POLYTECHNIC UNIVERSITY OF THE PHILIPPINES QUEZON CITY

Enhancing Algorithm for Fingerprint and Face Biometric Authentication in E-Wallet Systems: A User Perspective

A Research Study

Presented to the

Information Technology Department

Polytechnic University of the Philippines- Quezon City Branch

In Partial Fulfillment
Of the Requirements for
Fundamentals of Research

By

Battung, John Paulo P.

Parungao, Rafael Joar D.

Reyes, Jarrell I.

BSIT 3-1

October 2023

TABLE OF CONTENTS

Chapter 1

THE PROBLEM AND ITS BACKGROUND

Introduction

In the 21st century, mobile technology has come a long way, going from physical buttons to touchscreens. This progress is driven by what people want and need from their devices, both in terms of how they look and the apps they use. With all this complexity, keeping mobiles safe has become very important. We've moved from using things like Personal Identification Number (PIN) and patterns as passwords to something more advanced called biometrics. This means we use unique things about a person, like their fingerprint or face, to make sure only the right people can access their mobile device. This is a big step forward in mobile security. The introduction of biometrics into mobile devices was a reaction to the drawbacks of older techniques like PINs and passwords, which were frequently erratic and insecure. The use of unique physical characteristics to ensure that only authorized users can access personal data has since become a standard security measure in modern smartphones, providing both convenience and enhanced protection. In response to the escalating challenges posed by hackers and thieves, who have become increasingly adept at exploiting vulnerabilities, mobile companies are compelled to enhance the user experience of security measures to safeguard their clients. This means not only strengthening the protective layers but also ensuring that the security features are user-friendly and seamlessly integrated into the mobile experience. Balancing robust security with user convenience is now a pivotal aspect of the mobile industry's commitment to shielding users from evolving threats.

The Philippines emerged as a pioneer in advancing digital payments by introducing mobile money in 2001. Over the years, the nation has been steadily transitioning towards a fully digital payment ecosystem, witnessing a consistent and increasing utilization of electronic payments since its initial launch. (Delos Reyes et al, 2021). E-wallet providers like GCash and PayMaya have experienced substantial development in recent times, as they've adopted state-of-the-art biometric authentication technologies. These platforms have smoothly incorporated fingerprint and facial recognition for secure access and payment verification. This innovative strategy not only improves the ease and security of digital transactions but also underscores the nation's dedication to remaining a leader in financial technology and digital progress. With the integration of biometric authentication, users can now relish the simplicity of quicker and more secure transactions, representing a notable stride in advancing the Philippines towards a cashless, digital economy.

A significant challenge for users concerning security is that, despite the adoption of biometric safeguards, malicious individuals can manipulate these features to circumvent mobile device security. This issue extends to fingerprint recognition, where, despite each user having distinct fingerprints, hackers and thieves have managed to exploit various methods to gain unauthorized access to devices. While mobile fingerprint biometrics are widely used and convenient for enhancing security, they have faced numerous issues and vulnerabilities over recent years.

However, it is crucial to address the potential usability problems and challenges that could affect the user experience. Ensuring that biometric authentication methods are not only secure but also user-friendly is paramount. Our research aims to delve into these usability issues, specifically examining the correlation between user perceptions of usability and their willingness to embrace biometric authentication. By identifying and addressing these concerns, our research endeavors to contribute to the development of more user-friendly mobile security solutions. Striking the right balance between stringent security measures and a seamless user experience remains a paramount concern for the mobile industry, as it strives to shield users from the ever-evolving threats in the digital realm.

Theoretical Framework

Technology Acceptance Model

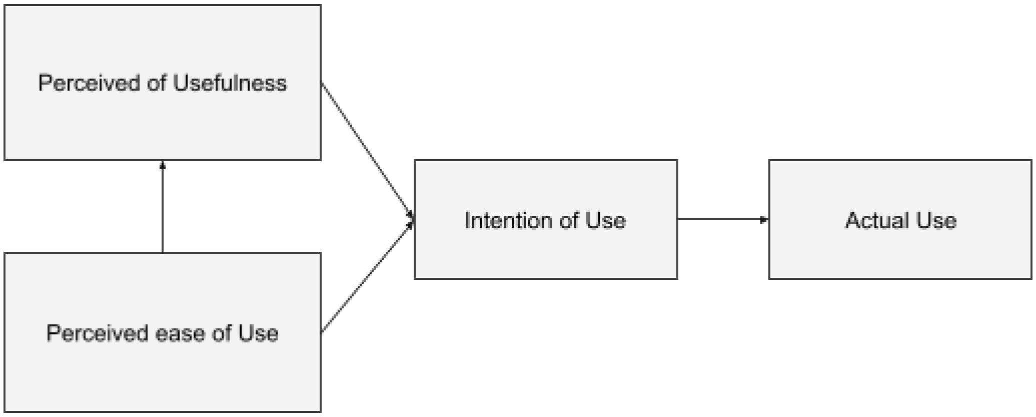

Figure 1. Technology Acceptance Model

The potential of technology to deliver benefits has long motivated IS management research to examine the willingness of individuals to accept innovative technology (Davis, 1989). The research on the adoption of technology became of primary importance in the 1980s, which coincided with the growth of the use of personal computers.

The Technology Acceptance Model (TAM) is a three-stage process where external factors trigger cognitive responses (perceived ease of use and perceived usefulness) and affective responses (attitude toward using technology/intention), influencing use behavior. TAM represents the behavior as the outcome predicted by perceived ease of use, perceived usefulness, and behavioral intention. The model has made significant theoretical contributions and practical value, allowing for the evaluation of user motivation to adopt various technologies.

Wong-In, S., Netinant, P., & Rukhiran, M. (2021) The TAM model was used in the study to examine the factors influencing the acceptance of face recognition technologies for examination attendance. The authors adopted and extended the TAM model by adding trust and security as a construct that affects perceived usefulness, attitude, and behavioral intention to use. The authors found that perceived ease of use, trust and security, and perceived usefulness significantly affect the students' behavioral intention to use biometric recognition technologies. The authors concluded that biometric recognition technologies can enhance the examination attendance system in higher education and that the TAM model is a useful tool to assess the user's acceptance of the system.

Utilisation Focus Model

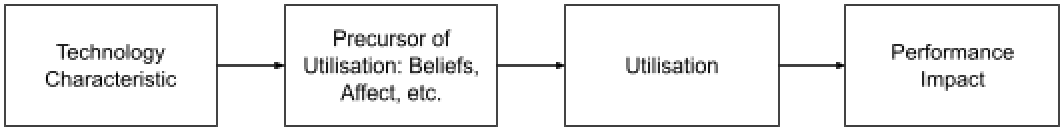
Technology Characteristic
Precursor of Utilisation: Beliefs, Affect, etc.
Utilisation
Performance Impact

Figure 2. Utilisation Focus Model

The Utilisation Focus model under Task Technology Fit (TTF) model, as depicted in above, proposes that the alignment of the task, technology, and individual characteristics plays a pivotal role in determining an individual's performance. TTF posits that the acceptance of technology is contingent upon how well the technology aligns with the requirements of the task, and the harmony between task demands, individual attributes, and technological capabilities characterizes it. In most prior research, TTF is used to gauge users' perceptions regarding the extent to which systems meet their task requirements and facilitate task execution. Research indicates that task technology fit influences users' perceptions in a task-oriented environment and yields mixed results when it comes to its impact on performance. The researchers incorporate the TTF concept as a foundational framework to elucidate the effects on learning outcomes at the individual, task, and technology levels in our model.

Clark, R. A. (2021) use the Task-Technology Fit (TTF) theory to explore the relationship between the tasks performed by mobile banking customers and the biometric technology, and how it affects their acceptance and use of the technology. They measure the TTF by assessing the perceived ease of use, trust and security, and perceived usefulness of the biometric technology. They hypothesize that TTF has a positive effect on the behavioral intention to use biometric technology with mobile banking. They test their hypothesis using structural equation modeling and find that TTF is a significant predictor of behavioral intention. They also find that TTF mediates the effects of performance expectancy, effort expectancy, and facilitating conditions on behavioral intention. They conclude that TTF is an important factor for understanding the user acceptance of biometric technology with mobile banking.

Conceptual Framework

Figure 3. The Study's Conceptual Framework

As seen in Figure 3, the researchers aimed to compile information regarding user insights in biometric authentication from various relevant literature sources. The foundation of the study will be the data that the researchers collect from respondents through survey questionnaires. To find out how much respondents agree with various problems, the researchers will conduct and provide a comprehensive survey questionnaire. Once the data is collected, it is analyzed through statistical computation by the researchers and used as the foundation for improving the biometric authentication algorithm. it will be used as the basis to improve the biometric algorithm. All gathered data and related studies will be use as basis for enhanced algorithm.

Statement of the Problem

The study sought to answer the following questions in the study of biometric authentication:

1. What is the respondents' level of agreement on the usability of fingerprint and face biometric authentication in different e-wallets in terms of:

1.1 Efficiency

1.2 Usability

1.3 Reliability

1.4 Functionality

2. What is the respondents' level of agreement with the common issues of fingerprint and face recognition in terms of:

2.1 Negative Identification

2.2 Fingerprint Placement

2.3 Data Aggregation

3. What is the level of user satisfaction with the use of facial and fingerprint recognition as biometric authentication methods in e-wallet security based on the Technology Acceptance Model (TAM)?

3.1 perceived ease of use

3.2 perceived usefulness

3.3 behavioral intention

3.4 perceived security

4. What is the extent of user preference for fingerprint and facial recognition as means to enhance the usability of e-wallets?

4.1 Value

4.2 Risk

4.3 Time preference

5. Is there a significant difference between the level of agreement of end-users in the usability of fingerprint and face biometrics in e-wallet security and their willingness to use fingerprint and facial recognition as authentication methods?

5.1 Usability Perception

5.2 Security Perception

5.3 Privacy Concerns

Hypothesis

H0: There is no significant difference between the level of agreement of end-users in the usability of fingerprint and face biometrics in e-wallet security and their willingness to use fingerprint and facial recognition as authentication methods.

H1: There is a significant difference between the level of agreement of end-users with the usability of fingerprint and face biometrics in e-wallet security and their willingness to use fingerprint and facial recognition as authentication methods.

Scope and Limitation

This study focuses on assessing user perceptions and acceptance of fingerprint and face biometric authentication in e-wallet systems. GCash and Paymaya are the specific e-wallet systems that will be used for this study. The research will take place at the Polytechnic University of the Philippines, Quezon City Branch. The respondents of this study focused on Polytechnic University of the Philippines, Quezon City Branch, selected students from 1st year to 4th year. The study will be available to the public upon completion. The selected students from different courses will be the basis of this study. This helps the researchers gather more information and useful ideas about the usability of biometric authentication in e-wallets.

Significance of the study

The use of fingerprint and face authentication in e-wallet systems has been a trend for the system's security. This study is significant as it will provide insights into the usability and security issues of fingerprint and face authentication. This study aims to contribute to the development of more effective and user-friendly e-wallet systems while also addressing potential security concerns related to biometric authentication methods. In addition, researchers want to make e-wallets better and safer, so people don't have to worry about their money. The study is intended to be beneficial specifically to the following:

For End-users/Consumers - This study aims to enhance the user experience of biometric authentication methods in e-wallet systems. By improving the usability and security of e-wallets, users can have peace of mind regarding their financial transactions.

For Students - The study holds significance for students due to their inherent involvement with technology. It offers an opportunity for students to acquire a deeper understanding of E-wallets and the intricacies of biometric authentication, thereby enhancing their knowledge in these critical areas. This knowledge can empower them to make informed decisions and navigate the evolving landscape of digital financial systems more effectively.

For Professors - The teachers/professors are the facilitators of the class. This study will give them insights about the importance of security in using e-wallets.

To E-Wallet Service Providers - This study will serve as a guide for the improvement of biometric authentication in their e-wallet systems. This will benefit them by improving their e-wallet security algorithm to make it secure and efficient. It will serve as a guide for improving biometric authentication in their e-wallet systems.

To Future Researchers: The researchers would like to welcome future researchers to develop a similar thesis about biometric authentication. This study will serve as their reference and provide insights for their future studies.

Definition of terms

Algorithm - An algorithm refers to a set of well-defined and ordered steps or procedures designed to solve a specific problem or accomplish a particular task. In this study, Algorithms are used in this study to the enhanced set of steps and procedures used for biometric authentication in e-wallets, specifically for face and fingerprint recognition.

Assessment - Assessment refers to the systematic process of collecting, analyzing, and evaluating data or information to make informed judgments or decisions. This was used to refer to the systematic evaluation of user perceptions, acceptance, and satisfaction with the biometric authentication system in e-wallets, based on data collected through surveys, interviews, and usability tests.

Biometric - This term refers to an individual's distinct physical and behavioral characteristics.

Biometric Authentication - This term refers to the process of verifying the user/person's distinct personal and behavioral characteristics.

E-Wallets - This term refers to a digital or electronic mobile application wallet, which is provided by companies to facilitate online financial transactions for consumers. This is used in this study to be the basis of a biometric authentication application.

Fingerprint - This term refers to the person's distinct ridge patterns in the person's fingers and thumbs.

Fingerprint Recognition - This term refers to the process of verifying the user's identity using their fingerprint to the stored data of the fingerprint. A person's fingerprints are a unique physical attribute.

Face Recognition - This term refers to the process of verifying a user's identity by comparing their facial features captured through the device's camera with the stored facial data in the biometric authentication system. Face recognition refers to a unique physical trait of a person.

Users - In this study, the users are used as individuals who use the e-wallets mobile application. The users of the study were the individuals who use the e-wallets such as students.

CHAPTER 2

REVIEW OF RELATED LITERATURE

Mobile Biometric

Over the past decade, several strategies have been developed and tested to ensure the reliability of using mobile devices and associated technologies. Due to its uniqueness, biometrics, which rely on specific characteristics present in every individual, is used for personal identification with fingerprint recognition being widely accepted and used on mobile devices by means of successful techniques to identify a person. In this chapter, the researchers will be providing related studies necessary to help the readers familiarize themselves with information that is relevant in the study. The researchers want to offer a deep understanding on the effectiveness of fingerprint biometrics in securing mobile devices. This will act as a guide and foundation for our very own research. Throughout this chapter, Researchers will look at the most recent research results, industry standards, and new developments in fingerprint biometrics for mobile device security. This review will set the stage for our investigation into the efficacy of fingerprint biometrics in enhancing mobile device security.

Mombeuil, C. (2020) stated that in the recent years, tech companies such as Google, Apple, and Samsung have capitalized on the distribution of smart devices, the increase in penetration of Internet, and e-commerce platforms as well as on their brand recognition and their direct access to user data to establish their mobile payment platform, representing serious challenges for the traditional payment methods. The researcher wants to investigate several key factors that could influence an increase of adoption, such as "relative convenience," "relative advantage," "perceived privacy," and "perceived security." These factors are important for understanding how experienced users make decisions regarding the adoption of mobile wallets. The researcher found out that all the independent variables in the study gives positive influence in renewed adoption intentions but among these identified factors, “relative advantage” and “perceived security” turned out to be the most influential predictors of renewed adaptation intention which proves that users' wants to use mobile wallets because of its advantage and security.

Iqbal, S., et al.,(2020) stated that digital wallet or mobile wallet applications are used to pay shopping bills using a mobile device such as a mobile phone. Digital wallet applications store payment card(s) on the client side and being compatible with most of the e-commerce applications offers numerous benefits to customers such as anytime, anywhere immediate payment facility. However, the elderly find digital payment applications difficult to operate and unsecure. Since traditional authentication mechanisms are complicated it is common for the elderly population to experience difficulty using digital payment applications. Among these difficulties are security and usability problems, which may discourage people from taking advantage of the convenience offered by digital payment systems. To resolve this, the researcher proposed a novel digital payment mechanism that makes use of the availability of fingerprint authentication on mobile devices which provides user-friendly and secure digital wallet payment facilities specifically focused to the elderly population. By Utilizing the Bluetooth technology as a means of enabling billing at the point of sale. The researchers are successful in implementing the proposed methodology that addresses the usability and security concerns of elderly users. It doesn't only satisfy them but also enhances their ease of use when engaging in digital payment transactions.

Ismail, S., & Yahaya, N. A. (2023) stated that the ongoing transition toward a cashless society in Malaysia is reshaping the payment landscape, prompting a reevaluation of existing payment methods such as physical currency, cards, and online banking. These traditional methods often necessitate the use of tangible materials such as cash, smartphones, or cards, demanding consumers to carry these physical items for everyday transactions. The users utilizing banking or credit cards find it hard to memorize their IDs and password specially when they have multiple cards. The researchers wanted to learn how Malaysian customers feel about using facial recognition technology for making transactions in their usual payments and to examine the fundamental characteristics of applications for facial recognition. These features are meant to serve as the foundation for the development of a system that will monitor and regulate the quality standards necessary for the implementation of face recognition cashless payment (FRCP) systems in Malaysia. 385 respondents were chosen at random from Malaysia's major cities and high-density state capitals for the study. Data was collected through face-to-face structured questionnaires. The initial objective of the study was to create a user acceptance model using the Product Quality Requirement Model and UTAUT2 (Unified Theory of Acceptance and Use of Technology). The results show that relative advantage has a big impact on whether or not users accept facial recognition as a form of payment (FRCP).

Sulaiman, S. N. A., & Almunawar, M. N. (2022) wanted to investigate factors that influence customers' adoption of biometric-based point-of-sale in Brunei. In order to understand how trust and a few other variables affect users' attitudes toward using biometric point-of-sale terminals for payment transactions in Brunei, the research expands on the framework of the Technology Acceptance Model (TAM). Multiple regression analysis is used in the research methodology to test the hypotheses related to these nine variables, offering a thorough and data-driven approach to understand the factors affecting user adoption. The study's findings indicate that users' decisions to accept biometric authentication for payments are greatly influenced by perceived usefulness and trust, with innovativeness and shared experiences showing a positive correlation with trust.

The COVID-19 pandemic really sped up the use of digital wallets because people had to shift to online shopping and payments due to social distancing. To understand why folks like digital wallets, there's this thorough model created by Ilieva and their team in 2023. This model looks at stuff like how useful and easy to use digital wallets are, how friends and family influence our choices, the conditions that make using them easier, whether they fit our lifestyle, and how much we trust them. They also considered factors like age, income, and education in their study. They gathered and organized customer data using both traditional number-crunching methods and more modern Machine Learning techniques to figure out how all these factors affect what people think of digital wallets. By giving us a methodical way to get our heads around what folks think and do when it comes to e-wallets, this study is pushing the envelope. What they found is that most people think digital wallets are a pretty efficient way to make payments, and they pointed out the good things about them. But some folks who weren't so keen on them had concerns about internet reliability, security issues, and fees for making payments. And the folks in the middle, who were neither here nor there, liked the idea of e-wallets but saw some downsides to using them for online payments.

The world of Financial Technology (Fintech) is always changing, and it comes with lots of new developments and challenges. Rani, M. S. B. A. (2021) took a closer look at different aspects of Fintech, such as what customers think of it, how they use it, what they worry about when using it, and how it affects their behavior. One of the big roadblocks to Fintech catching on in the short and long term is concerns about security, and a big player in this is something called the Technology Acceptance Model (TAM). Despite loads of research on trust, how useful it is, how easy it is to use, the risks, whether it works well with other stuff, and performance, security often gets the short end of the stick. But it's actually super important to make sure Fintech is secure, because it's a big deal for keeping customers safe in this growing industry, and that means we should dig into it more. A big chunk of Fintech research, mostly of the chatty kind, focuses on what customers think, using models like SERVQUAL, TAM, UTAUT, and DOI. They look at stuff like how secure it is, how dependable it is, whether it plays nicely with other things, how much it costs, how easy it is to use, how useful it is, and how well the system works. The review points out that there's a gap in research on Fintech adoption in Malaysia and says that we really need to think about what people think and also how important security is in making sure people are happy with it. Making sure personal info is safe, especially when it's being sent and stored during financial stuff, is really important to have safe Fintech for banking and money things.

In recent years, modern technology has played a pivotal role in revolutionizing financial transactions. Shin, S., & Lee, W. J. (2021) aimed to understand the patterns and security concerns surrounding electronic payments by analyzing 131 research articles published between 2010 and 2020. The results showed that during the study period, there was a significant rise in interest in and use of online payment methods and e-wallets. Particularly, as electronic payments became more common, researchers focused more on security-related topics, realizing how important it is to have strong security measures in this area. The study emphasized the need for particular security attributes, such as authenticity, non-repudiation, integrity, availability, authorization, and confidentiality, in electronic payment systems. These characteristics are thought to be essential for trustworthy and safe electronic transactions. Compared to traditional web security concerns, security issues in the world of electronic payments have become more demanding and complex. This change in emphasis highlights the necessity of increased caution and security measures in electronic payment systems. Electronic transaction providers can strengthen their security protocols and tackle the changing obstacles in the electronic payment industry by utilizing the valuable insights obtained from this review. This study lays the groundwork for future research initiatives in this field and advances our understanding of electronic payment security.

In today's ever-changing landscape of retail and banking, there's a growing demand for innovative payment methods, especially when it comes to covering medical clinic fees. Lai, Y. H. (2012) conducted a detailed investigation into the utilization of e-wallet technology, with a particular focus on how people were embracing small payment methods and the factors that drove their preferences for IC stored value cards in this context. The ultimate goal was to gain valuable insights that could guide the development of efficient small payment solutions within the local retail and banking sectors. The primary findings of the study shed light on the efficacy of the Technology Acceptance Model (TAM) in helping us understand how users perceive and intend to use e-wallets for clinic fee payments. Notably, the study revealed that user attitudes were significantly shaped by their perception of the usefulness and ease of use of these e-wallets, emphasizing the importance of offering user-friendly and practical e-wallet options, like the Taipei Easy Card, to streamline clinic fee payments in a professional setting.

In recent years, the demand for mobile wallets has seen significant growth, a trend that has been accelerated during the COVID-19 pandemic. Numerous studies have explored user intentions and perspectives in this context, shedding light on the adoption of mobile payment services. Alswaigh, N. Y., &

Aloud, M. E. (2021) advances the field by introducing a comprehensive conceptual model that combines behavioral factors with the Technology Acceptance Model (TAM). Finding the critical elements impacting users' preferences to accept mobile payments is the main goal. In order to do this, the study combines extra determinants with the TAM and the Unified Theory of Acceptance and Use of Technology (UTAUT) models. These additional variables include safety, reliability, supportive environments, and compatibility with a person's way of life. This study provides important insights into the factors influencing user behavior when adopting mobile wallet services through a thorough analysis of survey data obtained from 394 Saudi citizens via an online platform. The study's findings demonstrate the significant influence of various factors on users' attitudes and intentions regarding the adoption of mobile wallets. Notably, the acceptance of mobile wallet payments by users is directly predicted by factors such as perceived usefulness, perceived ease of use, lifestyle compatibility, and facilitating conditions. In addition to providing empirical support for the acceptance of mobile payments, this study highlights the important role that perceived advantage and lifestyle compatibility play. It also underscores the pandemic-induced change, as a significant proportion of participants adopted mobile wallet services as a result of the modified conditions brought about by COVID-19.

PHAN, T. N., HO, T. V., & LE-HOANG, P. V. (2020) conduct a research study of the Venkatesh, Morris, Davis, and Davis (2003) framework known as the Unified Theory of Acceptance and Use of Technology (UTAUT) constructs and how they interact with the security and privacy components of Bauer's (1960) Theory of Perceived Risk (TPR). The study focuses on young people in Vietnam's e-wallet usage habits, which is an important topic in the current digital environment. 200 internet users between the ages of 18 and 25 participated in the study. The data was gathered in two stages: first, through qualitative research, to create the research scale; then, through quantitative research, Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM) were used to assess the research model. The integration of the UTAUT and TPR models in this study provides important insights into the online payment landscape that are essential to researchers studying technology as well as online payment management. The examination of data from 200 youth users highlights several important conclusions. Particularly, it shows how important social influence is in influencing young people's intentions to use e-wallets for payments, even though behavioral intention appears to be less affected by security, privacy, and effort expectancy. However, the effect of favorable circumstances continues to influence e-wallet usage behavior. The study recognizes some limitations despite these insightful observations, one of which is the relatively low explanatory power of the suggested model. It suggests that future studies broaden the scope of the UTAUT and TPR models by adding more variables to improve the models' predictive ability, particularly with regard to electronic payments. Furthermore, looking into the e-payment habits and behavioral intent of the senior population could be an effective topic for research.

This study examines the use and acceptance of biometric technologies—which use different physiological or behavioral traits to identify people—among Australian victims of identity theft and misuse (Unar, Seng, & Abbasi 2014). According to Liljander, A. (2019) biometric technologies include a wide range of techniques, such as body-odor authentication, gait recognition, ear geometry, vein-pattern analysis, and keystroke dynamics, in addition to more unusual methods like fingerprint matching, facial imaging, signature recognition, retina and iris recognition, and voice recognition. Recent member surveys of the Biometrics Institute reveal that the field is expected to be dominated by voice, face, fingerprint, and iris recognition, with a growing focus on multi-modal approaches that combine multiple biometrics (Biometrics Institute 2015). According to a survey conducted by the Biometrics Institute, voice, iris, fingerprint, and facial recognition technologies are predicted to play major roles in the biometrics industry. It is also expected that multi-modal approaches, which integrate multiple biometric techniques, will become popular. The successful implementation of biometric technologies requires a thorough understanding of user acceptance. The degree to which people are willing to adopt these technologies has a big impact on how effective they are. To promote user acceptability, issues with privacy, data security, and possible health hazards need to be addressed. Novel technologies are being developed to address privacy and security issues related to biometrics, like cancellable fingerprint templates and bio cryptography.

This study examines the use and acceptance of biometric technologies—which use different physiological or behavioral traits to identify people—among Australian victims of identity theft and misuse (Unar, Seng, & Abbasi 2014). According to Liljander, A. (2019) biometric technologies include a wide range of techniques, such as body-odor authentication, gait recognition, ear geometry, vein-pattern analysis, and keystroke dynamics, in addition to more unusual methods like fingerprint matching, facial imaging, signature recognition, retina and iris recognition, and voice recognition. Recent member surveys of the Biometrics Institute reveal that the field is expected to be dominated by voice, face, fingerprint, and iris recognition, with a growing focus on multi-modal approaches that combine multiple biometrics (Biometrics Institute 2015). According to a survey conducted by the Biometrics Institute, voice, iris, fingerprint, and facial recognition technologies are predicted to play major roles in the biometrics industry. It is also expected that multi-modal approaches, which integrate multiple biometric techniques, will become popular. The successful implementation of biometric technologies requires a thorough understanding of user acceptance. The degree to which people are willing to adopt these technologies has a big impact on how effective they are. To promote user acceptability, issues with privacy, data security, and possible health hazards need to be addressed. Novel technologies are being developed to address privacy and security issues related to biometrics, like cancellable fingerprint templates and bio cryptography.

According to Riaz, S., Mushtaq, A., & Ibrar, H. (2022, May) that as biometric devices are a necessary part of everyday life, it is important to assess their security and usability. To improve security and service delivery, the United Arab Emirates implemented a facial recognition authentication system in its public transportation sector in October 2021. However, this action has sparked widespread worries about the confidentiality and security of biometric data, which has resulted in withdrawals in certain situations. The public's perception of biometric technologies, such as fingerprint, facial recognition, and iris identification, and how these perceptions might affect the technology's widespread adoption are areas of unmet research need. In comparison to iris recognition and fingerprint authentication, public transportation users in the United Arab Emirates have a poorer opinion of facial recognition technology, according to the study, which was conducted through an analysis of survey data using a comparative statistical model in SPSS. As a result, some contend that the impact of public opinion could eventually present challenges to the broad implementation of facial recognition technology. This study helps to bridge the knowledge gaps and public perceptions of biometric applications, which is important information for usability experts and promotes the adoption of biometric technology.

Hadzidedic, S., et al., (2022) wanted to focus on understanding how young individuals in Mexico and Bosnia and Herzegovina perceive and utilize various authentication methods, including text and graphical passwords, biometrics, and hardware tokens. The study aims to fill a gap in the existing literature by examining the criteria young users apply when creating text passwords. In order to do this, an online survey with 197 responses was sent out to university students in these two regions in the spring of 2019. The results show that most people believe fingerprint-based authentication to be the most practical and safe option. However, text passwords continue to be the most widely used option for unlocking computer devices. It's interesting to note that participants frequently use personal criteria—like password length and the mix of letters and special characters—while creating text passwords, which frequently follow accepted password conventions. The analysis of young adults' views and preferences regarding different authentication techniques, which reflects the growing concerns about security breaches and consequences, is what makes this study unique. Moreover, it clarifies the authentication strategies frequently employed by young people in these two particular regions—a viewpoint that hasn't been thoroughly examined previously.

Moriuchi, E. (2021) investigates consumers' intentions to use biometric facial recognition as a payment method, focusing on the trust factor associated with these innovative technologies. With the growing interest in technology innovation, organizations are collaborating with technology providers and marketers to integrate biometric systems for convenience and security. Despite the potential benefits, consumers have some conflict about using technology that requires their biometric data. Two studies that examined people's attitudes toward, and use of biometric payment systems were done in order to address these worries. The first study, which used a survey to gather data, determined the main variables affecting consumers' attitudes, trust, and use of these systems. Following the results of the initial research, the investigation presented a pair of shopping methods for additional assessment. The findings suggest that biometric payment systems in physical stores are generally preferred by customers over online platforms.

Zhang, W. K., & Kang, M. J. (2019) studied the factors influencing Chinese consumers' willingness to adopt facial-recognition payment systems. It recognizes the challenges and limitations of traditional payment methods, such as credit cards and QR codes, and highlights the advantages of facial-recognition technology in terms of efficiency, security, and user experience. Although plenty of research has been done on the technical aspects of facial recognition technology, there is still an important void regarding non-technical factors as they relate to the end user. This study focuses on the aspects of facial recognition payment that are important to consumers and the variables that influence their intentions to use this technology. The study investigates how feature variables such as security, visibility, expected effort, and social image affect the uptake of facial recognition payment systems. The results show that these factors can both directly and indirectly influence consumers' intent to use the system, depending on how valuable they believe the technology to be. The study also takes into account the moderating role that consumers' personality trait known as "Openness" plays in the relationship between security, expected effort, and usage intention. By providing insight into the user's viewpoint and the variables that can help or hinder the adoption of this advanced technology in the Chinese market, this study adds to the growing body of knowledge on facial recognition payment systems. The knowledge gathered from this study can help guide future investigations and real-world financial technology uses for facial recognition payment systems.

Instead of using fingerprint and facial authentication to improve the protection of Digital wallet, Gupta, A., Kaushik, D., & Gupta, S. (2020, May) proposes an iris-based biometric security system integrated with Canny edge detection to mitigate the limitations of existing security methods. MATLAB software is employed for simulation, and the iris-based security system is suggested for future adoption due to its potential for improved security. It offers a methodical approach to the iris-based biometric system that includes important stages such as segmentation, pre-processing, feature extraction, and matching/classification. The primary goal is to create a stronger security framework for e-wallets. Beyond digital wallets, this novel strategy promises more secure digital transactions and payment systems for the bigger financial industry.

According to Nakisa, B., et al., (2023) biometric authentication technology, which validates an individual's identity through specific physiological or behavioral traits, has garnered attention in both public and private sectors. However, its user adoption has been slower than expected. To investigate the factors influencing individual acceptance of biometric authentication technologies, specifically facial authentication devices, the researchers used a comprehensive Technology Acceptance Model (TAM) that explores novel constructs such as Personal Innovativeness (PI), Perceived Enjoyment (PE), Trust (T), and

Perceived Risk (PR). The study used face authentication devices as well as palm vein scanners for its two phases of data collection. A biometric authentication device integrated into a self-serve coffee machine was used by 100 participants in each phase. Structural Equation Modeling (SEM) was used to assess the collected data's goodness-of-fit and to evaluate the proposed model and hypotheses. The Technology Acceptance Model (TAM) was used in the study to determine participants' attitudes regarding the use of facial authentication technology in self-service scenarios. The findings indicated that while most users enjoy using facial recognition technology, user-friendly design is crucial. Its adoption is influenced by things like how much they enjoy using it, trust, and perceived risk. It is easier to use when people are enjoying it (PE), adopting it requires trust (T), but people may be hesitant to use it because of perceived risk (PR). By integrating information from this research with another related to palm vein scanners, the model was enhanced, and facial authentication became more commercially feasible.

So, imagine your home becoming smarter with sensors making things more convenient and safer. Now, picture adding a facial recognition system to boost security. To make this transition successful, we need to understand how people feel about using this technology in their homes. Strangely, there hasn't been much research on how our thoughts, needs, and social influences affect our acceptance of this facial recognition tech at home. To fill this gap, Hizam, S. M., et al., (2021) conducted a survey to find out how willing people are to use facial recognition in their smart homes. They used a model called the Technology

Acceptance Model and included two more factors: social influence and how people perceive the system's quality. They gathered data from 475 people who filled out online surveys. Then, they used fancy techniques like artificial neural networks and structural equation modeling to analyze the data. The study highlights the growing importance of facial recognition in smart homes and the need to understand how our thoughts, needs, and social influences all come together to shape our decision to embrace this technology at home.

According to Habibu, T., et al., (2022) biometric technology, like using your fingerprints or face for security, is getting popular because it's safe and easy. But what regular people think about it matters a lot. If they have worries or doubts, it can cause problems and make the technology less useful. To understand how people feel about using biometrics, According to Habibu, T., et al., (2022) prepared a survey to ask 300 people what they think. The results showed that people are generally open to using biometrics, but they are worried about their biometric data's safety. They don't want it to be shared with others, misused, or used for identity theft. To fix this, the study suggests using encryption, which means turning the data into a secret code to protect it. This helps users trust that their data is safe. It also makes the application better at spotting fraud and keeping data secure. This research is essential for Uganda's digital economy because it deals with making biometric technology secure, easy to use, and respectful of people's privacy. It will help users and companies make better decisions about using biometric applications and services.

In the realm of financial technology (Fin-tech), the adoption of biometric recognition payment devices (BRPD) has garnered significant attention as a transformative technological advancement. As part of this evolving landscape, consumers' acceptance and adoption of biometric authentication methods, such as fingerprint and face recognition, within e-wallet applications play a pivotal role. To shed light on the factors influencing users' perceptions and intentions regarding these biometric methods, Liu, D., & Tu, W. (2021) integrated the Unified Theory of Acceptance and Use of Technology (UTAUT) model with the concept of initial trust, explores key determinants affecting consumers' behavioral intention to adopt BRPD technology in their research. Demographic factors like gender, age, and knowledge levels are examined as potential moderating variables. The findings contribute insights into the interplay between user behavior and BRPD technology adoption, offering practical implications for e-wallet providers and researchers. Building on this foundation, our study aims to investigate user perceptions of using fingerprint and face recognition as authentication methods in e-wallets. In doing so, we hope to establish links and parallels between the findings of the cited study and the specific context of biometric authentication within the realm of e-wallets.

Sanchez, J. A. R., & Tanpoco, M. (2023) explore the factors determining the continuation intention of mobile wallet usage in the Philippines, with a focus on perceived ease of use, utility, security, and trustworthiness, and employing user satisfaction as a mediator. Mobile wallets gained popularity, particularly during the pandemic, but their continued usage currently confronts obstacles. To discover significant correlations between these characteristics, the study adopts a descriptive-causal design and mediation analysis. The findings highlight the significance of perceived utility, security, and trustworthiness as direct predictors of users' intent to continue using mobile wallets. User satisfaction reduces the effects of perceived usefulness and trustworthiness on continuation intention to some extent. The report emphasizes the need for FinTech companies to prioritize trust, security, and user-friendliness in order to maintain users' involvement.

Cacas, A., et al., (2022) investigated the Generation X when in comes to the usage of Gcash, a mobile wallet application in the Philippines. Perceived risk, simplicity of use, rebates, and social influence are the focus in this study as an important factors that influences Generation X’s intention to use Gcash. 385 non-user respondents were surveyed and the finding shows that the influencing factors have a beneficial effect on Generation X’s desure to use Gcash which shows connection between influencing factors and their behavioral intention. The study’s conclusion shows the importance of these elemts in Gcash adoption in Generation X. Perceived danger didn’t have positive impact. Simplicity of use, refunds, and social influence had a positive impact on their behavioral intention. Within these factors, social influence is the most significant element implying that Gcash should use this knowledge in their marketing strategy to effectively target and persuade Generation X to use their application.

Diaz, J., et al., (2022) investigated the socioeconomic profiles, platform choices, and factors influencing customer satisfaction among customers in the General Santos City, Philippines, mobile money service ecosystem. In terms of demographics, the survey showed a diversified user base, with gender, age, civil status, educational attainment, length of usage, and monthly income all indicating variety across users. It clearly shows a gender imbalance, with the majority of users being female. Users' platform preference are emphasized in this study. First place is Gcash with 96% adoption rate, PayMaya comes in second with 70%, and CoinsPh comes in third with 52% adoption rate. This data shows that Gcash is the most popular in terms of mobile wallet among local users. "System Availability" has a good effect on satisfaction of the users while "Reliability" has a negative effect. Other elements that influence overall satisfaction are convenience, security, trust, and correctness.

Vitug, E. G. (2023) explores the acceptance and use of e-wallets in Central Luzon, Philippines. The researcher focused on the elements that influence the adoption of e-wallets such as perceived utility and social uncertainty. The study highlights the problems encountered during the adoption process including network connectivity issues in payment counterparties and ICT infrastructure. The findings show that Gcash is the most preferred e wallet platform accounting 89.66% usage. Microenterprises are progressively incorporating e-wallet services into their operation with client payments accounting for 77.59% of transactions. The study shows that perceived usefulness is a primary driver of e-wallet adoption while social uncertainty being a significant influence suggesting security and trust issues. The key factors influencing customer intent are perceived trust, security of e-wallet systems and network connectivity issues.

Reyes et al., (2021) aims to identify which e-wallet application offers the most signification benefits to users based on various factors including aesthetics, benefits/rewards, ease of use, loading convenience, range of transactions, security, and service fees. An online survey was conducted users to measure customer satisfaction. Using Analytical Hierarchy Process (AHP) decision-making tool and Expert Choice software the data was analyzed. To generate the global weight for each payment option assisting as a critical element the collected criteria and local weights were utilized to assist in determining which of the three options is the most advantageous. Paymara emerged as the best pick when all these variables were considered, particularly security. It emphasizes the significance of security and user happiness in digital payment systems.

Gumasing et al. (2023) tested Gcash, PayMaya (Maya), and GrapPay for usability and customer satisfaction in their study. Usability and satisfaction are tested in each e-wallets to determine which application provides the best user experience. Online surveys were sent via Google Forms to obtain responses from 165 e-wallets users for the study. System Usability Scale (SUS) and Satisfaction Rating were asked in the questionnaire. The findings shows that the three e-wallets shows similarities in overall design, content, and organization but different in terms of usability, overall functionality, and accessibility. Gcash emerged as the top performer with the highest usability score (SUS Score = 80.55) and highest user satisfaction in functionality and accessibility. PayMaya and GradPay received lower usability and functionality score. GrabPay is the least accessible of the three. The study confirms that Gcash is the most popular e-wallet among respondents with the highlight on its strengths in usability and user experience.

Chauhan & Singh (2022) introduced an innovative approach to enhance the security of digital wallets. Since digital wallet usage has been growing and making sure that it is secured is important. Security mechanisms and approaches exist but they often have limitations ranging from modest security to poor performance. The researchers combined biometric security systems by using iris-based biometrics along with the edge detection techniques. They also wanted to improve the security of digital wallet while addressing the limitations by using edge detection. The canny-based edge detection method is used to reduce the storage space required by the biometric model and the time used for comparison processes. Improving the efficiency of biometric comparisons and reducing file sizes to optimize storage stage were the focused of the researchers. In terms of both time and space savings that solves the digital wallet security, the proposed method has proven to be effective.

The digital wallets usage in India increased by 44% when COVID-19 pandemic lockdown happened. However, this increased in adoption also brought an 86% increase in cyber-crime attacks. Undale et al. (2021), aimed to capture the security concern and comfortability when using eWallets during the pandemic. Demographic such as gender and income were also investigated if these factors influenced the adoption rate. 100 active user of eWallets were selected as respondents. Multi-method approach were used for analysis employing both traditional statistical method and the robust DCa bootsrap method. According to the findings, a sizable proportion of the respondents were concerned about eWallets' security and their discomfort with digital transactions. Security concerns were high with 44% of the respondents believing that their money wasn't safe with eWallets. 45.2% were concerned about the possibility of their accounts being hacked which shows the need to enhance the security measures of it. Surprisingly, some respondents thought that features like OTP, fingerprint recognition, and face recognition could improve the security of eWallet. Fingerprint recognition is the preference of 44.2% respondents while 7% preferred adding face recognition as additional security features.

Evolet is an E-wallet payment system with Fingerprint Authentication which designed to be an application in a smartphone for payment purposes with extra security and convenience. Instead of using physical currency, its primary aim is to replace it with virtual payment system that can accessed by smartphones which will enhance transaction convenience and security. This application allows the users to make payments using their smartphones. This is vital in today's society that prioritizes speed and efficiency. The study shows that the 6-digit passcode used by other e-wallet application can sometimes be redundant and be an inconvenient for users. Security could be compromised by people surrounding the users in that particular time. According to Wong el at. (2020), fingerprint authentication doesn't only address these concern but it also aligns with the main objective of QR code payment methods which is user-friendliness. The fingerprint-based authentication in e-wallets presents advantages with enhanced speed and convenience being the most notable. Users can securely complete transactions without having to remember their passcodes which will improve the payment experience of the users.

The conventional unimodal biometric model has been widely used in the world of wireless multimedia authentication but it is plagued with issues like susceptibility to spoofing and limited accuracy. Kumar et al. (2021), proses an innovative approach by fusing the feature of face and fingerprint recognition system which resulted in an Improved Biometric Fusion System (IBFS) that offers enhanced performance to resolve the plagued issues. This proposed system improves the authentication accuracy and effectively reduces the risk of fraudulent access. The Improved Face Recognition System (IFRS) and the Improved Fingerprint Recognition System (IFPRS) are two separate authentication that makes the IBFS. Maximally Stable External Regions (MSER) has been used to Improved Face Recognition System in order to improve facial recognition capabilities and Whale Optimization Algorithm (WOA) has been used by the Improved Fingerprint Recognition System in combination with minute features for fingerprint recognition. To optimize the IBFS model and to attain higher classification accuracy, the Pattern Net model is sued as a classification algorithm to train the IBFS by utilizing support from Vector Machines (SVM). With 99.8% positive rate and accuracy at 99.6%, the proposed fusion system produced promising results. The system incorporates cutting-edge techniques such as WOA optimization approach and MSER for feature extraction. The system achieves great accuracy by utilizing the Pattern Net model and SVM for classification with a true positive rate of 99.2% and minimal false negative and false positive values. It also has an outstanding average precision, recall, and f-measure, each with 99.8% and average recognition accuracy of 99.6%.The system also exhibits significant improvements in precision, recall, f-measure, and accuracy which improves the overall authentication system by 12.3% when trained on a larger dataset of images.

Given its ultra-lightweight encryption capabilities, the PRESENT encryption algorithm has emerged as a promising solution for protecting sensitive data in an Internet of Things (IoT) environment. However, Using block encryption algorithms like PRESENT presents a serious risk since it could unintentionally reveal security holes that hackers could use to crack encryption keys. This problem is especially noticeable when working with fingerprint templates, which frequently have a lot of zero blocks and headers, which can create unique patterns that make it simpler for malevolent actors to decrypt encryption keys. To address this critical concern, Katuk, N., & Chiadighikaobi, I. R. (2022) introduced a novel approach called the "header and zero blocks bypass method" during the block pre-processing phase.

The process of improving fingerprint images is essential to the accurate identification and verification of people's identities. Noise frequently affects the acquisition of fingerprint images, leading to the capture of low-quality images. Variations in ink uniformity and finger-to-scanner contact cause these low-quality images to produce disparities in the gray level values along the ridges and furrows. These differences can have a substantial effect on minutiae extraction algorithms' accuracy and possibly lead to the extraction of inaccurate minutiae. During post-processing, these errors consequently have an impact on the fingerprint matching procedure. Patel, M. B., et al., (2020) presented the application of normalization techniques that emerges as a crucial pre-processing step to improve the quality of fingerprint images. Normalization serves to eliminate noise and standardize the range of pixel intensity values in the acquired images. It achieves this by employing statistical measures such as mean and variance to reduce the variability in gray-level values along the ridges and valleys of the fingerprint. The results of applying a widely recognized global normalization technique are presented in this paper, and the approach is supported by empirical analysis of a fingerprint image. The findings highlight the effectiveness of normalization as a valuable enhancement process that results in noise-free fingerprint images. These improved images are ready to be used in subsequent stages of fingerprint recognition. The study's emphasis on fingerprint image enhancement via normalization emphasizes the importance of this pre-processing step in ensuring the accuracy and reliability of fingerprint recognition systems. This contribution is significant in the context of biometric authentication because it serves as a foundational component for the development of more robust and precise fingerprint recognition methods.

Popoola, O. P., & Lasisi, R. A. (2020) introduced a biometric fusion system that amalgamates fingerprint and face images to develop an Ergonomic-Based Enrolment and Verification System. The objective is to harness features from both fingerprints and faces, thereby creating a novel biometric template characterized by improved performance and an elevated level of reliability for identification purposes. The fusion approach encompasses the combination of Histogram of Gradients (HOG) and Local Binary Pattern (LBP) features derived from an individual's fingerprint and facial images. The comparison between the database template and input data is executed using Manhattan Distance, which decisively determines acceptance or rejection. The paper also delves into the development of various "matching score thresholds" to assess the interaction between False Rejection Ratio and False Acceptance Ratio, which serves as a traditional benchmark for evaluating system performance. The experiments in this study resulted in the identification of an optimal threshold range, roughly between 75% and 80%, which corresponds closely to the Equal Error Rate (EER) point. The EER, which is calculated by combining the False Accept Rate (FAR) and the False Reject Rate (FRR), is a critical indicator of system performance. This result reflects the system's robustness and adaptability to varying operational requirements, allowing for threshold adjustments to account for variations in the desired level of system confidence.

Omotosho, L., et al., (2021) introduces a robust and efficient multimodal biometric recognition system that leverages the power of combining face and iris recognition for enhanced performance. Multimodal biometric systems are designed to address the limitations of unimodal systems by integrating multiple biometric modalities into a unified approach. However, such integration often leads to increased complexity and higher-dimensional feature sets. To tackle these challenges, the authors have developed a biometric recognition system based on convolutional neural networks (CNNs) that handles feature extraction, fusion at the feature level, training, and matching. Preprocessing steps to standardize and normalize input images are followed by a sequence of convolutional layers within the CNN. The system was tested with a dataset of 700 iris and facial images, 600 for training and 100 for testing. This experimental study's results are very promising, with a remarkable recognition accuracy (RA) of 98.33% and an impressively low equal error rate (EER) of 0.0006% at a learning rate of 0.0001. The results show that multimodal biometric systems have the potential to be a reliable and effective solution for real-time authentication needs. This system significantly improves biometric authentication performance by utilizing CNN-based approaches for feature extraction, training, and testing. The reduction in complexity and dimensionality helps to improve recognition accuracy even more. This technology has a lot of potential for use in access control and personal identification applications.

Fingerprint recognition has become a vital component in modern identification, gradually supplanting traditional methods. This technology relies on the unique ridge and valley patterns found on fingertips. Nonetheless, the quality of fingerprint images can vary significantly, presenting challenges for accurate identification. To address this challenge, Socheat and Wang (2020) proposed a three-step approach to tackle these issues. The researcher's method begins by improving image quality with brightness and Gabor filters, with a focus on darkening ridgelines to provide clearer ridge patterns. Following that, minutiae points are extracted and refined from binary-format fingerprint images to correct any anomalies. Finally, matching algorithms compare minutiae results with a database to confirm an individual's identity. This approach ensures the biometric system's robustness by addressing image quality, minutiae extraction, and matching algorithms. Because of its dependability in fingerprint recognition, minutiae-based matching is recommended.

Biometric systems, which authenticate individuals based on their unique physiological characteristics, face various challenges when relying on a single trait. Multimodal biometric systems offer a promising solution by integrating information from multiple sources. Kant and Chaudhary (2021) introduced a novel multimodal biometric system that combines finger knuckle print, fingerprint, and palmprint at the match-score level. This approach improves authentication reliability and robustness, addressing challenges like large-scale population coverage, noisy sensor data, and security issues. Experimental results support the system's effectiveness in terms of key performance metrics, including False-Accept-Rate (FAR), False-Reject-Rate (FRR), and Genuine-Accept-Rate (GAR). By combining multiple biometric traits and match-score fusion, this study demonstrates the potential of multimodal biometrics to enhance accuracy and security in biometric authentication systems. Kant and Chaudhary's multimodal biometric system offers a robust solution to the limitations of unimodal systems, showing promise in improving the reliability of biometric authentication and addressing various challenges in this field.

Since the events of September 11, 2001, biometric technology has gained prominence in enhancing security measures. One significant advancement in this field is the incorporation of multiple biometric traits, which addresses limitations of unimodal systems such as non-universality, noisy data, and spoof attack vulnerability. Sujatha et al. (2021) presented a novel multimodal biometric algorithm that incorporates Genetic Algorithms and Particle Swarm Optimization for system optimization. This optimization primarily focuses on lowering false acceptance and rejection rates while also improving accuracy. The selected biometric traits for integration include iris, finger vein, and fingerprint recognition, known for their reliability. The study utilizes the SDUMLA-HMT database for experiments, evaluating the algorithm's performance using metrics like false acceptance rate, false rejection rate, equal error rate, and accuracy. This study emphasizes the importance of multimodal biometric systems in improving authentication by combining multiple traits. It demonstrates the effectiveness of score-level fusion and optimization methods in improving system accuracy and security, presenting a promising path for biometric technology development.

T. Kumar et al. (2019) introduced the Improved Biometric Fusion System (IBFS), which combines fingerprint and face recognition subsystems. This system incorporates the Atmospheric Light Adjustment (ALA) algorithm to enhance image quality. The Improved Fingerprint Recognition System (IFPRS) uses Genetic Algorithms with minutiae features, while the Improved Face Recognition System (IFRS) employs Speed Up Robust Feature (SURF). An Artificial Neural Network (ANN) serves as the classifier. To assess its efficiency, the study evaluates quality-based parameters and uses optimization techniques like Particle Swarm Optimization (PSO) and Bacterial Foraging Optimization (BFO). The results show that the proposed model outperforms other techniques, achieving a 2% accuracy improvement. The ALA algorithm significantly contributes to image quality and, when combined at the score level, leads to a 99.1% accuracy rate. Compared to PSO and BFO, this approach results in a 2% and 4% accuracy improvement, respectively, along with a 5% increase in False Acceptance Rate (FAR) compared to BFO and a 1% increase compared to PSO. These improvements are consistent across various evaluation metrics. The study suggests the potential for incorporating iris recognition alongside face and fingerprint recognition to enhance the robustness of IBFS using artificial intelligence concepts.

The last three decades have seen a significant surge in research aimed at advancing biometric systems, encompassing the realms of fingerprint, voice, iris, facial recognition, and innovative biometric techniques. Developing effective biometric recognition systems involves addressing the multifaceted process of handling variable data, which includes capturing biometric information from sensors, preprocessing, feature extraction, biometric identification, labeling, verification, and clustering. The entire process leverages image processing, pattern recognition, machine learning, and artificial intelligence to analyze sensor data from various perspectives. Ghosh, U. B., et al., (2022) wanted to offer an overview of the current state of biometric systems, to shed light on strategies for overcoming challenges, and outline potential research avenues. The researchers particularly emphasizes the evolution of different biometric pattern detection and recognition approaches. The results and analysis section includes two critical segments: the first section introduces a mathematical derivation for enhancing fingerprint recognition, while the second section presents a comparative analysis of various iris recognition approaches. Additionally, the discussion explores the latest biometric recognition approaches in the context of wearable devices and acquisition tools. Finally, it provides an overview of different metrics, their corresponding accuracies, and their capacity to differentiate individuals based on features derived from diverse biometric detection methods.

Alsaadi (2021) Authenticating or identifying persons automatically based on their unique physical or behavioral traits is known as biometrics recognition. As a terminology, biometrics refer to the Greece words 'Bio' which means (life) and 'Metrics' which means (measure). characteristics are unique for each individual and cannot be stolen, plagiarized or 100% identical even among twins. Each human being is born with his/her unique observed characteristics such as face. Therefore, we categorize people based on their inherent characteristics. The use of an individual's property, such as ID cards and PINs, is another way to verify their identification. To illustrate, researchers provided an example where an individual attempts to access their bank account or engage in other online activities by using a combination of their username and password. This approach is contingent on the individual's knowledge. Assessing a person's behavior is the last step in determining their authenticity. These recognition systems have drawn a lot of attention from academics since they are user-friendly, more affordable than physiological features, and challenging to imitate someone else's typing habits. It makes sense to use these authentication techniques rather than PINs and passwords, which can be easily forgotten or lost.

El-Shafai (2021) stated that the use of biometric identification for access control in many different systems and applications has developed quickly. It is essential for protecting original templates from unwanted access. The categories of physical and logical features used in biometric identification include fingerprints, speech patterns, and keystroke patterns in addition to aspects like facial features and fingerprints. By validating the distinct properties of the human body, these strategies guarantee secure access to services. Cryptographic keys have traditionally been protected by tokens and passwords, but the practice of using the same passwords across many applications puts users' privacy and security at danger. Employing authentication techniques like PINs and passwords, organizations try to safeguard their data and service networks. More recently, technology like magnetic cards and PINs have improved security.

According to Abazi, B., Qehaja, B., & Hajrizi (2019), biometric authentication serves as a means to verify the identity of a user on a given device, granting access only upon successful verification of an inherent factor through an authentication mechanism. This method proves to be highly effective in enhancing security for mobile devices, effectively thwarting unauthorized access to sensitive data. The authors also distinguish between two primary types of biometric recognition: physical and behavioral biometrics. Physical biometrics rely on identifying individuals through their physical attributes, such as fingerprints, facial features, or hand characteristics (Bhattacharyya et al., 2009). In contrast, behavioral biometrics center around the unique behavioral traits that characterize a user, encompassing aspects like writing style, voice patterns, and signatures (Bhattacharyya et al., 2009). Abazi and colleagues conducted a study involving various performance measurements on different biometric methods to assess their error rates. The results indicated that, under normal conditions, iris recognition emerged as the most accurate form of authentication, followed by keystroke dynamics, face recognition, fingerprint recognition, with voice recognition showing the highest error rate among the methods tested.

Weichbroth and Łysik (2020) conducted research aimed at fostering a broader discussion among researchers and practitioners regarding the escalating mobile security threats posed by the infiltration of smartphones, tablets, and other mobile OS-enabled devices by malware apps. These devices serve as repositories for sensitive data, and the proliferation of smartphones and the mobile workforce has led to a direct increase in mobile device attacks. While researchers acknowledged the risks linked to physical and social factors, the majority of respondents in the study favored the utilization of built-in methods to counteract the adverse effects of malicious software and social-engineering scams. The study's findings contribute to the mobile security theory by identifying and investigating various concerns related to threats and best practices, offering practical applications at both individual and enterprise levels. Furthermore, the research underscores the importance of comprehending the factors influencing users' intentions and motivations to enhance the security of mobile applications.

Zaidi et al. (2021) highlighted the vulnerabilities associated with conventional security methods. First of all, these techniques frequently require users to use plain passwords that are simple to guess. By trying popular passwords, unauthorized users may take advantage of this. Second, the practice of shoulder-surfing, in which an outsider watches someone enter a password or PIN, presents a serious security danger. Once the attacker has this information, they can access the device even if the owner is not holding it. Notably, PINs have lost some of their appeal among users, mainly because many people find it unpleasant to constantly type the code to access their devices (Lee and Lee, 2017b).

Due to its potential for enhanced security, the use for Biometric authentication has been increasingly adopted using unique physical or behavioral characteristics. According to Ahmed, I., & Asghar, A. (2023) that while all five techniques (fingerprint recognition, facial recognition, iris recognition, voice recognition, and hand geometry) have potential for authentication in healthcare, their suitability varies depending on specific circumstances. Fingerprint recognition was found to be widely acceptable due to its ease of use and cost-effectiveness, despite concerns related to data privacy. Fingerprint is highly sensitive and personal, and the misuse of this data can lead to serious privacy breaches. Since stolen biometric information cannot be changed, unlike passwords, there is concern that it presents special risks. The likelihood of fooling fingerprint scanners has increased due to fingerprint replication from multiple sources. Artificial fingerprints that were created using stolen fingerprint database information have occasionally been used to get around security measures. This emphasizes how important it is to protect biometric data, whether it is being stored or sent. The study's findings present a fascinating chance for improving security and through the use of two or more methods, digital healthcare authentication accuracy can be increased. methods, also referred to as MFA (multi-factor authentication). By utilizing the advantages of several biometric methods, MFA can produce a more robust and reliable technology, greatly reducing the dangers of single-factor authentication methods.

The use of fingerprint authentication technology has gained significant attention due to its focus on security and control within digital authentication systems. Harikrishnan, D., et al (2021) stated that to address vulnerabilities, various authentication methods like biometric cryptosystems, cancellable templates, and bio-hashing have been developed. This paper introduces a novel FPGA-based fingerprint authentication system aimed at enhancing accuracy. It begins with the generation of a finger code template (FCT) through a transformation function applied to finger code and a biometric key derived from a randomization process. The second phase involves creating an 80-bit extended finger code (efc) from 40-bit binary strings and random numbers generated by the True Random and Time Stamp Generator (TRSG). The efc is then compared to stored primary data in a database, resulting in reduced complexity and LUT utilization, enhancing the biometric authentication system's performance. With increasing demand for enhanced security and person identification in various applications, such as electronic payments and data management, biometric features like fingerprints have gained popularity. These systems are appealing due to their reliability, quick response time, and user-friendly nature. In this context, fingerprint biometrics offer a well-established and dependable solution. As the need for secure personal verification and individual confirmation techniques continues to grow, personalized identification methods become crucial. Researchers have explored biometric recognition methods, including those based on PRNU and contactless line scanning. Biometric technologies require an initial one-time enrollment of an authorized user's fingerprint(s) for authentication, with the fingerprint data stored securely in a database. To create cost-effective and flexible hardware-software co-design systems, this work explores FPGA-based architectures as alternatives to traditional, expensive personal computer platforms. The aim is to ensure real-time performance, adaptability for continuous improvements, reliability, security, and cost-efficiency.

There are several researches that proposed a way to enhance the security and performance of fingerprint biometric templates using symmetric hashing. Symmetric hashing is a process of transforming data using a specific algorithm and a shared key. Ajish, S., & Kumar, K. A. (2020) proposed a modified symmetric hash function that is a combination of salting and non-invertible transformation. The experiments used in the study to assess the updated symmetric hash algorithm revealed considerable improvements in both accuracy and security when compared to earlier techniques. In order to address concerns about reversibility and linkability, the improved technique strengthens the security of the hashed templates while simultaneously improving the precision of fingerprint template matching during authentication.

To test the fingerprint for security, it is also proposed to be used in mobile internet voting systems. According to Ajish, S., & AnilKumar, K. S. (2021) it is possible to use biometric methods to authenticate the voter with the use of mobile internet voting systems. The biometric image can either be processed at the mobile device to create the biometric template and send it to the server, or it can be encrypted at the mobile device before being sent to the server. The technique must typically be simplified when using biometrics on mobile devices in order to account for the battery life and CPU processing power limitations. Wavelet-based AES encryption is demonstrably superior to AES encryption and template production, according to the experimental examination of three methods (AES encryption, wavelet-based AES encryption, and biometric template generation). The security analysis of the three approaches reveals that the protection offered by the biometric template is surpassed by that of AES and wavelet-based AES encryption.

Many researchers have focused on enhancing the ability to recognize fingerprint patterns under adverse conditions. For example, Wang et al., (2010) suggested the adaptive image pre-processing method. This proposed technique aimed to improve the clarity and quality of fingerprint image in order to determine the minutia extraction’s accuracy and reliability in an automatic fingerprint recognition system. Using a minutiae matching technique in an embedded system context, Hariyanto et al. (2015) proposed a hardware-based artificial neural network for effective fingerprint pattern analysis. This hardware sped up and increased effectiveness of the matching process. An image enhancement approach was put forth by Jain et al. (Jain et al., 2016) to enhance the quality of newborn baby fingerprints and enable identification of infants older than four weeks. In parallel, Feng et al. (Feng, Li, & Wang, 2016) presented a user identification system that makes use of unique fingerprint data and uses MD5 to secure critical data. The test results showed how more trustworthy, secure, and easily accessible this authentication mechanism was. Silasai, O., & Khowfa, W. (2020) stated that the practical attacks on biometric recognition approaches available presently are stated along with the future work of biometric authentication. As a result, to improve accuracy and to enhance resistance against many types of attack on mobile devices, dynamic authentication with machine learning and deep learning techniques and applying biometric as two-factor authentication should be considered.

CHAPTER 3

METHODOLOGY

Research Design

This study aims to enhance an algorithm used in biometric authentication by assessing user perceptions and acceptance of face and fingerprint biometric authentications in e-wallets. The research design used is descriptive research design. The quantitative research design is a type of research that focuses on collecting numerical data and using statistical methods to analyze and interpret the data.

Source of Data

The target respondents for this study will be students from the Polytechnic University of the Philippines Quezon City Branch. The student population size is estimated to be *number* from the following courses: Bachelor of Science in Information Technology, Bachelor of Science in Business Teacher's Education, Bachelor of Science in Business Administration Major in Marketing Management, Bachelor of Science in Business Administration Major in Human Resource Development Management, Bachelor of Science in Business Administration Major in Entrepreneurship, Bachelor of Public Administration Major in Public Financial Management, and Diploma in Office Management Technology.

Taking the estimated number of the population and using the formula to determine the sample size came to a total of *number of students* which are all equally divided into the 7 courses.

Table 1

Sample Size Per Course

SAMPLE SIZE PER COURSE		
COURSE	**SAMPLE**	**%**
Bachelor of Science in Information Technology		
Bachelor of Science in Business Teacher’s Education		
Bachelor of Science in Business Administration Major in Marketing Management		
Bachelor of Science in Business Administration Major in Human Resource Development Management		
Bachelor of Science in Business Administration Major in Entrepreneurship		
Diploma in Office Management Technology		
Bachelor of Public Administration Major in Public Financial Management		
TOTAL:		**100%**

The sampling technique used in this study is purposive sampling. According to Nikolopoulou (2022), purposive sampling is defined as a non-probability sampling technique wherein units are selected because they have characteristics that are needed in the sample. This sampling method will be used for the study to focus on respondents with the specific criterion, and allow a smaller sample of respondents. The researchers believe that this is the appropriate method of sampling for this study as the target respondents are the best respondents for the data needed for this study. The following criterion was used by the researchers in selecting the target respondents for this study: (a) respondents that have used the face and fingerprint biometric authentication in GCash and or Paymaya.

The researchers collected the data from the population of Polytechnic University of the Philippines, Quezon City Branch excluding the university faculty and staff. The proposed study would solely focus on the students from the seven mentioned courses in the university who have used face and fingerprint biometric authentication in GCash and or Paymaya.

Research Instrument

The study's research instrument is a survey questionnaire that is aligned with the study's statement of the problem. The survey questionnaire would be composed of n () parts. The survey questionnaire comprises the demographics of the respondents, the respondents' level of agreement on the usability of fingerprint and face biometric methods in e-wallet systems in terms of (1) efficiency, (2) usability, (3) reliability, (4) and functionality, the respondent's level of agreement with the common issues of fingerprint and face recognition in terms of (1) negative enrollment, (2) fingerprint placement, (3) and data aggregation, the respondent's level of agreement on using face and fingerprint recognition as biometric authentication methods in e-wallet security based on the Technology Acceptance Model, and the respondent's degree of preference for fingerprint and face recognition in enhancing the usability of e-wallets, respectively. The researchers will use an online survey questionnaire through Google Forms which will be distributed to the respondents.

Data Gathering Procedure

The researchers will create an online survey questionnaire for the collection of data that is relevant to the study. The said questionnaire will be created and administered through Google Forms, which then will be distributed to the respondents. The future respondents of the study will be given a brief orientation before the link to the survey questionnaire is distributed. Below is a thorough explanation of the process of the data collection:

1. The researchers will ask the participants for their consent, their approval of the survey questionnaire, and briefly orient the participants on the nature of the study. Participants will also be assured of the safety of their personal information.

2. The researchers will then begin to distribute the link to the online survey questionnaire either through email or social media accounts of the participants who have given their consent to participate in the study. The use of the participants' email and social media accounts is solely for the distribution of the survey questionnaire.
3. The researchers will give ample amount of time for the participants to complete the survey.
4. The completed questionnaires will be compiled and stored digitally through Google Sheets. Each answer from the survey will be measured by the researchers by statistical analysis for the percentage and weighted mean for the data to be interpreted and analyzed.

Ethical Consideration

The researchers will ensure that all respondents participating in the study are aware of the nature and focus of the topic and will be informed that their answers in the survey questionnaire will only be used as variables for the researchers to measure the scale of their responses. The privacy of the respondent's personal information will be discussed ensuring that it will remain strictly confidential, no personal information such as names, email, and even phone numbers will be kept by the researchers for external use, in compliance with the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) which protects the fundamental human right to privacy in communication. The researchers will ensure that the respondent is in a safe environment, such as the comfort of their homes, a private establishment, and or within the campus. The researchers will ensure the safety of the respondents wherein they will not be harmed nor be in any form of danger, as well as ensuring the great physical and mental state of the respondents so they may complete the survey without discomfort from external factors.

Data Case Analysis

Data that has been gathered from the collected responses of the respondents will be interpreted using statistical methods. The statistical analysis method that will be used by the researchers is the percentage & frequency, and weighted mean.

A. Percentage and Frequency will be used to calculate the demographic profile from the study's respondents, the formula for the percentage and frequency:

$$P = fn\, x\, 100$$

Wherein:

p = percentage

f = frequency

n = total number of respondents

$$F = nN$$

Wherein:

n = the total number of responses

N = the total number of respondents

B. Weighted Mean will be used to determine and measure the response to the questions from the survey questionnaires, profiles such as age and identification of the respondents are excluded for this method, the formula for weighted mean:

$$Mean \;=\; \sum fn$$

Wherein:

f = number of occurrences from the number of respondents

Mean = population mean or total score

n = the number of sources observed from the respondents

C. One-Way ANOVA or one-way analysis of variance, is used to ascertain whether any variations between them are statistically significant. the averages of two or more separate, unconnected groups. (Statistical Laerd, 2018). This will used to determine a significant difference in the responses of the respondents in the survey questionnaire.

Table 3

Likert Scale - Level of Agreement

Numerical Value	**Scale**	**Verbal Interpretation**	**Description**
5	4.20 - 5.00	Strongly Agree	The respondents strongly agree with the statement
4	3.40 - 4.19	Agree	The respondents agree with most of the statement's claims
3	2.60 - 3.39	Neutral	The respondents neither agree nor disagree with the statement's claims
2	1.80 - 2.59	Disagree	The respondents disagree with the statement
1	1.00 - 1.79	Strongly Disagree	The respondents strongle disagree with the statement

A Likert scale is a rating scale that is used to measure opinions, attitudes, or behaviors (Bhandari and Nikolopoulou, 2020). The researchers will use the Likert scale as it is believed to be the appropriate method of scaling and measuring future data from the responses of the respondents from the survey questionnaire. The researchers will use the Likert scale with a five-point rating scale to give a sufficient understanding of the responses of the respondents and their interpretation. Table 3 corresponds with the level of agreement that will be gathered from the respondents that will be tallied according to the result once the survey is

REFERENCES

Abazi, B., Qehaja, B., & Hajrizi, E. (2019b). Application of biometric models of authentication in mobile equipment. IFAC-PapersOnLine, 52(25), 543–546. https://doi.org/10.1016/j.ifacol.2019.12.602

Ahmed, I., & Asghar, A. (2023). Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare. International Journal of Responsible Artificial Intelligence, 13(7), 1-12. https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/7

Alswaigh, N. Y., & Aloud, M. E. (2021). Factors affecting user adoption of e-payment services available in mobile wallets in Saudi Arabia. International Journal of Computer Science & Network Security, 21(6), 222-230. https://koreascience.kr/article/JAKO202121055557980.page

Cacas, A., Diongson, M. B. A., & Olita, G. M. (2022). Influencing Factors on Mobile Wallet Adoption in the Philippines: Generation X's Behavioral Intention to Use GCash Services. Journal of Business and Management Studies, 4(1), 149-156. https://al-kindipublisher.com/index.php/jbms/article/view/2911/2655

Diaz, J., Viray, A., Cruz, L. D., & Tabudlong, J. (2022). Factors Affecting Customer Satisfaction on Mobile Money Services (Gcash, PayMaya, and CoinsPh) in General Santos City, Philippines. https://www.researchgate.net/publication/368904869_Factors_Affecting_Customer_Satisfaction_on_Mobile_Money_Services_GcashPayMaya_and_CoinsPh_in_General_Santos_City_Philippines eBusiness@Newcastle. (n.d.). Task-Technology Fit - TheoryHub - Academic theories reviews for research and T&L. https://open.ncl.ac.uk/theories/3/task-technology-fit/

eBusiness@Newcastle. (n.d.). Technology Acceptance Model - TheoryHub - Academic theories reviews for research and T&L. https://open.ncl.ac.uk/theories/1/technology-acceptance-model/

eBusiness@Newcastle. (n.d.). Unified Theory of Acceptance and Use of Technology - TheoryHub - Academic theories reviews for research and T&L. https://open.ncl.ac.uk/theories/2/unified-theory-of-acceptance-and-use-of-technology/

Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. (2021). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9439504

El-Shafai(2021) Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications: A Review 2021. https://www.researchgate.com/profile/Israa-Alsaadi-2/publication/348662448_Study_On_Most_Popular_Behavioral_Biometrics_Advantages_Disadvantages_And_Recent_Applications_A_Review/links/6009c63b299bf14088b188e8/Study-On-Most-Popular-Behavioral-Biometrics-Advantages-Disadvantages-And-Recent-Applications-A-Review.pdf

Ghosh, U. B., Sharma, R., & Kesharwani, A. (2022). Symptoms-based biometric pattern detection and recognition. In Augmented Intelligence in Healthcare: A Pragmatic and Integrated Analysis (pp. 371-399). https://link.springer.com/chapter/10.1007/978-981-19-1076-0_19

Gupta, A., Kaushik, D., & Gupta, S. (2020, May). Integration of biometric security system to improve the protection of digital wallet. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3595302

Habibu, T., Luhanga, E. T., & Sam, A. E. (2022). Assessment of how users perceive the usage of biometric technology applications. Recent Advances in Biometrics, 45. https://www.intechopen.com/chapters/80525

Harikrishnan, D., Kumar, N. S., Joseph, R. S., Nair, K., Nishanth, R., & Joseph, A. J. (2021). FPGA implementation of fast & secure fingerprint authentication using trsg (true random and timestamp generator). Microprocessors and Microsystems, 82, 103858. https://www.sciencedirect.com/science/article/abs/pii/S0141933121000375

Hizam, S. M., Ahmed, W., Fahad, M., Akter, H., Sentosa, I., & Ali, J. (2021). User behavior assessment towards biometric facial recognition system: A SEM-neural network approach. In Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 2 (pp. 1037-1050). https://link.springer.com/chapter/10.1007/978-3-030-73103-8_75

Huining Li University at Buffalo and the State University of New York. (n.d.). VocalPrint | Proceedings of the 18th Conference on Embedded Networked Sensor Systems. ACM Conferences. https://dl.acm.org/doi/abs/10.1145/3384419.3430779

Ilieva, G., Yankova, T., Dzhabarova, Y., Ruseva, M., Angelov, D., & Klisarova-Belcheva, S. (2023). Customer Attitude toward Digital Wallet Services. Systems, 11(4), 185. https://www.mdpi.com/2079-8954/11/4/185

Ismail, S., & Yahaya, N. A. (2023). AN EXPLORATORY STUDY OF HUMAN BEHAVIOR TOWARDS INTENTION TO USE FACIAL BIOMETRIC PAYMENT AMONG MALAYSIAN CONSUMERS. International Journal of Technology Management and Information System, 5(2), 16-29. https://myjms.mohe.gov.my/index.php/ijtmis/article/view/22628

Iqbal, S., Irfan, M., Ahsan, K., Hussain, M. A., Awais, M., Shiraz, M., ... & Alghamdi, A. (2020). A novel mobile wallet model for the elderly using fingerprint as an authentication factor. IEEE Access, 8, 177405-177423. https://ieeexplore.ieee.org/abstract/document/9201279/

Katuk, N., & Chiadighikaobi, I. R. (2022). An Enhanced Block Pre-Processing of PRESENT Algorithm for Fingerprint Template Encryption in the Internet of Things Environment. International Journal of Communication Networks and Information Security (IJCNIS), 13(3). https://d1wqtxts1xzle7.cloudfront.net/88495993/486-libre.pdf?1657613029=&response-content-disposition=inline%3B+filename%3DAn_Enhanced_Block_Pre_processing_of_PRES.pdf&Expires=1699183850&Signature=dvNgL5radnpxqaGu8r0eg-pxSIs9xPqvHhN1vL2n53WtazRVqakvBJuQE-BLeOycF8XE23w1Z0nwPixQPi1~YTFJF1ZuNvsPg1Hxa8lhuHuZiY3CHOmsxFeE73Lha~ujArRIKcBUBspvv~4x6rvkTSbRXNk0-XjcW3~l47VKvUNvRpJq-rYZ0Gz38Cr52XRIe9wt5JwRRy5NoTrF2Zu1LZA8BUTCJSR0h1qA6M6O70CRaDwFn~GLG0toucYXS~bDcd4ofoult4NcjDWBMc~9zd6n1txt-xRg2cS~XtxgjXM8ZGJNq2xRIX04184Bn93GjvcbuCheajVGFwM4QuEI5g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Kumar, T., Bhushan, S., & Jangra, S. (2021). An improved biometric fusion system of fingerprint and face using whale optimization. International Journal of Advanced Computer Science and Applications, 12(1). https://www.researchgate.net/profile/Tajinder-Kumar-Saini/publication/349026768_An_Improved_Biometric_Fusion_System_of_Fingerprint_and_Face_using_Whale_Optimization/links/60642b50a6fdccbfea1aa30b/An-Improved-Biometric-Fusion-System-of-Fingerprint-and-Face-using-Whale-Optimization.pdf

Kumar, T., Bhushan, S., & Jangra, S. (2019). An improved biometric fusion system based on fingerprint and face using optimized artificial neural network. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(11). https://www.researchgate.com/profile/Tajinder-Kumar-Saini/publication/33602207

7_An_Improved_Biometric_Fusion_System_Based_on_Fingerprint_and_Face_using_Optimized_Artificial_Neural_Network/links/5d8b45a5299bf10cff0b7cd4/An-Improved-Biometric-Fusion-System-Based-on-Fingerprint-and-Face-using-Optimized-Artificial-Neural-Network.pdf

Liljander, A. (2019). Attitudes towards biometric authentication technologies between cultures: acceptance in Finland and Brazil. https://jyx.jyu.fi/handle/123456789/66405

Liu, D., & Tu, W. (2021). Factors influencing consumers' adoptions of biometric recognition payment devices: combination of initial trust and UTAUT model. International Journal of Mobile Communications, 19(3). https://www.inderscienceonline.com/doi/pdf/10.1504/IJMC.2021.114324

Lai, Y. H. (2012). The study of technology acceptance for e-wallets application of clinic fees payment. https://www.scirp.org/html/12-8201759_24894.htm

Moriuchi, E. (2021). An empirical study of consumers' intention to use biometric facial recognition as a payment method. Psychology & Marketing, 38(10). https://onlinelibrary.wiley.com/doi/abs/10.1002/mar.21495

Nakisa, B., Ansarizadeh, F., Oommen, P., & Kumar, R. (2023). Using an extended technology acceptance model to investigate facial authentication. Telematics and Informatics Reports, 12. https://www.sciencedirect.com/science/article/pii/S2772503023000592

Omotosho, L., Ogundoyin, I., Adebayo, O., & Oyeniyi, J. (2021). AN ENHANCED MULTIMODAL BIOMETRIC SYSTEM BASED ON CONVOLUTIONAL NEURAL NETWORK. Journal of Engineering Studies and Research, 27(2). https://jesr.ub.ro/1/article/view/276/258

Patel, M. B., Parikh, S. M., & Patel, A. R. (2020). Global normalization for fingerprint image enhancement. In Computational Vision and Bio-Inspired Computing: ICCVBIC 2019. https://link.springer.com/chapter/10.1007/978-3-030-37218-7_111

Phan, T. N., Ho, T. V., & Le-Hoang, P. V. (2020). Factors Affecting the Behavioral Intention and Behavior of Using E–Wallets of Youth in Vietnam. The Journal of Asian Finance, Economics and Business (JAFEB), 7(10). https://www.researchgate.com/profile/Phuong-Viet-Le-Hoang/publication/344595851_Factors_Affecting_the_Behavioral_Intention_and_Behavior_of_Using_E-Wallets_of_Youth_in_Vietnam/links/5f8313ffa6fdccfd7b581dd1/Factors-Affecting-the-Behavioral-Intention-and-Behavior-of-Using-E-Wallets-of-Youth-in-Vietnam.pdf

Popoola, O. P., & Lasisi, R. A. (2020). A Biometric Fusion System of Face and Fingerprint for Enhanced Human Identification Using HOG-LBP Approach. Journal of Engineering Research, 25(2). http://jer.unilag.edu.ng/article/view/1002

Rasiah, D., & Yen, Y. Y. (2020). User acceptance of ATM biometric authentication. Global Journal of Computer Sciences: Theory and Research, 10(1). https://www.researchgate.com/publication/341595982_User_acceptance_of_ATM_biometric_authentication

Rani, M. S. B. A. (2021). Study on customer satisfaction, adoption, perception, behavior, and Security on financial technology (fintech) services. In International Conference on Multidisciplinary Innovation and Economics (Vol. 8, p. 9th). http://icmie.nilai.edu.my/icmie/images/eProceedings%20of%20ICMIE%202021/ICMIE%202021_ID43.pdf

Reyes, J. M. D., Dural, L. M., Mangaoang, J. S., Victor, G. M., & Borres, R (2021). An Application of Analytical Hierarchy Process in the Comparison of the Use of GCash, Paymaya, and Debit Card Applications as a Payment Option in the Philippines. https://ieomsociety.org/proceedings/2021rome/637.pdf

Riaz, S., Mushtaq, A., & Ibrar, H. (2022, May). Analyzing and Comparing Public Perception of Facial Recognition, Iris Verification and Fingerprints Based Authentication Systems. In 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT) (Vol. 1, pp. 641-646). IEEE. https://ieeexplore.ieee.org/abstract/document/9803965

Sanchez, J. A. R., & Tanpoco, M. (2023). Continuance Intention of Mobile Wallet Usage in the Philippines: A Mediation Analysis. Review of Integrative Business and Economics Research, 12(3). https://buscompress.com/uploads/3/4/9/8/34980536/riber_12-3_12_b23-054_128-142.pdf

Security and performance enhancement of fingerprint biometric template using symmetric hashing. (2020). Ajish, S., & Kumar, K. A. Computers & Security, 90, 101714. https://www.sciencedirect.com/science/article/abs/pii/S016740482030002X

Shin, S., & Lee, W. J. (2021). Factors affecting user acceptance for NFC mobile wallets in the US and Korea. Innovation & Management Review, 18(4). https://www.emerald.com/insight/content/doi/10.1108/INMR-02-2020-0018/full/html

Silasai, O., & Khowfa, W. (2020). The study on using biometric authentication on a mobile device. NU. International Journal of Science, 17(1). https://www.thaiscience.info/Journals/Article/NUSJ/10991443.pdf

Socheat, S., & Wang, T. (2020). Fingerprint Enhancement, Minutiae Extraction and Matching Techniques. Journal of Computer and Communications, 8(5). https://www.scirp.org/journal/paperinformation.aspx?paperid=100501

Sulaiman, S. N. A., & Almunawar, M. N. (2022). The adoption of biometric point-of-sale terminal for payments. Journal of Science and Technology Policy Management, 13(3). https://www.emerald.com/insight/content/doi/10.1108/JSTPM-11-2020-0161/full/html

Sujatha, E., Sathiya Jeba Sundar, J., Deivendran, P., & Indumathi, G. (2021). Multimodal biometric algorithm using iris, finger vein, finger print with hybrid ga, pso for authentication. In Data Analytics and Management: Proceedings of ICDAM (pp. 267-283). Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-15-8335-3_22

Undale, S., Kulkarni, A., & Patil, H. (2021). Perceived eWallet security: impact of COVID-19 pandemic. Vilakshan-XIMB Journal of Management, 18(1). https://www.emerald.com/insight/content/doi/10.1108/XJM-07-2020-0022/full/html

Vitug, E. G. (2023). E-wallets as the forefront of future payment platforms: technology adoption and utilization of businesses in Central Luzon, Philippines. Partnership, 16. https://romanpub.com/resources/ijaet%20v5-2-2023-12.pdf

Wong, J. S., Lukose, J., & Chong, M. M. (2020). E-Wallet System with Fingerprint Authentication (Evolet). https://dif7uuh3zqcps.cloudfront.net/wp-content/uploads/sites/11/2020/11/02172037/E-Wallet-System-with-Fingerprint-Authentication-Evolet.pdf

Wong-In, S., Netinant, P., & Rukhiran, M. (2021). User Acceptance Factors of Biometric Recognition Technologies of Examination Attendance in Higher Education. Sustainability, 15(4), 3092. https://doi.org/10.3390/su15043092

Zaidi, A. Z., Chong, C. Y., Jin, Z., Parthiban, R., & Sadiq, A. S. (2021). Touch-based continuous mobile device authentication: State-of-the-art, challenges, and opportunities. Journal of Network and Computer Applications, 191. https://doi.org/10.1016/j.jnca.2021.103162