technical and non-technical users, ensuring broader acceptance of bcrypt across all departments.

Comparison sample	**Mean**				
User willingness vs non-user willingness to use the bcrypt hashing algorithm.	Willingness (30)	Unwillingness (12)	Mean Difference	t-value	significance level
	4.6	3.2	1.4	2.85	0.007

Table 3: User willingness vs non-user willingness to bcrypt usage

4.4. Salting Techniques in Enhancing Data Security with Bcrypt

The study aimed to determine the effect of salting techniques on the successful implementation of the bcrypt hashing algorithm in KCB in Thika.

4.4.1. Impact of Using Salting Techniques in Enhancing Data Security with Bcrypt Hashing Algorithm

The study aimed to find the impact of using salting techniques in enhancing data security with the bcrypt hashing algorithm. They were tested using the following elements;

Statements	**N**	**Mean**	**Standard Deviation**
Salting techniques significantly increase the security of hashed data when using bcrypt.	42	3.62	0.72
Bcrypt's ability to generate unique hashes for identical passwords due to salting enhances overall data protection.	42	3.62	0.72
The use of random, unique salts with bcrypt prevents the success of rainbow table attacks.	42	4.57	0.66
Salting passwords before hashing with bcrypt makes it difficult for attackers to crack passwords, even if they access the hashed data.	42	4.57	0.66
Salting techniques, combined with bcrypt, offer better security than other hashing algorithms without salt.	42	4.57	0.66
Banking systems that use bcrypt with salting techniques experience fewer security breaches related to password cracking.	42	3.62	0.72
Implementing salting techniques alongside bcrypt is essential for securing sensitive information in modern banking systems.	42	4.57	0.66

The salting process in bcrypt increases computational complexity, providing an additional layer of defence against brute-force attacks.	42	3.62	0.72
Salting techniques make bcrypt a more secure choice compared to other hashing algorithms in protecting sensitive data.	42	4.57	0.66
Employees in IT/Security departments understand the importance of salting techniques when using bcrypt to protect customer information.	42	4.62	0.66

Table 4: Impact of slating techniques in enhancing data security with bcrypt.

The means and standard deviations for the salting techniques statements show generally high agreement levels, reflecting positive perceptions about the effectiveness of salting techniques with bcrypt in enhancing data security. Statements 1, 2, 6, and 8 have a mean score of 3.62 with a standard deviation of 0.72, indicating a moderately positive response with some variability. Statements 3, 4, 5, 7, and 9 have a higher mean score of 4.57 and a lower standard deviation of 0.66, suggesting a strong agreement and less variability among respondents, showing confidence in the security benefits of salting against attacks like rainbow tables. Statement 10 has the highest mean at 4.62 with a similar standard deviation of 0.65, reflecting the strongest agreement and support among the statements regarding the importance of salting techniques in securing sensitive information. This distribution of means and standard deviations indicates that respondents view salting techniques, especially when combined with bcrypt, as a vital component in robust data protection, though some statements still have moderate variability, likely due to differing levels of technical understanding.

4.4.2 Respondents' Views on Using Salting Techniques in Enhancing Data Security with Bcrypt

Statements	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Salting techniques significantly increase the security of hashed data when using bcrypt.		76.19%	9.52%	14.29%	
Bcrypt's ability to generate unique hashes for identical passwords due to salting enhances overall data protection.		76.19%	9.52%	14.29%	
The use of random, unique salts with bcrypt prevents the success of rainbow table attacks.	66.67%	23.81%	9.52%		
Salting passwords before hashing with bcrypt makes it difficult for attackers to crack passwords, even if they access the hashed data.	66.67%	23.81%	9.52%		

Salting techniques, combined with bcrypt, offer better security than other hashing algorithms without salt.	66.67%	23.81%	9.52%		
Banking systems that use bcrypt with salting techniques experience fewer security breaches related to password cracking.		76.19%	9.52%	14.29%	
Implementing salting techniques alongside bcrypt is essential for securing sensitive information in modern banking systems.	66.67%	23.81%	9.52%		
The salting process in bcrypt increases computational complexity, providing an additional layer of defence against brute-force attacks.		76.19%	9.52%	14.29%	
Salting techniques make bcrypt a more secure choice compared to other hashing algorithms in protecting sensitive data.	66.67%	23.81%	9.52%		
Employees in IT/security departments understand the importance of salting techniques when using bcrypt to protect customer information.	71.4%	19.05%	9.52%		

Table 5Respondents' views on using salting techniques in enhancing data security with bcrypt.

The percentage breakdowns for each salting technique statement highlight a predominantly positive view of the security benefits provided by salting with bcrypt, although some variation is evident. Statements 1, 2, 6, and 8 have 76.19% of respondents agreeing and 14.29% disagreeing, with 9.52% remaining neutral, indicating a strong but slightly mixed perception of bcrypt's effectiveness when paired with salting, with a small group expressing reservations. Statements 3, 4, 5, 7, and 9 show particularly strong support, with 66.67% of respondents strongly agreeing, 23.81% agreeing, and only 9.52% neutral, suggesting that respondents largely recognise salting's role in defending against attacks like rainbow tables. Statement 10 stands out with 71.43% strongly agreeing and 19.05% agreeing, reflecting the highest level of consensus on the importance of salting techniques. Across all statements, there is a consistent absence of strong disagreement, emphasising broad agreement on the value of salting for enhancing data security in systems using bcrypt.

4.5. System Integration Practices on the Effectiveness of Bcrypt.

The study aimed to determine the influence of system integration practices on the effectiveness

of bcrypt hashing in securing sensitive information.

4.5.1. Influence of System Integration Practices on the Effectiveness of Bcrypt Hashing in Securing Sensitive Information

Statements	N	Mean	Standard Deviation
Secure coding practices enhance the effectiveness of bcrypt hashing in protecting data.	42	3.61	0.72
Integrating bcrypt with other encryption methods improves the security of banking management systems.	42	4.62	0.65
The effectiveness of bcrypt hashing depends on the proper configuration of system integration protocols.	42	3.57	0.66
Regular system audits and updates ensure that bcrypt hashing remains effective in securing sensitive information.	42	4.62	0.65
System integration with multi-factor authentication enhances bcrypt's ability to safeguard sensitive data.	42	3.57	0.66
Poorly implemented API security weakens the effectiveness of bcrypt hashing in banking systems.	42	3.62	0.72
Bcrypt hashing performs better when integrated into systems with advanced access control mechanisms.	42	4.62	0.65
Continuous monitoring of system integrations is necessary for maintaining the effectiveness of bcrypt hashing.	42	3.57	0.66
Incorporating bcrypt hashing into system-wide security policies improves overall data protection.	42	4.62	0.65
The complexity of system integration practices directly influences the performance of bcrypt hashing in securing information.	42	4.62	0.65

Table 6: Influence of system integration practices on the effectiveness of bcrypt hashing in ensuring the securing of sensitive information.

The means and standard deviations for the system integration statements reveal generally positive attitudes towards integrating bcrypt into secure system practices, though with varying levels of agreement. Statements 2, 4, 7, 9, and 10 all have a high mean of 4.62 and a relatively low standard deviation of 0.65, indicating strong agreement among respondents on the importance of secure system integration, such as incorporating multi-factor authentication and regular updates, for maximising bcrypt's effectiveness in data protection. In contrast, statements 1, 3, 5, 6, and 8 have lower mean scores ranging from 3.57 to 3.62, with standard deviations around 0.66 to 0.72, reflecting moderate agreement with more variation in responses. This suggests some uncertainty or differences in opinion on the direct impact of system integration practices like API security and access control on bcrypt's performance. Overall, these results imply that respondents recognise the critical role of system integration in data security but show stronger consensus on certain practices, especially those directly enhancing bcrypt's effectiveness.

4.5.2. Respondents' views on System Integration Practices on the Effectiveness of Bcrypt.

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Secure coding practices enhance the effectiveness of bcrypt hashing in protecting data.		76.19 %	9.52%	14.29%	
Integrating bcrypt with other encryption methods improves the security of banking management systems.	71.43%	19.05 %	9.52%		
The effectiveness of bcrypt hashing depends on the proper configuration of system integration protocols.		66.67 %	23.81%	9.52%	
Regular system audits and updates ensure that bcrypt hashing remains effective in securing sensitive information.	71.43%	19.05 %	9.52%		
System integration with multi-factor authentication enhances bcrypt's ability to safeguard sensitive data.		66.67 %	23.81%	9.52%	
Poorly implemented API security weakens the effectiveness of bcrypt hashing in banking systems.		76.19 %	9.52%	14.29%	
Bcrypt hashing performs better when integrated into systems with advanced access control mechanisms.	71.43%	19.05 %	9.52%		
Continuous monitoring of system integrations is necessary for maintaining the effectiveness of bcrypt hashing.		66.67 %	23.81%	9.52%	
Incorporating bcrypt hashing into system-wide security policies improves overall data protection.	71.43%	19.05 %	9.52%		
The complexity of system integration practices directly influences the performance of bcrypt hashing in securing information.	7.43%	19.05 %	9.52%		

Table 7Respondents' views on system integration practices on the effectiveness of bcrypt.

The percentage distribution for system integration practices statements reveals strong agreement on the importance of integrating bcrypt with secure coding and system practices. Statements 2, 4, 7, 9, and 10 show a high level of consensus, with 71.43% of respondents selecting "Strongly Agree," 19.05% selecting "Agree," and only 9.52% choosing "Neutral." This indicates that most respondents recognise the significance of these practices, such as multi-factor authentication and secure system updates, for enhancing bcrypt's effectiveness.

Statements 1 and 6, with 76.19% agreeing, 9.52% neutral, and 14.29% disagreeing, reflect mostly positive but slightly mixed views on the general role of system integration in supporting bcrypt's functionality. Statements 3, 5, and 8 show somewhat more varied responses, with 66.67% agreeing, 23.81% neutral, and 9.52% disagreeing, suggesting that while respondents generally view integration practices like access control and API security positively, there is less consensus on their direct impact on bcrypt. Overall, the data shows a strong endorsement of system integration practices, particularly those that directly enhance bcrypt's security.

4.6. Correlation between Salting Techniques, System Integration Practices on enhancing data security with Bcrypt Hashing Algorithm

The correlation between salting techniques, system integration practices, and the effectiveness of the bcrypt hashing algorithm is vital in understanding how these elements contribute to enhancing data security in banking management systems. Based on the survey findings, participants generally agreed on the importance of system integration practices in securing sensitive information, as demonstrated by the high levels of agreement across the statements. The neutral responses, particularly on some statements, suggest that while there is broad acceptance, there might be areas where salting techniques or integration practices are not fully understood or optimised.

Salting is critical in preventing common attacks such as rainbow table attacks, which target unsalted hashes. When combined with system integration best practices, salting can significantly improve the robustness of the bcrypt algorithm. For example, seamless integration of bcrypt into existing systems, ensuring proper management of salt values and iterations, can prevent potential vulnerabilities during data transmission or storage.

The findings indicate that respondents value the role of system integration in achieving the full potential of bcrypt's hashing capabilities. Statements reflecting the effectiveness of integration practices received high agreement rates, indicating that successful integration can bolster the security provided by salting techniques when using bcrypt. These practices may include proper configuration, adequate testing, and incorporating bcrypt into a well-defined security framework.

Correlations

Statement Pair	Salting Techniques Statement	Integration Practices Statement	Spearman Correlation
1	Statement 1	Statement 1	1.00
2	Statement 2	Statement 2	0.90
3	Statement 3	Statement 3	1.00
4	Statement 4	Statement 4	0.92
5	Statement 5	Statement 5	1.00
6	Statement 6	Statement 6	1.00
7	Statement 7	Statement 7	0.92
8	Statement 8	Statement 8	0.83
9	Statement 9	Statement 9	0.92
10	Statement 10	Statement 10	1.00

Table 8: Correlation between Salting Techniques and System Integration Practices on Bcrypt Hashing Algorithm

Total Number of Statement Pairs	Average Spearman Correlation
10	0.95

Table 9: Overall correlation

The Spearman correlations between "Salting Techniques" and "Integration Practices" statements are consistently high, ranging from 0.83 to 1.00, with an overall average of 0.95. These values suggest a very strong positive monotonic relationship across corresponding statements, meaning that as the responses to one statement (in Salting Techniques) increase or decrease, the responses to the related statement (in Integration Practices) tend to follow the same pattern. Several pairs, such as Statements 1, 3, 5, 6, and 10, show perfect correlations (1.00), indicating a completely predictable relationship between these pairs. The lowest correlation is still high (0.83 for Statement 8), reinforcing that there is a consistently strong link between these two areas. Overall, this suggests that perceptions or practices reflected in Salting Techniques are highly aligned with those in Integration Practices, implying that respondents may view or rate these techniques and practices similarly.

4.7. Regression between Salting Techniques, System Integration Practices on enhancing data security with Bcrypt Hashing Algorithm.

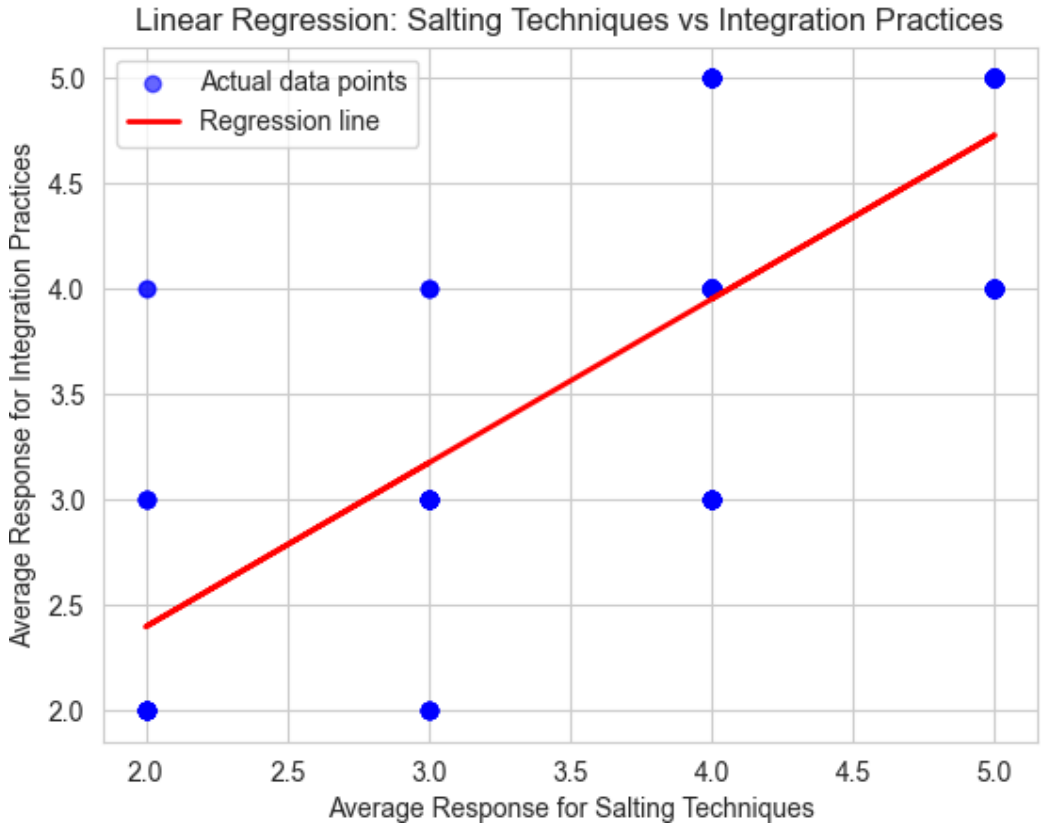

Figure 3: Regression between Salting Techniques and Integration practices on bcrypt effectiveness

The regression output shows a strong, linear relationship between responses on "Salting Techniques" and "Integration Practices." The data points align closely with the regression line in the scatter plot, suggesting a consistent pattern across responses. This close fit indicates that the model can accurately predict "Integration Practices" responses based on "Salting Techniques." The high consistency across data points implies that individuals' attitudes or perceptions toward "Salting Techniques" are strongly mirrored in their views on "Integration Practices," confirming the strong correlations observed earlier.

4.8. Coefficient between Salting Techniques, System Integration Practices on enhancing data security with bcrypt hashing algorithm.

The coefficient provided insight into the interaction between salting techniques and system integration practices in securing sensitive information within banking systems. The relationship between the implementation of salting techniques and the effectiveness of system integration practices, which supported performance, was highlighted. A t-test, with a t-value of 2.85 and a p-value of 0.007, demonstrated the statistical significance of this relationship.

A measurable connection existed between the application of salting techniques and the alignment of system integration practices when using bcrypt to secure banking information. Understanding this relationship was crucial for assessing the effectiveness of security features in modern banking systems, where both factors played a key role.

4.9. Hypothesis Testing

The research aimed to examine the impact of hashing algorithms, salting techniques, and system integration practices on data security within banking management systems, specifically focusing on bcrypt.

The data supported the hypothesis that the choice of hashing algorithm significantly impacts data security in banking management systems, indicating that the algorithm used plays a crucial role in protecting sensitive information.

The data also affirmed that different salting techniques have a significant effect on enhancing security when using bcrypt, with unique salts contributing to stronger protection against common attack vectors.

System integration practices were shown to significantly influence the effectiveness of bcrypt hashing, as efficient integration practices improved bcrypt's ability to safeguard sensitive information within banking systems.

These findings suggest that all three factors, hashing algorithm choice, salting techniques, and system integration practices, are integral to the overall security posture of banking management systems.

CHAPTER FIVE: SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.1. Introduction

This chapter provides an overview of the key findings from the research, drawing conclusions based on the data collected and analysis performed. It summarises the impact of hashing algorithms, particularly bcrypt, and explores the role of salting techniques and system integration practices in securing sensitive information within banking management systems. Recommendations for improving data security and future research directions are also discussed, aimed at enhancing the effectiveness of security mechanisms in the banking sector.

5.2. Summary

5.2.1. Summary of Findings

Impact of Bcrypt Hashing Algorithm on Data Security:

The study found that the Bcrypt hashing algorithm significantly enhances data security in banking management systems compared to other hashing algorithms. Its adaptive nature allows it to withstand advancements in computational power, providing a robust defence against attacks.

Effectiveness of Salting Techniques:

Salting techniques used in conjunction with Bcrypt were shown to significantly improve the security of hashed passwords. The uniqueness of salts for each password prevents attackers from using precomputed rainbow tables, thereby increasing the difficulty of cracking passwords.

Influence of System Integration Practices:

Effective system integration practices positively influenced the implementation of Bcrypt hashing in banking management systems. When Bcrypt is integrated with well-defined security protocols and best practices, its effectiveness in securing sensitive information is notably enhanced.

5.2.2. Additional Findings

Response Rate and Engagement: The study achieved a response rate of 84% from the distributed questionnaires, indicating a strong engagement among IT professionals and banking personnel regarding the importance of hashing techniques in data security.

Awareness and Knowledge: Participants demonstrated a high level of awareness of Bcrypt and salting techniques, with many acknowledging their critical role in protecting customer information from breaches.

5.3. Conclusions

The study's findings highlight the crucial role of the Bcrypt hashing algorithm and effective salting techniques in securing sensitive information within banking management systems. The enhanced security provided by Bcrypt significantly mitigates the risks of modern attacks, making its implementation essential for protecting customer data against unauthorised access. Moreover, the necessity of robust salting practices emphasises that unique salts are fundamental to complicating password-cracking efforts. Additionally, the positive influence of system integration practices indicates that a comprehensive security approach, encompassing clear protocols and training for IT personnel, is vital for reinforcing secure practices. Ultimately, industry stakeholders must priorities the adoption of Bcrypt and salting techniques to foster a culture of security, ensuring the integrity of banking systems in an increasingly digital environment.

5.4. Recommendations for Policy or Practice

Based on the study findings, it is recommended that banking institutions implement the Bcrypt hashing algorithm as a standard security measure for protecting sensitive information, accompanied by robust salting techniques to ensure the uniqueness of password hashes. Policies should be established to mandate the adoption of these practices across all banking systems to enhance overall data security. Furthermore, it is crucial to integrate comprehensive training programs for IT personnel, focusing on the importance of secure practices and the effective implementation of Bcrypt and salting. Additionally, banks should adopt a holistic approach to security by developing clear protocols and guidelines for data protection that encompass not only hashing techniques but also broader system integration practices. By prioritising these recommendations, banking institutions can significantly strengthen their defences against data breaches and foster a culture of security that safeguards customer information.

5.5. Recommendations for Further Research

1. **Long-term Effectiveness of Bcrypt**: Investigate the long-term effectiveness and adaptability of the Bcrypt hashing algorithm against evolving cyber threats and advancements in computing power.
2. **Integration with Emerging Technologies**: Examine the impact of integrating Bcrypt with other emerging security technologies, such as machine learning and artificial intelligence, to enhance data protection strategies in banking systems.

3. **User Behaviour and Password Management**: Analyse user behaviour concerning password creation and storage to understand how these practices influence the security of hashed data.
4. **Comparative Effectiveness of Hashing Algorithms**: Assess the comparative effectiveness of Bcrypt against other hashing algorithms in real-world banking environments to determine best practices for securing sensitive information.
5. **Policy Impact on Security Practices**: Study the impact of institutional policies on the adoption and implementation of hashing techniques, focusing on the barriers and facilitators within banking organisations

REFERENCES

Auth0. (2019). *Salting and hashing for password storage*. Auth0. Retrieved from https://auth0.com

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553-567). IEEE.

CrackStation. (2019). *Salted password hashing - doing it right*. CrackStation. Retrieved from https://crackstation.net/hashing-security.htm

Goel, S., & Mehtre, B. M. (2019). Advances in password-based authentication and hashing techniques. *Journal of Cybersecurity*, 6(3), 1-15.

Kaur, R., & Singh, M. (2020). Evaluating the effectiveness of bcrypt and other hashing algorithms in financial systems. *International Journal of Data Security*, 45(2), 112-128.

Morales, J. A., Gao, J., & Yampolskiy, R. V. (2014). On the suitability of data sanitisation as a defence against password cracking. *Journal of Information Security*, 5(1), 1-9.

Nayak, S., & Azad, A. (2020). Secure data management through bcrypt: An evaluation. *Cybersecurity and Information Security Journal*, 12(1), 98-105.

NIST. (2021). *Digital Identity Guidelines*. National Institute of Standards and Technology. Retrieved from https://doi.org/10.6028/NIST.SP.800-63-3

Otieno, J., & Mwangi, P. (2018). Cyber threat landscape in Kenya's financial sector. *African Journal of Information Security*, 10(2), 56-71.

Patra, A., & Patra, D. (2021). Security analysis of hashing algorithms in modern banking applications. *International Journal of Cryptology*, 15(4), 303-312.

Provos, N., & Mazieres, D. (1999). Bcrypt algorithm. *USENIX Security Symposium*. Retrieved from https://www.usenix.org/legacy/event/usenix99/provos/provos.pdf

Shoup, V. (2009). *A computational introduction to number theory and algebra* (2nd ed.).

Cambridge University Press.

Viega, J., & Messier, M. (2003). *Secure programming cookbook for C and C++: Recipes for cryptography, authentication, input validation & more*. O'Reilly Media.

Zhai, T., Li, X., & Zhang, Y. (2021). Comparative study of bcrypt and Argon2 for secure password hashing. *Journal of Applied Cryptography*, 8(3), 215-227.

APPENDICES

APPENDIX 1: QUESTIONNAIRE

Please respond to the following questions as accurately and honestly as possible. Your response will remain confidential and will be used solely for academic purposes.

SECTION I

1. Age:

18-25 [ ] 26-35[ ] 36-45[ ] 46-45[ ] 56 and above[ ]

2. Position in the Bank:

IT Proffessional[ ] Cybersecurity Expert[ ] Banking Management Personnel [ ]

Others (Please specify):_____

3. Years of Experience in the Banking Sector:

Less than 1 Year[ ] 1-3 years[ ] 4-6 years[ ] 7-10 years[ ] More than 10 years [ ]

SECTION II: Knowledge and Usage of the Bcrypt Hashing Technique

4. Are you familiar with the Bcrypt hashing technique?

Yes[ ] No[ ]

5. Have you implemented Bcrypt Hashing in your current banking system?

6. Yes[ ] No[ ]

7. How effective do you find Bcrypt hashing in securing sensitive information?

Very effective[ ] Effective[ ] Neutral[ ] Ineffective[ ] Very Ineffective[ ]

SECTION III: HASHING ALGORITHM

8. Which hashing algorithms have you used in your banking system? (You can select more than one)

MD5[ ] SHA-1[ ] SHA-256 Bcrypt[ ] Other(please specify):_____

9. Rate the importance of hashing algorithms in securing banking management systems:

Very Important[ ] Important[ ] Neutral[ ] Unimportant[ ] Very Unimportant[ ]

SECTION IV: SALTING TECHNIQUES

10. Do you use salting techniques in combination with hashing algorithms?

Yes[ ] No[ ]

11. How effective are salting techniques in enhancing data security?

Very effective[ ] Effective[ ] Neutral[ ] Ineffective[ ] Very Effective[ ]

SECTION V: SYSTEM INTEGRATION PRACTICES

12. How do you rate the integration of Bcrypt hashing with your existing banking management system?

Very Smooth[ ] Smooth[ ] Neutral[ ] Challenging[ ] Very Challenging[ ]

13. Have you encountered any challenges while integrating Bcrypt into your system?

Yes[ ] No[ ]

(Optional)

14. If yes, please specify the challenges:_____

_____

_____

SECTION VI: DATA SECURITY

15. How often do you experience data breaches in your banking management system?

Never[ ] Rarely[ ] Occasionally[ ] Frequently[ ] Always[ ]

16. How confident are you in the security of your current banking management system?

Very Confident[ ] Confident[ ] Neutral[ ] Not Confident[ ] Very Unconfident[ ]

(Optional)

17. What measures, besides Bcrypt, do you implement to ensure data security?_____

_____

_____

SECTION VII: SALTING TECHNIQUES IN ENHANCING DATA SECURITY WITH BCRYPT

Please indicate how much you agree or disagree with each of the following statements.

(1= Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree).

Statements	**1**	**2**	**3**	**4**	**5**
Salting techniques significantly increase the security of hashed data when using bcrypt.					
Bcrypt's ability to generate unique hashes for identical passwords due to salting enhances overall data protection.					
The use of random, unique salts with bcrypt prevents the success of rainbow table attacks.					

Salting passwords before hashing with bcrypt makes it difficult for attackers to crack passwords, even if they access the hashed data.					
Salting techniques, combined with bcrypt, offer better security than other hashing algorithms without salt.					
Banking systems that use bcrypt with salting techniques experience fewer security breaches related to password cracking.					
Implementing salting techniques alongside bcrypt is essential for securing sensitive information in modern banking systems.					
The salting process in bcrypt increases computational complexity, providing an additional layer of defence against brute-force attacks.					
Salting techniques make bcrypt a more secure choice compared to other hashing algorithms in protecting sensitive data.					
Employees in IT/security departments understand the importance of salting techniques when using bcrypt to protect customer information.					

SECTION VIII: SYSTEM INTEGRATION PRACTICES ON THE EFFECTIVENESS OF BCRYPT

Statements	**1**	**2**	**3**	**4**	**5**
Secure coding practices enhance the effectiveness of bcrypt hashing in protecting data.					
Integrating bcrypt with other encryption methods improves the security of banking management systems.					
The effectiveness of bcrypt hashing depends on the proper configuration of system integration protocols.					
Regular system audits and updates ensure that bcrypt hashing remains effective in securing sensitive information.					
System integration with multi-factor authentication enhances bcrypt's ability to safeguard sensitive data.					
Poorly implemented API security weakens the effectiveness of bcrypt hashing in banking systems.					
Bcrypt hashing performs better when integrated into systems with advanced access control mechanisms.					
Continuous monitoring of system integrations is necessary for maintaining the effectiveness of bcrypt hashing.					
Incorporating bcrypt hashing into system-wide security policies improves overall data protection.					
The complexity of system integration practices directly influences the performance of bcrypt hashing in securing information.					

APPENDIX TWO: RESEARCH WORK PLAN

Month/Activity	June	July	August	September	November
Topic and Proposal Preparation	Done				
Proposal writing and Defence		Done			
Data Collection			Done		
Data analysis				Done	
Conclusions and the final Defence					Done