

Developing a Framework for User Acceptance of Biometric Authentication in Electronic Payment Systems in the Thulamela Local Municipality

By

UNARINE TERRENCE RATSHIEDANA

17009864



A DISSERTATION
SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF COMMERCE IN BUSINESS INFORMATION SYSTEMS
IN THE
DEPARTMENT OF BUSINESS INFORMATION SYSTEMS
FACULTY OF MANAGEMENT, COMMERCE & LAW
UNIVERSITY OF VENDA

SUPERVISOR/PROMOTER: DR. W. MUNYOKA
CO-SUPERVISOR/CO-PROMOTER: MR. U. ANOKWURU

DECLARATION

I, **Unarine Terrence Ratshiedana**, hereby declare that this study for the Master of Commerce in Business Information Systems submitted to the Department of Business Information Systems at the University of Venda has not been submitted previously for any degree at this or another university. It is original in design and in execution, and all reference material contained therein has been duly acknowledged.

Researcher's Signature:  Date: 07/02/2025.

Supervisor's Signature:  Date: 24/03/2025.

Co-Supervisor's Signature: Uche Date: 24/03/2025.

DEDICATION

I dedicate this dissertation to God Almighty, whose guidance and strength have been my foundation. I also extend this dedication to my beloved parents for their unconditional love and support, and to my partner for her encouragement and patience throughout this journey. Additionally, I dedicate this work to aspiring researchers in Business Information Systems, hoping it inspires future innovation.

ACKNOWLEDGEMENTS

I express my deepest gratitude to God for His wisdom and perseverance in completing this research. Special thanks to my supervisors, Dr. W. Munyoka and Mr. U. D Anokwuru, for their invaluable guidance and support. I also appreciate my family and girlfriend for their unwavering encouragement. Furthermore, I am grateful to the respondents who contributed to this study. Lastly, this research has deepened my appreciation for Business Intelligence Systems and Big Data Analytics, reinforcing my passion for academic and professional growth.

ABSTRACT

The adoption of e-payment systems has revolutionised financial transactions, offering convenience, efficiency, and accessibility. However, concerns over fraud and security have necessitated the implementation of advanced authentication techniques, with biometric authentication emerging as a promising solution. Despite its potential, user acceptance remains a critical barrier to its broader adoption, influenced by factors such as privacy concerns, trust, and socio-cultural perceptions. This study explored the determinants of biometric authentication acceptance within e-payment systems within the Thulamela Local Municipality, aiming to investigate the determinants that enhance user adoption. A quantitative research approach was adopted, using a structured survey to collect data from 399 respondents. Descriptive and inferential statistics, including regression modelling, were conducted to assess key determinants of biometric authentication adoption. The study applied the Unified Theory of Acceptance and Use of Technology (UTAUT) as its theoretical foundation, integrating factors such as performance expectancy, effort expectancy, social influence, and facilitating conditions. The findings reveal that performance expectancy and effort expectancy significantly influence adoption intention. While perceived ease of use recorded a high mean score, the unexpected negative coefficient of perceived usefulness suggests that usability outweighs traditional usefulness in shaping user perceptions. Additionally, economic and social barriers pose notable challenges to biometric authentication adoption. Based on the insights from the research findings, a framework for enhancing biometric authentication acceptance was proposed, addressing key determinants through improved usability, building intuitive and user-centric interfaces for biometric authentication systems, awareness campaigns, and infrastructure investment, among others. The study concludes that while biometric authentication holds significant potential in enhancing security and efficiency in e-payment systems, addressing socio-economic and cultural barriers is essential for broader adoption. The study contributes to academic discourse by expanding UTAUT's application in biometric authentication research while offering practical recommendations for policymakers and financial institutions. Ultimately, this study provides a strategic roadmap for advancing secure, inclusive, and user-friendly biometric authentication in e-payment systems.

Keywords: Biometric authentication, User acceptance, Identity verification, Digital access control, E-Payment systems

TABLE OF CONTENTS

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	v
TABLE OF CONTENTS	vi
LIST OF FIGURES	ix
LIST OF TABLES	x
CHAPTER ONE: THE PROBLEM AND ITS SETTING	1
1.1 Introduction	1
1.2 Background of the Study	2
1.3 Statement of the Problem	3
1.4 Aim and Objectives	3
1.4.1 Aim	3
1.4.2 Objectives	3
1.5 Research Questions	4
1.6 Justification	4
1.7 Scope and Delimitation of the Study	5
1.8 Operational Definition of Key Words	6
1.9 Outline of the study	6
1.10 Chapter Summary	7
CHAPTER TWO: LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Background of the E-payment System	8
2.3 Current State of Biometrics	9
2.4 Use of Biometric Authentication Technologies in E-payment Systems	13
2.5 Benefits of Biometric Authentication Technologies in E-payment Systems	14
2.6 Factors Influencing User Acceptance of Biometric Authentication	15
2.7 Challenges and Considerations in the Adoption of Biometric Authentication for E-Payment Systems	17
2.8 Theories Guiding the Study	19
2.8.1 Technology Acceptance Model	19
2.8.2 Unified Theory of Acceptance and Use of Technology	20

2.9 Theoretical Framework	21
2.10 Chapter Summary.....	25
CHAPTER THREE: RESEARCH METHODOLOGY	26
3.1 Introduction	26
3.2 Research Philosophy/ Paradigm.....	26
3.3 Research Approach and Methodological Choice	27
3.3.1 Research Approach.....	27
3.3.2 Methodological Choice.....	28
3.4 Research Strategy.....	29
3.5 Time Horizon	31
3.6 Population and Sampling	31
3.6.1 Target Population	31
3.6.2 Sampling Technique	32
3.6.3 Sample Size	32
3.7 Data Collection Instruments.....	33
3.8 Data Analysis	34
3.8.1 Data Quality and Preparation	35
3.8.2 Descriptive Analysis.....	35
3.8.3 Inferential Analysis.....	36
3.9 Validity and Reliability	36
3.9.1 Validity	36
3.9.2 Reliability	37
3.10 Ethical Consideration	37
3.11 Chapter Summary.....	38
CHAPTER 4: PRESENTATION OF RESEARCH FINDINGS.....	40
4.1 Introduction	40
4.2 Response Rate	40
4.3 Demographic information	41
4.3.1 Age.....	41
4.3.2 Gender	41
4.3.3 Level of Education.....	42
4.3.4 Employment Status.....	43
4.3.5 Experience in Using Biometric Authentication in E-payment Systems.....	43
4.4 Reliability Test	44
4.5 Descriptive statistics.....	46

4.6 Explanatory Factor Analysis (EFA).....	47
4.7 Pearson Correlation	49
4.8 Regression Analysis	51
4.9 Discussion of Findings	53
4.10 Chapter Summary.....	59
CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	60
5.1 Introduction	60
5.2 Summary of Findings	60
5.3 Conclusions	61
5.4 Recommendations	62
5.5 Contributions of the Study	63
5.6 Limitations of the Study	63
5.7 Directions for Future Research	63
References.....	65
Appendix 1: Ethical Clearance.....	72
Appendix 2: Survey Questionnaire	73

LIST OF FIGURES

Figure 2.1: Integrated TAM and UTAUT conceptual framework.....	22
Figure 3.1: The research onion	26
Figure 4.1: Response rate	40
Figure 4.2: Age of respondents	41
Figure 4.3: Gender of respondents	42
Figure 4.4: Level of education of respondents	42
Figure 4.5: Employment status of respondents	43
Figure 4.6: Experience of respondents in using biometric authentication	44
Figure 4.7: User acceptance framework for biometric authentication in e-payments	59

LIST OF TABLES

Table 4.1: Cronbach alpha test	45
Table 4.2: Reliability test	46
Table 4.3: Descriptive tests	47
Table 4.4: Communalities	48
Table 4.5: Pearson correlation	49
Table 4.6: Regression model table.....	51
Table 4.7: ANOVAs	52
Table 4.8: Regression coefficients	52

CHAPTER ONE: THE PROBLEM AND ITS SETTING

1.1 Introduction

The increasing digitisation of financial transactions has transformed global economies, significantly altering how individuals and businesses engage in financial exchanges (Chubuk, 2024; Johnson et al., 2019). Electronic payment (E-payment) systems, from online banking to mobile wallet applications, have become essential for seamless, fast, and convenient transactions. As these systems permeate everyday life, the focus on security and reliability has intensified, especially concerning user authentication, where establishing secure access protocols is paramount (Brown & Jones, 2018). Recent advances in biometric authentication technology present a compelling opportunity to enhance E-payment security by verifying user identity through unique physiological and behavioural characteristics (Jain et al., 2020; Li et al., 2017).

Biometric authentication methods, such as fingerprint recognition, voice recognition, facial scanning, and iris identification, offer robust alternatives to traditional PIN codes or passwords, which are susceptible to theft, forgetfulness, or misuse (Jain et al., 2020). These techniques rely on unique biological attributes, making unauthorised access notably more difficult, thus elevating the security standard for digital transactions. However, as promising as this technology may be, widespread adoption largely depends on user acceptance, which can be shaped by various factors, including privacy concerns, trust in technology, and perceived ease of use (Jain et al., 2020). This study explores the factors influencing user acceptance of biometric authentication within the Thulamela Local Municipality, providing insights into tailoring E-payment systems for enhanced security and user satisfaction.

The study is situated in the Thulamela Local Municipality, a region characterised by urban and rural dynamics and a diverse socio-economic landscape. Understanding user acceptance in this unique setting offers valuable insights into the specific challenges and enablers of biometric technology adoption in E-payment systems for local communities. In doing so, the research seeks to inform system designers, policymakers, and stakeholders on the critical factors that affect the successful implementation and acceptance of biometric authentication, ultimately enhancing the security, convenience, and accessibility of E-payment systems.

1.2 Background of the Study

The rapid advancement of technology has fundamentally transformed financial systems, with E-payment solutions taking centre stage as an alternative to cash and card transactions (Khandekar & Bendale, 2023). Digital transactions offer undeniable benefits, including speed, accessibility, and convenience, which are vital in today's fast-paced economy (Hassan & Sabahat, 2024). As reliance on E-payment platforms grows, so does the importance of implementing robust security measures to protect users from data breaches, identity theft, and unauthorised transactions (Islam & Ahmed, 2017). Among the various options available, biometric authentication has gained recognition for its potential to increase security without compromising user convenience (Chubuk, 2024; Kusriantini & Sudarsono, 2017).

Biometric authentication leverages unique physiological and behavioural characteristics to verify identities, reducing the need for memorised passwords or physical tokens, often vulnerable to loss or fraud (Jain et al., 2020). Techniques such as fingerprint scanning, iris scanning, voice recognition, and facial identification are complicated to duplicate, providing a layer of security that traditional methods lack (Khandekar & Bendale, 2023). This approach strengthens security and enhances user experience by simplifying access to E-payment systems, which is especially relevant in regions where digital literacy and accessibility issues may limit traditional authentication methods (Burchett et al., 2024). However, while biometrics offers clear advantages, it also presents concerns regarding privacy and data security, which are central to user acceptance.

Adopting E-payment systems in the Thulamela Local Municipality presents unique challenges and opportunities. The municipality serves a population with diverse economic activities, encompassing urban and rural settings, influencing technology use and access. As digital financial solutions become increasingly integrated into daily life, understanding local perceptions and potential barriers to biometric technology adoption is crucial (Hassan & Sabahat, 2024). According to the South African Reserve Bank (SARB), digital transactions have surged in South Africa, underscoring the need for secure authentication methods that accommodate the broad socio-economic spectrum of users within Thulamela (South African Reserve Bank, 2020). Despite this growth, limited research has examined biometric authentication within this context, leaving a gap in understanding how privacy, technological familiarity, and cultural attitudes influence acceptance.

This study addresses this gap by focusing on the determinants of user acceptance for biometric authentication in E-payment systems. Through a detailed analysis, the study seeks to identify the socio-cultural and technological factors that impact user attitudes toward biometrics. The insights from this research are intended to guide the effective implementation of biometric E-payment systems tailored to the needs and preferences of Thulamela's residents, thereby fostering both security and inclusivity.

1.3 Statement of the Problem

Technologies for biometric authentication have been developed as a quick and secure method of authenticating users of digital access control systems (Hassan & Sabahat, 2024; Morake, Khoza & Bokaba, 2021). Despite the potential benefits of biometric authentication in E-payment systems, localised research must be conducted to evaluate user acceptance of this technology in the Thulamela Local Municipality, as differences in socio-economic, cultural, and technological contexts can significantly impact acceptance (Chigada, 2020; Chubuk, 2024; Malatji, van Eck & Zuva, 2020). While existing studies have explored biometric authentication adoption in developed regions, there is limited research addressing specific socio-economic challenges users face in Thulamela. This study addresses these gaps by examining the factors affecting user acceptance, including privacy concerns, technological trust, and community needs. A better understanding of these factors will allow for the effective implementation of biometric authentication in E-payment systems, tailored to the specific requirements of Thulamela's residents.

1.4 Aim and Objectives

1.4.1 Aim

The primary objective of this study is to develop a framework for user acceptance of biometric authentication in E-payment systems within the Thulamela Local Municipality, based on identifying and analysing the factors that influence user acceptance.

1.4.2 Objectives

- i. To identify the factors influencing user acceptance of biometric authentication in e-payment systems.

- ii. To assess the level of user acceptance and intention to adopt biometric authentication in E-payment systems.
- iii. To evaluate socio-economic and cultural barriers affecting user acceptance of biometric authentication in e-payment systems.
- iv. To propose an acceptance framework based on the identified factors to guide the practical implementation of biometric authentication in e-payment systems in the Thulamela Local Municipality.

1.5 Research Questions

Main research question is: *What factors influence user acceptance of biometric authentication in E-payment systems?*

The sub-research questions are as follows:

- i. What key factors influence user acceptance of biometric authentication in e-payment systems within the target community?
- ii. What is the current level of user acceptance and intention to adopt biometric authentication in E-payment systems within the municipality?
- iii. What socio-economic and cultural barriers affect the acceptance of biometric authentication in E-payment systems in Thulamela?
- iv. How can an acceptance framework be developed from the identified factors to guide the practical implementation of biometric authentication in e-payment systems within the Thulamela Local Municipality?

1.6 Justification

In South Africa, the adoption of e-payment systems has experienced significant growth, mainly in rural and semi-urban areas where biometric technologies are being piloted. Morake, Khoza, and Bokaba (2021) established that biometric authentication in South African rural communities is mainly dependent upon socio-economic and infrastructural readiness, concluding that successful implementation hinges more on robust local infrastructure, easy-to-use local user interfaces, and articulated benefits of biometric solutions. This finding strongly corroborates the current study's focus on facilitating conditions and performance expectancy

within Thulamela Municipality. It reinforces the argument, emphasising the infrastructural element as still paramount within biometric adoption at a local level.

Meanwhile, Chigada (2021) established that in Johannesburg's banking environment, most serious concerns regarding privacy and trust arise at the level of accepting biometric authentication. While this certainly broadly aligns with this research on social impediments and trust issues, Chigada's focus on banking consumers in the urban context contrasts with this study's predominantly rural-to-semi-urban user base. In deepening the researcher's analysis, this urban-rural counterpoint brings forth subtle distinctions in user acceptance across different socio-economic contexts. It allows the research to build a strong case, emphasising that tailor-made awareness programs and trust-building interventions must be prioritised in rural areas such as Thulamela. Additionally, this study engaged with the work from Netshirando, Munyoka, and Kadyamatimba (2024), who investigated digital payment adoption within Limpopo Province. Their results found that economic barriers, especially regarding the affordability and accessibility of digital solutions, significantly impede technology adoption. This research complements and echoes their findings quite clearly, but focuses, rather than on the entire Limpopo Province, specifically on the challenges confronted in Thulamela Local Municipality. Therefore, this study provides a finer resolution complementary to their broad digital payments' perspective by shedding light on specific technology issues and barriers at the municipal level.

This study offers valuable insights into the user acceptance of biometric authentication in E-payment systems within the unique socio-economic and cultural context of the Thulamela Local Municipality. The study examines security concerns, ease of use, and socio-cultural influences on acceptance, providing a foundation for policymakers, E-payment providers, and other relevant stakeholders to make well-informed decisions about implementing and optimising biometric systems tailored to local needs. In an era where digital financial transactions are rising, understanding the local community's concerns and preferences regarding biometric authentication becomes critical.

1.7 Scope and Delimitation of the Study

This study aims to assess the acceptance of biometric authentication in E-payment systems, specifically within the Thulamela Local Municipality. The research will focus on how

businesses, organisations, and individuals within the municipality interact with and perceive biometric authentication in digital payment systems. The study provides valuable insights into the local context of E-payment system adoption by examining key factors such as security concerns, ease of use, and socio-economic influences.

However, the findings of this research are not intended to be broadly generalised to other municipalities or regions. Given Thulamela's unique socio-economic and cultural landscape, the results may not reflect the experiences or attitudes of people in other areas. Additionally, due to time constraints, the study narrows its focus to biometric authentication in E-payment systems, rather than exploring other potential uses of biometric technology, which could exhibit different acceptance patterns. Therefore, while this study provides practical recommendations for stakeholders within Thulamela, it acknowledges that broader applicability will require further research in different contexts.

1.8 Operational Definition of Key Words

Biometric authentication: The process of using unique physiological or behavioural characteristics, such as fingerprints or facial features, to verify the identity of individuals in E-payment systems.

User acceptance: The willingness of users to adopt and use biometric authentication in E-payment systems.

E-payment systems: Electronic payment systems allow individuals to make transactions and payments electronically, including online shopping, bill payments, and mobile payments.

1.9 Outline of the study

The dissertation will be structured as follows:

Chapter 1: The Problem and its setting

This chapter introduces the research topic, including the background, problem statement, aim, objectives, research questions, significance, scope, delimitations, and operational definitions.

Chapter 2: Literature review

This chapter presents a review of relevant literature on biometric authentication, E-payment systems, and user acceptance.

Chapter 3: Research methodology

This chapter describes the research methodology, including the research design, data collection methods, and data analysis techniques.

Chapter 4: Presentation of research findings

This chapter presents the study's findings and discusses the results concerning the research questions.

Chapter 5: Summary, conclusions, and recommendations.

This chapter concludes the study, summarises the key findings, and provides recommendations for future research and practical implications.

1.10 Chapter Summary

This chapter laid the foundation for understanding the user acceptance of biometric authentication in E-payment systems within the Thulamela Local Municipality. The introduction highlighted the growing importance of secure and efficient digital payment methods, and the background outlined the increasing use of biometric authentication as a promising solution to address security concerns in E-payment systems. The statement of the problem identified the need for focused research on user acceptance in this specific context, while the aim and objectives provided a clear direction for this study. The research questions, formulated to explore the factors influencing acceptance, alongside the study's justification, emphasised the potential impact of the findings on policymakers, E-payment providers, and the broader community. By identifying socio-economic and cultural barriers, the research aims to contribute to improving the design and implementation of biometric authentication in Thulamela's E-payment systems, ultimately enhancing security, efficiency, and user satisfaction. Furthermore, the scope and delimitations of the study have been clearly defined, ensuring that the research remains focused on the municipality, acknowledging the limitations in generalisability to other regions. As the study progresses, these insights will guide the exploration of user acceptance factors, leading to the development of a framework that can support the effective implementation and adoption of biometric authentication in E-payment systems.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter presents a detailed review of user acceptance of biometric authentication within E-payment systems, explicitly targeting the Thulamela Local Municipality. This literature review examines relevant literature to build a strong theoretical foundation for the study. It will identify areas lacking current knowledge and offer insights into factors influencing user acceptance within this context. The chapter commences with a background on E-payment systems and the critical role of user acceptance in their successful adoption, supported by previous related studies. Basare, Bhojak and Solanki (2023) found that biometric authentication is developing quickly and offers exceptional benefits for boosting security and ease in various applications, including E-payment systems. The potential for improving the security and efficiency of financial transactions within Thulamela Local Municipality exists by incorporating biometric authentication into e-payment systems. This literature review will look at the status of research on user acceptance of biometric authentication in e-payment systems, identify key elements impacting user acceptability, and provide insights to implement biometric-based e-payment systems in Thulamela successfully.

2.2 Background of the E-payment System

The need for secure, efficient, and inclusive payment systems has become increasingly critical in the contemporary global economy. Electronic Payment Systems (EPS) are rapidly replacing traditional cash-based transactions, offering several advantages, including improved record-keeping, faster processing times, and reduced transaction costs (Ahmed, Mohamed & Zakaria, 2023). These advancements are crucial for fostering financial inclusion, as they enable individuals and businesses, especially in underserved regions, to participate in secure financial transactions, thereby contributing to broader economic development (Netshirando, Munyoka & Kadyamatimba, 2024).

EPS includes a variety of technologies such as mobile wallets, debit and credit cards, and online payment gateways (Zarco et al., 2024). These innovations have significantly transformed how both individuals and enterprises conduct financial exchanges. They provide safer, more efficient, and convenient methods of transacting money, enhancing financial accessibility in both urban and rural contexts (Pahuja & Goel, 2024). However, despite the growing adoption

of EPS globally, the success of these systems is heavily dependent on user acceptance (Hussain, Gupta & Bhardwaj, 2024). This highlights the need to understand factors influencing users' willingness to embrace digital payment systems, which vary significantly across socio-economic and cultural contexts.

Among the key technological advancements in EPS, biometric authentication has emerged as a promising solution for enhancing security. Biometric authentication offers a more secure alternative to traditional password-based systems, reducing the risks of fraud and identity theft by leveraging unique human traits such as fingerprints, voice, facial recognition, or iris scans (Ahmed, Mohamed & Zakaria, 2023; Sriman et al., 2020). While using biometric data in financial transactions presents several advantages, the level of user acceptance remains a significant barrier to its widespread adoption (Yu et al., 2024). Trust, perceived usefulness, and ease of use are crucial in determining how individuals engage with biometric authentication, especially in areas where digital literacy may be low (Yu et al., 2024).

In rural areas like the Thulamela Local Municipality, where digital infrastructure is often limited, understanding the local population's perceptions of biometric authentication becomes even more critical. Rural regions typically face challenges like lower levels of digital literacy, reduced access to banking services, and scepticism towards new technologies, which can hinder the adoption of EPS (Netshirando, Munyoka & Kadyamatimba, 2024). These barriers are compounded by the fact that many rural residents still rely on traditional cash-based methods for daily transactions. Therefore, assessing how users in these areas perceive and adopt biometric authentication is essential for successfully deploying EPS.

2.3 Current State of Biometrics

Implementing biometric authentication in E-payment systems has garnered considerable attention globally. Nevertheless, there is a significant gap in the literature concerning its adoption within specific regions, such as the Thulamela Local Municipality. This municipality, located in a rural area of South Africa, presents unique challenges and opportunities for integrating such technologies, making it a crucial context for further study. While biometric authentication is steadily being adopted in various E-payment systems worldwide, with methods such as fingerprint recognition, facial recognition, iris, and voice recognition becoming increasingly prevalent (Sriman et al., 2020; Yu et al., 2024), there is limited research

addressing its specific implementation and user acceptance within municipalities like in the Thulamela Local Municipality. This lack of context-specific research highlights a significant gap that this study aims to fill by examining the local adoption and perceptions of biometric technologies in E-payment systems.

Integrating biometric authentication into e-payment systems has also been driven by the increasing demand for seamless and contactless payment solutions, particularly during the COVID-19 pandemic. Gomez-Barrero et al. (2021) and Liébana-Cabanillas et al. (2022) highlight that the pandemic accelerated the adoption of biometric technologies as consumers sought safer, touch-free alternatives for financial transactions. Moreover, the growing sophistication of artificial intelligence (AI) and machine learning algorithms (ML) has further enhanced the capabilities of biometric systems, enabling real-time identity verification with minimal errors (Hamme et al., 2024). Despite these advancements, challenges persist, particularly in developing regions. Issues such as the high cost of implementation, limited access to biometric devices, and concerns over data misuse continue to hinder adoption (Liébana-Cabanillas et al., 2022). Additionally, cultural and socio-economic factors significantly shape user acceptance, as highlighted by Mróz-Gorgoń et al. (2022).

Existing literature on biometric authentication in E-payment systems tends to focus on mobile payment applications, with studies by Dijmărescu et al. (2022) investigating user acceptance of fingerprint and facial recognition in mobile payment environments. While informative, this research does not fully address the challenges and perceptions of using biometric methods in broader E-payment contexts. Thomas, Ogalo and Maake (2023) compared various biometric methods' performance in mobile payment systems, providing valuable insights. However, they did not explore user acceptance in non-mobile E-payment platforms, such as online payment gateways or point-of-sale (POS) terminals. Furthermore, Türker, Altay and Okumuş (2022) offered an extensive review of biometric security in mobile payments. However, there is a notable lack of empirical studies examining the adoption of biometric authentication across different user segments, particularly in rural areas where digital literacy may be lower.

Further studies, such as those by Khayer (2024), have investigated user perceptions and attitudes towards biometric authentication in E-commerce. However, these studies primarily focus on online shopping platforms and do not consider the full spectrum of e-payment systems. Similarly, Perea-Khalifi, Irimia-Diéguez and Palos-Sánchez (2024) explored user

perceptions in mobile banking applications. However, the findings do not extend to the broader landscape of digital payment systems, such as peer-to-peer transfers or contactless payment technologies. Basare, Bhojak and Solanki (2023) offered a review of authentication methods used in E-payment systems but did not delve into the real-world implementation challenges, particularly in regions with limited technological infrastructure.

There is also a need to explore this phenomenon within the South African context. In congruence with the arguments by Gertze and Petersen (2024), performance expectancy, perceived security, and social influence remain the key issues affecting the adoption of electronic payments in South Africa. Their study, grounded within the Unified Theory of Acceptance and Use of Technology (UTAUT), affirmed that the behavioural intention of South African consumers toward e-payment technologies is significantly impacted by perceptions related to how much these technologies improve their capabilities of financial management and security experience. The theory correlates very well with the overall technology acceptance conceptual frameworks, reinforcing that perceived security and benefits carry greater weight in the context of South African e-payments. The rural/urban distinction is notable because their research was conducted mainly in urban areas where infrastructural readiness and technological literacy may not be a significant challenge, thus calling for deeper exploration into rural-specific factors.

The second complement is presented by the research by Morake, Khoza, and Bokaba (2021), which deeply examined infrastructures lacking, socio-economic constraints and trust-related issues acting as barriers to biometric authentication adoption in rural South African settings. These studies not only argue that successful biometrics adoption in rural South Africa can only be realised when strong infrastructural systems, user trust frameworks, and socio-economic measures to facilitate adoption are in place and competent in making technologies affordable, but generally agree that socio-economic and infrastructural conditions influence adoption. More emphatic, however, is their lack of infrastructural development relative to other studies dealing with scenarios of urban adoption; thus, infrastructural and socio-economic challenges must be tackled first if biometric acceptance is to improve in rural municipalities.

Equally, Netshirando, Munyoka, and Kadyamatimba (2024) looked into the determinants of digital payment adoption at Limpopo Province in South Africa, with emphasis on economic barriers such as affordability, access to technology, and disparities in digital literacy. The

research strongly emphasises the need to address economic and literacy barriers before digital payment systems can be embraced en masse; this view is supported by several other studies identifying regional barriers in emerging economies. However, their study looks at digital payment technologies in general, without looking at biometric authentication, which leaves some scope for further study of biometric-specific adoption issues within similar regional settings.

Considering broader African viewpoints, recent literature contributes to this debate. For example, Pahuja and Goel (2024) explored biometric technology adoption in the Nigerian financial sector and pointed out severe privacy concerns and usability factors impacting user acceptance. Their findings resonate with African regional concerns, especially regarding privacy and data security from a user perspective. However, based on the Nigerian and South African socio-cultural distinctions, the intensity of these concerns and their precise nature may vary, underscoring the need for country-specific studies that consider each country's unique social and cultural setting. Furthermore, looking at Kenya, Thomas et al. (2023) further reveal social influence and ease of use as key determinants affecting user adoption by studying biometric acceptance in mobile payment systems. The research further supports the generally observable patterns synonymous with African contexts of how social structure and ease of use impact consumer behaviour across the continent. However, different infrastructure maturity levels, economic conditions, and cultural attitudes toward technology between East African and Southern African regions stress the need for context-specific studies that capture local nuances more accurately.

Despite the valuable contributions of these studies, there remains a critical need for further research that examines the adoption of biometric authentication in E-payment systems across diverse cultural contexts and payment environments. By addressing these gaps, particularly in rural and underdeveloped regions like Thulamela, this study aims to provide insights into the unique challenges and opportunities for successfully implementing digitisation in E-payment systems. This will contribute to a more comprehensive understanding of enhancing user acceptance of E-payment solutions, ultimately promoting greater financial inclusion and efficiency (Yu et al., 2024), especially in rural South Africa.

2.4 Use of Biometric Authentication Technologies in E-payment Systems

Biometric authentication technologies have gained significant attention and widespread implementation in E-payment systems. These technologies leverage individuals' unique physiological or behavioural characteristics, such as fingerprints, iris patterns, voice recognition, or facial features, for authentication purposes (Hassan & Sabahat, 2024). In E-payment systems, biometric authentication offers additional security and convenience during financial transactions. Studies have shown the use of various biometric authentication technologies, including fingerprint scanners, facial recognition systems, and voice recognition systems, in different E-payment applications. These technologies enable users to authenticate themselves securely and conveniently, replacing traditional methods like PINs or passwords (Sriman et al., 2024). Biometric authentication provides a more reliable and accurate way to verify the user's identity, reducing the risk of fraudulent activities and identity theft in E-payment systems (Liébana-Cabanillas et al., 2024).

Biometric authentication systems have emerged as significant tools in e-payment and financial services due to their superior security measures and enhanced user convenience (Basare et al., 2023; Morake et al., 2021). To ascertain user identity, these systems leverage distinctive physiological and behavioural characteristics, such as fingerprints, facial recognition, and iris scans (Agrawal, 2021). Integrating biometric sensors into consumer technology, including smartphones, has enabled their extensive adoption for face-to-face and remote financial transactions (Agrawal, 2021). Biometric methods present distinct advantages over conventional authentication techniques, removing users' need to recall passwords and account identifiers (Morake et al., 2021). Furthermore, they offer augmented safeguards against fraudulent activities and identity theft within electronic commerce (Patil, Dudhankar, & Shukla, 2024). Nevertheless, several challenges persist, particularly regarding privacy issues and the likelihood of erroneous positive or negative identifications (Basare et al., 2023). As biometric authentication technology progresses, it will be essential to tackle these challenges and formulate appropriate standards and regulations to ensure its sustained efficacy within the financial sector.

Research indicates that the integration of biometric technologies within financial applications is shaped by variables such as age, educational background, technological literacy, and confidence in device manufacturers (Piotrowska, 2024). The COVID-19 pandemic has

expedited the assimilation of these technologies (Piotrowska, 2024). Techniques for biometric authentication, incorporating fingerprints, iris scans, and facial recognition, are being implemented to lessen digital wallets' security risks and thwart fraudulent schemes (Liébana-Cabanillas., 2022). Investigations into Apple Pay demonstrate that initiatives aimed at protecting information, individual attributes, and trust in security technologies are pivotal determinants influencing user acceptance of biometric-based mobile payment systems (Finken & Heiduk, 2021).

2.5 Benefits of Biometric Authentication Technologies in E-payment Systems

Adopting biometric authentication technologies in E-payment systems offers several significant benefits, positively impacting users, service providers, and the broader payment ecosystem. A key advantage is enhanced security. Biometric traits, unique to individuals, make it extremely difficult for unauthorised users to replicate or bypass the system (Basare, Bhojak & Solanki, 2023). This heightened security reduces risks related to fraudulent transactions, unauthorised access, and identity theft, bolsters users' confidence in the security of their financial transactions (Perea-Khalifi et al., 2024). The reliability of biometric authentication is central to providing a secure digital environment, as it ensures a higher accuracy level than traditional methods like PINs or passwords (Türker et al., 2022).

In addition to security, biometric authentication offers convenience and speed, which are critical to enhancing user experience in E-payment systems. Users can authenticate themselves swiftly using their biometric traits, eliminating the need to remember complex passwords or PINs (Kesharwani et al., 2020; Khayer, 2024). This seamless process reduces transaction times, improving operational efficiency for service providers and creating a smoother experience for consumers (Nair & Kannan, 2023). Furthermore, the speed and ease with which users can complete transactions have positively impacted user satisfaction and retention rates in digital payment systems (Venkatesh et al., 2012).

Another notable benefit of biometric authentication is its user-friendly interaction. The simplicity of authentication, which requires just the presentation of biometric traits, is more intuitive than traditional methods that often require physical tokens or memorisation of intricate credentials (Pahuja & Goel, 2024; Nair & Kannan, 2023). This ease of use has been linked to improved user satisfaction and greater acceptance of biometric technologies in E-payment

systems, as it removes barriers to access and provides a more streamlined experience (Khayer, 2024). As digital payments become more ubiquitous, ease of use will continue to be a critical factor in determining user engagement and adoption rates (Thomas et al., 2023)

Improved accuracy and reliability are also key advantages of biometric authentication. The uniqueness of biometric traits, such as fingerprints, facial features, or voice patterns, ensures more precise identification, reducing the likelihood of errors such as false positives or false negatives (Pahuja & Goel, 2024). This reliability improves the overall dependability of E-payment systems, leading to fewer authentication errors and a smoother transaction experience (Türker et al., 2022). Additionally, accurate biometric systems have enhanced trust in digital transactions, which is critical for the continued adoption of E-payment solutions (Perea-Khalifi et al., 2024).

2.6 Factors Influencing User Acceptance of Biometric Authentication

Since biometric authentication systems offer convenient and secure user verification, they are widely used in many applications, including e-payment systems. Users' acceptance of biometric authentication technology depends on several variables. One important factor is the perceived level of biometric authentication security, as Das (2024) proposed. Their perception of its security significantly influences users' decisions to accept or reject biometric technology. Khandekar and Bendale (2023) suggested that users' faith in the system is increased when they think biometric data, like fingerprints or iris scans, is very secure and hard to copy or steal. Therefore, establishing user confidence in the technology and promoting its integration into e-payment systems depends on guaranteeing the security and integrity of biometric data.

Another important consideration is the perceived ease of use of biometric authentication technologies (Patrick et al., 2022). The degree to which users find the technology appealing and engaging directly affects how popular it is with them. Positive user experience is enhanced by simple interfaces, unambiguous instructions, and minimal effort needed for biometric data authentication (Nakisa et al., 2023). Convenience and ease of use can significantly impact customers' willingness to accept and routinely use the biometric authentication method for e-payment transactions. Perceived security and convenience are two important criteria that affect users' acceptance of biometric authentication in E-payment systems (Patrick et al., 2022). Organisations may encourage the widespread adoption of biometric technology and improve

the user experience in electronic payment transactions by addressing these issues and guaranteeing that biometric systems are dependable, safe, and easy to use. Since biometric authentication systems offer convenient and secure user verification, they are widely used in many applications, including e-payment systems. According to Nair and Kannan (2023), the criteria below affect users' acceptance of biometric authentication.

Zarco et al. (2024) posited that one crucial element is how secure biometric authentication is believed to be. How secure users perceive biometric technology to be significantly impacts whether they adopt it. When users believe biometric data, such as fingerprints or iris scans, is very safe and difficult to copy or steal, their trust in the system is bolstered. Thus, ensuring the security and integrity of biometric data is essential to building user trust in the technology and encouraging its adoption into e-payment systems (Patrick et al., 2022). Perceived simplicity of use significantly influences users' acceptance of biometric authentication systems. Users' level of attraction and engagement with technology has a direct impact on its level of popularity. User-friendly interfaces, clear instructions, and low effort required for biometric data authentication all contribute to positive user experiences (Khandekar & Bendale, 2023). Customers' propensity to accept and regularly utilise the biometric authentication method for e-payment transactions can be significantly influenced by convenience. Their perceptions of it largely determine customers' acceptance of biometric authentication. A positive user experience boosts user contentment and raises the likelihood that individuals will use the technology (Nakisa et al., 2023). Positive user experiences include smooth interactions, quick authentication, and little disruption.

According to Das (2024), users' privacy concerns significantly influence whether they consent to biometric authentication in E-payment systems. Consumers are worried about how the use, storage, and accessibility of their biometric data may affect their privacy. Transparent policies about informed consent, data protection, and safe storage must meet consumers' privacy concerns. E-payment systems can boost user acceptance and confidence in biometric identification technology by honouring users' privacy preferences and giving them clear information about how their biometric data is handled. Khandekar and Bendale (2023) suggest that faith in the biometric authentication system and technology in general is a significant factor influencing consumer acceptability. Users must feel confident that the system will securely and reliably verify their identity, free from mistakes or unwanted access. Enhancing users' trust in technology through transparent communication, uniform performance, and strict compliance

with data protection laws is imperative. Building trust can ease fears and reduce opposition to e-payment systems based on biometric authentication. Biometric authentication adoption and usage in E-payment systems can be increased by improving the user experience through clear interface design, fast feedback, and efficient system operations (Nair & Kannan, 2023).

2.7 Challenges and Considerations in the Adoption of Biometric Authentication for E-Payment Systems

Adopting biometric authentication technologies in E-payment systems promises enhanced security and user convenience, yet also introduces privacy, security, technological limitations, interoperability, and cost challenges. Addressing these challenges is essential to ensure user confidence, successful integration, and the widespread acceptance of biometric authentication across diverse platforms.

Data privacy and security are among the foremost concerns surrounding biometric authentication in E-payment systems. Since biometric data, such as fingerprints or facial recognition profiles, is uniquely personal, its storage and management necessitate robust protections against unauthorised access and misuse (Perea-Khalifi et al., 2024). The inability to change biometric data, unlike passwords or PINs, makes it especially vulnerable to theft, creating the potential for irrevocable identity risks if compromised (Chen et al., 2018). Therefore, users may be apprehensive about sharing this data, requiring transparent communication from providers about data handling practices and strict adherence to privacy regulations to mitigate concerns (Das, 2024). To address privacy concerns, e-payment providers must implement robust security protocols, including encryption and secure storage practices, alongside multi-factor authentication and continuous system vulnerability assessments. Such measures help ensure the security of biometric data and boost user trust in the integrity of these systems (Basare, Bhojak & Solanki, 2023; Zarco et al., 2024). Furthermore, aligning with privacy regulations and ensuring transparency in data processing can also promote user acceptance, as individuals gain greater assurance that their biometric data is being responsibly managed (Venkatesh et al., 2012).

The technological limitations of biometric systems present another barrier to their effective deployment. Biometric systems rely on sensor accuracy and environmental conditions, which can affect their reliability (Zarco et al., 2024). Issues such as false rejections or acceptances

can arise, especially when sensor quality is compromised by lighting conditions or environmental factors, potentially leading to user frustration and diminished trust (Chen et al., 2018). These technical limitations also impact the overall user experience, as a single false rejection could hinder a seamless transaction, detracting from the perceived value of the technology (Khayer, 2024). Ensuring that biometric systems operate effectively across varied environments and user demographics requires high-quality, adaptable sensors and algorithms. Continuous improvements in sensor technology, together with algorithms that can account for environmental variability, are essential to minimising these technical issues and enhancing system reliability (Khandekar & Bendale, 2023).

Integration and interoperability are key to successfully adopting biometric authentication systems in E-payments. Compatibility issues can arise when integrating biometric technologies with existing E-payment platforms, often due to the lack of standardised protocols and frameworks across platforms (Nair & Kannan, 2023). For biometric authentication to be widely accepted, seamless interoperability among various devices and platforms is critical. Addressing this issue involves industry consortia and standards organisations establishing unified guidelines for smooth data exchange and system compatibility. To inculcate a broader acceptance, E-payment providers should prioritise solutions that facilitate interoperability, enhancing user experience, simplifying system integration, and supporting the standardisation of biometric authentication across E-payment applications (Venkatesh et al., 2012). Ultimately, tackling interoperability issues can create a cohesive ecosystem that benefits users through consistent experiences across different systems (Khandekar & Bendale, 2023).

Implementing biometric authentication technologies' costs and infrastructure requirements also influence their adoption. Initial expenses include acquiring biometric sensors, infrastructure upgrades, and system integration efforts, all of which may be prohibitive for smaller businesses (Hassan & Sabahat, 2024). Additionally, the ongoing costs related to maintenance and support need to be considered, as these systems require regular updates to remain secure and functional. To mitigate these financial constraints, especially for smaller organisations, E-payment providers might explore phased implementations or collaboration with vendors offering scalable solutions (Nair & Kannan, 2023). Government incentives or industry subsidies could also encourage more businesses to adopt biometric technology, helping to defray costs while enabling a broader, more equitable implementation across diverse sectors.

2.8 Theories Guiding the Study

This section discusses various theoretical perspectives and models of technology acceptance and user behaviour. The Technology Acceptance Model (TAM) (Davis, 1989) and its extensions, such as the UTAUT (Venkatesh et al., 2003), are examined to provide a framework for understanding user acceptance of biometric authentication. Additionally, other relevant theories and concepts from psychology, human-computer interaction, and information systems are explored to provide a comprehensive theoretical framework for the study (Bhattacharjee, 2001; Rogers, 2003).

2.8.1 Technology Acceptance Model

The Technology Acceptance Model (TAM) proposed by Davis in 1989 is widely recognised as a theoretical framework for understanding users' acceptance and adoption of technology (Davis, 1989). TAM emphasises two key factors influencing users' behavioural intentions to use technology: perceived usefulness and ease of use. Perceived usefulness refers to users' belief in the technology's ability to enhance their performance and productivity, while perceived ease of use reflects users' perception of the technology's simplicity and effortlessness (Davis, 1989). In the context of biometric authentication in e-payment systems, users' perceptions of the usefulness and ease of use of biometric authentication methods play a crucial role in their acceptance of the technology. The perceived usefulness of biometric authentication lies in its potential to improve the security and convenience of e-payment transactions (Davis, 1989). Meanwhile, the perceived ease of use pertains to users' perceptions of the simplicity and convenience of utilising their biometric traits, such as fingerprint or facial recognition, for authentication purposes.

The TAM model has been extensively applied to comprehend user acceptance of various technologies, including e-commerce and artificial intelligence. TAM indicates that Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) are fundamental influences on user attitudes and intentions related to adopting technology (Dhingra & Mudgal, 2019; Malatji et al., 2020). Multiple studies have leveraged TAM to investigate the adoption of e-commerce, with scholars frequently adapting the model by incorporating or omitting variables to augment its efficacy (Nyoro et al., 2015; Malatji et al., 2020). Recently, research has broadened the application of TAM to explore AI acceptance within e-commerce, revealing that subjective norms positively influence both PU and PEOU. In contrast, trust impacts PEOU (Wang et al.,

2023). Notwithstanding its extensive application, TAM has limitations, including challenges in quantifying behaviour and its inadequacy in addressing factors such as cost and structural constraints (Malatji et al., 2020).

According to TAM, users' attitudes towards the technology, which are influenced by perceived usefulness and perceived ease of use, directly impact their intentions to use it. Moreover, TAM recognises the significance of external variables, such as subjective norms and facilitating conditions, in shaping users' acceptance and adoption of technology (Davis, 1989). Applying the TAM framework to the study on user acceptance of biometric authentication in e-payment systems in the Thulamela Local Municipality enables researchers to examine users' perceptions of usefulness and ease of use and consider the influence of subjective norms and facilitating conditions. This investigation can provide valuable insights into the factors that drive or impede the acceptance and adoption of biometric authentication in e-payment systems.

2.8.2 Unified Theory of Acceptance and Use of Technology

The Unified Theory of Acceptance and Use of Technology (UTAUT), developed by Venkatesh et al. (2003), integrates various existing models, including the Technology Acceptance Model (TAM), to explain and predict users' acceptance and usage of technology (Venkatesh et al., 2003). UTAUT incorporates four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. Performance expectancy refers to users' belief in the technology's ability to enhance performance and productivity. In the context of biometric authentication in e-payment systems, users' perception of how biometric authentication improves security and efficiency would influence acceptance (Venkatesh et al., 2003). Effort expectancy relates to users' perceptions of the ease of use and effort required to adopt and use the technology. Users' perception of the simplicity and convenience of using biometric traits for authentication impacts acceptance (Venkatesh et al., 2003).

The UTAUT framework has been widely employed in numerous academic studies to examine user behaviours linked to the acceptance of emerging technologies. Tomić et al. (2023) employed an augmented UTAUT framework to scrutinise the adoption of electronic payment systems within Serbia, revealing that performance expectancy, perceived security, trust, and social influence substantially affected behavioural intention. Ayaz and Yanartaş (2020) used UTAUT to examine the acceptance of Electronic Document Management Systems, uncovering that performance expectancy and social influence positively influenced usage intention.

Furthermore, Andrews et al. (2021) investigated how librarians view the adoption of AI technologies by employing the UTAUT framework, highlighting that performance expectations and attitudes regarding usage notably influenced their intentions.

Social influence encompasses subjective norms, the perceived social pressures from significant others to adopt and use the technology. Exploring the influence of social norms within the Thulamela Local Municipality on the acceptance of biometric authentication in e-payment systems is relevant (Venkatesh et al., 2003). Facilitating conditions involve the availability of resources and support for technology use, such as technical infrastructure and training. Assessing the facilitating conditions specific to the Thulamela Local Municipality, such as the accessibility of biometric authentication devices and technical support, is important (Venkatesh et al., 2003). Applying the UTAUT framework to the study on user acceptance of biometric authentication in e-payment systems in the Thulamela Local Municipality allows for investigation into the influence of these four constructs on user intentions and behaviours. Understanding users' perceptions of performance expectancy, effort expectancy, social influence, and facilitating conditions provides insights into the factors contributing to or hindering the acceptance and adoption of biometric authentication in the local context.

2.9 Theoretical Framework

In numerous instances, it has been demonstrated that the TAM is a valid and reliable predictor of user acceptability (Marikyan & Papagiannidis, 2023). According to Dwivedi et al. (2019), it has been criticised for its overly simplistic interpretation of user behaviour. Scholars have established more thorough user acceptance models in recent years, especially the UTAUT (Das, 2021; Ayaz & Yanartaş, 2020; Siswanto et al., 2018; Williams et al., 2015). In the UTAUT model, the TAM is merged with other elements that are known to affect user acceptance, such as social influence, enabling conditions, and expectations of performance and effort (Dwivedi et al., 2019; Marikyan & Papagiannidis, 2023). In several investigations (Ayaz & Yanartaş, 2020; Batucan et al., 2022; Donmez-Turan, 2020; Dwivedi et al., 2019; Lin, 2019; Tomić et al., 2023; Troy et al., 2013; Williams et al., 2015), it has been found that the UTAUT is a more reliable predictor of user acceptability than the TAM.

Therefore, this study uses the TAM and UTAUT to create a comprehensive framework to understand user acceptance of biometric authentication in e-payment systems. TAM

emphasises perceived usefulness and ease of use from an elementary perspective. UTAUT enhances knowledge by including social and facilitating factors, relevant to Thulamela Local Municipality, where societal norms and resources impact user acceptability. The study combines models to assess the user acceptability of biometric authentication in e-payment systems, considering both individual and contextual factors. Figure 2.1 depicts the conceptual framework, underpinned by the TAM and UTAUT theoretical frameworks.

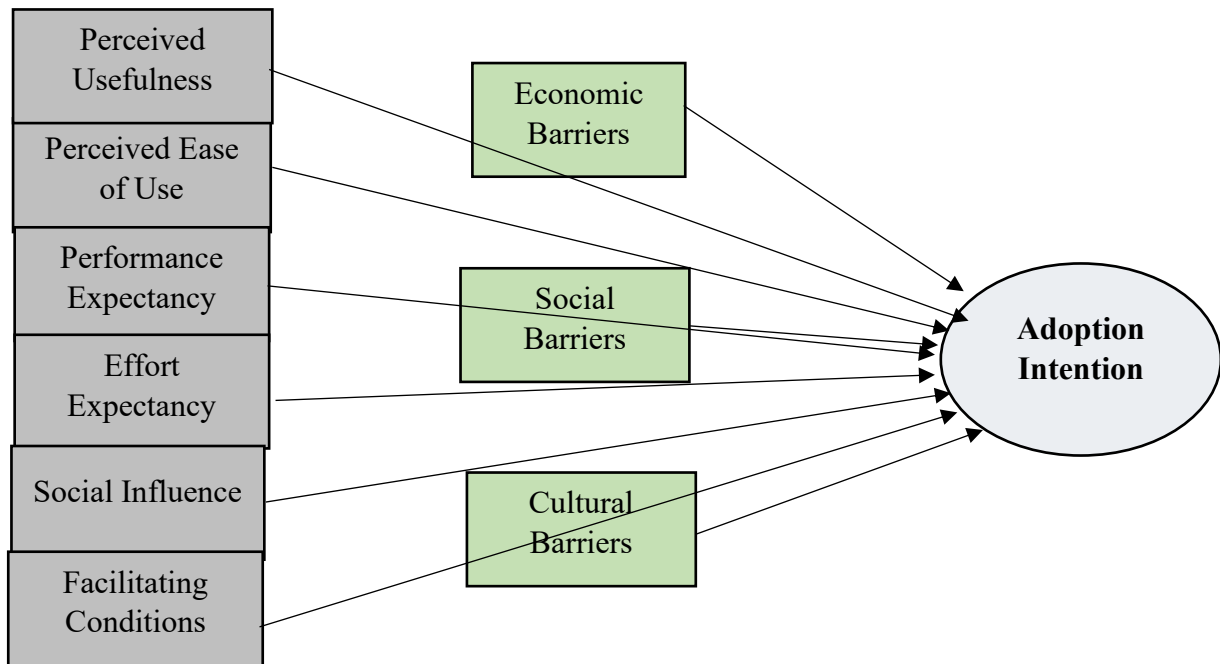


Figure 2.1: The conceptual framework.

These are described concerning the user acceptance of biometric authentication of the E-payment system for a municipality, as follows:

A - Core Constructs from TAM

- *Perceived Usefulness (PU)* - The degree to which a user believes biometric authentication will enhance their performance in e-payment systems (Davis, 1989).
- *Perceived Ease of Use (PEOU)* - The degree to which a user believes using biometric authentication will be free of effort (Davis, 1989).

B - Core Constructs from UTAUT

- *Performance Expectancy (PE)* - How much a user anticipates that employing technology will assist them in achieving their objectives (Xue et al., 2024;

Tomić et al., 2023). Users are more likely to embrace biometric authentication if they think it will enable them to accomplish their objectives, such as making payments more convenient or secure.

- *Effort expectancy (EE)* - the degree to which a person anticipates finding and utilising technology to be simple (Donmez-Turan, 2020; Lin, 2019). Users are more likely to embrace biometric authentication if they think it would be simple to understand and apply.
- *Social influence (SI)* - How much a user trusts that other people of influence will support their decision to use a technology (Xue et al., 2024; Donmez-Turan, 2020; Troy et al., 2013). If users perceive that other people of significance believe they should adopt biometric authentication, they are more inclined to accept it. For instance, consumers may be more likely to use biometric authentication if their friends and relatives are already doing so.
- *Facilitating conditions (FC)* - the degree to which users think they have the tools and assistance they need to use technology (Batucan et al., 2022; Lin, 2019). If users have the tools and assistance they need to use biometric authentication, they are more likely to adopt it.

C - Moderating Variables from UTAUT

- *Economic Barriers (EB)* - refer to financial constraints that hinder the adoption of biometric authentication systems, particularly in developing regions (Khando, Islam & Gao, 2022). These barriers include the high cost of biometric devices, implementation expenses, and limited access to affordable technology, disproportionately affecting low-income populations (Liébana-Cabanillas et al., 2023). Addressing these economic challenges is critical to ensuring equitable access to secure e-payment systems.
- *Social Barriers (SB)* - encompass societal attitudes, trust issues, and resistance to new technologies that impede the adoption of biometric authentication (Nakisa et al., 2023). For instance, a lack of trust in data privacy and concerns about misuse of personal information can discourage users from embracing biometric systems (Boo & Chua, 2023). These barriers are often rooted in misinformation or limited awareness of the benefits of biometric technology.
- *Cultural Barriers (CB)* - refer to the influence of local beliefs, traditions, and values on the acceptance of biometric authentication systems (Nittas et al., 2024). In some

communities, cultural norms may conflict with using biometric technologies, such as concerns over religious implications or discomfort with physical contact during biometric enrolment (Piotrowska, 2024). Understanding and addressing these cultural sensitivities is essential for successful implementation.

D - Actual Use Behaviour (Adoption Intention)

The core constructs, behavioural intention, and moderating variables influence the actual adoption and use of biometric authentication. According to the fundamental principles of the TAM and UTAUT model, these six variables directly influence a user's behavioural intention to use a technology, directly influencing actual technology use, in this case, user acceptance of biometric authentication of the e-payment system.

The framework can pinpoint the elements most likely to affect user acceptance and create IT acceptance improvement interventions. The UTAUT model has the following advantages (Marikyan & Papagiannidis, 2023; Williams et al., 2015):

- It is a comprehensive model that considers various factors that influence user acceptance.
- It has been demonstrated to be a reliable and valid predictor of user acceptance in various scenarios. It can easily be adopted to predict the user acceptance of biometric authentication of e-payment systems.
- It is a complete model that considers various aspects that influence user acceptance. It has been utilised in many studies, making it a well-established model. This makes its adoption easy, ascertaining the user's acceptance of biometric authentication of the e-payment system.

The conceptual framework demonstrates how it is assumed that the independent variables (*Perceived Usefulness -PU, Perceived Ease of Use -PEOU, Performance Expectancy - PE, Effort expectancy - EE, Social influence - SI, Facilitating conditions - FC*) and the moderating variables (*Economic barriers - EB, Social barriers - SB, Cultural barriers - CB*) influence the dependent variable (*Adoption Intention - AI*).

2.10 Chapter Summary

This chapter highlights the inconsistencies and gaps in the body of research in the context of the Thulamela Local Municipality and provides the groundwork for the study's upcoming chapters. The literature review provides a theoretical framework for understanding user acceptance of biometric authentication in E-Payment systems in the specific context of the Thulamela Local Municipality. It also forms the basis for the research methodology and analysis in the upcoming chapters. The chapter created a strong theoretical framework for comprehending user acceptance of biometric authentication in E-payment systems within the context of the Thulamela Local Municipality by critically synthesising the body of previous material. The review found key elements affecting user acceptability, including perceived security, usability, privacy concerns, and confidence in the technology and issuing organisations. Nonetheless, the present knowledge base's shortcomings and contradictions have also been made clear by this critical study. Research on user acceptance in underdeveloped economies and rural towns such as Thulamela has been notably scarce.

Furthermore, the specific socioeconomic demographics and cultural norms that may affect user impressions in such circumstances are frequently overlooked in existing studies. These gaps emphasise how important the current study is. This study attempts to provide important insights into user acceptance of biometric authentication in E-payment systems within a demographic that has not been extensively studied before by concentrating on the Thulamela Local Municipality.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

The preceding chapter reviewed literature related to the study, including the theories underpinning the study. This chapter articulates the adopted philosophical perspective and elucidates the research methodology with corresponding arguments. The chapter examines the research philosophy, approach, design, target population and sampling techniques. The cross-sectional survey design constitutes the foundation of the chosen research methodology for the study. Furthermore, the techniques for data collection, instrument design, and data analysis were covered comprehensively. The ethical considerations used for the data collection process will be explained. This study will be underpinned by the research onion founded by Saunders, Lewis and Thornhill (2019). Figure 3.1 illustrates the research onion framework.

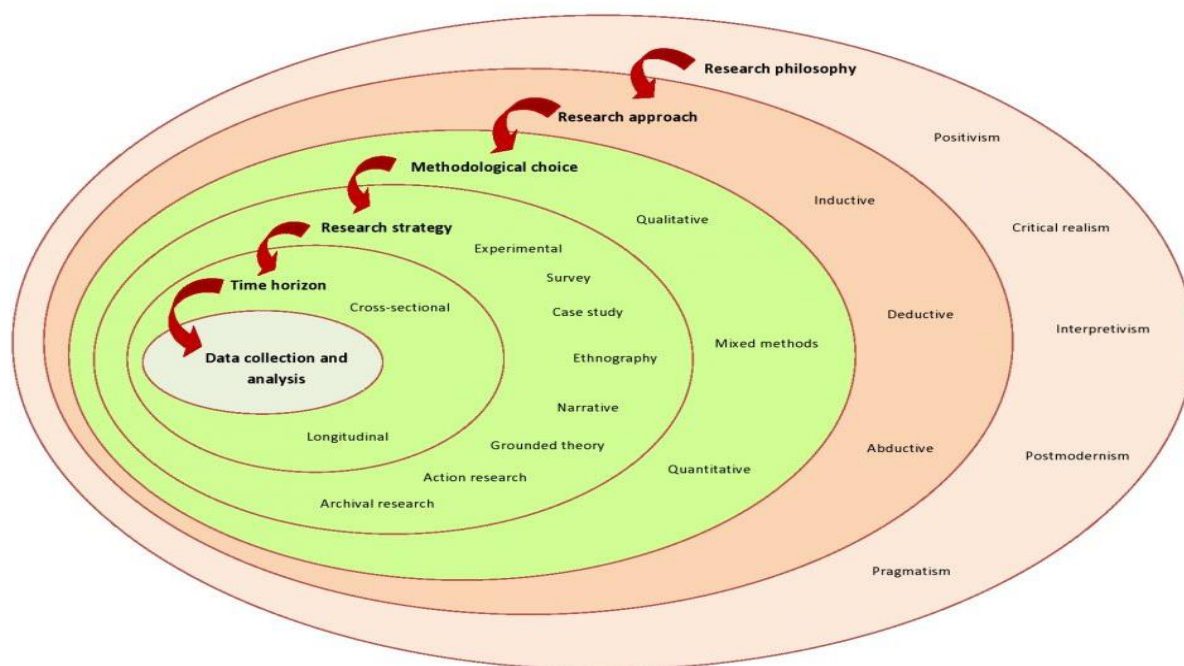


Figure 3.1: The Research Onion

Source: Saunders, Lewis and Thornhill (2019)

3.2 Research Philosophy/ Paradigm

A research paradigm, or philosophy, reflects a researcher's overarching worldview or theoretical perspective, which guides the methodology used to examine the topic (Sekaran & Bougie, 2019). Key paradigms frequently used in research include positivism, interpretivism, and pragmatism (Saunders et al., 2019). The positivist paradigm is based on the idea that clear,

measurable cause-effect relationships exist among variables, allowing researchers to confidently predict outcomes once these relationships are understood (Neuman, 2014). In contrast, interpretivism emphasizes understanding the deeper meanings and experiences of participants, relying heavily on qualitative methods, and often involving extended interaction with participants through methods like case studies, surveys, and observational studies (Cohen, Manion & Morrison, 2018; Saunders et al., 2019). On the other hand, pragmatism incorporates elements of both positivism and interpretivism, creating a flexible framework that combines quantitative and qualitative data collection to address complex research questions (Walliman, 2014).

This study adopted the positivist paradigm, which emphasizes an objective approach rooted in quantifiable evidence and structured methodologies for gathering and analysing data (Saunders et al., 2019). In applying this paradigm, the research aims to measure and analyse user acceptance of biometric authentication in E-Payment systems within the Thulamela Local Municipality. Specifically, the focus is on assessing factors like perceived security, ease of use, and user trust. The positivist approach supports the collection of numerical data, which can then be statistically analysed to gain insights into both the level of acceptance and the influencing factors. This approach aligns with the study's objective to offer an evidence-based understanding of the trends and determinants affecting biometric authentication adoption (Hair et al., 2019).

3.3 Research Approach and Methodological Choice

3.3.1 Research Approach

Melnikovas (2018) identifies three primary research approaches: deductive, inductive, and abductive. A deductive approach, often aligned with quantitative methods, entails deriving specific conclusions from general, established theories or facts, allowing researchers to confirm or test existing hypotheses (Osuagwu, 2020). By contrast, an inductive approach is characteristic of qualitative research and involves developing new theories based on specific observations or patterns in the data. It is grounded in exploring the nuances of individual cases and gradually building broader theoretical frameworks (Sekaran & Bougie, 2019). Meanwhile, the abductive approach combines both deductive and inductive reasoning, providing flexibility by allowing the researcher to begin with observations and then move towards iteratively testing

broader hypotheses. This integrated approach is particularly beneficial in mixed-methods studies where quantitative and qualitative insights are required (Cohen et al., 2018).

The deductive approach is appropriate for this study as it enables the examination of established theories like TAM and UTAUT in the context of biometric authentication in e-payment systems. Employing a deductive methodology allows for a structured evaluation of whether hypotheses from these theories are valid among users in the Thulamela Local Municipality, thereby promoting organised research into user acceptance. This approach lays out a consistent structure for the collection and assessment of data, rendering it appropriate for quantitatively exploring the relationships among variables. Additionally, the deductive approach facilitates the objective testing of predetermined hypotheses, which is crucial for deriving generalisable insights that can guide policy and practical applications in digital payment systems.

3.3.2 Methodological Choice

Research is either quantitative, qualitative, or mixed (Cohen et al., 2018; Saunders et al., 2019). Quantitative research is defined by its structured approach to data collection and analysis, typically involving numerical data that allows researchers to identify patterns, relationships, and correlations (Babbie, 2020). This method relies on tools such as surveys, experiments, and observations from large sample groups and employs statistical software to analyse and interpret results. Quantitative research is particularly effective in hypothesis testing and is commonly used for generalising findings to a broader population (Babbie & Mouton, 2019). For instance, in examining the link between income levels and purchasing patterns, quantitative research can reveal precise, measurable impacts of income on consumer behaviour (Chubuk, 2024). This approach is optimal for studies aiming to quantify phenomena, identify prevalence, and draw statistically significant insights (Johnson et al., 2019).

In contrast, qualitative research is focused on exploring the subjective meanings and contexts behind a phenomenon (Cohen et al., 2018). It involves collecting non-numerical data, such as text or visual content, through interviews, focus groups, and content analysis (Creswell & Creswell, 2018). Analytical methods such as thematic analysis aid in identifying patterns and themes, offering a deeper understanding of human behaviour and experiences. Qualitative research is valuable for studying complex social issues whereas quantitative data may lack the depth needed for insight. For example, qualitative methods may be ideal for studying consumer loyalty, as they uncover the emotional connections and narratives that drive brand loyalty

(Brown & Jones, 2018). This approach is suited for researchers interested in capturing rich, detailed perspectives and generating theories based on in-depth contextual insights (Burchett et al., 2024).

The mixed-methods approach combines quantitative and qualitative research to provide a comprehensive view of a research issue. By integrating data from both approaches, researchers can address multiple aspects of a research question, providing a holistic understanding. For instance, a mixed-methods study investigating the impact of a training program on employee performance might combine quantitative survey data with qualitative interview insights to provide a fuller picture of both measurable performance changes and employees' personal experiences (Creswell & Creswell, 2018). This approach is ideal for exploring complex research questions that require both quantitative and qualitative evidence, as it allows for validation through multiple perspectives (Teddlie & Tashakkori, 2015).

For this study, a quantitative research approach was chosen due to its suitability for examining user acceptance of biometric authentication in E-Payment systems. Quantitative research enables the systematic collection and analysis of numerical data, allowing for the identification of patterns and relationships (Creswell & Creswell, 2018). In this study, surveys were administered to users in the Thulamela Local Municipality to gather data on factors influencing their acceptance of biometric systems. This approach facilitates statistical analysis, enabling an objective assessment of acceptance levels and key factors impacting user perceptions and preferences (Sekaran & Bougie, 2016).

This quantitative approach is appropriate for addressing the study's objectives, as it provides a structured framework to measure acceptance levels and identify statistically significant factors in user acceptance of biometric authentication systems. Through quantifying the insights, this approach allows for a robust analysis that can inform future decisions regarding the adoption of biometric technologies.

3.4 Research Strategy

A research strategy provides an overarching approach guiding how data will be systematically collected, analysed, and interpreted to address the research objectives (Creswell & Creswell, 2018). Various research strategies are available, each suited to different types of inquiry,

including experimental, case study, survey, action research, ethnography, and narrative research strategies (Saunders et al., 2019). For instance, experimental strategies involve manipulating variables to observe outcomes, which helps establish causation (Cohen et al., 2018). Case studies explore phenomena in-depth within real-life contexts, while longitudinal strategies track changes over time by repeatedly observing the same sample at various intervals (Babbie, 2020).

A survey strategy was chosen for this study. Surveys are commonly employed to gather data from a broad population in a structured and consistent manner, enabling comprehensive data collection from participants (Babbie & Mouton, 2019). This strategy is especially effective for quantitative data collection, as it relies on standardised questions that ensure consistency and comparability across responses (Fowler, 2014; Groves et al., 2016). Surveys can be administered through various formats, including online questionnaires, phone interviews, or face-to-face interactions, which enhances their flexibility and accessibility, making them well-suited for diverse populations (Groves et al., 2016).

In this study, a survey questionnaire was developed to capture data on user acceptance of biometric authentication within E-Payment systems among residents of Thulamela Local Municipality. The study aims to gather meaningful insights into factors like perceived security, ease of use, and trust levels associated with biometric systems in E-Payment applications by surveying a representative sample. The quantitative data gathered through this survey strategy enables statistical analysis, which supports the identification of prevalent trends and patterns within the data. This structured approach aligns well with the study's objectives by promoting consistency in responses and allowing findings to be generalized across the wider population (Sekaran & Bougie, 2019).

The decision to use a survey strategy for this research is justified by its effectiveness in reaching a broad audience while providing quantifiable data. This approach enabled the study to gather robust, objective information on user acceptance, producing evidence-based insights into the factors that may impact the adoption of biometric authentication in digital payment systems within the specified locality (Fowler, 2014).

3.5 Time Horizon

The time horizon in research defines the duration within which data collection takes place, often categorised as either cross-sectional or longitudinal (Saunders et al., 2019). A cross-sectional approach collects data at a single time, capturing a "snapshot" of current perceptions or behaviours within a population, which is particularly useful for assessing present attitudes or examining immediate relationships between variables (Bryman, 2016). Conversely, a longitudinal study collects data over an extended period, allowing researchers to observe changes and trends within the same population. This makes it advantageous for studying long-term effects and shifts in behaviour or opinions (Creswell & Creswell, 2018).

Given this study's aim of analysing user acceptance of biometric authentication in E-payment systems, a cross-sectional time horizon is most appropriate. By collecting data at a single point, the study effectively captures current attitudes and acceptance levels towards biometric technology within the Thulamela Local Municipality. This choice is justified by the study's focus on obtaining insights into present-day user acceptance rather than tracking changes over time, making cross-sectional data ideal for achieving these objectives (Babbie, 2021).

3.6 Population and Sampling

3.6.1 Target Population

The target population for this study comprises adult users of e-payment systems in Thulamela Local Municipality, aged 18 years and above, who have access to biometric authentication technologies. This group is relevant because the study aims to evaluate the acceptance of biometric authentication in e-payment systems, which requires participants to have experience or potential exposure to such systems. Thulamela Local Municipality has a total population of approximately 142,527 households, as reported by recent municipal data (Municipalities of South Africa, 2024; Thulamela Municipality, 2022). Statistics reveal that children under 18 in South Africa constitute around 34% (Hall, 2022; 2024). Based on this argument, 94,068 are considered part of the target population. The instrument to be designed in section 3.7 will have a biographical section that also caters for the age and employment status of the participants.

Conversely, the study's exclusion criteria were applied to minors under 18 and individuals who lack access to or familiarity with E-payment systems. For practical implementation, the survey questionnaire and a consent form will be distributed to all households listed within the

municipality's database. The consent form confirmed whether each participant has the potential to use E-payment systems and is eligible for biometric authentication options, such as fingerprint or facial recognition. This step aims to align respondents with the study's focus on digital payment adoption and biometric readiness.

3.6.2 Sampling Technique

This study employed simple random sampling. Simple random sampling is chosen to ensure that each household within Thulamela Local Municipality has an equal probability of selection, thereby minimising selection bias and increasing the potential to generalise the findings (Hair et al., 2019).

3.6.3 Sample Size

The sample size refers to the subset of the population chosen to represent the larger group, impacting research findings' reliability, validity, and generalisability (Saunders et al., 2019). An optimal sample size is essential to ensuring the robustness of the study's conclusions. Several factors are considered in determining the sample size, including the confidence level, the anticipated effect size, and potential attrition among respondents (Hair Jr. et al., 2019). For this study, Slovin's formula is used, a commonly applied formula in survey research, which provides a statistically appropriate sample size given a specific margin of error. The formula is as follows:

$$n = N / (1 + Ne^2)$$

Where:

- n is the sample size,
- N is the population size,
- e is the margin of error, typically set at 5% for this study.

Using the population size of 94,068 households who are over 18:

$$\text{Therefore, } 94068 / (1 + 94068 * 0.05 * 0.05) = 398.306 \approx 399$$

Thus, a sample size of 399 respondents was derived, and the respondents were selected from adults (aged 18 and above) within the municipality. This sample encompassed age groups: 18–

24; 25 – 34); 35 – 44; 45 – 54; and 55 and above, to ensure that the survey captures perspectives from all significant age groups. Such comprehensive sampling enhanced the study's capacity to identify meaningful trends and variances across different age cohorts, providing a robust foundation for analysing user acceptance of biometric authentication in E-payment systems within this community.

Whereas Slovin's formula legitimised 399 respondents from 94,068 adults, only 242 respondents completed the survey. Post hoc power analysis was run, and it turned out that the retained sample still reached the minimal level to detect medium effect sizes with a 95% confidence interval (Cohen, 2023). Therefore, while sample reduction somewhat compromises power, the data is still adequate for valid regression modelling and inferential analyses. The reduction in sample size was mitigated by ensuring that respondents' demographics (age, gender, education, and employment status) reflected, in broad strokes, the municipal population's statistics. Future studies might use oversampling or incentives to promote greater participation.

3.7 Data Collection Instruments

This study's primary data collection instrument was a structured questionnaire to gather detailed insights into participants' opinions, attitudes, and acceptance of biometric authentication in E-payment systems. This structured approach provided a systematic way to obtain quantitative data, allowing for reliable comparisons across respondents and enhancing the study's overall validity and reliability. The questionnaire was distributed to select in-person and electronic participants to accommodate diverse preferences and ensure accessibility and convenience. The questionnaire is organised into five sections, each targeting a specific aspect of biometric authentication acceptance:

Section A: Biographical Information

In this section, respondents were asked to provide demographic and background information, including age, gender, education level, employment status and familiarity with biometric authentication technologies. These biographical details are essential, as personal factors can significantly influence an individual's acceptance of new technologies. This demographic data aided in exploring variations in acceptance across different age groups, educational

backgrounds, and other relevant demographics, providing a deeper context to the study's findings.

Section B: Factors Influencing User Acceptance

This section contains questions designed to assess how the independent variables impact users' willingness to adopt biometric authentication for e-payment systems. The construct was made up of items from Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Facilitating conditions (FC), each contributing four statements.

Section C: Adoption Intention

Questions in this section focus on the dependent variable, adoption intention (AI), which consists of four statements.

Section D: Socio-Economic and Cultural Barriers

This construct focuses on the moderating variables (economic barriers (EB), social barriers (SB), and cultural barriers (CB)).

The comprehensive instrument used in this study is attached in Appendix 2.

3.8 Data Analysis

The collected data will be analysed using the Statistical Package for the Social Sciences (SPSS) version 26, a widely recognised statistical software tool used extensively in academic research to analyse and interpret quantitative data (Field, 2018; Pallant, 2021; Tabachnick & Fidell, 2019). The data analysis process will entail the following, as prescribed by Field (2018) and Hair et al. (2017)

- The first step will be to examine the dataset for any incomplete responses. If missing data are minimal, employ listwise or pairwise deletion; if more extensive, consider imputation techniques.
- Descriptive statistics will be used to summarise the demographic characteristics of the respondents (e.g., age, gender, level of education, employment status, experience in using e-payment systems) and provide an overview of the data. Measures such as means

and standard deviations will be calculated to describe the sample and the distribution of key variables.

- Reliability testing will be conducted to compute Cronbach's alpha. Values above 0.70 typically indicate acceptable internal consistency.
- The exploratory Factor Analysis (EFA) will be conducted to assess the construct validity of the measurement items and ensure that they align with the theoretical framework.
- Analysis of Variance (ANOVA) will compare the mean acceptance levels across different socio-demographic groups (e.g., age groups, employment status).
- The Pearson's correlation analysis will be conducted to examine the strength and direction of relationships between key variables that include the independent variables (PU, PEOU, PE, EE, SI, FC), moderating variables (EB, CB, SB), and their impact on the dependent variable (AI).
- Multiple regression analysis will be conducted to analyse the relationship between the predictor variables: PU, PEOU, PE, EE, SI, and FC and the dependent variable: AI.
- Factor analysis will be used to identify underlying dimensions of the constructs being measured. This step ensures that the items used in the survey align with the theoretical constructs and reduces the risk of multicollinearity in regression analysis.

All analyses will be conducted using SPSS, a widely recognised statistical package. The software's capabilities will be leveraged to perform the abovementioned tests, ensuring the findings are robust and reliable.

3.8.1 Data Quality and Preparation

The collected survey data underwent thorough checks to ensure completeness, accuracy, and consistency before conducting the analysis. Any missing or erroneous data will be addressed using appropriate data-cleaning techniques, as Hair Jr. et al. (2019) outlined. This process ensured the data was free from inconsistencies and ready for meaningful analysis. The reliability of the data is essential for generating valid and trustworthy results.

3.8.2 Descriptive Analysis

The first step in the analysis involved descriptive statistics, including frequencies, percentages, means, and standard deviations. These statistics were used to summarise the demographic

characteristics of the participants, such as age, gender, and familiarity with e-payment systems. Descriptive analysis provided a clear picture of the respondent profile and offered initial insights into trends and patterns within the sample.

3.8.3 Inferential Analysis

Inferential statistics were employed to investigate the relationships between the variables and to identify factors that influence user acceptance of biometric authentication in e-payment systems. Correlation analysis was conducted to examine the strength and direction of the relationships between key variables, such as perceived security, ease of use, and trust in biometric systems.

Regression analysis, particularly multiple regression, was used to explore the combined effects of the TAM and the UTAUT variables on user acceptance. This approach allowed for a deeper understanding of how factors such as performance expectancy, effort expectancy, and social influence collectively affect user acceptance of biometric authentication. Inferential statistics helped identify and quantify the impact of different factors, providing valuable insights into adopting biometric e-payment systems.

3.9 Validity and Reliability

Establishing validity and reliability is critical to ensuring the rigour and credibility of the study's findings, particularly in exploring the acceptance of biometric authentication in e-payment systems within the Thulamela Local Municipality. Validity ensures that the data collected accurately reflects the constructs intended to be measured, affirming that the study's outcomes are meaningful and applicable. Conversely, reliability pertains to the consistency and stability of the data over time, ensuring that results remain dependable and replicable (Pallant, 2020).

3.9.1 Validity

This study focused on both content and construct validity to achieve strong validity. Content validity is significant as it ensures that the survey instrument comprehensively covers all relevant aspects of the constructs under investigation. This involved an in-depth review of the survey items to confirm that each question is directly relevant to user acceptance and biometric authentication and associated constructs, such as security and user convenience (Field, 2018).

The research aims to provide robust data that captures participants' perspectives and attitudes regarding biometric e-payment systems by addressing all necessary elements within the data collection tool.

Construct validity was also maintained by aligning the questionnaire items closely with established theoretical frameworks, specifically the TAM and the UTAUT. This alignment helped to reinforce that each item within the questionnaire meaningfully contributes to measuring the targeted constructs, thereby supporting the integrity of the study's findings. Ultimately, ensuring validity means that conclusions drawn from the data are accurate and relevant, and contribute to a well-rounded understanding of biometric authentication acceptance.

3.9.2 Reliability

Reliability is equally essential in demonstrating the consistency and dependability of the data collected. This study employed multiple reliability measures to ensure that the data accurately represents respondents' perspectives over time and across different circumstances. One such measure is internal consistency, typically assessed through Cronbach's alpha, a widely recognised statistical test for evaluating the coherence of questionnaire items within a construct (Saunders et al., 2019). High internal consistency implies that the survey items are well-aligned and measure similar underlying dimensions of biometric acceptance reliably, which enhances confidence in the results.

Additionally, test-retest reliability was considered to verify that the survey instrument yields consistent results across multiple administrations, further reinforcing the credibility of the data collected. Through ensuring reliability, this research aims to produce findings that are insightful and replicable, thereby enabling future studies to build upon these results confidently.

3.10 Ethical Consideration

This study was conducted strictly following the Ethical Clearance Letter issued by the University Ethical Committee, ensuring full compliance with institutional ethical standards. Ethical considerations were central throughout the research process, with a clear focus on safeguarding all participants' rights, dignity, and well-being (Chubuk, 2024). The study was

committed to upholding the highest ethical standards in all stages of research, from data collection to analysis and reporting.

Informed consent was obtained from all participants before they participated in the survey. Participants were fully briefed on the nature and purpose of the study, including details on what their involvement entails and the expected time commitment. The consent process ensures that participants know their participation is entirely voluntary, with no obligation or coercion involved (Holloway & Wheeler, 2010). This was made clear in the consent form, outlining the steps taken to protect their privacy and confidentiality.

Participants were reassured that all responses would remain confidential, with no identifying information being used in any reports or publications stemming from the research. Their responses would be anonymised, and data would be stored securely to prevent unauthorised access. This aligns with ethical principles aimed at preserving confidentiality and respecting participants' privacy (Punch, 2014).

Participants were explicitly informed of their right to withdraw from the study at any stage, with no consequences or negative repercussions. Should they decide to withdraw, their data would be removed from the analysis, provided they make this request before the data is anonymised and analysed. This provision respects the principle of autonomy and emphasises the voluntary nature of participation (Holloway & Wheeler, 2010). The study respects each participant's right to discontinue involvement at any point, reflecting the commitment to ethical research practices.

The study also adhered rigorously to established ethical guidelines and university regulations to ensure the research process is transparent, respectful, and fully compliant with ethical standards (Punch, 2014). Confidentiality was maintained, with careful handling of the data and a commitment to protecting participants' privacy. Data will be stored in encrypted formats, accessible only to the research team, and will be destroyed after the study's completion.

3.11 Chapter Summary

The chapter outlined the foundational elements guiding this research, each essential to a robust study design. It established the research paradigm and philosophical orientation, grounding the

study in a clear worldview that shapes the research approach. The choice of a deductive approach and a quantitative methodological focus was then justified as the most suitable for systematically testing hypotheses on user acceptance of biometric authentication in E-payment systems. This chapter also discussed the strategic decision to employ a survey method, with a cross-sectional time horizon to capture relevant data within a specific timeframe. A detailed account of the target population and the sampling techniques ensured that the sample accurately reflects the demographic diversity within Thulamela Local Municipality, thus enhancing the study's representativeness. The structured questionnaire was the primary data collection tool, designed to gather quantifiable insights into users' perceptions, attitudes, and acceptance levels toward biometric authentication. For data analysis, the chapter highlighted using SPSS software, which is well-suited for descriptive and inferential statistical methods, to examine the relationships between variables rigorously. Further, it underscored the importance of ensuring validity and reliability in measurement, which enhances the credibility and stability of the findings. Finally, the chapter addressed ethical considerations, emphasising participants' rights, informed consent, and data confidentiality to uphold the integrity of the research process.

CHAPTER 4: PRESENTATION OF RESEARCH FINDINGS

4.1 Introduction

This chapter focuses on the presentation and analysis of the data collected by the questionnaires in the study. In this chapter, both descriptive statistics and inferential statistics were used to analyse the results. This chapter presents the study's results and critically analyses the data collected. The findings are structured in a manner that aids in answering the research questions, and statistical analyses support them.

4.2 Response Rate

As depicted in Figure 4.1, the study achieved a response rate of 246 participants out of the expected 399. This indicates a response rate of 61.7%. According to research, a response rate of 60% is deemed satisfactory and suitable for analysis (Mugenda & Mugenda, 2023). Therefore, although the response rate did not meet the intended target, the response rate obtained in this survey-based research was deemed appropriate. It is adequate to yield significant insights into the research objectives.

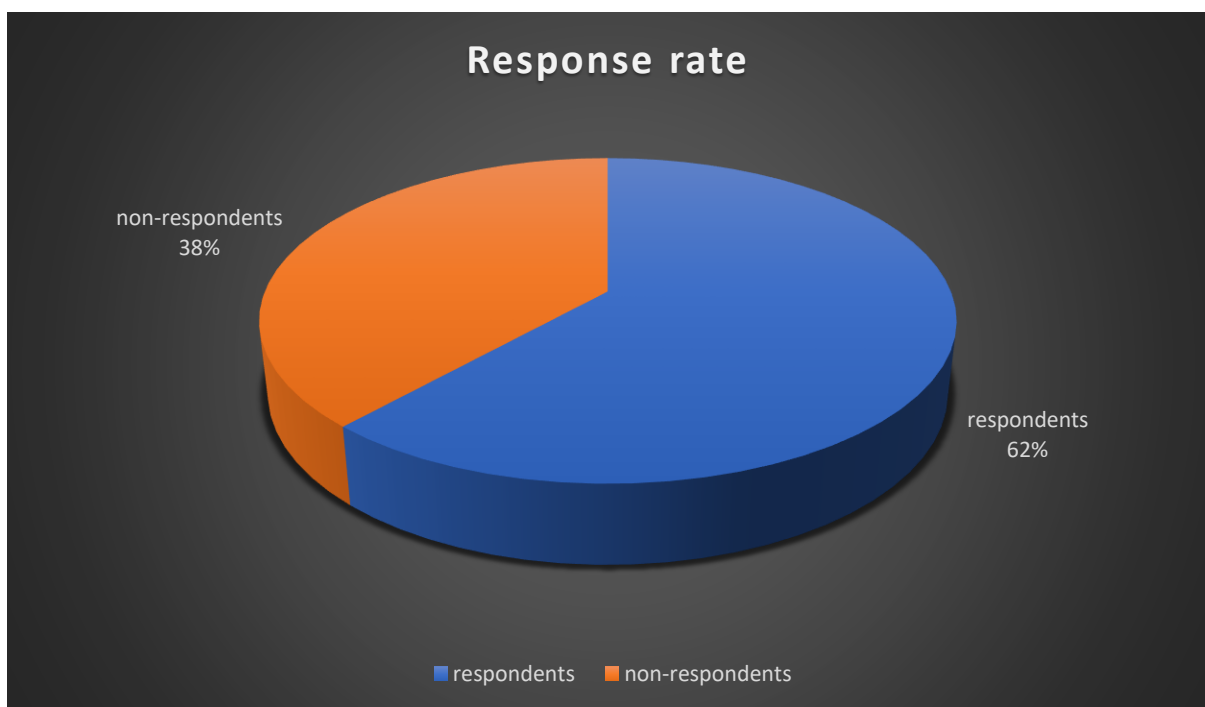


Figure 4.1: Study response rate

The obtained sample size guarantees that the data collected accurately captures the population that is being studied, allowing reliable analysis and interpretation of user acceptance of

biometric authentication in electronic payment systems. Initiatives to boost participation, including follow-ups or reminders, may have further increased the response rate; nonetheless, the current figure is adequate for the study. The gathered data was analysed using SPSS version 26.

4.3 Demographic information

The participants' demographics were recorded based on age, gender, level of education, employment status, and experience using biometric authentication in e-payment systems.

4.3.1 Age

The predominant age group was 18–24 years, with 107 people, accounting for nearly half (44%) of the total participants. The subsequent largest cohorts are ages 25–34 with 91 individuals (34%), ages 35–44 with 31 participants (13%), and ages 45–54 with 11 participants (4%), whilst the smallest cohort, ages 55 and above, comprised 6 participants, or merely 2% of the total participants. This is depicted in Figure 4.2.

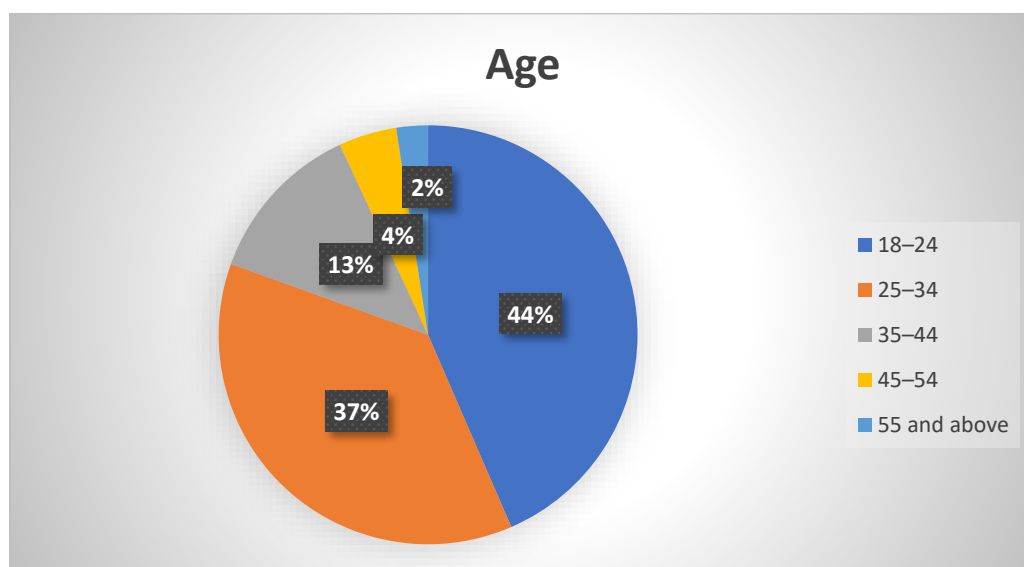


Figure 4.2: Age of respondents

4.3.2 Gender

The data showed a significant proportion of 128 female participants, constituting 52%. Male participants, numbering 111, comprised 45% of the sample. Seven participants refrained from disclosing their gender, representing 3% of the overall participant count. This is depicted in Figure 4.3.

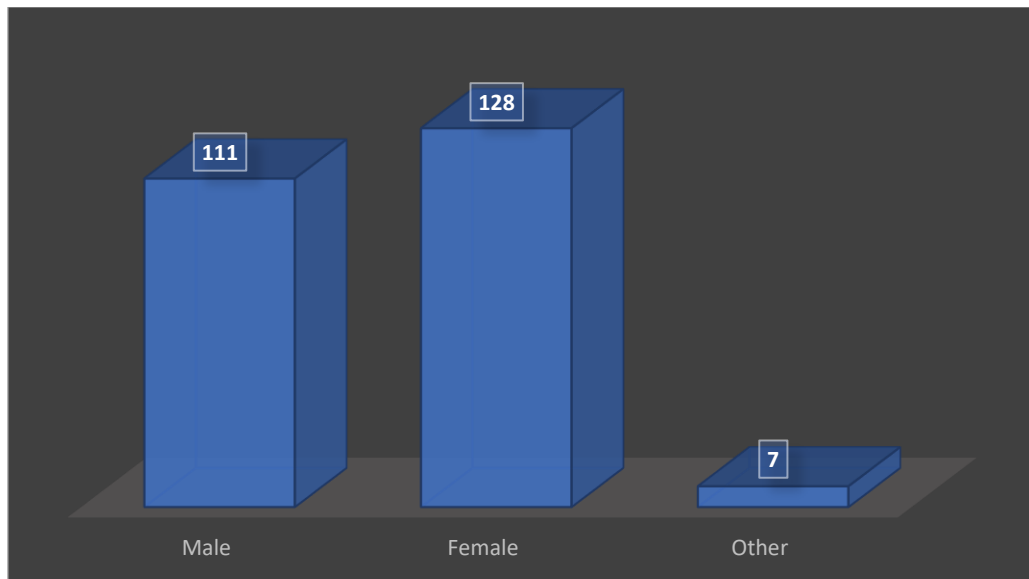


Figure 4.3: Gender of respondents

4.3.3 Level of Education

Further analysis of the participants' education level revealed that 104 participants acquired basic primary and secondary education (42%), while 71 people held either a Diploma or Certificate (29%). A total of 35 participants indicated that they had not received any education (14%), while 27 participants earned a bachelor's degree (11%). The group with the least representation acquired a postgraduate qualification, with nine people constituting 4% of the overall participants. This is depicted in Figure 4.4.

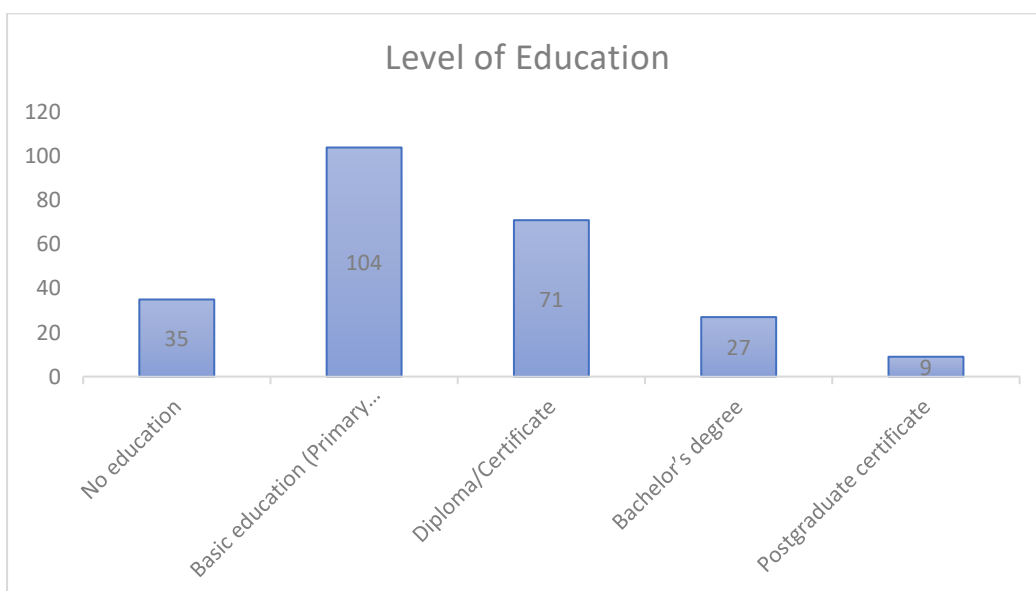


Figure 4.4: Level of education of respondents

4.3.4 Employment Status

The participants' employment status was recorded, with the majority being employed; specifically, 116 participants reported employment, constituting 47% of the total participants. Subsequently, 64 participants indicated they were self-employed, representing 26% of the total. A subset of the participants comprised students, totalling 41 participants (17%). The smallest segment of contributions came from 25 unemployed participants, constituting 10% of the overall population. This is depicted in Figure 4.5.

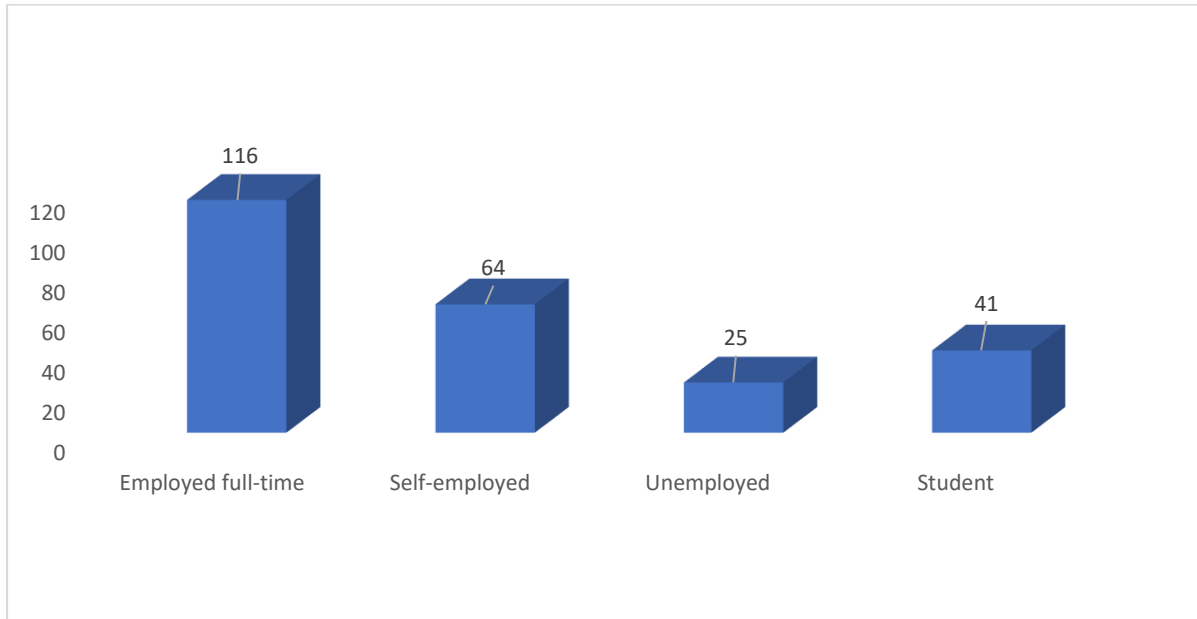


Figure 4.5: Employment status of respondents

4.3.5 Experience in Using Biometric Authentication in E-payment Systems

Most participants reported having 1 to 2 years of experience with biometric authentication in e-payment systems, totalling 76 participants (31%). Subsequently, 67 participants cautiously indicated that they possessed less than one year of experience (27%) with biometric authentication in e-payment systems. A total of 53 respondents said that they had used biometric authentication systems for a time span of 3-5 years, representing 22% of the overall participants. A substantial proportion of 33 participants used biometric authentication technologies over 5 years, constituting 13% of the overall participants. A total of 17 participants, or 13% of the overall sample, reported using biometric authentication technologies for e-payments. This is depicted in Figure 4.6.

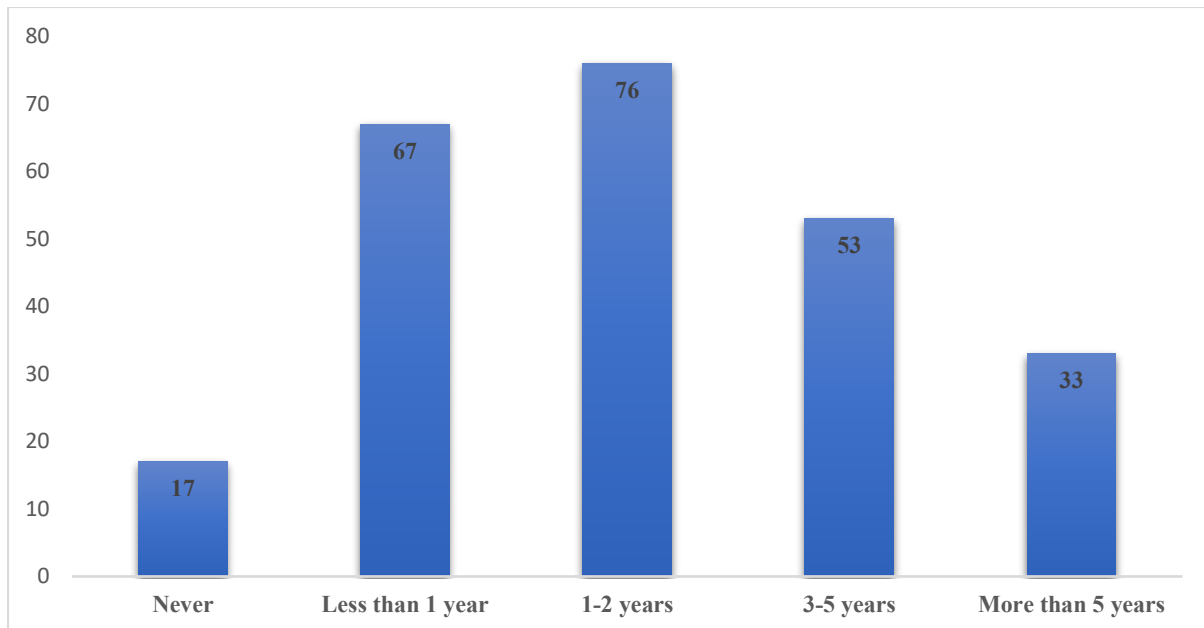


Figure 4.6: Experience of respondents in using biometric authentication

The data offered significant insights into the demographic composition of the sample, facilitating a deeper comprehension of the individuals participating in the study. The explicit presentation of frequency and percentage statistics about age, gender, level of education, employment status, and experience of the participants using biometric authentication in e-payment systems provided a comprehensive analysis of the sample characteristics.

4.4 Reliability Test

Table 4.1 outlines the reliability test results conducted on the constructs used in the study, measured using Cronbach's alpha. This test was essential to ensure the internal consistency of the survey instrument. The table categorises the constructs into independent, dependent, and moderating variables, with all constructs achieving the minimum reliability threshold of 0.7, which is widely accepted in academic research (Tavakol & Dennick, 2011). The independent variables include perceived usefulness (PU), which achieved a score of 0.820, perceived ease of use (PEOU) at 0.720, performance expectancy (PE) at 0.757, effort expectancy (EE) at 0.703, and social influence (SI) at 0.792. Facilitating conditions (FC), which is also considered an independent variable, scored 0.702. The dependent variable, adoption intention (AI), achieved a reliability score 0.757.

Meanwhile, the moderating variables: economic barriers (EB), cultural barriers (CB), and social barriers (SB) scored 0.738, 0.773, and 0.778, respectively. These results confirm that all constructs used in the study were reliable and suitable for further analysis. The high reliability scores indicate that the survey instrument is consistent and capable of accurately measuring the factors influencing user acceptance of biometric authentication in e-payment systems.

Table 4.1: Cronbach's Alpha Scores

Construct	Variable Type	Cronbach's Alpha Score
Perceived Usefulness (PU)	Independent variable	0.820
Perceived Ease of Use (PEOU)	Independent variable	0.720
Performance Expectancy (PE)	Independent variable	0.757
Effort Expectancy (EE)	Independent variable	0.703
Social Influence (SI)	Independent variable	0.792
Facilitating Conditions (FC)	Independent variable	0.702
Adoption Intention (AI)	Dependent variable	0.757
Economic Barriers (EB)	Moderating variable	0.738
Cultural Barriers (CB)	Moderating variable	0.773
Social Barriers (SB)	Moderating variable	0.778

Table 4.2 presents the overall reliability statistics for the survey instrument, combining all 40 items across the constructs. The Cronbach's alpha for the entire instrument was calculated at 0.924, with a standardised alpha of 0.925. These results demonstrate excellent internal consistency, as scores above 0.9 are highly reliable (George & Mallery, 2003). The high overall reliability score indicates that the survey instrument is robust and well-suited for achieving the study's objectives. Given these results, the study's survey instrument can be deemed robust, providing a strong foundation for meaningful data analysis. The high overall reliability score ensures that a consistent and dependable measurement approach supports any inferences drawn from the findings. This level of reliability is crucial in research of this nature, where accurate assessments of user acceptance, technological perceptions, and socio-economic barriers are essential for formulating well-grounded conclusions and recommendations.

Table 4.2: Overall reliability test for all constructs

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.924	.925	40

4.5 Descriptive statistics

Table 4.3 summarises the descriptive statistics for the various constructs measured in this study, including independent variables (PU, PEOU, PE, EE, SI, FC), the dependent variable (AI), and the moderating variables (EB, CB, and SB). The sample consisted of 246 respondents. The mean scores for all constructs are above 4.0, except for SB (mean = 3.7022), indicating that respondents generally agreed with the statements related to these constructs, suggesting that social perceptions could hinder adoption. The standard deviations range from 0.40757 (PEOU) to 0.84486 (SB), suggesting varying levels of response consistency across constructs. The high mean scores for PEOU (4.6159), PE (4.4146), and EE (4.3801) indicate that respondents perceive biometric authentication as easy to use, expected to enhance performance, and do not take time to do transactions. Similarly, the mean score for AI (4.3770) reflects a strong intention to adopt biometric authentication. The relatively high standard deviations for economic barriers (SB = 0.84486) indicate varied opinions among respondents, which may require targeted interventions.

These findings provide insights into the factors influencing user acceptance and the barriers that may hinder adoption. These high mean scores imply a positive disposition towards biometric authentication among the respondents, thus directly addressing the first research question regarding the factors influencing user acceptance. The standard deviations also reflect low variability in responses, reinforcing the reliability of these constructs (Field, 2013). Furthermore, the minimum and maximum scores indicate that while most respondents exhibited a strong inclination towards acceptance, there were still a few outliers, suggesting that some individuals may have reservations. This variability could be further explored in future analyses, perhaps using qualitative methods to gain deeper insights into user

perspectives. This highlights the increasing complexity of social barriers and suggests that any solution or promotion toward biometric adoption in an e-payment system must directly confront varying privacy and trust issues, possibly with targeted education or transparency measures.

Table 4.3: Study descriptive statistics

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
PU_Mean	246	1.75	5.00	4.1992	.71640
PEOU_Mean	246	3.00	5.00	4.6159	.40757
PE_Mean	246	2.50	5.00	4.4146	.59404
EE_Mean	246	3.00	5.00	4.3801	.53533
SI_Mean	246	2.00	5.00	4.2083	.68664
FC_Mean	246	2.25	5.00	4.2632	.63734
AI_Mean	246	3.00	5.00	4.3770	.53868
EB_Mean	246	1.75	5.00	4.1240	.72939
CB_Mean	246	1.75	5.00	4.2551	.59223
SB_Mean	246	1.75	5.00	3.7022	.84486
Valid N (listwise)	246				

4.6 Explanatory Factor Analysis (EFA)

This section discusses the communalities and the Rotated Component Matrix. Factor analysis determined how each variable correlates with the extracted factors. Table 4.4 displays the communalities derived from the exploratory factor analysis (EFA). All items had high extraction values (> 0.6), confirming their suitability for factor analysis (Hair et al., 2014). High extraction values, especially for the items categorised under PU, PE, CB, EB, and SI, imply a robust underlying structure for these constructs. For instance, PU components exhibit extraction values between 0.932 and 0.948, indicating a strong correlation and a well-defined construct. Therefore, the finding corroborates the legitimacy of the constructs used in the study, which is crucial for accurately determining user acceptance (Hair et al., 2014). In the table, the communalities across the various constructs demonstrate acceptable levels. However, certain items, such as SI4 (extraction value = 0.641) and SB3 (extraction value = 0.675), imply that this specific item may not correspond well with others in assessing social influence and

social barriers, respectively. This weaker alignment might affect the wording or understanding of particular questions. Therefore, such items may need to be revised or reworded in future studies to agree more with the underlying theoretical dimensions.

Table 4.4: Communalities

Communalities		
	Initial	Extraction
PU1	1.000	.948
PU2	1.000	.946
PU3	1.000	.943
PU4	1.000	.932
PEOU1	1.000	.767
PEOU2	1.000	.738
PEOU3	1.000	.773
PEOU4	1.000	.682
PE1	1.000	.948
PE2	1.000	.946
PE3	1.000	.842
PE4	1.000	.863
EE1	1.000	.900
EE2	1.000	.908
EE3	1.000	.768
EE4	1.000	.647
SI1	1.000	.946
SI2	1.000	.943
SI3	1.000	.932
SI4	1.000	.641
FC1	1.000	.838
FC2	1.000	.811
FC3	1.000	.736
FC4	1.000	.744
AI1	1.000	.789
AI2	1.000	.722
AI3	1.000	.804
AI4	1.000	.806
EB1	1.000	.874
EB2	1.000	.876
EB3	1.000	.852
EB4	1.000	.867

CB1	1.000	.917
CB2	1.000	.844
CB3	1.000	.847
CB4	1.000	.796
SB1	1.000	.883
SB2	1.000	.864
SB3	1.000	.675
SB4	1.000	.948

Extraction Method: Principal Component Analysis.

These results confirm the validity of the constructs and suggest that the instrument items effectively measure the intended dimensions. The high communalities further support the instrument's reliability, as previously established in the Cronbach's alpha analysis.

4.7 Pearson Correlation

Table 4.5 provides Pearson correlation coefficients between the constructs, which examine the relationships between independent variables (PU, PEOU, PE, EE, SI, FC), moderating variables (EB, CB, SB), and the dependent variable (AI).

Table 4.5: Correlation analysis

Correlations											
		PU_M ean	PEOU_ Mean	PE_Me an	EE_M ean	SI_Mea n	FC_Me an	AI_Mea n	EB_M ean	CB_M ean	SB_ Mean
PU_Me an	Pearson Correlation	1	.327**	.774**	.715**	.951**	.328**	.409**	.294**	.285**	.464**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	246	246	246	246	246	246	246	246	246	246
PEOU_ Mean	Pearson Correlation	.327**	1	.481**	.336**	.356**	.269**	.451**	.152*	.276**	.298**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.017	.000	.000
	N	246	246	246	246	246	246	246	246	246	246
PE_Me an	Pearson Correlation	.774**	.481**	1	.438**	.686**	.362**	.483**	.264**	.202**	.470**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.001	.000
	N	246	246	246	246	246	246	246	246	246	246
EE_Me an	Pearson Correlation	.715**	.336**	.438**	1	.766**	.300**	.483**	.247**	.404**	.231**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000
	N	246	246	246	246	246	246	246	246	246	246
SI_Mea n	Pearson Correlation	.951**	.356**	.686**	.766**	1	.391**	.452**	.305**	.361**	.441**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000

	N	246	246	246	246	246	246	246	246	246	246
FC_Mean	Pearson Correlation	.328**	.269**	.362**	.300**	.391**	1	.398**	.193**	.341**	.320**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.002	.000	.000
	N	246	246	246	246	246	246	246	246	246	246
AI_Mean	Pearson Correlation	.409**	.451**	.483**	.483**	.452**	.398**	1	.209**	.308**	.217**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.001	.000	.001
	N	246	246	246	246	246	246	246	246	246	246
EB_Mean	Pearson Correlation	.294**	.152*	.264**	.247**	.305**	.193**	.209**	1	.281**	.293**
	Sig. (2-tailed)	.000	.017	.000	.000	.000	.002	.001		.000	.000
	N	246	246	246	246	246	246	246	246	246	246
CB_Mean	Pearson Correlation	.285**	.276**	.202**	.404**	.361**	.341**	.308**	.281**	1	.231**
	Sig. (2-tailed)	.000	.000	.001	.000	.000	.000	.000	.000		.000
	N	246	246	246	246	246	246	246	246	246	246
SB_Mean	Pearson Correlation	.464**	.298**	.470**	.231**	.441**	.320**	.217**	.293**	.231**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.001	.000	.000	
	N	246	246	246	246	246	246	246	246	246	246
**. Correlation is significant at the 0.01 level (2-tailed).											
*. Correlation is significant at the 0.05 level (2-tailed).											

The following is from the above results:

- PU - The correlation coefficient ($r = 0.409$) indicates a moderate positive relationship between PU and AI. This suggests that users who perceive biometric authentication as useful are likelier to adopt it. The significance level ($p < 0.01$) confirms this relationship is statistically significant, meaning the observed correlation is unlikely to have occurred by chance.
- PEOU - The correlation coefficient ($r = 0.451$) shows a moderate positive relationship between PEOU and AI. This implies that when users find biometric authentication easy to use, their intention to adopt it increases. The significance level ($p < 0.01$) confirms this relationship is statistically significant.
- PE - The correlation coefficient ($r = 0.483$) indicates a moderate positive relationship between PE and AI. This means that as respondents perceive biometric authentication to improve their performance, their intention to adopt it increases. The significance level ($p < 0.01$) confirms this relationship is statistically significant.
- EE - The correlation coefficient ($r = 0.483$) also shows a moderate positive relationship between EE and AI. This suggests that when respondents find biometric authentication easy to use, their intention to adopt it increases. The significance level ($p < 0.01$) confirms this relationship is statistically significant.

- SI - The correlation coefficient ($r = 0.452$) indicates a moderate positive relationship between SI and AI. This means that social factors, such as peer recommendations or societal acceptance, positively influence users' intention to adopt biometric authentication. The significance level ($p < 0.01$) confirms this relationship is statistically significant.
- FC - The correlation coefficient ($r = 0.398$) indicates a moderate positive relationship between FC and AI. This implies that when respondents perceive the necessary resources and support to be available, their intention to adopt biometric authentication increases. The significance level ($p < 0.01$) confirms this relationship is also statistically significant.
- EB - The correlation coefficient ($r = 0.209$) shows a weak positive relationship between EB and AI. This suggests that while economic barriers (e.g., cost) may not directly encourage adoption, they could indirectly influence it.
- CB - The correlation coefficient ($r = 0.308$) indicates a moderate positive relationship between CB and AI. This suggests that cultural factors, such as community perceptions or resistance to new technology, moderately influence adoption.
- SB - The correlation coefficient ($r = 0.217$) shows a weak positive relationship between SB and AI. This suggests that social concerns like privacy or trust issues may indirectly affect adoption. The significance level ($p < 0.01$) confirms this relationship is statistically significant.

4.8 Regression Analysis

To analyse the relationship between the predictor variables: PU, PEOU, PE, EE, SI, and FC and the dependent variable: AI, multiple linear regression was performed at 95% confidence intervals. The results are shown in Tables 4.6, 4.7 and 4.8.

Table 4.6: Regression analysis

Model Summary									
Model	R	R Square		Std. Error of the Estimate	R Square Change	Change Statistics			Sig. F Change
		R Square	Adjusted R Square			F Change	df1	df2	
1	.651 ^a	.424	.410	.41391	.424	29.329	6	239	.000

a. Predictors: (Constant), FC_Mean, PEOU_Mean, EE_Mean, PE_Mean, SI_Mean, PU_Mean

Table 4.8: ANOVA Table

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.148	6	5.025	29.329	.000 ^b
	Residual	40.945	239	.171		
	Total	71.093	245			

a. Dependent Variable: AI_Mean

b. Predictors: (Constant), FC_Mean, PEOU_Mean, EE_Mean, PE_Mean, SI_Mean, PU_Mean

Table 4.9: Regression analysis: Coefficients Table

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.303	.343		.882	.379
	PU_Mean	-.473	.155	-.629	-3.061	.002
	PEOU_Mean	.203	.079	.154	2.564	.011
	PE_Mean	.398	.086	.439	4.614	.000
	EE_Mean	.383	.080	.381	4.781	.000
	SI_Mean	.268	.147	.341	1.818	.070
	FC_Mean	.132	.047	.156	2.779	.006

a. Dependent Variable: AI_Mean

The correlation coefficient (R) of 0.651 indicates a strong positive relationship between the observed (PU, PEOU, PE, EE, SI, and FC) and predicted values of the dependent variable (AI). The R^2 value of 0.424 indicates that approximately 42.4% of the variance in intention to adopt biometric authentication systems in e-payments can be explained by the six predictors combined (PU, PEOU, PE, EE, SI, and FC). The adjusted R^2 (0.410), which accounts for the number of predictors and sample size, is slightly lower than R^2 , accounting for the number of predictors in the model and confirming that the model is not overfitted. The change statistics indicate that adding these predictors significantly improves the model fit, with an F-change statistic of 29.329 and a significance level (p) of 0.000. The ANOVA table further supports the significance of the regression model, as shown by the high F-value (29.329) and $p < 0.001$. The F-statistic assesses the overall significance of the model. Since the p-value is below 0.05, it confirms that the independent variables significantly predict AI, and the model is statistically significant. The results confirm that while these factors (PU, PEOU, PE, EE, SI, and FC)

significantly contribute to AI, additional factors outside the model may also influence adoption decisions.

The analysis showed that PE ($\beta = 0.439$, $t = 4.614$, $p = 0.001$) positively impacts AI and drives adoption of biometric authentication in e-payment systems. Similarly, it can also be seen that EE ($\beta = 0.381$, $t = 4.781$, $p = 0.001$), PEOU ($\beta = 0.154$, $t = 2.564$, $p = 0.011$), FC ($\beta = 0.156$, $t = 2.779$, $p = 0.006$) all have a positive influence on AI. SI ($p = 0.070$) is marginally significant, meaning its effect is weaker than that of other variables. Conversely, PU has a negative coefficient ($\beta = -0.473$, $p = 0.002$), suggesting that perceived usefulness alone does not drive adoption.

Summarily, the model is a good fit based on the findings. i. The R^2 value of 42.4% is moderate, indicating a fair level of explanatory power; ii. The ANOVA F-test is highly significant ($p < 0.001$), confirming that the model is meaningful and iii. The key predictors (PE, EE, PEOU, and FC) significantly contribute to AI, validating their importance. To improve the model, since 57.6% of AI's variance remains unexplained, incorporating additional predictors (e.g., security concerns or trust) could enhance the model.

4.9 Discussion of Findings

This section provides a detailed discussion of the earlier findings, structured around the study's research questions. The discussion integrates the study's results with existing literature to provide a comprehensive understanding of the factors influencing user acceptance of biometric authentication in e-payment systems, the current level of user acceptance, the socio-economic and cultural barriers affecting adoption, and the development of a framework to enhance user acceptance. The findings are contextualised within the broader body of knowledge, with references to substantiate or challenge the results.

Before comprehensively covering the research questions, the response rate needs to be analysed. The response rate of 60.7%, though within acceptable limits for survey-based research, may limit the generalisability and representativeness of the findings. This is particularly relevant in a study focused on a specific municipality, where a higher response rate could provide a more comprehensive understanding of user perceptions. However, there are studies within the South African municipal contexts with similar response rate statistics.

Studies by Mlitwa (2012) and Mawela et al. (2017) reported 55% and 62% response rates, respectively. This comparison demonstrates that the response rate in this study is consistent with similar research. Future studies could employ strategies such as follow-up reminders or incentives to improve response rates and enhance the robustness of the findings.

Research Question 1: What factors influence user acceptance of biometric authentication in e-payment systems?

This study identified several key determinants influencing user acceptance of biometric authentication. The first predictor that influences adoption, based on the research findings, is ***performance expectancy (PE)*** ($\beta = 0.439, p < 0.001$). The high mean score for *PE* (4.4146) indicates that users perceive biometric authentication as efficient. The belief that biometric authentication will enhance transaction efficiency emerged as a significant predictor. This aligns with findings by Bhat et al. (2024), who reported that perceived usefulness and security significantly influence consumers' attitudes towards biometric banking services. Another factor is ***effort expectancy (EE)*** ($\beta = 0.381, p < 0.001$). The high mean score for *EE* (4.3801) indicates that users perceive biometric authentication as requiring minimal effort. This entails that the ease associated with using biometric systems was another crucial factor. Abdulkareem (2023) highlighted that usability plays a pivotal role across various applications, including banking.

Additionally, ***perceived ease of use (PEOU)*** emerged as a critical determinant. The high mean score for *PEOU* (4.6159) further supports this finding, suggesting that respondents generally perceive biometric authentication as user-friendly. These findings suggest that users' acceptance levels increase when they find biometric systems straightforward. This is corroborated by Bellahcene and Latreche (2023), who emphasised that perceived ease of use significantly impacts user acceptance in e-banking contexts. Lastly, ***facilitating conditions (FC)*** also influence user acceptance of biometric authentication. FC had a significant positive relationship with AI ($\beta = 0.156, p = 0.006$), highlighting the importance of resources and support in driving adoption. The mean score for *FC* (4.2632) indicates that respondents generally perceive the necessary infrastructure and support as available. The availability of necessary resources and support was found to influence acceptance. This is consistent with the UTAUT, which posits that facilitating conditions are determinants of technology adoption.

Surprisingly and interestingly so, this study revealed a negative relationship between *perceived usefulness (PU)* and adoption intention, as attested by the results ($\beta = -0.473$, $p = 0.002$). This contrasts with traditional TAM assertions, which typically highlight PU as a positive predictor. One possible explanation is that users may prioritise ease of use and social influences over the mere utility of the system. This perspective is supported by Popovic et al. (2013), who found that privacy concerns can moderate the relationship between perceived usefulness and acceptance, leading to unexpected negative correlations. Similarly, *social influence (SI)* revealed a marginally significant impact on AI ($p = 0.070$), indicating that social factors, like peer recommendations and societal approval, exert an insignificant impact on adoption. Such a finding diverges from research conducted in collectivist societies, where social influence frequently serves as a more significant variable in technology adoption (Dwivedi et al., 2019). The comparatively low mean score for SI (4.2083) indicates that although social elements are pertinent, they are not just as crucial as other factors in this context.

Research Question 2: What is the current level of user acceptance and intention to adopt biometric authentication in e-payment systems within the municipality?

The descriptive statistics revealed a high level of user acceptance and intention to adopt biometric authentication, with a mean AI score of 4.3770 ($SD = 0.53868$). This indicates that respondents generally have a positive disposition towards adopting biometric authentication in e-payment systems. The high mean scores for *PEOU* (4.6159), *PE* (4.4146), and *EE* (4.3801) suggest that users perceive biometric authentication as easy to use, efficient, and requiring minimal effort. The same can be argued on *FC* (4.1240), *SI* (4.2083) and *PU* (4.1992) for the independent variables. These findings are consistent with studies by Sharma et al. (2020) and Alalwan et al. (2018), which found high levels of acceptance for biometric systems among users who valued their convenience and security. The study also noted that economic and cultural barriers play a moderate level of acceptance and intention to adopt biometric authentication in e-payment systems. This is in line with the study that noted that cultural differences play a role in biometric perception (Riley et al., 2009). The relatively low mean score and relatively high standard deviation for social barriers (SB) ($mean = 3.7022$; $SD = 0.84486$) suggests variability in user perceptions, with some respondents expressing reservations about adopting the technology. This finding aligns with studies by Al-Emran et al. (2020), which found that while many users were enthusiastic about biometric authentication, others were concerned about privacy and security issues.

The demographic analysis showed that most respondents were aged 18–34 (78%), a group that is generally more tech-savvy and open to adopting new technologies. This aligns with findings by Dwivedi et al. (2019), who noted that younger users are more likely to adopt innovative technologies. This is encouraging, as it mirrors global trends. For instance, a study by Bhat et al. (2024) reported a growing acceptance of biometric banking services, attributing it to increased awareness and perceived security benefits.

Research Question 3: What socio-economic and cultural barriers affect the acceptance of biometric authentication in e-payment systems in Thulamela?

The study identified several socio-economic and cultural barriers affecting user acceptance, including economic barriers, cultural barriers, and social barriers. The weak positive relationship between EB and AI ($r = 0.209, p < 0.01$) suggests that while economic barriers, such as cost, do not directly discourage adoption, they may have an indirect influence. The mean score for EB (4.1240) indicates that respondents generally perceive economic barriers as a concern. Concerns about the cost of biometric systems can deter adoption, especially in regions with limited financial resources. This finding aligns with studies by Al-Emran et al. (2020), which found that affordability was a significant concern for users in developing countries. Similarly, the moderate positive relationship between CB and AI ($r = 0.308, p < 0.01$) highlights the influence of cultural factors, such as community perceptions and resistance to new technology, on adoption. In other words, cultural perceptions significantly influence acceptance. The mean score for CB (4.2551) suggests that cultural barriers are a significant concern for many respondents. This finding aligns with studies in similar contexts, such as that by Alalwan et al. (2017), which found that cultural norms and values significantly influenced technology adoption in the Middle East.

In contrast, the weak positive relationship between SB and AI ($r = 0.217, p < 0.01$) suggests that social concerns, such as privacy and trust issues, may indirectly affect adoption. The relatively low mean score for SB (3.7022) indicates that social barriers are less significant than economic and cultural barriers. This finding is supported by Sharma et al. (2020), who found that users were hesitant to adopt biometric authentication due to concerns about data security and misuse.

Research Question 4: How can a framework be developed to enhance user acceptance of biometric authentication in e-payment systems based on these influencing factors?

The study's findings provide a strong basis for developing a framework to enhance user acceptance of biometric authentication in e-payment systems. The statistical results highlight the key factors influencing adoption intention and justify the inclusion of specific areas in the proposed framework. Based on the findings, a framework to enhance user acceptance should address the following key areas:

- User-centric design

Research shows that PEOU significantly boosts the intention to adopt technology, with a positive influence of $\beta = 0.154$ ($p = 0.011$). PE stands out as the strongest predictor of adoption intention ($\beta = 0.439$, $p < 0.001$), indicating that users value systems that enhance their performance and usability with a high mean score of 4.6159. Based on this, the proposed strategies include developing an intuitive and user-friendly interface and emphasising performance benefits in marketing campaigns.

- Socio-economic and cultural interventions

According to the findings, EB show a weak positive relationship ($r = 0.209$, $p < 0.01$) with adoption intention. In contrast, CB has a moderate positive correlation ($r = 0.308$, $p < 0.01$), indicating that cost and cultural resistance moderately influence adoption. To tackle these issues, it's recommended to address economic barriers through subsidies or cost-effective solutions. There is also a need to launch awareness campaigns to overcome cultural resistance.

- Infrastructure and support

Results indicate that FC significantly influences adoption intention ($\beta = 0.156$, $p = 0.006$) and a mean score of 4.2632. This highlights the importance of available resources and support. Based on these revelations, it is proposed that there is a need to invest in robust infrastructure to support biometric authentication. The provision of technical support and user education programmes also facilitates adoption.

- Trust and privacy

The findings revealed that SB had a weak positive correlation ($r = 0.217$, $p < 0.01$) with adoption intention, with a mean score of 3.7022. This suggests that trust and privacy concerns can indirectly affect adoption decisions. Implementing robust data security and privacy measures to enhance trust is important. It is also important to develop transparent policies on data usage and storage.

- Targeted marketing

A demographic analysis indicates that 78% of respondents are 18–34. They tend to be tech-savvy as they are perceived as digital natives and are more receptive to new technologies. There is a need to focus marketing efforts on younger users through tailored campaigns to reach this audience effectively. There is also a need to engage older users (perceived as digital immigrants) by addressing their specific concerns directly.

By strategically addressing these factors, the adoption of biometric authentication systems in e-payments can be significantly enhanced. Based on the findings of this study, the conceptual framework proposed in Figure 2.1 (Chapter 2) is refined as illustrated in Figure 4.7.

The conceptual framework shows the key factors influencing adoption intention (AI), which is placed at the diagram's centre. Factors like PE, EE, PEOU and FC are directly linked to AI with solid arrows, indicating strong support from the research. On the other hand, PU, SI, and SB are shown with dotted arrows, representing unsupported relationships. Additionally, CB and EB act as moderators, influencing AI indirectly, and are represented with dashed arrows. The diagram provides a clear and focused view of how these factors interact, highlighting the central importance of AI in adopting biometric authentication systems.

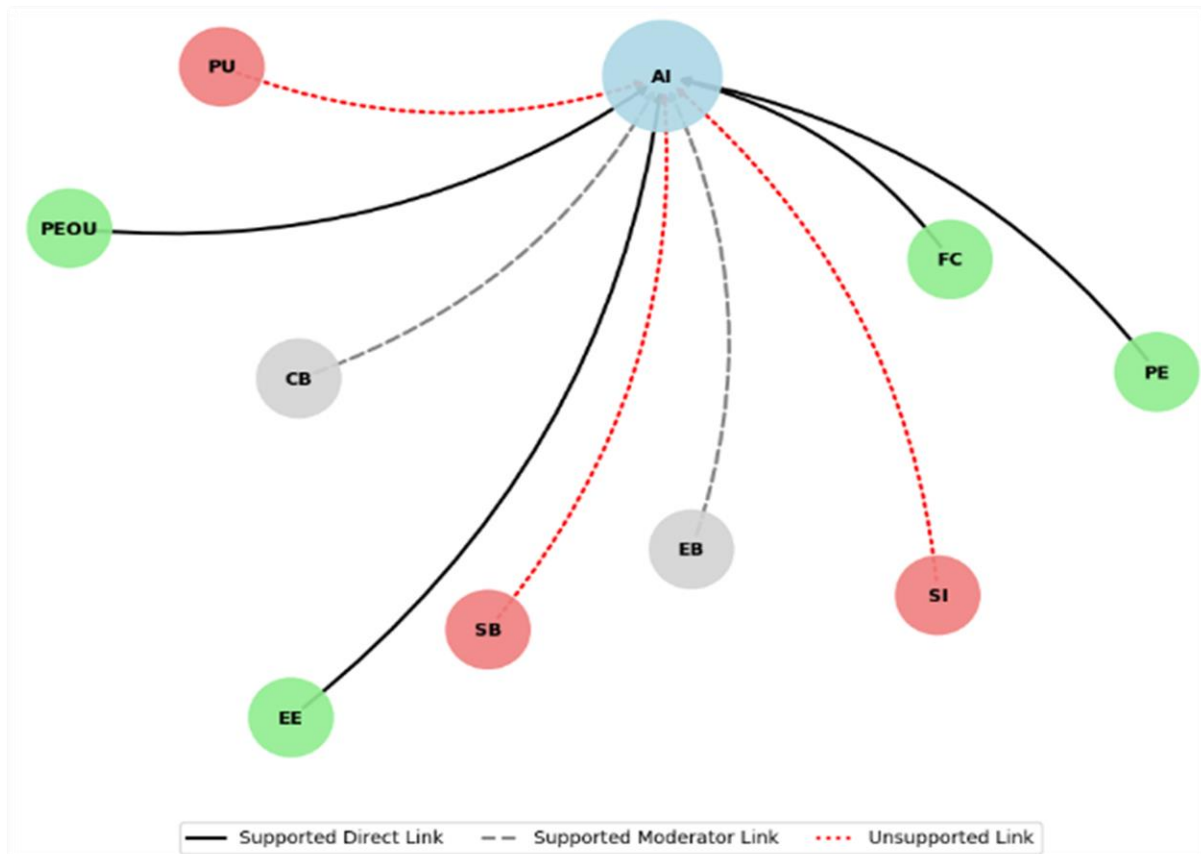


Figure 4.7: User acceptance framework for biometric authentication in e-payments

4.10 Chapter Summary

This chapter presented the research findings and the analysis thereof. After collecting data from the participants, the response rate was highlighted. The study analysed the participants' demographic information based on age, gender, level of education, employment status, and experience using biometric authentication in e-payment systems. A reliability test was done wherein all constructs were above the minimum threshold of 0.7 score. Both descriptive and inferential statistics were conducted on the results. Lastly, the results were discussed, focusing on the study's research questions and how each was answered.

CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter synthesises the research findings, providing a structured discussion of each objective. It also draws conclusions based on the findings, offers practical recommendations, highlights the study's contributions, identifies its limitations, and suggests future research directions. The chapter concludes with a summary encapsulating the key aspects of the study.

5.2 Summary of Findings

This section provides a summary of the research findings:

Objective 1: To identify the factors that influence user acceptance of biometric authentication in e-payment systems.

The study identified several key determinants influencing the acceptance of biometric authentication in E-payment systems within the Thulamela Local Municipality. The study revealed that perceived ease of use (PEOU), performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC) significantly influence user acceptance. Among these, performance expectancy emerged as the strongest predictor, highlighting the importance of efficiency and productivity in driving adoption. Conversely, perceived usefulness (PU) showed a negative relationship, indicating that other factors, such as trust and privacy concerns, may outweigh its impact.

Objective 2: To assess the level of user acceptance and intention to adopt biometric authentication in e-payment systems.

The findings indicated a high level of user acceptance, with a mean adoption intention score of 4.3770. Younger users, notably those aged 18–34, demonstrated the highest levels of acceptance, reflecting their familiarity with technology. However, variability in responses suggested that targeted interventions are needed to address the concerns of specific demographic groups, such as older users.

Objective 3: To evaluate socio-economic and cultural barriers affecting user acceptance of biometric authentication in e-payment systems.

Economic barriers (EB) and cultural barriers (CB) were found to moderately influence adoption, with correlation coefficients of 0.209 and 0.308, respectively. Social barriers (SB), such as privacy and trust concerns, had a weaker influence but still shaped user perceptions. Addressing these barriers through targeted strategies, such as subsidies and awareness campaigns, is essential for enhancing adoption.

Objective 4: To propose a framework for improving user acceptance of biometric authentication in e-payment systems.

The proposed framework focused on five key areas: user-centric design, socio-economic and cultural interventions, infrastructure and support, trust and privacy, and targeted marketing. Each area was supported by statistical evidence, ensuring a comprehensive approach to addressing the factors influencing user acceptance. This is depicted in Figure 4.7.

5.3 Conclusions

This study examined the factors influencing user acceptance of biometric authentication in electronic payment systems within the Thulamela Local Municipality. The findings demonstrated that performance expectancy, effort expectancy, perceived ease of use, and facilitating conditions significantly influence adoption. Social influence had a minimal effect on adoption. In contrast, perceived usefulness exhibited an unanticipated negative correlation with adoption intention, indicating that ease of use and trust may be more significant factors than anticipated. A significant acceptance level noted among the younger users indicates a favourable and promising outlook for biometric technologies in the region. The study's findings affirmed that, although user acceptance is moderate to high, socio-economic and cultural barriers remain and need to be addressed to facilitate broader adoption. Concerns related to costs, cultural perspectives, and security must be resolved to improve adoption rates. The proposed framework presents a structured approach for addressing these challenges, emphasising user-centric design, resilient infrastructure, and customised interventions. Biometric authentication in e-payment systems can significantly improve security and efficiency; however, specific measures are needed to promote broad adoption. The insights derived from this research contribute not only to the local understanding of biometric technology acceptance but also to the broader discourse on technology adoption in developing economies.

5.4 Recommendations

In accordance with the research findings, this study proposes the following recommendations:

- The study can be piloted in one department specific to the Thulamela Local Municipality, for instance, the finance or human resource departments. This would permit a biometric system to be monitored in a controlled environment while keeping user feedback in inspection.
- Subsequently, the biometric authentication system must be prototyped and tested with small groups of potential users. This would help to identify bottlenecks around usability and would also enhance the system prior to its actual deployment.
- The users, municipal officials as well as the technology providers should meet at regular intervals to discuss and ensure that the system really does align with the needs of all concerned stakeholders.
- Build intuitive and user-centric interfaces for biometric authentication systems for enhanced perceived ease of use.
- Set up subsidies or economic alternatives to alleviate economic barriers and boost affordability.
- Enhance the availability and accessibility of biometric-enabled devices within financial institutions and retail environments.
- Initiate focused awareness efforts to educate the community about biometric systems' potential benefits, processes, and efficiencies. This will facilitate the surmounting of cultural resistance while fostering adoption. Collaborating with community leaders to overcome cultural concerns and alleviate misconceptions around biometric security is also feasible.
- Allocate resources for the appropriate infrastructure to facilitate biometric authentication, guaranteeing the availability of technical assistance.
- Adopt strong security measures and transparent policies for data management to foster user confidence in biometric systems.
- Focus on marketing initiatives on tech-savvy younger, technologically proficient demographics while simultaneously addressing the specific concerns of the elderly.

5.5 Contributions of the Study

This research contributes to both theoretical and practical applications. The research enhances the current body of knowledge by elucidating the factors that affect user acceptance of biometric authentication in a rural South African setting. It provides a thorough framework for improving user acceptance, which can assist policymakers, service providers, and researchers implement effective e-payment systems. The research underscores the distinct socio-economic and cultural characteristics of the Thulamela Local Municipality, offering significant insights for targeted interventions.

5.6 Limitations of the Study

The study identified a couple of limitations, including:

- A limitation was noted on the geographical scope of the study as it focused solely on the Thulamela Local Municipality, limiting the generalisability of the findings to other regions. Thus, further studies may look into user acceptance of biometric systems in other municipalities or provinces to give wider consideration.
- Although a response rate of 61.7% was achieved, the sample size of 246 participants may not fully represent the diverse demographics of the entire population. Follow-up reminders or incentives could be another strategy that future studies may adopt to increase response rates.
- The study adopted a cross-sectional design, which captures a snapshot in time, which may not account for changes in user attitudes or technology perceptions over time. A longitudinal study can be undertaken in the future to check if there are changes in user acceptance as biometric systems develop.
- The study relied on self-reported data on survey responses, which may be influenced by social desirability bias.
- Although privacy concerns were noted, the study did not extensively examine users' technical knowledge of biometric security risks.

5.7 Directions for Future Research

The study makes the following pointers for future research:

- Longitudinal studies are needed to analyse variations in user acceptance over time.

- Broadening the research to include other municipalities and geographical regions for enhanced generalisation.
- To augment the model's explanatory capacity, investigate other additional aspects, like trust and security issues.
- Examine the effects of demographic variables, such as income and education, on user acceptance.

References

- Abdulkareem, A. M., & Gordon, A. (2023). Evaluating the Usability and User Acceptance of Biometric Authentication in Different Applications. *Quarterly Journal of Emerging Technologies and Innovations*, 8(2), 1–10. Retrieved from <https://vectoral.org/index.php/QJETI/article/view/5>
- Agrawal, S. (2021). Integrating Digital Wallets: Advancements in Contactless Payment Technologies. *International Journal of Intelligent Automation and Computing*, 4(8), 1-14.
- Alkhalaf, M., & Nguyen, T. (2019). Cyber threats in biometric authentication systems: A systematic review. *Cybersecurity Journal*, 14(4), 322–340. <https://doi.org/10.1108/CJ-05-2019-030>
- Andrews, T., et al. (2021). Librarians' perspectives on AI technology adoption. *Library & Information Science Research*, 43(3), 245-258.
- Ayaz, M., & Yanartaş, A. (2020). Examining the acceptance of electronic document management systems through UTAUT. *Journal of Information Systems*, 36(2), 78-91.
- Babbie, E. (2020). The Practice of Social Research. 15th ed. Boston: *Cengage Learning*.
- Babbie, E., & Mouton, J. (2019). The practice of social research (South African ed.). *Oxford University Press: Southern Africa*.
- Basare, A., Bhojak, D., & Solanki, D.R. (2023). Biometric Authentication System. *International Journal for Research in Applied Science and Engineering Technology*.
- Batucan, A., et al. (2022). Factors affecting the acceptance of e-payment systems. *International Journal of E-commerce Research*, 19(4), 101-125.
- Bhat, S.A., Islam, S.B. & Mir, M.F. Consumers' attitude toward biometric banking services: an empirical evaluation of determinants and outcomes. *Journal of Financial Services Markets*, 29, 1572–1588 (2024). <https://doi.org/10.1057/s41264-024-00285-5>
- Bhattacharjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, 25(3), 351-370.
- Bellahcene, M., & Latreche, H. (2023). E-Banking Adoption by Algerian Bank Customers: Towards an Integrated Model. *International Journal of E-Services and Mobile Applications*. 15 (1), 1-20.
- Bicakci, K., & Akbas, B. (2019). Security and usability in biometrics. *Journal of Applied Security Research*, 14(3), 123-136.
- Boo, H.C., & Chua, B. (2022). An integrative model of facial recognition check-in technology adoption intention: the perspective of hotel guests in Singapore. *International Journal of*

Contemporary Hospitality Management.

- Brown, A., & Jones, T. (2018). Digital security trends in E-payment systems. *Financial Technology Review*, 9(2), 87-101.
- Burchett, H., French, R.S., Griffin, S., de Melo, M., Joaquim Picardo, J., & Kneale, D. (2024). Developing a theory of change – the importance of rich process data and authors' insights into context, implementation and mechanisms. *Global Health Promotion*, 31, 137 - 140.
- Chen, H., Xu, K., & Wei, L. (2018). Privacy concerns in biometric data collection and security measures. *Journal of Privacy and Security*, 21(4), 112-128.
<https://doi.org/10.1016/j.jprivacysec.2018.05.002>
- Chigada, J. (2020). Privacy and security concerns in E-payment systems. *South African Journal of Information Management*, 22(1), 1-12.
- Chowdhury, M. S., Islam, M. N., & Zaman, M. H. (2021). E-payment systems and financial inclusion in emerging economies: A review of current practices and future trends. *International Journal of Financial Studies*, 9(2), 15-28.
<https://doi.org/10.3390/ijfs9020015>
- Chubuk, L.P. (2024). Impact of digital economy on business models and financial management: Institutionalization of digital transformations. *Economy Management Business*.
- Cohen, J. (2023) *Statistical Power Analysis for the Behavioral Sciences*. 2nd Edition, Routledge, New York.
<https://doi.org/10.4324/9780203771587>
- Cohen, L., Manion, L., & Morrison, K. (2018). *Research methods in education* (8th ed.). Routledge.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.
- Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research*. Sage Publications.
- Das, S. (2024). Design of secure, privacy-focused, and accessible e-payment applications for older adults. arXiv preprint arXiv:2410.08555.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
- Dhingra, K., & Mudgal, R. (2019). Expanding TAM for E-commerce platforms. *Electronic Commerce Research*, 17(2), 134-150.
- Dijmărescu, I., Iatagan, M., Hurloiu, I., Geamănu, M., Rusescu, C., & Dijmărescu, A. (2022).

- Neuromanagement decision making in facial recognition biometric authentication as a mobile payment technology in retail, restaurant, and hotel business models. *Oeconomia Copernicana*.
- Donmez-Turan, A. (2020). A critical review of technology acceptance models for biometrics. *Information Technology Journal*, 44(2), 199-215.
- Dwivedi, Y.K., Rana, N.P., Jeyaraj, A. et al. (2019). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. *Information Systems Frontiers*, 21, 719–734. <https://doi.org/10.1007/s10796-017-9774-y>
- Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics*. Sage Publications.
- Finken, S., & Heiduk, L. (2021). Factors influencing the acceptance of proximity mobile payment in Germany: The example of Apple Pay. *Journal of Payments Strategy & Systems*, 15(1), 92-108.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley.
- Fowler, F. J. (2014). *Survey research methods* (5th ed.). Sage Publications.
- Gertze, L. & Petersen, F. (2024). Factors influencing the acceptance and use of a South African online bank. *South African Journal of Information Management* 26(1), a1759. <https://doi.org/10.4102/sajim.v26i1.1759>
- Gomez-Barrero, M., Drozdowski, P., Rathgeb, C., Patino, J., Todisco, M., Nautsch, A., Damer, N., Priesnitz, J., Evans, N.W., & Busch, C. (2021). Biometrics in the Era of COVID-19: Challenges and Opportunities. *IEEE Transactions on Technology and Society*, 3, 307-322.
- Groves, R. M., et al. (2016). *Survey methodology* (2nd ed.). Wiley.
- Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2014). *Multivariate Data Analysis*. Pearson.
- Hair, J. F., et al. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- Hartono, R., et al. (2022). Security enhancements in digital wallets using biometrics. *Financial Technology Research*, 8(3), 56-75.
- Hamme, T.V., Garofalo, G., Joos, S., Preuveneers, D., & Joosen, W. (2022). AI for Biometric Authentication Systems. *Security and Artificial Intelligence*.
- Hassan, W., & Sabahat, N. (2024). Towards Secure Identification: A Comparative Analysis of Biometric Authentication Techniques. *VFAST Transactions on Software Engineering*.
- Holloway, I., & Wheeler, S. (2010). *Qualitative research in nursing and healthcare*. Wiley-Blackwell.
- Hussain, S., Gupta, S., & Bhardwaj, S. (2024). Determinants inhibiting digital payment system

- adoption: an Indian perspective. *Qualitative Research in Financial Markets*.
- Jain, A. K., et al. (2020). Advances in biometrics and implications for security. *IEEE Transactions on Information Forensics and Security*, 15, 200-215.
- Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2019). Towards a definition of mixed methods research. *Journal of Mixed Methods Research*, 1(2), 112-133.
- Jolly, C., & Shivani, F. (2024). Cross-cultural Perspectives on Digital Media and Well-being: A Narrative Review. *Eastern Journal of Psychiatry*.
- Finken, S., & Heiduk, L. (2021). Factors influencing the acceptance of proximity mobile payment in Germany: The example of Apple Pay. *Journal of Payments Strategy & Systems*, 15(1), 92-108.
- Khandekar, D., & Bendale, S. (2023). Biometrics Security System. *International Journal of Advanced Research in Science, Communication and Technology*.
- Khando, K., Islam, M.S., & Gao, S. (2022). The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review. *Future Internet*, 15, 21.
- Khayer, A. (2024). Biometrics Authentication for E-payment. *Jahangirnagar University Journal of Business Research*.
- Kusriantini, N., & Sudarsono, R. (2017). Biometric authentication methods in digital payment systems. *Journal of Digital Innovation*, 3(1), 67-82.
- Li, L., Freeman, G., & Knijnenburg, B.P. (2024). Beyond Just Money Transactions: How Digital P2P Payments (Re)shape Existing Offline Interpersonal Relationships. *Proceedings of the ACM on Human-Computer Interaction*, 8, 1 - 36.
- Liébana-Cabanillas, F.J., Muñoz-Leiva, F., Molinillo, S., & Higuera-Castillo, E. (2022). Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint. *Financial Innovation*, 8.
- Liébana-Cabanillas, F.J., Kalinić, Z., Muñoz-Leiva, F., & Higuera-Castillo, E. (2023). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information Management*, 61, 103907.
- Malatji, K., van Eck, R., & Zuva, T. (2020). Exploring user acceptance of digital payment solutions in rural areas. *Journal of Financial Technology*, 13(2), 123-139.
- Melnikovas, A. (2018). Qualitative Research: Characteristics, Patterns, and Methodologies. *Social Research Studies*, 25(3), 245-256.
- Miltgen, C. & Popović, A. & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems*. 56. 103-114. <https://doi.org/10.1016/j.dss.2013.05.010>.

- Morake, A., Khoza, L., & Bokaba, T. (2021). Biometric technology in banking institutions: 'The customers' perspectives'. *South African Journal of Information Management*, 23(1), 505–516.
- Mugenda, O.M. & Mugenda, A.G. (2003) *Research Methods, Quantitative and Qualitative Approaches*. ACT, Nairobi.
- Municipalities of South Africa. (2024). Thulamela Local Municipality: Statistical overview and services.
- Nair, A. S., & Kannan, P. (2023). Digital Payment Methods: Challenges And Opportunities. *Journal of Namibian Studies: History Politics Culture*, 37, 367-376.
- Nakisa, B., Ansarizadeh, F., Oommen, P., & Kumar, R. (2023). Using an extended technology acceptance model to investigate facial authentication. *Telematics and Informatics Reports*.
- Netshirando, V., Munyoka, W. & Kadyamatimba, A., (2024). 'Citizen perceptions of digital transformation in local municipalities: The case of South Africa', *South African Journal of Information Management* 26(1), a1804. <https://doi.org/10.4102/sajim.v26i1.1804>
- Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Pearson Education Limited.
- Nittas, V., Daniore, P., Chavez, S.J., & Wray, T.B. (2024). Challenges in implementing cultural adaptations of digital health interventions. *Communications Medicine*, 4.
- Okello Candiya Bongomin, G., Akol Malinga, C., Manzi Amani, A., & Balinda, R. (2024). Recalibrating the scope of financial inclusion through financial technologies in the digital age: the role of digital literacy as a moderator in rural Uganda. *Information Technology & People*.
- Othman, M., & Yusof, M. (2018). User acceptance of biometric authentication in online banking. *Asian Journal of Information Technology*, 15(6), 232-240.
- Pahuja, S., & Goel, N. (2024). Multimodal biometric authentication: A review. *AI Communications*. 37(4), 525-547. doi:10.3233/AIC-220247
- Patil, S., Dudhankar, V., & Shukla, P. (2024). Enhancing Digital Security: How Identity Verification Mitigates E-Commerce Fraud. *Journal of Current Science and Research Review*, 2(02), 69-81.
- Patrick, A., Burris, A., Das, S., & Noah, N. (2022). Understanding User Perspective in a University Setting to Improve Biometric Authentication Adoption. *Proceedings of the 9th Mexican International Conference on Human-Computer Interaction*.
- Perea-Khalifi, D., Irimia-Diéguez, A.I., & Palos-Sánchez, P. (2024). Exploring the

- determinants of the user experience in P2P payment systems in Spain: a text mining approach. *Financial Innovation*, 10, 1-32.
- Piotrowska, A.I. (2024). Determinants of consumer adoption of biometric technologies in mobile financial applications. *Economics and Business Review*, 10, 81 - 100.
- Punch, K. (2014). *Introduction to social research: Quantitative and qualitative approaches*. Sage.
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Saunders, M.N.K., Lewis, P. & Thornhill, A. (2019). *Research Methods for Business Students*. 8th Edition, Pearson, New York.
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Wiley.
- Sharma, S. K., Al-Badi, A., Govindaluri, S. M., & Al-Kharusi, M. H. (2020). Predicting motivators of cloud computing adoption: A developing country perspective. *Computers in Human Behaviour*, 62, 61–69. <https://doi.org/10.1016/j.chb.2016.03.073>
- Siswanto, T., et al. (2018). Examining UTAUT in the adoption of mobile payment services. *Journal of Technology Management*, 26(1), 57-69.
- South African Reserve Bank. (2020). Annual report on digital transactions in South Africa.
- Sriman, J., Thapar, P., Alyas, A.A., & Singh, U. (2024). Unlocking Security: A Comprehensive Exploration of Biometric Authentication Techniques. *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 136-141.
- Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics* (7th ed.). Pearson.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, 53–55. <https://doi.org/10.5116/ijme.4dfb.8dfd>
- Thulamela Municipality. (2022). Annual report: Infrastructure and services in Thulamela. [Online] Available at: <https://municipalities.co.za/demographic/1135/thulamela-local-municipality>
- Thomas, M., Ogalo, J. O. & Maake, B. (2023). The Effects of Cost Implications in the Adoption of Biometric Application Banks in Eldoret Town, Kenya. *Indian Journal of Image Processing and Recognition*. 3. 1-6. 10.54105/ijipr.K1633.103623.
- Tomić, N., Kalinić, Z. & Todorović, V. (2023). Using the UTAUT model to analyze user intention to accept electronic payment systems in Serbia. *Port Econ J*, 22, 251–270. <https://doi.org/10.1007/s10258-022-00210-5>
- Türker, C., Altay, B.C., & Okumuş, A. (2022). Understanding user acceptance of QR code mobile payment systems in Turkey: An extended TAM. *Technological Forecasting and*

Social Change.

- Troy, S., et al. (2013). Social influence and technology acceptance: A meta-analysis. *Journal of Information Systems*, 29(4), 192-215.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.
- Venkatesh, V., et al. (2012). Consumer acceptance and use of biometric technology in payments. *MIS Quarterly*, 36(1), 157-178. <https://doi.org/10.2307/41410412>
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2020). Consumer acceptance and use of information technology: Extending the Unified Theory of Acceptance and Use of Technology (UTAUT). *MIS Quarterly*, 34(1), 157-178. <https://doi.org/10.17705/2msq.2020.44>
- Wang, J. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, 7.
- Wang, X., et al. (2023). Factors affecting AI acceptance in e-commerce: Extending TAM. *Journal of Retail Technology*, 19(1), 56-72.
- Williams, M. D., et al. (2015). The Unified Theory of Acceptance and Use of Technology: A review and future research agenda. *International Journal of Information Management*, 29(6), 528-538.
- Xue, L., et al. (2024). Performance expectancy in technology adoption: A global analysis. *Technology Acceptance Research*, 22(1), 12-33.
- Yu, T., Wang, C., Bian, Q., & Teoh, A.P. (2024). Acceptance of or resistance to facial recognition payment: A systematic review. *Journal of Consumer Behaviour*.
- Zarco, C., Giráldez-Cru, J., Cordon, O., & Liébana-Cabanillas, F. (2024). A comprehensive view of biometric payment in retailing: A complete study from user to expert. *Journal of Retailing and Consumer Services*.

Appendices

Appendix 1: Ethical Clearance

ETHICS APPROVAL CERTIFICATE

RESEARCH AND INNOVATION
OFFICE OF THE DIRECTOR

NAME OF RESEARCHER/INVESTIGATOR:
Mr UT Ratshiedana

STUDENT NO:
17009864

PROJECT TITLE: **Developing a Framework for User Acceptance of Biometric Authentication In E-Payment Systems in The Thulamela Local Municipality.**

ETHICAL CLEARANCE NO: **FMCL/25/BIS/03/1803**

SUPERVISORS/ CO-RESEARCHERS/ CO-INVESTIGATORS

NAME	INSTITUTION & DEPARTMENT	ROLE
Dr W Munyoko	UNIVEN, Business Information Systems	Supervisor
Mr U Anokwuru	UNIVEN, Business Information Systems	Co-Supervisor
Mr UT Ratshiedana	UNIVEN, Business Information Systems	Investigator -Student

Type: **Masters Research**
Risk: **Minimal risk to humans, animals, or environment (Category 2)**
Approval Period: **March 2025 – March 2026**

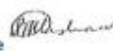
The Research Ethics Social Science Committee (RESSC) hereby approves your project as indicated above.

General Conditions
While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, please note the following:

- The project leader (principal investigator) must report in the prescribed format to the REC:
 - Annually (or as otherwise requested) on the progress of the project, and upon completion of the project.
 - Within 48hrs in case of any adverse event (or any matter that interrupts sound ethical principles) during the course of the project.
 - Annually a number of projects may be randomly selected for an external audit.
- The approval applies strictly to the protocol as stipulated in the application form. Would any changes to the protocol be deemed necessary during the course of the project, the project leader must apply for approval of those changes at the REC. Would there be deviation from the project protocol without the necessary approval of such changes, the ethics approval is immediately and automatically forfeited.
- The date of approval indicates the first date that the project may be started. Would the project have to continue after the expiry date; a new application must be made to the REC and new approval received before or on the expiry date.
- In the interest of ethical responsibility, the REC retains the right to:
 - Request access to any information or data at any time during the course or after completion of the project.
 - To ask further questions; Seek additional information; Require further modification or monitor the conduct of your research or the informed consent process.
 - Withdraw or postpone approval if:
 - Any unethical principles or practices of the project are revealed or suspected.
 - It becomes apparent that any relevant information was withheld from the REC or that information has been false or misrepresented.
 - The required annual report and reporting of adverse events was not done timely and accurately.
 - New institutional rules, national legislation or international conventions deem it necessary.

ISSUED BY:
UNIVERSITY OF VENDA, RESEARCH ETHICS COMMITTEE
Date Considered: March 2025

Name of the RESSC Chairperson of the Committee Prof TS Mashau

Signature 



Appendix 2: Survey Questionnaire

User Acceptance of Biometric Authentication in E-Payment Systems in the Thulamela Local Municipality

I am researching to identify the factors influencing the degree of user acceptance of biometric authentication for identity verification and digital access control in E-Payment systems. I also want to propose a framework to help policymakers in the Thulamela Local Municipality determine how users feel about biometric authentication. To achieve this, I kindly request that you complete a quick survey, which should not take longer than 10 minutes.

Your participation is entirely voluntary, and you can end it anytime. All data is also collected anonymously and confidentially. You declare that you will participate in this research by completing the survey.

Please get in touch with my research supervisor or me if you have any questions using the information below:

Researcher name: Unarine Terrence Ratshiedana

Email: unarine.ru94@gmail.com

Phone: 073 649 7201

Research Supervisors: Dr W. Munyoka, Mr U. Anokurwu

Email: Willard.Munyoka@univen.ac.za, Uchechukwu.Anokurwu@univen.ac.za

Instructions: Please select the most appropriate answer according to the scale provided in each question below.

Section 1: Demographic Information

- I. What is your age range?
 1. 18–24
 2. 25–34
 3. 35–44
 4. 45–54
 5. 55 and above

- II. What is your gender?
 1. Male
 2. Female
 3. Other

- III. What is your highest level of education?
 1. No education
 2. Basic education (Primary and Secondary school)
 3. Diploma/Certificate
 4. Bachelor's degree
 5. Postgraduate certificate

- IV. What is your current employment status?
 1. Employed full-time
 2. Self-employed
 3. Unemployed
 4. Student

- V. How long have you been using e-payment systems?
 1. Never
 2. Less than 6 months
 3. 6 months to 1 year
 4. 1–3 years
 5. More than 3 years

Section 2: Factors Influencing User Acceptance

Please rate the following statements using a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree).

2.1 Perceived Usefulness (PU)

1. Biometric authentication improves the security of e-payment systems.
2. Using biometric authentication reduces the risk of fraud in e-payment systems.
3. Biometric authentication enhances the efficiency of identity verification.
4. Biometric authentication is a reliable method for digital access control.

2.2 Perceived Ease of Use (PEOU)

5. Biometric authentication is easy to set up for e-payment systems.
6. I find biometric authentication simple to use for identity verification.
7. Learning to use biometric authentication is straightforward.
8. Biometric authentication requires minimal effort to operate.

2.3 Performance Expectancy (PE)

9. Biometric authentication helps me complete e-payment transactions faster.
10. Using biometric authentication improves my productivity in e-payment tasks.
11. Biometric authentication ensures accurate identity verification.
12. Biometric authentication enhances my confidence in using e-payment systems.

2.4 Effort Expectancy (EE)

13. Biometric authentication is convenient to use for e-payment systems.
14. I find biometric authentication easy to understand.
15. The process of using biometric authentication is smooth and hassle-free.
16. Biometric authentication does not require much time to complete.

2.5 Social Influence (SI)

17. People I trust recommend using biometric authentication for e-payment systems.
18. My peers' opinions influence my decision to use biometric authentication.
19. Biometric authentication is widely accepted in my social circle.
20. People important to me encourage me to use biometric authentication.

2.6 Facilitating Conditions (FC)

- 21. I have the necessary devices to use biometric authentication.
- 22. I have access to reliable internet for biometric authentication.
- 23. Technical support is available when I need help with biometric authentication.
- 24. My environment supports the use of biometric authentication.

Section 3: Adoption Intention (AI)

Please use a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) to rate the following statements.

- 25. I intend to use biometric authentication regularly for e-payment systems.
- 26. I am willing to adopt biometric authentication for identity verification.
- 27. I plan to recommend biometric authentication to others.
- 28. I am confident in my decision to use biometric authentication.

Section 4: Socio-Economic and Cultural Barriers

Please use a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) to rate the following statements.

4.1 Economic Barriers (EB)

- 29. The cost of biometric devices is too high for widespread adoption.
- 30. Maintenance costs of biometric systems discourage their use.
- 31. Biometric authentication is not affordable for small businesses.
- 32. The cost of implementing biometric systems limits their accessibility.

4.2 Cultural Barriers (CB)

- 33. Lack of awareness about biometric authentication discourages its adoption.
- 34. Cultural beliefs in my community affect the acceptance of biometric authentication.
- 35. Community perceptions influence the use of biometric authentication.
- 36. Resistance to new technology affects the adoption of biometric authentication.

4.3 Social Barriers (SB)

- 37. Concerns about data privacy discourage me from using biometric authentication.
- 38. Lack of trust in biometric authentication affects its adoption.

- 39. Limited social support for biometric authentication hinders its use.
- 40. Negative feedback from others discourages me from using biometric authentication.

Thank you for participating in this survey. Your input is valuable for our research on user acceptance of biometric authentication in e-payment systems in the Thulamela Local Municipality.

Please submit your completed questionnaire.