computers

MDPI

Article

Strengthening Cybersecurity Resilience: An Investigation of Customers' Adoption of Emerging Security Tools in Mobile Banking Apps

Irfan Riasat *, Mahmood Shah * and M. Sinan Gonul

Newcastle Business School, University of Northumbria at Newcastle, Newcastle Upon Tyne NE1 8ST, UK; sinan.gonul@northumbira.ac.uk

* Correspondence: irfan.riasat@northumbira.ac.uk (I.R.); mahmood.shah@northumbira.ac.uk (M.S.)

Abstract: The rise in internet-based services has raised risks of data exposure. The manipulation and exploitation of sensitive data significantly impact individuals' resilience—the ability to protect and prepare against cyber incidents. Emerging technologies seek to enhance cybersecurity resilience by developing various security tools. This study aims to explore the adoption of security tools using a qualitative research approach. Twenty-two semi-structured interviews were conducted with users of mobile banking apps from Pakistan. Data were analyzed using thematic analysis, which revealed that biometric authentication and SMS alerts are commonly used. Limited use of multifactor authentication has been observed, mainly due to a lack of awareness or implementation knowledge. Passwords are still regarded as a trusted and secure mechanism. The findings indicate that the adoption of security tools is based on perceptions of usefulness, perceived trust, and perceived ease of use, while knowledge and awareness play a moderating role. This study also proposes a framework by extending TAM to include multiple security tools and introducing knowledge and awareness as a moderator influencing users' perceptions. The findings inform practical implications for financial institutions, application developers, and policymakers to ensure standardized policy to include security tools in online financial platforms, thereby enhancing overall cybersecurity resilience.

Keywords: emerging technology; security tools; biometric authentication; SMS alert; password; multifactor authentication; TAM

Academic Editor: Leandros Maglaras

Received: 2 February 2025
Revised: 23 March 2025
Accepted: 27 March 2025
Published: 1 April 2025

Citation: Riasat, I.; Shah, M.; Gonul, M.S. Strengthening Cybersecurity Resilience: An Investigation of Customers' Adoption of Emerging Security Tools in Mobile Banking Apps. *Computers* **2025**, *14*, 129. https://doi.org/10.3390/computers14040129

1. Introduction

In the contemporary digital landscape, rapid technological advancement offers several services and opportunities. The COVID-19 pandemic further accelerated the adoption and utilization of these technologies [1]. However, this evolution has simultaneously introduced critical cybersecurity challenges, particularly for individual users, by significantly increasing the amount of sensitive data online and exposing individuals' vulnerabilities to cybercriminals. In the recent past, the upsurge in internet users has opened new horizons for cybercrimes, resulting in increased cyber threats [2]. This rising threat landscape has made cybersecurity and authentication systems a critical concern across all levels—ranging from nations to organizations and individual users.

Within this growing concern, individuals are increasingly becoming targets of various cyberattacks [3]. In the banking industry, both financial institutions and mobile banking customers face a wide range of cybersecurity threats, including malware, phishing, and

vishing attacks [4–6]. In response, advancement in machine learning and artificial intelligence (AI) has led to the introduction of modern security tools, such as AI-based alerts, multifactor authentication (MFA), and biometric authentication.

While technological tools continue to evolve to encounter security threats, the human factor remains a central point of concern in cybersecurity ecosystems. The effectiveness and success of technology or internet-based services largely depend on their users' ability to effectively navigate the risks. Although technology strives to provide a range of security tools and measures for the safety of sensitive information, the adoption and success of these security tools ultimately depend on users' behavior, which is often regarded as the weakest link in the cybersecurity chain [7]. This raises a critical question: Why has individual behavior remained the weakest link despite advancements in technology? Ali and Shah [8] attribute this to users' lack of awareness or their perception of security tools as complex, unnecessary, or unreliable. As a result, such perceptions often lead to low adoption rates of important security tools.

Considering these challenges, enhancing cybersecurity resilience becomes critical to mitigate behavioral vulnerabilities. Cybersecurity resilience is defined as the ability to prepare for, protect, and recover from adverse cybersecurity incidents [9] while minimizing their harm [10]. Resilient individuals, due to their proactive mindset, are better equipped to protect themselves from cyberattacks and use technology effectively. They view cyberattacks as learning opportunities to understand more about evolving threats and adopt new security tools and measures to strengthen their defense.

In this context, the continued reliance on digital solutions continues to grow, and so does the need to protect against cyber threats. Emerging technologies provide advanced security tools to enhance cybersecurity resilience [11]. The utilization of these tools primarily depends on users' behavior. They perceive some tools to be more effective and beneficial compared to others. Moreover, they resist adopting certain tools due to complexity or the need for specific knowledge to implement and use them [12].

These adoption challenges become more evident when security tools are evaluated in real-world applications. For instance, AI-based systems analyze huge volumes of data in real-time to detect anomalies and potential threats [13–15]. Moreover, multifactor authentication (MFA) and biometric authentication are proving to be effective security tools to protect sensitive information compared to traditional numbers or password methods, which are more susceptible to breaches [16]. Despite advancements, several users are hesitant to adopt new security tools due to a lack of awareness, perceived complexity, or skepticism about the effectiveness of security tools. This is especially observed in mobile banking, where users often rely on basic security tools like passwords and underutilize other emerging tools such as MFA.

These challenges are further amplified in developing countries, where cybersecurity awareness is limited despite rising digital adoption. In developing countries, particularly Pakistan, the rapid utilization of online financial services has been observed. According to the annual payment systems review report issued by the State Bank of Pakistan (SBP), users of mobile banking have reached 18.7 million, which is projected to reach 19.6 million by early 2025 [17]. Despite this rapid growth, knowledge and awareness of security tools remain low [18] due to outdated security practices [19], socioeconomic disparity, and limited access to cybersecurity education and resources [20].

SBP has adopted the National Institute of Standards and Technology's (NIST) Cybersecurity Framework and the Bank for International Settlements (BIS) guidelines to enhance cybersecurity in the banking sector. These standards are localized and embedded into SBP's regulatory frameworks, such as the Enterprise Technology Governance and Risk Management Framework [21], converting them into actionable instructions for banks. For instance,

based on NIST's core functions, SBP directs banks to conduct regular risk assessments, implement security controls, and establish real-time monitoring systems to ensure the protection and reinforcement against emerging cyber threats [22,23]. Additionally, ISO/IEC 27001 standards are also adopted to develop strong Information Security Management Systems (ISMS) to secure customer-sensitive data [24]. To integrate the best international practices into banking operations, SBP emphasizes risk-based internal controls, periodic audits, and compliance reporting.

SBP also enforces the Regulations for Electronic Banking and Payment System Operators/Service Providers (PSO/PSP), aligned with NIST SP800-53, ISO/IEC 20022. These regulations direct providers of mobile banking services to implement authentication controls, such as two-factor authentication, session time-outs, re-authentication, and risk assessment based on emerging threats, application changes, customer preferences, and actual security breaches [25,26]. Moreover, measures like real-time SMS alerts, strong and dual password policies, and customer awareness are also emphasized in BPS regulations [26].

SBP also collaborates with the Pakistan Telecommunication Authority (PTA) for cybersecurity awareness campaigns and the establishment of a Cybersecurity Emergency Response Team (CERT) to detect and respond to cyber incidents in real time [27]. Together, these efforts translate international security standards into tangible protective measures for customers helping stronger authentication mechanisms and enabling timely detection and response.

Despite these regulatory efforts, the financial sector continues to face cyber threats. According to the PTA report, the financial sector experiences the highest rate of malware attacks, with phishing attacks ranking second, indicating that it is appealing to cybercriminals [28]. Despite Pakistan being placed in the Tier 1 category by the International Telecommunication Union (ITU), the country is still ranked among the top twenty countries in internet crime reports issued by the FBI, highlighting a substantial challenge [29,30]. During August 2024, banking customers in Pakistan faced a surge in cyberattacks, leading to unauthorized financial transactions. Banks issued advisories to caution customers against using public Wi-Fi and unknown websites for financial transactions, emphasizing vigilance against phishing attacks [31]. Moreover, a notable spread of smishing activities in Pakistan was reported, targeting mobile banking customers and stealing their sensitive data for sale on the dark web [32,33]. This indicates a lack of awareness among online banking customers in Pakistan to secure their sensitive details. Additionally, a Kaspersky report, highlighted by Rizvi, shows a drastic rise in spyware attacks, increasing concerns about data espionage and exfiltration directly impacting individual security [34].

These national-level threats turn into a direct risk for mobile banking customers who face various types of cyberattacks including fraud, identity theft, SMS spoofing, and malicious mobile apps that steal sensitive credentials [35]. Several recent mobile banking attacks have been reported in Pakistan, highlighting growing threats to digital financial services. According to Khalil [36], a range of common cyber threats to compromise mobile banking accounts include phishing, malware infections, card cloning, and SIM swapping. Similarly, Maheen [37] noted a sharp rise in OTP scams, fake banking calls (vishing), and fraudulent mobile apps designed to steal user credentials.

In another report, Fareedi [38] highlighted the real-life consequences faced by victims of mobile banking fraud, who described delayed investigations and lack of support from financial and public institutions. This often discourages victims from reporting such scams. Abbasi [39], in his report, interviewed banking customers who had recently experienced a wide range of mobile banking cyberattacks, including phishing, vishing, impersonation scams, lottery and prize fraud, fake kidnapping schemes, fake transaction or refund scams, OTP scams, identity theft, caller ID spoofing, insider threats, banking app hijacking, and

credential stuffing. When asked about reporting these incidents, most victims stated that relevant institutions do not take responsibility for investigations. As Fareedi [38] reported, victims grow tired of being passed between institutions and receiving no resolution. Eventually, in the end, they give up and blame themselves for sharing sensitive credentials [39]. Many victims feel that reporting such fraud is a waste of time and resources. As a result, no statistical data on financial fraud are available in the context of Pakistan.

Given the challenging cybersecurity landscape and diverse nature of cyberattacks, it becomes essential to explore how mobile banking customers protect their sensitive information. The ever-evolving cybersecurity challenges make it even more important. It is crucial to understand how users perceive, accept, and adopt security tools to protect their sensitive information and banking accounts from unauthorized access.

This study utilizes the Technology Acceptance Model (TAM) as a foundational framework to explore and understand users' adoption behavior of these security tools. The model was proposed by Davis [40], and it is widely regarded as a powerful framework for examining how individuals adopt technology based on perceived ease of use and usefulness. However, its application in cybersecurity contexts presents certain limitations. To address the limitations, the model has been extended over time to include new factors, particularly in the cybersecurity context. Although the existing literature on the TAM framework is dominated by quantitative studies, there is a lack of qualitative insights into users' perceptions and adoption of security tools, particularly in cybersecurity.

Moreover, the existing literature on the adoption of security tools is scattered among developed and developing countries. For instance, studies in countries like the USA, the UK, and South Korea show that higher digital literacy positively impacts the adoption of security tools, such as multifactor authentication and biometric tools [41–43]. Knowledge, awareness, and digital literacy are relatively higher in developed countries compared to developing countries. Conversely, in developing countries like Pakistan, factors such as low awareness [18], the perceived complexity of new technologies, and trust issues [8] significantly influence user behavior. Furthermore, while the focus of the existing literature is on biometric authentication, coverage of MFA remains comparatively limited. To date, studies on the adoption of AI-based message alerts are notably absent. This lack of research on how various factors impact the adoption of new security tools in mobile banking applications within developing countries underlines a gap in the current body of knowledge.

In response to these gaps, this research study aims to investigate the acceptance and adoption of modern security tools—biometric authentication, SMS alert, MFA, and a strong password—among mobile banking customers. It examines how customers' perceptions of ease of use, trust, and usefulness influence their attitudes and intentions to adopt security tools. Furthermore, this study also attempts to address a methodology gap by exploring how mobile banking customers adopt multiple security tools through a qualitative research method. It examines multiple security tools in a single study, particularly in the context of developing countries, where knowledge and awareness about security tools are quite limited.

To guide this investigation, this study proposes an extended version of the TAM framework to include knowledge and awareness as a moderator, influencing customers' perceptions. It also includes trust as a mediator, along with usefulness and ease of use, directly influencing customers' attitudes towards use. This framework provides a distinct understanding of how security tools affect users' acceptance and adoption to enhance cybersecurity resilience.

This research offers key insight into mobile banking customers' perceptions and behavior toward the adoption of security tools. It addresses financial institutions, application developers, and policymakers to design effective strategies to implement robust security

tools and educate customers. It bridges the research gap by providing context-specific results relevant to developing countries, particularly mobile banking customers in Pakistan. Additionally, the proposed framework can be used to inform the standardized security policies for digital financial platforms to improve cybersecurity resilience.

RQ 1: What are the factors behind the acceptance and adoption of security tools for mobile banking customers in Pakistan?

RQ 2: How does trust along with perceived ease of use and perceived usefulness influence attitudes and intentions to adopt security tools?

RQ 3: What role do knowledge and awareness play in shaping attitudes and adoption?

2. Literature Review

Cybersecurity resilience refers to the ability to prepare for, protect against, and recover from cyberattacks, ensuring the security and integrity of financial data [44]. Due to the convenience and accessibility of mobile banking, its adoption has grown significantly. However, this growth has increased the risk of various cyberattacks including malware, phishing, and vishing attacks, exploiting users' weaknesses [3–6]. Mobile banking customers face several social engineering tactics, aimed at collecting sensitive data [4–6].

To respond to these growing threats, emerging technologies are developing advanced security tools. With advancements in machine learning and artificial intelligence (AI), modern technology has introduced many security tools to counteract security threats. AI can play a significant role in enhancing overall security and protecting user privacy [45]. Modern tools include AI-based message alerts, biometric authentication, and MFA, designed to enhance cybersecurity resilience [46]. AI-based alerts are generated by AI systems that can analyze large volumes of data within a short period, to identify any irregular patterns indicating security threats [47,48]. Similarly, biometric authentication, including fingerprint scanners, facial recognition, retina scans, and voice recognition, provides enhanced security through unique physical traits that are difficult to replicate [49,50]. During biometrics registration, physical features are stored in the database and used for later verification purposes [51]. The physical traits set individuals apart and cannot be reproduced or stolen, unlike the conventional password systems [52], making them more reliable and trustworthy. Due to their reliability and security, financial institutions are rapidly adopting this system [53].

Another essential security tool for enhancing cybersecurity is multifactor authentication (MFA), which adds additional layers of security. It allows access to an online account only after successfully providing more than one verification factor or form of verification, which may be in the form of a one-time password or biometric authentication [54].

However, despite the availability of advanced security tools, the adoption of such tools depends on how users perceive their usefulness, trustworthiness, and ease of use. They prefer security tools they find effective, reliable, and easy to use, while those perceived as complex or difficult to set up are often resisted [12]. Trust plays a critical role, as users are more likely to adopt security tools they perceive as dependable and secure. Additionally, the knowledge and awareness of these tools significantly impact adoption decisions. Users are attracted to tools they understand and feel confident using.

For instance, biometric authentication systems are readily accepted in many applicable areas for authentication purposes [55]. Due to its security advantages, it has gained users' trust over traditional systems of numbers and passwords. Stylios, Kokolakis [56] collected 545 surveys from individuals from different working groups and students in the USA, Canada, and the European Union and found that trust has a significant positive while perceived usefulness has a weak–moderate positive relation with adoption behavior. Another quantitative study in the USA found that nearly all participants preferred

biometric authentication due to ease of use and perceived security compared to PIN [57]. Hino [58], while investigating the adoption of biometric authentication in e-shopping, identified that adoption is significantly influenced by consumers' perceptions of expectancy, credibility, privacy, social influence, and awareness of technology. Akinnuwesi, Uzoka [59] found ease of use to be an important factor for the adoption of biometric authentication compared to complex ones. Similarly, Lovisotto, Malik [60] found that individuals prefer biometrics for financial transactions, perceiving it to be more secure and easy to use. Other factors identified by Piotrowska [61] include age, education level, experience, trust, and personal innovativeness.

Another modern security tool gaining attention in cybersecurity is AI, particularly for its real-time threat detection capabilities These systems use algorithms of machine learning to detect an anomaly [62] in data traffic and generate an alert. Additionally, algorithms based on machine learning make systems flexible to adopt security protocols [63]. They not only help system security but also help individuals with online security. For instance, in the context of banks, it helps to detect fraudulent transactions [64] by generating SMS alerts sent to customers' phones. AI-driven systems are part of the proactive posture that analyzes the data patterns and generates alerts in real time [49]. In the context of customers, these alerts provide real-time notifications and warnings about security threats or any change in information, enabling individuals to take timely measures [65]. Their accuracy and immediacy allow them to respond promptly to potential security threats [66,67].

In addition to biometrics and AI-based alerts, MFA plays a critical role in securing user accounts. It improves security by using more than one type of login method. These methods are independent of each other—for example, a password, a one-time code sent via SMS or an authentication app, or even a fingerprint or face scan [68]. MFA adoption is influenced by users' security concerns [69]. Zimmermann and Gerber [70] noted that users perceived varied MFA methods uniquely and that the perceived usability and ease of use significantly impact adoption. Users tend to prefer fingerprint authentication and passwords due to their ease of use and low effort. Mehraj, Jayadevappa [71] found that perceived threat and responsibility strongly influence MFA adoption on social media platforms—users are more likely to use MFA when they perceive a high risk of account compromise. Similarly, Abbott and Patil [72] emphasized that acceptance of MFA depends on implementation scope, user experience, perceived necessity, and mandatory enforcement. While broader and mandatory enforcement makes it inconvenient, leading to resistance and reduced acceptance, it is readily adopted when protecting sensitive information.

In addition to perceived usability and security concerns, knowledge and awareness also play a significant role in the adoption of security tools. Users with higher knowledge illustrate higher levels of awareness and are more likely to adopt protective tools [73]. Similarly, Shillair, Esteve-González [74] also argues that cybersecurity education, awareness, and training positively impact the adoption of security tools for a more vital and secure cyber environment. Due to digital literacy, users opt to utilize security practices to secure their online data. Lack of knowledge of security tools hinders the creation of a secure environment.

To better understand the impact of these factors on adoption behavior, the TAM provides a well-established theoretical framework. It explains that the users' acceptance of technology depends on perceived usefulness and ease of use. The model has been used in diverse fields to understand technology adoption such as IoT and cloud systems [75], healthcare [76], and digital services [77]. Not only these fields but several other studies have shown that perceived usefulness and ease of use significantly impact users' adoption behavior for technology. In recent years, the model has been increasingly applied to

investigate the adoption of cybersecurity tools. Studies have shown that fundamental factors of TAM influence users' readiness to accept and adopt these security tools [52,78].

Although TAM offers a foundational framework to understand technology adoption, researchers have identified limitations in its application, particularly in cybersecurity contexts. Rahimi and Oh [79] noted that the model overemphasizes individual-level factors and has a limited variable scope. These limitations may prevent TAM from capturing the contextual factors that influence the adoption of security tools. Moreover, due to its narrow scope, TAM does not account for risk perception, which is particularly relevant in cybersecurity where the perception of trust and perceived risk have a significant influence on adoption. These gaps make TAM insufficient to address the need for evolving technologies.

As a result, researchers have continued to extend TAM either by adding new factors or integrating with other models. For example, Rukhiran, Wong-In [80] and Buabeng-Andoh [81] combined TAM with the Theory of Reasoned Action to study the adoption of biometric authentication. Similarly, Muñoz-Leiva, Climent-Climent [82] incorporated Innovation Diffusion Theory to include factors like risk and trust. Zainal [83] and Afzal, Ansari [84] added cybersecurity knowledge and awareness, while Wang [85], based on the literature review, modified TAM by introducing perceived trust and privacy.

To overcome these limitations, several researchers have incorporated additional dimensions relevant to cybersecurity. Gusnan and Utomo [86] found that TAM's fundamental constructs—perceived ease of use and usefulness—did not significantly influence the adoption of security tools, highlighting the limitations of the fundamental model. To address this, they extended the model by adding behavioral factors. Likewise, Fallatah, Kävrestad [87], proposed cybersecurity training TAM (CTAM) and Hanif and Lallie [88] introduced a model that integrates cybersecurity-specific variables to better reflect adoption behavior.

In addition to theoretical limitations, the existing literature also highlights methodological gaps that this study seeks to address. It is notable that most of the existing literature focuses on the adoption of a single security tool at a time. In contrast, this study takes a broader approach by examining how users adopt multiple security tools, such as biometric authentication, MFA, and AI alerts within a single framework. Additionally, the literature largely overlooks the adoption of SMS alerts as a security tool. This thorough approach is particularly appropriate in the context of developing countries, where knowledge and awareness of new security tools remain limited.

3. Methodology

3.1. Selection of Data Collection Method

A qualitative research method utilizing semi-structured interviews was used to collect data. There are three types of interviews used in qualitative data collection, i.e., unstructured, semi-structured, and structured interviews [89]. Semi-structured interviews offer flexibility and deeper insights into the phenomenon under study [90,91] compared to surveys, which are restricted to specific responses. Additionally, semi-structured interviews provide consideration of personal context and deeper insights through tailored probing questions [92]. Therefore, based on the aim of the research, semi-structured interviews were conducted to obtain a deeper insight into the acceptance and adoption of multiple security tools and explore factors impacting the adoption behavior. The research process is presented in Figure 1.

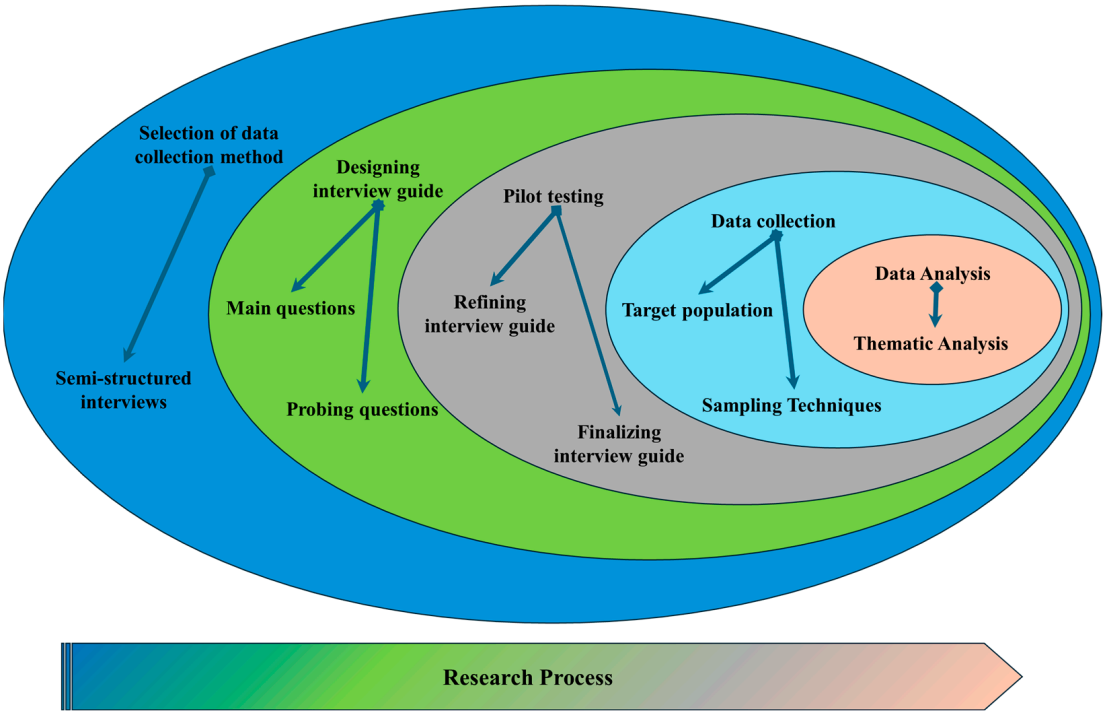

Figure 1. Onion diagram of research process.

3.2. Designing Interview Guide

Based on the aim of this research, an interview guide was designed to capture rich information. To ensure the content validity and quality of interview questions, experts and academicians from relevant fields were consulted for their expert opinions. Their expert opinions served as internal validation of the interview guide [93]. This helped with improvements and in shaping a preliminary interview guide ready for field testing.

Initially, the interview guide was in English, which was translated into Urdu with the help of a bilingual expert who was not part of the study. Reverse translation was conducted to check for translation errors and retention of original meaning, as suggested by Bulmer and Warwick [94].

3.3. Pilot Testing

To assess the feasibility and reliability of the interview guide and improve the quality of the study [95], a pilot study was conducted. An invitation through text message and email was sent to five individuals who were active users of mobile banking. Two of them expressed their non-availability due to personal engagements, while one did not respond. Two of them agreed to take part in the pilot study. Before the interview, each participant was briefed about the purpose of the study and was allowed to ask any questions for clarification. The purpose of the pilot study was also conveyed to them. At the end of each interview, the participants' feedback was also requested for improvement.

The results of the pilot study helped to refine the interview guide. It was found that some questions needed to be rearranged to ensure fluent conversation and to avoid repetition. Additionally, some probing questions were also asked during interviews which were also incorporated in the interview guide. Based on feedback from participants, some questions were rephrased for better understanding and clarity. Interview transcripts were analyzed to ensure that interview protocols provided the intended results. These modifications and improvements finalized the interview guide ensuring clarity, effectiveness, and structure to capture valuable insights from participants.

3.4. Target Population

The population for this study included users of mobile banking from Pakistan who were using mobile banking applications to access online banking services. The study context of Pakistan being a developing country represents an increased rate of internet and smartphone penetration. According to the SBP [96], rapid growth is seen in mobile banking users, which has reached nineteen million. This upsurge has created a significant reliance on online financial services. However, cybersecurity knowledge and resilience remain low among online banking customers, as highlighted by Johri and Kumar [97] and Cain, Edwards [98], respectively. Moreover, Malik, Xing [18] highlighted that more than half of Pakistani internet users are unaware of basic cybersecurity practices. This makes Pakistan an ideal context for studying the adoption of security tools.

In line with this context, the mobile banking application used by participants is central to this study, as it handles information critical to conducting transactions and other activities. The application is protected by credentials such as usernames, passwords, PINs, and other modern security tools commanding a high level of protection. To ensure better insights, mature responses, and a good qualitative dataset, the age limit of 18 years and above was set.

3.5. Sampling Technique

Data required for the study demanded the recruitment of experienced and knowledgeable participants. Purposive sampling allows the selection of participants having relevant knowledge and experience [99]. Therefore, the study employed this method to identify and select the most suitable participants. To expand the pool of participants, snowball sampling was also used. These sampling techniques were necessary because suitable participants with expertise in cybersecurity tools were not easily identifiable. Moreover, participants were reluctant to talk about their security tools and procedures. This approach helped reach the required participants.

The approach has an inherent bias of limiting the sample to an interconnected network or similar backgrounds. To minimize this bias, efforts were made to recruit participants from diverse fields and professional backgrounds.

3.6. Sample Size

The sample size in qualitative research is still debatable, and no rule exists for its determination [100]. As a result, no universally agreed-upon sample size has been established to date [101]. Researchers recommend different ranges for sample size in qualitative research. For instance, Creswell and Poth [102] suggested a range from five to twenty-five, whereas Guest, Bunce [103] recommended a range of six to eight participants. Qualitative research always aims to obtain a deeper understanding of the phenomenon, and a predetermined sample size may overlook valuable insights from other participants.

Therefore, based on suggestions from Easterby-Smith, Jaspersen [104]'s recruitment and analysis process continued until no new information sparked unique insight, a point called data saturation [105]. The sample size for this study was not predetermined. The interview process continued until there was no unique outcome. On reaching twenty-one participants, data saturation was assumed. To ensure no potential information was missed, one more participant was interviewed, confirming data saturation. The interview process was then stopped with a total of twenty-two participants.

3.7. Data Collection

Data were collected during the first half of the year 2024. Participants were selected through purposive sampling. Initial participants were asked to refer other individuals

who met the study criteria. Finally, twenty-two participants with diverse demographic characteristics (Table 1) were interviewed. They provided a rich dataset for qualitative analysis. This approach facilitated deep discussion regarding the usage of security tools to secure financial accounts and sensitive data and benefit from online services.

Table 1. Demographics of participants interviewed.

Profession	Designation	Qualification	Count
Lawyer	Lawyer in High Court	LLB	2
University Teacher	Lecturer (English)	M. Phil	1
Medical Practitioner	Physician (skin specialist)	BA ***	1
University Employee	Estate Officer	MS (Mgt. Sci.) †††	1
	UDC	BA ***	1
	Procurement Officer	BBA †	1
Bank Employee	Banking Services Officer (entry level)	BBA †	2
Government Employee	Secondary School Teacher	B.Sc. ****	1
	Primary School Teacher	BA ***	1
	Computer Operator	HSSC **	1
Self-employed	Auto Parts Salesman	SSC *	1
	Shopkeeper (sole proprietor)	HSSC **	1
	Shopkeeper (sole proprietor	BA ***	1
	Pharmacist (sole proprietor)	Pharma D	2
	Visa/Immigration Consultant	BBA †	1
	Manager Training Institute	MBA ††	1
	Event Organizer	BA ***	1
Employee in Private Insurance	Assistant Branch Manager	MBA ††	1
	Sales Officer	BA ***	1
Total Participants			**22**

* Secondary school certificate, ** higher secondary school certificate, *** Bachelor of Arts, **** Bachelor of Science, † Bachelor of Business Administration, †† Master of Business Administration, ††† Management Sciences.

As the snowball sampling technique has inherent selection bias, the initial participants may refer to other individuals from their social circle with similar knowledge. To reduce selection bias, efforts were put into selecting participants with qualifications in different disciplines and professions, as indicated in Table 1. This diversity in professions and disciplines helped ensure that participants did not have similar levels of knowledge and awareness. No participant possessed qualifications relevant to information technology, a field relevant to knowledge of cybersecurity compared to other disciplines.

Although the self-employed shared a significant portion of the sample, they had varying levels of education and qualification across diverse fields. Additionally, they used mobile banking more frequently to conduct financial transactions. This diversity in professions and education helped minimize selection bias.

3.8. Procedure

Semi-structured face-to-face interviews were conducted at places convenient for the participants. Before the interview, the purpose of the study was discussed, and only those participants who were experienced and knowledgeable were included. Prior consent was

obtained from participants to record audio and take notes. Therefore, all interviews were audio recorded with the help of a recording device.

To ease the participants, the interviews were started with general questions regarding their experience with mobile banking and how long they have been using it. Then, they were asked about the procedures for securing their devices and the security tools they utilize to protect their mobile banking account. To explore the factors impacting the adoption and utilization of specific security tools, participants were asked why they preferred one security tool over the other.

The average time for an interview was 30–45 min. After each interview, the recorded audio was transcribed into text with help from online tools. Interviews with new participants continued until no new information came out. After reaching 22 participants, data saturation was assumed, and the process was stopped.

3.9. Data Analysis Approach

The most common techniques used for qualitative data analysis include content and thematic analyses. Both approaches enable researchers to analyze a large volume of textual data. Content analysis works on the frequency of words to identify themes and patterns [106]. However, it has an inherent limitation of overlooking potential information due to low frequency. In contrast, thematic analysis enables researchers to capture potential insights despite their low frequency [107]. Based on the study's requirements and the advantages of thematic analysis, this study utilized this method for data analysis.

3.10. Data Analysis Process

The data analysis involved a series of structured steps, starting with transferring audio recordings to the laptop, which were then transcribed into text. Each transcription was thoroughly checked for accuracy and subsequently translated into English. Once finalized, the transcripts were imported into qualitative data analysis software for systematic analysis.

Thematic analysis was conducted following the step-by-step approach suggested by Braun and Clarke [108], as illustrated in Figure 2. This method helped in finding frequent patterns and developing important themes from the data. Both deductive and inductive coding techniques were used. The deductive coding was guided by the Technology Acceptance Model, ensuring alignment with the theoretical framework, while inductive coding allowed emerging themes from these data themselves, ensuring no potential information was overlooked.

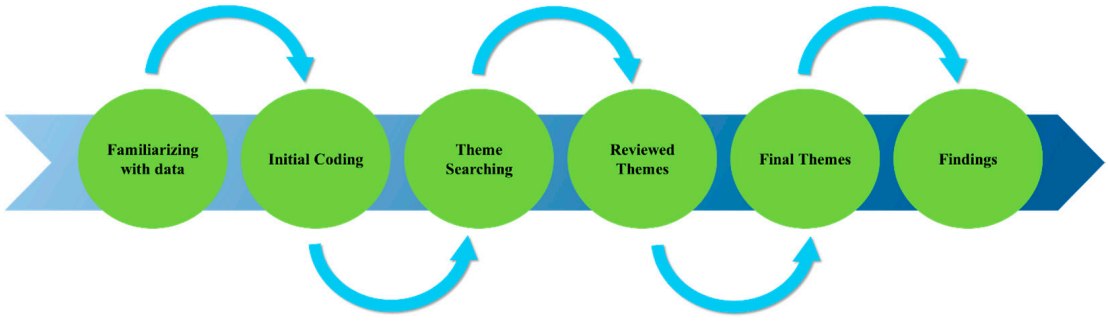

Figure 2. Thematic analysis process.

The analysis began with the first phase—familiarization with the data, where interview scripts were read multiple times to understand the depth and context. During this phase, a manual analysis was carried out in parallel to identify relevant codes and themes. Next is the second phase—initial coding, wherein the data were systematically coded based on the

TAM framework. These initial codes were developed around key factors such as perceived ease of use, perceived usefulness, trust, and awareness.

The next step—theme searching—involved clustering identical codes to identify potential patterns and meaningful themes. To ensure they accurately represented the data, the themes were reviewed and refined carefully. At this stage, similar sub-themes were merged together to improve clarity and relevance.

Following this, the final themes were developed by reviewing and organizing sub-themes under wider categories. This ensured that each theme was distinct and comprehensively covered the primary idea.

As Welsh [109] highlights, using software tools in qualitative data analysis enhances reliability and minimizes human errors compared to manual analysis. Two tools were used in this study to improve accuracy. In the first phase, Microsoft Excel was used for organizing and analyzing initial codes and quotations, following the approach suggested by Bree and Gallagher [110]. Relevant quotations were extracted and categorized in an Excel spreadsheet according to codes.

In the second phase, NVivo 15 software was used for deeper analysis and refinement, as recommended by Allsop, Chelladurai [111]. NVivo helped identify additional patterns that have been overlooked in previous phases, i.e., manual and Excel-based. Finally, codes, sub-themes, and main themes were cross-checked for consistency and accuracy. The overlapping themes were grouped for better clarity and interpretation.

The findings were then compiled by linking themes back to research questions and theoretical factors.

4. Findings

It was found that ease of use, usefulness, trust, and awareness are key factors influencing the adoption and utilization of security tools. Participants discussed four tools they use to secure their mobile banking accounts. These include biometric authentication, AI alerts in the form of text messages, passwords, and MFA.

Biometric authentication was widely used among participants, mainly due to its simplicity, trustworthiness, and perception of enhanced security. It requires minimal effort or technical knowledge to set up providing a quick login experience. In addition to biometrics, many participants also utilized SMS alerts to monitor their account activities highlighting the usefulness and importance of real-time notification.

On the other hand, a limited number of participants were familiar with MFA, though those who used it expressed strong confidence and trust in its security benefits. Many participants, however, were either unaware of MFA or lacked the knowledge to set it up. Similarly, password-based security was mentioned less frequently, and participants admitted using a simple or the same password, exhibiting a common vulnerability.

To visualize these findings, Figure 3 shows the usage distribution of different security tools based on qualitative coding in NVivo 15. The analysis was conducted on interviews with 22 mobile banking customers. Each segment size corresponds to the number of times a tool was referenced in the data, rather than individual participant counts. Biometric authentication received the highest number of references (28), indicating strong preference and adoption among participants due to its ease of use, uniqueness, and enhanced security—characteristics that are not easily replicated or stolen. SMS alerts were the second most frequently referenced tool (15 references), indicating their critical role in the real-time monitoring of account activity and detection of suspicious transactions.

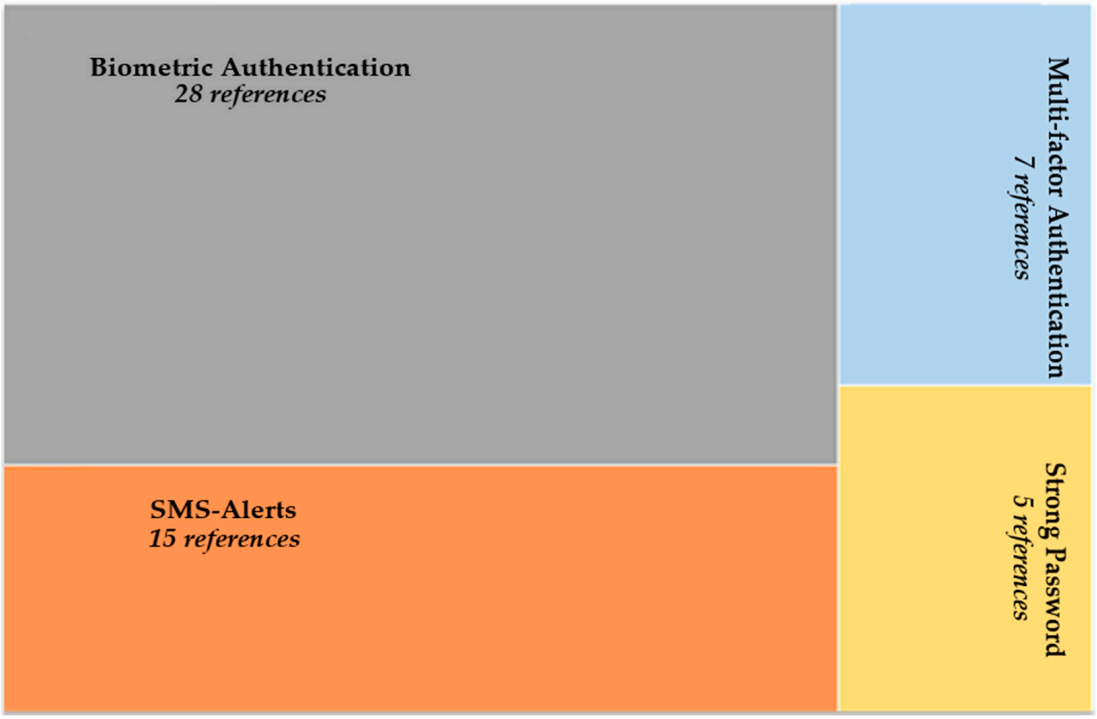

Figure 3. Usage ranking of modern security tools.

Despite the capability for enhanced security, multifactor authentication was mentioned only seven times, reflecting moderate adoption, due to a lack of awareness or implementation knowledge, as stated by participants. Strong passwords received the fewest references (five), undermining their importance as security tools.

It is important to note that due to the qualitative nature of this study and overlapping participant preferences, the figure represents the frequencies of thematic reference. Therefore, the above figure does not show the actual number or percentage of participants using each security tool. Together, these insights show that while participants favored biometric and SMS-based security tools, they tended to undervalue the significance of strong passwords and MFA—tools that are critical for additional security.

The data were analyzed using both inductive and deductive approaches. The extracted themes include usefulness, ease of use, trust, and awareness. These themes represent users' perceptions of various security tools they utilize in mobile banking.

4.1. Usefulness

This theme describes how security tools are useful and fulfill users' security requirements. It explains the degree to which security tools enhance or maintain the security of their accounts. Users expressed that each security tool provides an additional layer of protection, and they feel more confident that their accounts are safe and secure. The theme is described based on security tools as follows:

4.1.1. Biometric Authentication

Data highlight that biometric authentication methods, particularly fingerprint identification, are commonly utilized by users for the security of their accounts. Nearly all customers use biometric authentication, especially fingerprint recognition. They stated that fingerprints are the most effective security tool to prevent any unauthorized access or log into their accounts. The perceived usefulness is attributed to the specific factors and characteristics of biometric authentication.

Unique to everyone

Biometric authentication utilizes the physical characteristics of individuals, such as fingerprints, retina scans, and facial features. Participants expressed that biometric authentication is useful and secure due to the uniqueness of physical features inherent to everyone. This view was consistently supported by all participants, as highlighted in the following statements:

> *"I use fingerprint authentication to prevent anyone else from logging into my account. I consider fingerprints to be more secure because each person's fingerprint is unique".*
>
> (P-11)

> *"I have set up a fingerprint lock. I consider fingerprints to be 100% secure because they can never match".*
>
> (P-12)

> *"I find fingerprints more secure because no two people have the same fingerprints. So, if someone tries to log into my mobile or internet banking app, they won't be able to without my fingerprint".*
>
> (P-17)

The statements described that the participants emphasized the importance of the uniqueness of biometric features, specifically fingerprints, to avoid unauthorized access to their accounts. The statements highlight that the participants consistently associate uniqueness with their ability to prevent unauthorized access. The perception strengthens their belief that no two individuals can share similar physical characteristics, making this tool highly secure and reliable.

Absolute trust was also expressed by participants, with one describing fingerprint as "100% secure". Their confidence in the inability of biometric characteristics to "match" between two individuals enhances the perceived effectiveness of this security tool. Uniqueness is not only seen as a defining characteristic but also as a guarantee of security and exclusivity. It ensures that access to accounts is impossible without an exact fingerprint match. This reinforces their belief that the uniqueness of biometric characteristics prevents potential security breaches, making it a useful and valuable security tool.

The participants' emphasis on uniqueness positions it as an effective and useful security feature. For instance, the participant, while recognizing the uniqueness of fingerprints, pointed out that fingerprints prevent unauthorized access. Similarly, other statements also emphasize uniqueness, noting that no two individuals can have or share the same fingerprints. This uniqueness not only adds to a layer of security but also prevents unauthorized access to the account, giving participants confidence in fingerprints as a foolproof security measure. Consequently, uniqueness directly contributes to the usefulness of biometric authentication for account protection.

Cannot be copied

Another reason for biometric authentication's usefulness is its inability to be replicated. Unlike passwords, which can be stolen and easily misused, biometric features cannot be copied or stolen by criminals. This characteristic makes biometric authentication a useful security tool, as emphasized by participants in the following statements:

> *"I have set up a fingerprint lock on it, and as you know, everyone's fingerprints are unique and cannot be copied or stolen. . .I believe the fingerprint lock is 95% secure".*
>
> (P-7)

"Biometric features are unique to every individual and cannot be copied so for better security of my account I use face lock and fingerprint to secure my device so that no one can unlock it or access it".

(P-20)

The participants expressed strong trust in the usability of biometric authentication due to its inability to be copied or stolen. Participants explicitly stated that fingerprints cannot be replicated or stolen, reflecting the reliability of this security tool. This strong security ensures that no one can gain unauthorized access to their accounts, highlighting a strong perception of its practical benefits and usefulness. Participants acknowledged a high level of trust—"95% secure"—in biometrics due to their non-replicability. Their belief that fingerprints "cannot be copied or stolen" strengthens their perception of biometric authentication as a strong and reliable security solution.

Do not reveal login credentials

One of the important features of the biometric authentication system is that individuals do not need to enter their username and password, especially in shared or public places where there is a risk of identity theft through shoulder surfing. Many participants highlighted that this method eliminates the need for login credentials, which significantly helps protect sensitive information in potentially vulnerable environments, stating the following:

"... apps use face lock and fingerprint, so there's no need for a login ID and password. I mostly use fingerprints to log in so that I don't have to enter a password".

(P-14)

"In a crowded place, I first try not to log into my account. But if it is necessary, I use my fingerprint".

(P-8)

"I use the fingerprint option, so I don't need to enter my username and password, whether someone is watching me or not".

(P-20)

"If I am in a place where there are people around, I prefer to use the fingerprint option".

(P-22)

Participants highlighted their practice of utilizing fingerprints instead of typing a username and password, particularly in crowded public places where others may observe them and steal this information. For instance, one of the participants stated that he uses his fingerprint in public or crowded places to avoid entering passwords where someone might see them.

Similarly, another participant stated that this feature helps them log in discreetly, regardless of others watching them. It is also valued for bypassing the need for a username and password, thereby simplifying the login process while maintaining security, particularly in public places. It reduces the risk of exposure to sensitive credentials or having them remembered by someone nearby. Its ability to maintain security while avoiding the need to enter login credentials directly enhances its practical usefulness.

Overall, participants trust biometric authentication because its primary features, such as facial and fingerprint data, cannot be shared, copied, or replicated and are unique to everyone. Moreover, it allows secure login without revealing credentials in public places. These perceptions reinforce their trust in biometric systems and link them to the usefulness of fingerprints to prevent security breaches, making them a preferred choice.

4.1.2. SMS Alerts

Real-time monitoring, one of the security features, uses AI technology. From the security point of view, as suggested by Omolara, Alabdulatif [49], real-time monitoring helps detect any activity and generates an alert providing information or a security alert.

Real-time alerts to keep track of account activities

AI provides real-time monitoring of online activities. Timely information about any attempt to gain unauthorized access helps individuals take immediate action to secure their accounts. This feature is appealing because it allows them to keep track of account activities in real time. From the interview, it was found that almost all participants are actively using this feature provided by banks.

These alerts are delivered via SMS or emails to the phone number or email address registered with the bank. In mobile banking, these alerts notify users about logins, debits or credit transactions, or any updates to personal information.

These alerts are regarded not only to stay informed but as a critical tool for detecting attempts of unauthorized access. This is described by the participants below:

> *"I have SMS banking activated for my mobile banking. Whenever there is any transaction happening, whether money is being transferred or received, I receive a text message. For any type of activity like this, I get a text message".*
>
> (P-1)

> *"I have activated message alerts. Whenever a transaction occurs from my account, I immediately receive a message. So, if I am not logging in myself and there is an attempt to log into my account, I will know that someone is tampering with my account".*
>
> (P-5)

> *"...as soon as any transaction occurs, I immediately receive a text message, or as soon as any amount is transferred, I get the full details of which account the amount was transferred from. When I withdraw money from the ATM, I also immediately receive a message stating that a certain amount has been withdrawn via ATM".*
>
> (P-9)

> *"I have enabled message alerts for my account, so whenever there is any attempt to tamper with or log into my mobile banking account, I receive a message instantly".*
>
> (P-13)

Participants described the importance of SMS alerts as a valuable feature for monitoring bank accounts. These SMS alerts provide real-time updates on account activities such as transactions, credit, debit, ATM withdrawals, and login attempts. Instead of logging in and checking account activities manually, this feature enables them to receive instant updates through text messages, which helps them stay informed.

Additionally, this feature serves as a critical security measure, enabling them to detect and respond to unauthorized access attempts. For instance, participants described that these alerts inform them instantly if someone tries to log into their accounts without their permission, giving them an opportunity to take prompt security measures. The detailed information provided in SMS further enhances their reliability and preference.

This feature not only helps monitor account activity easily but also increases a sense of trust and peace of mind, as they are now able to stay updated on their accounts effortlessly. This highlights its overall usefulness in enhancing account security.

4.1.3. Multifactor Authentication (MFA)

This feature provides an additional layer of security by requesting extra authentication factors to allow access. After entering the username and password, it may ask to scan fingerprints, enter a verification code, or tap a number to confirm their identity. Although this is a good security feature, its actual usage among participants was limited. Only a few participants were found to be utilizing this security feature.

Provide extra security layer

The use of MFA was less among participants. However, those who used this security feature expressed a high level of trust in it. They feel more secure knowing that if anyone tries to gain access to their account, they will be prompted to verify through additional authentication factors. This extra verification serves as an alert that someone else is attempting to access their account without consent. Their trust in this feature is evident through their statements, as participants stated the following:

> *"... app has two-step verification, which I also use to add an extra layer of security".*
>
> (P-1)

The statement indicates that the participant is aware of the benefits of MFA. To add an extra layer of security, he is utilizing this tool. The following participant further explained their preference and trust in MFA in detail, stating the following:

> *"I am using two-step verification for my sensitive applications. And even if someone finds out my password, he still would not be able to log into my account because when he attempts to log into my account from another device using my credentials, it will ask for a verification number or authentication which will be received on my device. This will not only let me know if someone is trying to log into my account, but I can also stop the attempt".*
>
> (P-3)

The statement indicates that participants are very confident and satisfied with using two-factor authentication as a security tool. They express strong preference and trust in MFA because it provides an additional layer of security beyond login credentials. Trust and confidence are highlighted by the participants, even if their credentials are compromised or in public places where someone could potentially observe and steal their information.

Their confidence and trust stem from the assurance that unauthorized access attempts would still be prevented through the second verification step. Participants mentioned that they will receive a prompt to verify a number if someone attempts to access their account from another device. This immediate alert allows them to identify and stop unauthorized attempts. It reinforces their trust and preference for MFA as a reliable and effective security measure.

4.1.4. Passwords

Passwords, being fundamental and traditional security tools, are still preferred by individuals. They serve as a core element of security, while customers adopt additional security tools to enhance protection. Alongside passwords, biometric authentication, and SMS alerts are commonly used tools to add an extra layer of security.

A few participants in this study reported their preference for strong passwords to protect their financial accounts and devices. While passwords and PINs are generally considered vulnerable, especially in public or shared spaces, participants indicated that strong passwords are perceived as less susceptible to threats.

Strong passwords are difficult to guess

A few participants emphasized passwords compared to other security tools. For instance, they stated that they rely on passwords instead of biometric authentication in specific scenarios; one participant stated the following:

> *"I rely on strong passwords because if I am sleeping of unconscious someone can use my fingerprint to access my account, but the password is in my mind, and no one can know it".*
>
> (P-14)

It shows a strong commitment to passwords. The participant utilizes a strong password and is confident that it cannot be exploited in certain circumstances, i.e., unconsciousness or while sleeping. While addressing the strengths and benefits of a strong password, another participant reported the following:

> *"I use a strong password that is a combination of letters, symbols, and numbers, which a typical fraudster would find hard to guess".*
>
> (P-2)

Both participants expressed a preference for passwords depending on specific scenarios. One participant preferred a password over biometric authentication, stating that passwords provide better control and cannot be physically exploited while sleeping or being unconscious, as they are stored in the mind. The other participant highlighted the strength of passwords that include a combination of numbers, letters, and symbols, making them hard for fraudsters to guess or remember.

While passwords require effort compared to biometric security options, their customizability and complexity make them useful choices for securing accounts.

4.2. Trust

It is the belief or confidence that something is reliable, dependable, and capable of fulfilling the intended expectations without failure. This theme highlights the extent to which users trust the security tools they use to protect their account security.

4.2.1. Biometric Authentication

High trust in biometric authentication is expressed due to its uniqueness, inability to replicate or steal, and ability to bypass login credentials. One participant stated th following:

> *"I believe fingerprints to be more secure because each person's fingerprint is unique and cannot be copied or stolen like PIN or password".*
>
> (P-12)

The statement reflects strong trust and confidence in biometric authentication, especially fingerprint recognition, as a secure and reliable security tool. Trust is evident from participants' belief that the system uses unique physical features, making it exclusive, and enhancing their confidence that unauthorized access is not possible.

Their preference for using fingerprints in public places also highlights their trust in this system. Its ability to bypass login credentials, particularly in vulnerable environments, enhances their sense of security and trust. Participants trust that this system allows access only to authorized users and protects accounts from unauthorized access, significantly influencing the adoption of this security tool.

4.2.2. SMS Alerts

Users also express strong trust in SMS alerts provided by financial institutions. Their trust is evident, and almost all participants are utilizing it to monitor their accounts against

any suspicious activity. Participants stated that they have activated SMS alerts, which help them monitor any kind of activity occurring in their account, including the following:

> *". . . my bank provides an SMS alert facility that helps me track my debit, credit, and login activities through text messages and emails on my registered number and email address. Whenever there is any transaction happening, I receive a text message and email".*
>
> (P-4)

> *". . .as soon as any transaction occurs, When I withdraw or transfer money either thorough application or ATM, I immediately receive a message and an email stating that a certain amount has been transferred via online transaction or ATM. This full detail helps me keep track of transactions and account of my money".*
>
> (P-7)

A strong trust is reflected in the above statements regarding AI alerts, such as SMS notifications provided by financial institutions. Participants rely on them to monitor their accounts for security purposes. Consistent and real-time SMS notifications about account activities such as login, debit, or credit, help establish this trust. Participants feel a great sense of control over their accounts through this instant communication, which assures a prompt alert in case of any unusual activity.

This builds participants' trust that they will be instantly notified about all significant activities. Detailed messages containing relevant information, such as transaction channel, amount, and account details, enhance transparency and reliability, further strengthening their trust.

4.2.3. Passwords

Passwords are the fundamental and traditional security method, but are vulnerable, particularly in public places where others can observe them, or hackers can easily crack them. Typically, individuals use simple, easily guessed passwords, such as birth dates or names of loved ones. Despite their vulnerability, some users still prefer passwords over other security features, although this number is very limited. They show strong trust in passwords, with one participant stating the following:

> *"I do not trust in fingerprints or the other mode of security. I am afraid my fingerprint can be used while I am unconscious or sleeping but my password is in my mind that cannot be revealed . . . I also know that passwords can be copied or stolen but I am using a strong password that is a combination of alphabets, numbers, and special characters. It is strong enough that no one can guess or remember it at first glance. I trust password is the basic and most secure security tool".*
>
> (P-9)

Participants disregard fingerprints, stating they are vulnerable in certain situations. They express greater trust in passwords, particularly those with alphanumeric combinations. Passwords offer more control and privacy compared to fingerprints, due to fears that fingerprints can be used without their permission, especially if they are unconscious or sleeping. This reflects a lack of control over biometric data once captured.

Trust in passwords stems from the belief that they can be kept private and mentally stored, ensuring control over account security. Despite awareness of password vulnerabilities, they emphasize using strong passwords, which gives a greater sense of security. Moreover, strong passwords are difficult to guess or steal. Additionally, the ability to change passwords when needed further reinforces their trust in this security tool.

4.2.4. Multifactor Authentication

Multifactor authentication (MFA) is one of the important security tools. It provides additional layers of protection by requiring extra verification factors. After entering login credentials, users may be asked to enter a code, scan a fingerprint, or approve access via an app. These additional security steps ensure user authenticity and any mismatch or incorrect information results in access denial.

A limited number of participants were familiar with MFA and actively using it. However, they expressed strong trust in this tool, with one participant stating the following:

> *"I am using two-factor authentication, and I am confident that even if my username and password are compromised, no one can log into my account. If someone tries to log into my account from another device using my credentials, it will ask for a second step to approve via notification. This notification will be received on my phone, and I can deny it to stop access".*
>
> (P-16)

The statement shows strong trust in MFA as a reliable security method. Their confidence is evident in the belief that even if login credentials are compromised, the second verification step—such as a notification sent to their phone—ensures account protection. This added layer prevents unauthorized access without user approval.

The alert system within MFA further strengthens their trust. Even in public places, participants feel safe entering login credentials. They trust that the second layer of security will promptly notify them of any unauthorized access attempt. The system provides better control over their accounts, allowing immediate response to suspicious login attempts. This strong trust in MFA stems from the perception that it offers dependable protection against potential security threats.

4.3. Ease of Use

Among all the discussed factors, biometric authentication is the easiest to understand, implement, and use with minimal effort. Users prefer it because they do not need to enter login credentials, which can be time-consuming and vulnerable. With biometrics, users simply scan their fingerprint, face, or eye, which takes only a few seconds and grants access to their account.

4.3.1. Biometric Authentication

Biometric authentication does not require any specific knowledge and training, and any individual can use it. Furthermore, it is very easy to implement. Participants using biometric tools stated the following:

> *"Typing username and password takes time while fingerprint helps login within seconds. It's not only easy but also a quick way to log into the account".*
>
> (P-20)

> "Entering username and password is very boring. I use fingerprint to login because it is easy and logs me in quickly".
>
> (P-6)

These statements consistently illustrate that participants value this feature for its speed and convenience. While unlocking devices, it is easier to use fingerprints instead of typing a username and password. This simplicity is a key factor contributing to its ease of use. Moreover, using fingerprints saves time, allowing login within seconds. This makes it not only convenient but also an efficient way to access accounts.

Participants also mentioned that typing login credentials is "boring" and repetitive. Fingerprint authentication removes the need to manually enter login information, making it remarkably appealing.

Biometric authentication is particularly valued for combining ease of use and quick access, enhancing the user experience, and increasing their preference for managing account security with less time and effort.

4.3.2. SMS Alerts

SMS alerts are provided by the relevant bank. These are easy to implement, as users only need to submit an activation request, and the service is activated. The alerts require no additional knowledge or effort, making them highly user-friendly. Moreover, the information provided in these messages is clear and easy to understand. Due to their simplicity and benefits, almost all participants were using this system, as stated below:

> *"message alert does not require any additional effort. I went to the bank and asked them to activate SMS alert for my account and they activated it. Now I can know all activities of my account".*
>
> (P-14)

> *"I was not aware of this feature. One of my friends told me about it and told me what to do. It was very easy to implement. Just go to the bank and ask them to activate the service for the account without any additional documentation. I did not have to make any additional effort or learn about it".*
>
> (P-1)

As stated by participants, SMS alerts offer a high level of ease in both setup and usage. Participants stressed the straightforward nature of the activation process. A minimal effort is required: simply visiting the bank and requesting service activation. The service enables them to track their account activities. This simplicity reinforces their perception that the service is easy to use and does not involve a complex setup.

As mentioned in the second statement, no additional documentation or effort was needed, highlighting a quick and hassle-free activation process. Almost all participants use this service, reflecting its ease of implementation and accessibility. The consistent emphasis on simplicity and convenience enhances its appeal and reinforces its perceived ease of use.

4.4. Knowledge and Awareness

Knowledge and awareness is one of the important themes identified from the data. This theme describes how knowledge and awareness influence the adoption of security tools. Data revealed that only a limited number of participants use MFA, while others are either unaware of it or do not know how to implement it. Adoption is often limited to those who have sufficient knowledge and understanding of how to use these tools.

It is evident that participants use only those tools they are familiar with and understand how to implement. They are aware of biometric authentication, SMS alerts, and passwords, as well as their role in protecting account security. However, in the case of MFA, many participants lack awareness, which hinders the adoption and use of this robust security tool. When asked about security tools, participants readily named the tools they were using. For instance, participants shared the following:

> *"I know biometric authentication works on fingerprint, facial expressions, and eye retina. Mobile scans them when we set them up. It is not very difficult to set up biometric features"*
>
> (P-5)

"I was not using SMS-alert till one of my friends told me about it and advised me to activate it. The next day I went to my bank and requested them to activate this alert for my account and they did it within no time".

(P-3)

"No, I do not know about multifactor or two-factor authentication".

(P-5)

"I heard about multifactor before but do not know how I can use it for my account protection".

(P-9)

The above statements show that users are inclined to adopt only those security tools they are aware of and understand how to implement. For example, participants using biometric authentication were confident because they knew how to set it up and use it. The second statement illustrates that participants were not using SMS alerts until a friend informed them about their benefits. This reinforces the idea that users are unlikely to adopt a security tool unless they are made aware of it.

The last two statements highlight gaps in awareness about MFA. Participants either did not know about it or did not know how to implement or use it. This lack of knowledge and awareness prevents users from adopting MFA despite its strong security features.

These statements emphasize that knowledge and awareness are critical factors in adoption decisions for security tools. If they are unaware of a tool or do not understand how to implement it, they are unlikely to use it. As a result, even effective security tools may remain underutilized without proper awareness and understanding.

5. Proposed Conceptual Model

Figure 4 represents a conceptual framework derived based on findings from qualitative data. The model represents a significant advancement in understanding the adoption of security tools. It uniquely extends the technology acceptance model (TAM) framework. The distinction lies in a context-specific focus on security by examining the impact of different security tools, such as biometric authentication, SMS alerts, strong passwords, and MFA. The traditional TAM and its extensions primarily explore general technology adoption, while this conceptual model examines the distinctions of security tools.

Here, security tools collectively form an independent variable. Knowledge and awareness serve as a moderator. It moderates adoption through awareness of the existence of security tools, understanding of implementation, and perceptions of ease of use, usefulness, and trust.

The novelty of this model exists in introducing knowledge and awareness as a moderator. It influences users' awareness of security tools, understanding of implementation, and perception in terms of ease of use, usefulness, trustworthiness, attitude, and intention to use. Users first learn about tools, evaluate their usability, usefulness, and trustworthiness, and, finally, make intentions and decide to use them. This indicates that familiarity with security tools and knowing about potential threats shapes their security behavior, which is absent in traditional TAMs.

This model also incorporates trust as a core mediator, directly influencing attitude and intention. It recognizes the critical role of reliability and security for users, especially in the context where privacy and data protection are of utmost importance. It cannot be a derivative of usefulness because, in the context of security, users need to trust the integrity of tools before perceiving them to be useful. Hence, in this context, trust is more fundamental rather than a derivative. Unlike traditional TAMs, where trust is either missing or implied indirectly, it includes trust as a mediator, directly influencing adoption. Moreover, this model recognizes trust as essential for adopting security tools. Additionally,

the model also indicates a bidirectional influence between usefulness and trust, indicating that trust is reinforced through usefulness, and vice versa. However, initial trust is always necessary before users perceive a tool as useful.

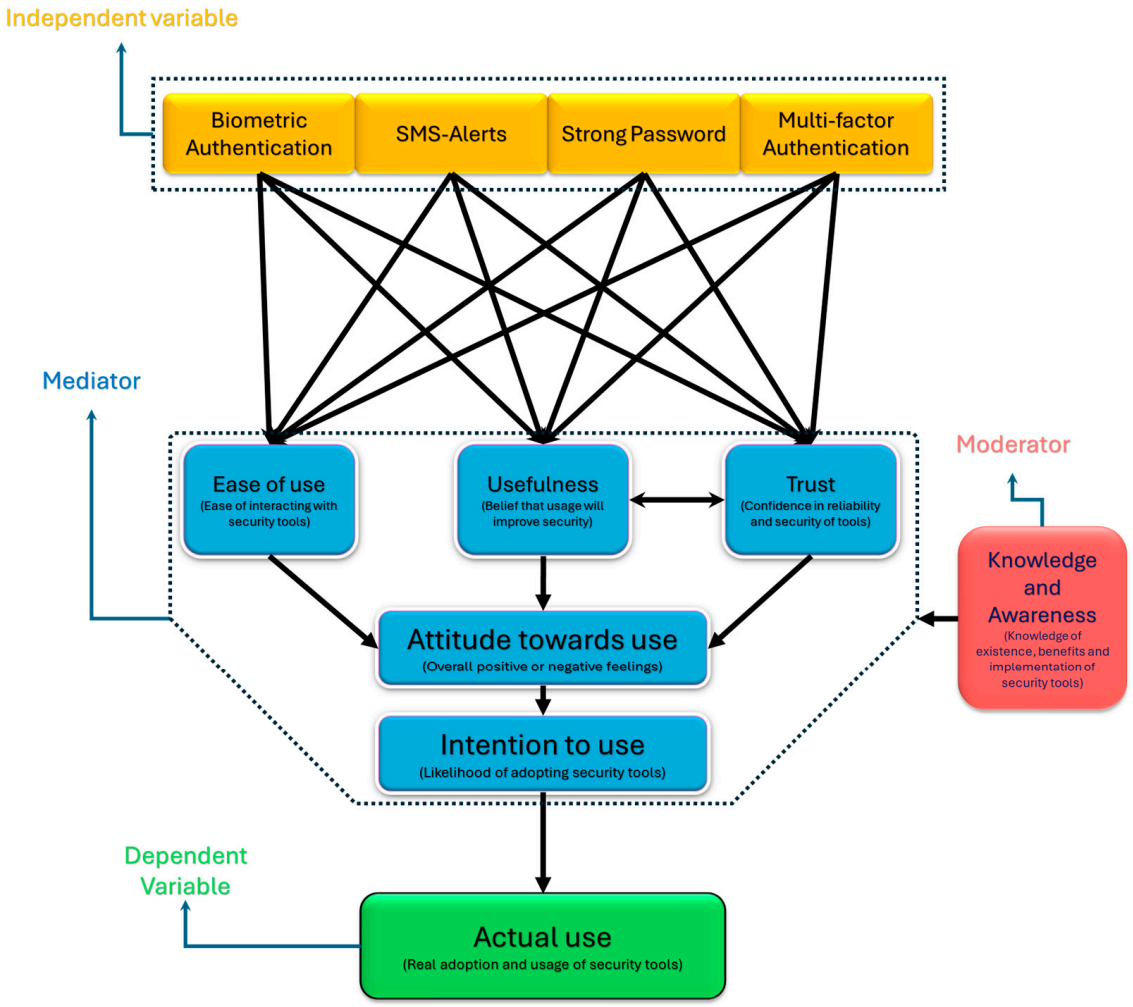

Figure 4. Proposed conceptual model derived from qualitative data (source: author).

The model extends traditional TAM by integrating emerging security tools, such as biometric authentication, SMS alerts, strong passwords, and MFA. By utilizing basic constructs of TAM like ease of use and usefulness, it provides a distinct understanding of how emerging security tools influence users' acceptance. This approach goes one step beyond traditional TAMs by directly connecting trust, knowledge, and awareness to the adoption of modern security tools.

6. Discussion

This study explored the users' acceptance and adoption of security tools provided by modern technology. The findings and derived model align with the technology acceptance model, which describes the actual intention to use a technology. It is seen that customers' acceptance and actual utilization of security tools depends on factors such as ease of use, usefulness, trust, and awareness. A major part of the literature on this model is based on quantitative research methods, utilizing statistical tools to find users' intentions (e.g., [75,76]. However, quantitative methods usually overlook deeper insights into users' perceptions and relative factors that influence adoption, which can be explored through qualitative approaches in a better way. This study fills this gap through the utilization of qualitative

interviews to uncover shaded perspectives on how knowledge, awareness, trust, usefulness, and ease of use shape adoption behavior in developing countries.

The findings revealed that mobile banking customers adopt security tools primarily based on perceived usefulness, ease of use, and trust. These factors consistently influence user behavior across both developed and developing country contexts, as supported by multiple quantitative studies from different regions. For instance, Nakisa, Ansarizadeh [112] conducted a quantitative study in Europe and found that trust is a significant determinant in the adoption of biometric security tools. Likewise, Stylios, Kokolakis [56], through empirical research in the USA, Canada, and the European Union confirmed that ease of use and trust significantly influence security tool adoption. However, Tam, Balau [113]'s mixed-method study in Portugal identified that trust may also function as a moderating variable impacting cybersecurity adoption behavior. This suggests a multifaceted role of trust—it can act both as a direct and moderating enabler of adoption.

In the context of developing countries, our findings align with the quantitative study by Hizam, Ahmed [114] in Malaysia, which highlighted perceived ease of use and usefulness as significant predictors of security tool adoption. Likewise, Wang [86] quantitatively identified trust to be an additional influencing factor alongside ease of use and usefulness among students in Taiwan.

Furthermore, this study emphasizes that knowledge and awareness act as moderating factors influencing adoption behavior. A higher level of knowledge corresponds to a higher adoption rate. This is supported by the quantitative findings of Dinev and Hu [115], who demonstrated that security tools are primarily used to avoid harm; therefore, knowledge and awareness about security threats have a stronger influence on adoption behavior than the basic TAM factors such as perceived ease of use and usefulness.

The moderating role of knowledge and awareness is further supported by quantitative studies conducted in Saudi Arabia by Alfalah [116] and Elrayah and Jamil [117]. In addition, a cross-country (Turkey, Slovenia, Poland, and Israel) quantitative study by Zwilling, Klien [73] further advocates that a deeper understanding of security concepts leads to a stronger translation of awareness into meaningful security behavior and an effective security tool adoption.

In developing country contexts, this is reflected in quantitative studies by Ladipo, Dixon-Ogbechi [118] in Nigeria and Afzal, Ansari [84] in India, who found that adequate knowledge and awareness positively influence the adoption of cybersecurity tools. In contrast, developed countries typically demonstrate higher levels of knowledge and awareness. Lesjak, Zwilling [119], in a cross-country quantitative study, observed that increased knowledge leads to significant adoption of security tools regardless of demographic differences. As a result, quantitative evidence from both developing and developed countries supports regional variation in adoption behaviors. Moreover, research in developed countries often move beyond core TAM factors, exploring additional determinants such as compatibility, innovation attributes, and privacy concerns, as examined by Stylios, Kokolakis [56].

Within this study, users highlighted four important security tools adopted based on ease of use, usefulness, trust, and knowledge and awareness. For biometric authentication, users expressed strong trust in their inability to be copied or stolen, perceiving it as accurate, reliable, and risk-free. This aligns with Zhang, Yang [120], who found that mobile app users consider biometric authentication highly secure and widely accepted.

The high trust is observed among customers, which reflects the work by Mutahar, Daud [78], who found that perceived risk negatively impacts adoption. This trust enhances its perceived usefulness, as also supported by Gusnan and Utomo [86], who emphasized its role in enhancing online security.

Users noted that biometric systems are easy to implement and require minimal knowledge and effort, supporting TAM and aligning with Rukhiran, Wong-In [80]. However, this contrasts with Gusnan and Utomo [86], who argue that usefulness and ease of use alone are insufficient, suggesting that the potential influence of other factors, such as risk perceptions or equal trust in modern and traditional methods, may influence adoption.

Despite strong trust, biometric tools are also vulnerable to significant challenges like spoofing and faking, as noted by Hussaini [121]. Techniques, like image replication or fake fingerprints, pose significant risks that users are unaware of. Hence, relying solely on biometrics may not be good for account security. Rather, it is more effective to integrate it with other security tools, such as MFA, as suggested by [55].

In addition to biometrics, AI-based message alerts also play an important role in security. These alerts, typically received via SMS or emails, are considered trustworthy, easy to use, and highly useful. They serve as real-time surveillance tools for online accounts by providing real-time and accurate alerts, which are helpful for the detection of unauthorized access. The findings indicate that AI alerts significantly improve security by providing real-time monitoring of accounts' activities. This enhanced view increases awareness of account activities and overall security posture. These findings align with those of Cadet, Osundare [122], who emphasized their use in cybersecurity. Similarly, the data support the results of Chirra [123], who found that AI alerts improve security and enhance resilience against security breaches by providing prompt alerts.

While MFA adds an additional layer of protection using multiple authentication factors, users in this study expressed strong trust and confidence in it, believing that their accounts are more secure—even in case their login credentials are compromised. This perceived sense of security aligns with the findings of Colnago, Devlin [124], who reported that users feel more confident in their account's protection after implementing MFA. However, this study revealed that knowledge and awareness act as a moderating factor influencing MFA adoption. Our findings align with the quantitative result of Busse, Schäfer [125], who found that non-expert individuals often lack awareness of two-factor authentication, which limits its adoption as a strong security tool.

Similarly, technical complexity and limited technical knowledge were identified as major barriers to MFA adoption. This is supported by the quantitative findings of Jelínek [126], the mixed-method results of Kendyala [127], and Anderson's [128] multi-method research, all highlighting technical complexity and lack of knowledge as barriers to MFA adoption. Basori and Ariffin [129] also found similar results in their review of 54 articles, identifying complexity as a significant factor influencing MFA adoption.

Implementation challenges, particularly the need for additional technical knowledge, often make MFA difficult to set up and use effectively [130]. Moreover, factors such as education level, prior technical background, and an understanding of MFA's importance also influence adoption behavior [130,131].

In addition to these quantitative and mixed-method studies, our findings are consistent with the qualitative insights of Henriksson [130], who also noted that technical complexity and low user awareness as key obstacles. Consequently, despite its proven benefits, MFA remains underutilized among users—a pattern that was also observed in this study.

In contrast, the adoption of MFA in developed countries is considerably higher, where users generally possess a higher level of cybersecurity knowledge and awareness [132,133]. This disparity highlights the critical role of digital literacy and users' education in enhancing the adoption of security tools in developing countries.

Alongside MFA, users in this study also identified the use of strong passwords as a trusted and useful security tool. Despite being vulnerable in shared and public places, customers still regard strong passwords as a reliable security tool. This trust builds upon

the belief that strong passwords—those containing a combination of words, numbers, and special characters—are difficult to guess and thus offer better protection. This is supported by Chanda [134], who stated that a strong password has higher entropy and greater strength, making it hard to crack. Zhang, Yang [120] also argues that passwords, as traditional authentication methods, remained preferred by users due to their perceived security, accuracy, and convenience.

Although perceived usefulness, ease of use, and trust significantly influence users' willingness to utilize security tools, this study emphasizes that knowledge and awareness about the existence and implantation of these tools are equally necessary for their adoption. In the case of MFA, it was evident that many mobile banking customers either remained unaware of the tools or lacked implementation knowledge. Conversely, those who had adopted MFA expressed strong trust and satisfaction with its security benefits. As noted by Ometov, Petrov [135], human interaction with technology is shaped by being user-friendly and its low-effort procedures. The lack of implementation knowledge highlights that MFA, by its nature, is a bit difficult to implement requiring effort and knowledge to set up, acting as an adoption barrier.

While security tools offer enhanced protection, they also have associated limitations and risks. However, most participants in this study who actively utilize biometric authentication were largely unaware of its potential negative aspects. Only a few of them indicated risks in specific scenarios. This highlights a clear knowledge gap, that many customers are unaware of associated hazards. Johri and Kumar [97] similarly observed that banking customers possess varying levels of awareness regarding cybersecurity tools, practices, and threats, with a significant number lacking basic cybersecurity concepts. A similar knowledge gap was observed in relation to MFA, highlighting a systemic concern around customers' education and digital literacy.

To address this concern, banks and financial institutions must proactively implement awareness campaigns to educate them, while technology providers should focus on simplifying the implementation process to enhance adoption and accessibility. Mutahar, Daud [78], along with Crossler and Bélanger [136], emphasized that knowledge and awareness significantly influence technology adoption and acceptance. These findings reinforce the need for a large-scale spread of knowledge and awareness about cybersecurity tools, practices, and basic understanding.

Building on these findings, key determinants influencing adoption behavior can be summarized and addressed through practical interventions. Drawing from the TAM framework, factors such as ease of use, perceived usefulness, trust, and awareness emerged as key drivers of adoption. Security tools—including biometric authentication, AI-based alerts, MFA, and strong passwords—each contribute uniquely to enhance security. Among these, biometric authentication stands out due to the strong customer trust it generates through its unique characteristics.

Nevertheless, a persistent gap is also highlighted regarding knowledge and awareness particularly for MFA, limiting its widespread adoption and utilization. Addressing this gap requires customized and targeted awareness campaigns and a simplified implementation process. Collaboration between policymakers, financial institutions, and technology developers is essential to design user-friendly tools with simple interfaces and step-by-step guides. Such efforts can effectively bridge the knowledge divide and foster widespread adoption of advanced tools.

Beyond practical implications, this study also contributes to the theoretical understanding of the technology acceptance model. Unlike most of the existing literature that adopts a quantitative approach, this study extends TAM by offering qualitative insights into the adoption of emerging security tools within the context of developing countries.

By emphasizing the interplay between knowledge, ease of use, usefulness, and trust, this study advances the TAM framework by situating it in the broader context of cybersecurity resilience and risk mitigation. It also explores underrepresented contexts such as developing countries, where knowledge and technological infrastructure impact adoption behavior. Through qualitative inquiry, this study offers a deep understanding of mobile banking customers' perspectives and highlights awareness as a critical factor in shaping adoption decisions.

7. Conclusions

This study explores the factors influencing the adoption of modern security tools among mobile banking customers in Pakistan through a qualitative research approach. Semi-structured interviews were conducted with twenty-two mobile banking customers recruited through purposive and snowball sampling techniques. Data were analyzed using thematic analysis in NVivo 15. The findings revealed that the adoption of modern security tools is primarily influenced by perceived usefulness, ease of use, and trust, while awareness and implementation knowledge act as moderating factors.

Among the tools explored in this study, biometric authentication—particularly fingerprint recognition—and AI-based alerts emerged as highly adopted and preferred by mobile banking customers. These tools were considered useful for enhancing security and were accepted for their ease of implementation and use. Similarly, AI alerts in the form of text messages were also preferred due to their usefulness in keeping customers informed about account activities including debit, credit, login, and any potential security threat, enabling them to take protective measures timely. Their implementation does not require any technical knowledge; thus, it is easy to use and implement.

However, not all security tools were equally adopted. MFA, despite being perceived as highly secure and trustworthy, showed limited usage due to low awareness and implementation knowledge. While users expressed confidence in MFA's ability to control account access but was hindered by a lack of technical knowledge about its setup processes. In contrast, despite the vulnerability associated with passwords, high trust was expressed for strong passwords. Customers perceived complex alphanumeric passwords as secure and effective. However, this strength also comes with a drawback. Strong passwords are hard to remember and need to be written down or saved somewhere, which can pose security risks.

Collectively, these findings demonstrate core factors like ease of use, usefulness, and trust shape adoption behavior. Customers perceived a high level of trust in biometric authentication, SMS alerts, strong passwords, and MFA. Each tool is unique to protect against unauthorized access and take prompt measures. Moreover, in the context of security when the privacy of sensitive data is paramount, trust in security tools, along with ease of use and usefulness, directly influence final adoption. Trust and perceived usefulness reinforce each other. When a tool is perceived as useful in protecting privacy, trust is reinforced and vice versa.

Importantly, this study revealed that awareness and knowledge of security tools and their implementation significantly moderate adoption behavior. A lack of awareness and knowledge leads to a low adoption rate, as seen in the case of MFA, where participants are either unaware of it or do not know how to implement it. Customers only use tools they are aware of and can set up without any additional effort or knowledge. Awareness of the existence and knowledge of implementation is very important for customers to adopt and use a security tool. Moreover, knowledge and awareness help share their attitudes by enhancing confidence and reducing fear of complexity, making them more open to

adopting security tools. By understanding the benefits, they perceive tools as useful and trustworthy, thereby reinforcing adoption behavior.

While awareness supports adoption, this study also highlights a limited understanding of the limitations and risks associated with certain tools. This knowledge gap is particularly evident with biometric authentication, where customers showed blind trust, without understanding potential vulnerabilities. Only a few of them expressed concerns over the risks of certain security tools. For instance, some mentioned that fingerprints can be used while a person is sleeping or unconscious, whereas usernames and passwords remain secure as they are stored in memory. This finding underscores the importance of spreading knowledge and awareness not only about the existence and implementation of security tools but also their limitations and risks.

To address these knowledge gaps and promote effective adoption, collaborative action from stakeholders is essential. The findings highlight a knowledge deficit and low awareness levels that deter the adoption of advanced security tools, particularly MFA. Bridging this gap requires a collaborative effort among application developers, policymakers, and financial institutions. They should work together to simplify the implementation processes and provide user-friendly tutorials to guide them through setup and usage without technical barriers.

8. Practical Implications

These findings can be important for other developing countries like Pakistan that share similar challenges. Individuals often lack cybersecurity awareness. Many follow poor cyber hygienic practices and are vulnerable to emerging cyber threats.

The findings provide actionable insights for application developers to improve the security tools by creating more user-friendly interfaces that highlight their usefulness. By designing intuitive interfaces to accommodate different digital literacy levels, developers can play an important role in ensuring accessibility and ease of use.

Organizations and financial institutions providing online services can use them to develop user-centric strategies, encouraging developers to incorporate effective security systems by improving the entrusted security tools, including, for instance, embedding MFA within the applications. Moreover, awareness campaigns should be conducted to increase cybersecurity literacy and bridge knowledge gaps. Additionally, they should encourage users to use multiple security tools for comprehensive security. Inherent limitations and risks should also be communicated to users. They can leverage social media for knowledge and awareness to enhance security and build trust in security tools.

Device manufacturers can also benefit by ensuring hardware and items used meet high-quality standards to minimize vulnerabilities in security tools like biometric authentication. For instance, improving facial recognition technology to prevent bypassing through photos. It can significantly increase users' trust and security.

Additionally, policymakers can use these findings to develop user-focused security policies and encourage developers to follow a consistent and standardized policy to develop and include strong security features across applications. They should enforce standardized security policies to include requirements for clear communication about the risks and benefits of security tools, thereby increasing trust and usefulness. Standardization will not only simplify security features making them easy to use without additional knowledge and effort but also foster trust through consistent security across different digital platforms, no matter which digital service they are using.

9. Novelty

Unlike previous research, this study utilizes a qualitative research design to explore the adoption of security tools. It integrates multiple security tools, whereas previous studies often focus on individual tools. Moreover, earlier studies dominantly focus on the primary constructs of TAM, overlooking the importance of knowledge and awareness. This study highlights their important role as moderators for actual adoption.

Along with usefulness and ease of use, trust is presented as a distinct mediator, recognizing its critical importance, particularly in the security context where users may be skeptical of security tools due to privacy concerns. While TAM has traditionally been used in the general context of technology adoption, this study specifically addresses the adoption of multiple security tools within a single framework. Additionally, this study explores the adoption of SMS alerts as a security feature by mobile banking customers.

10. Limitation and Future Study

This study is based on qualitative research methodology, which has inherent limitations of limited generalizability. Therefore, the findings of this research cannot be generalized to the larger population. Moreover, the findings would be applicable to only those countries sharing the same characteristics as Pakistan. Additionally, due to resource constraints, this study was not comparative and was limited to Pakistan.

Considering these limitations, a quantitative research study can be conducted to verify, compare, and generalize the findings. The model and pathways projected in it can be validated and modified through empirical testing in future research. Additionally, the impact of other factors, such as social, economic, cultural, and demographics (e.g., age, gender, profession), can also be explored.

Author Contributions: Conceptualization, methodology, software, validation, formal analysis, investigation, data curation, and writing—original draft preparation, I.R.; writing—review and editing, M.S. and M.S.G.; visualization, I.R.; supervision, M.S. and M.S.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data were directly linked to anonymous participants; therefore, due to privacy concerns, the data cannot be publicly shared.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
BIS	Bank for International Settlements
CERT	Cybersecurity Emergency Response Team
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OTP	One-time Password
PIN	Personal Identification Number
PTA	Pakistan Telecommunication Authority
SBP	State Bank of Pakistan
SMS	Short Messaging Service

TAM	Technology Acceptance Model
USA	United States of America

References

1. Mushtaq, S.; Shah, M. Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. *Information* **2024**, *15*, 619. [CrossRef]
2. John, M.S. Cybersecurity Stats: Facts And Figures You Should Know. Available online: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/ (accessed on 30 December 2024).
3. Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
4. Ghelani, D.; Hua, T.K.; Koduru, S.K.R. Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea* **2022**. *preprints*.
5. Acharya, S.; Joshi, S. Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. *PalArch's J. Archaeol. Egypt/Egyptol.* **2020**, *17*, 4656–4670.
6. Jerbi, D. Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends. *J. Curr. Trends Comp. Sci. Res.* **2023**, *2*, 191–195.
7. Hughes-Lartey, K.; Li, M.; Botchey, F.E.; Qin, Z. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* **2021**, *7*, e06522. [CrossRef]
8. Ali, A.; Shah, M. What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector. *Information* **2024**, *15*, 760. [CrossRef]
9. Rashed, M.; Kassim, N. Factors influencing user's intention to adopt ai-based cybersecurity systems in the uae. *Interdiscip. J. Inf. Knowl. Manag.* **2023**, *18*, 459–486.
10. Joinson, A.N.; Dixon, M.; Coventry, L.; Briggs, P. Development of a new 'human cyber-resilience scale'. *J. Cybersecur.* **2023**, *9*, tyad007. [CrossRef]
11. Ali, A.; Shah, M.; Foster, M.; Alraja, M.N. Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. *Computers* **2025**, *14*, 38. [CrossRef]
12. Bouramdane, A.-A. Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *J. Cybersecur. Priv.* **2023**, *3*, 662–705. [CrossRef]
13. Giwah, A.D.; Wang, L.; Levy, Y.; Hur, I. Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *J. Intellect. Cap.* **2020**, *21*, 215–233. [CrossRef]
14. Albahri, O.; AlAmoodi, A. Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. *Mesopotamian J. CyberSecurity* **2023**, *2023*, 158–169. [CrossRef]
15. Prince, N.U.; Faheem, M.A.; Khan, O.U.; Hossain, K.; Alkhayyat, A.; Hamdache, A.; Elmouki, I. AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction. *Nanotechnol. Percept.* **2024**, *20*, 332–353.
16. Alrawili, R.; AlQahtani, A.A.S.; Khan, M.K. Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Comput. Electr. Eng.* **2024**, *119*, 109485. [CrossRef]
17. SBP. Payment Systems Quarterly Review Q1 of FY25. Available online: https://www.sbp.org.pk/psd/reports/index.htm (accessed on 25 February 2025).
18. Malik, Z.U.A.; Xing, H.M.; Malik, S.; Shahzad, T.; Zheng, M.; Fatima, H. Cyber Security Situation in Pakistan: A Critical Analysis. *PalArch's J. Archaeol. Egypt/Egyptol.* **2022**, *19*, 23–32.
19. Shad, M.R. Cyber Threat Landscape and Readiness Challenge of Pakistan. *Strateg. Stud.* **2019**, *39*, 1–19. [CrossRef]
20. Khan, N.F.; Ikram, N.; Saleem, S. Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Secur. J.* **2023**. *online ahead of print*.
21. SBP. *Enterprise Technology Governance & Risk Management Framework for Financial Institutions*; Banking Policy & Regulations Department; SBP: Karachi, Pakistani, 2017; Available online: https://www.sbp.org.pk/press/2017/Pr-Ent-Risk-Govr-30-May-17.pdf (accessed on 18 March 2025).
22. NIST. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018; p. NIST-CSWP 04162018. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 18 March 2025).
23. SBP. *Guidelines_on_IT_Security*; SBP: Karachi, Pakistani, 2004; Available online: https://www.sbp.org.pk/bsd/2004/Guidelines_on_IT_Security.pdf (accessed on 18 March 2025).
24. ISO. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. ISO: Geneva, Switzerland. Available online: https://www.iso.org/standard/27001 (accessed on 18 March 2025).

25. SBP. Enhancing Digitization Initiatives in Banks/MFBs. Payment System Department. 2021. Available online: https://www.sbp.org.pk/psd/2021/C1.htm (accessed on 18 March 2025).
26. SBP. *Regulation for the Secuirty of Internet Banking*; SBP: Karachi, Pakistani, 2018; p. 8. Available online: https://www.sbp.org.pk/psd/2015/c3-annexure-a.pdf (accessed on 18 March 2025).
27. SBP. *Financial Stability Review*; SBP: Karachi, Pakistani, 2021; Available online: https://www.sbp.org.pk/FSR/2023/FSR%202023.pdf (accessed on 18 March 2025).
28. PTA. Cyber Security Annual Report. 2023. Available online: https://www.pta.gov.pk/category/cyber-security-annual-report-2022-963089105-2023-05-30 (accessed on 17 March 2025).
29. ITU. Global Cybersecurity Index. 2024. Available online: https://www.itu.int/hub/publication/d-hdb-gci-01-2024/ (accessed on 20 December 2024).
30. FBI. Internet Crime Report. 2023. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (accessed on 15 December 2024).
31. Hanif, U. Bank Customers Face Surge in Cyberattacks. 2024. Available online: https://tribune.com.pk/story/2517144/bank-customers-face-surge-in-cyberattacks (accessed on 10 January 2025).
32. Resecurity. Resecurity | Smishing Triad Is Targeting Pakistan To Defraud Banking Customers At Scale. 2024. Available online: https://www.resecurity.com/blog/article/smishing-triad-is-targeting-pakistan-to-defraud-banking-customers-at-scale (accessed on 11 August 2024).
33. Paganini, P. Smishing Triad Is Targeting Pakistan to Defraud Banking Customers At Scale. 2024. Available online: https://securityaffairs.com/164705/cyber-crime/smishing-triad-targets-pakistan.html (accessed on 11 August 2024).
34. Rizvi, J. Spyware Incidents Surge in Pakistan, Banking Malware Attacks Decline. 2024. Available online: https://www.thenews.com.pk/print/1187620-spyware-incidents-surge-in-pakistan-banking-malware-attacks-decline (accessed on 11 August 2024).
35. Gatla, T.R. Cybersecurity measures in mobile banking: Examining the latest cybersecurity. *Int. J. Creat. Res. Thoughts* **2021**, *9*, 777–781.
36. Khalil, B. Cybercrime Effecting Banking Sector/Economy of Pakistan. 2020. Available online: https://moderndiplomacy.eu/2020/03/22/cybercrime-effecting-banking-sector-economy-of-pakistan/ (accessed on 2 January 2025).
37. Maheen. The Growing Threat of Cyber-Fraud. 2022. Available online: https://tribune.com.pk/story/2355657/the-growing-threat-of-cyber-fraud (accessed on 18 March 2025).
38. Fareedi, T. Digital Frauds Cause Long Probes. 2023. Available online: https://tribune.com.pk/story/2446414/digital-frauds-cause-long-probes (accessed on 18 March 2025).
39. Abbasi, S. Pakistan's Web of Cyber Scammers. 2023. Available online: https://www.dawn.com/news/1764628 (accessed on 18 March 2025).
40. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]
41. Komandla, V.; Chilkuri, B. The Digital Wallet Revolution: Adoption Trends, Consumer Preferences, and Market Impacts on Bank-Customer Relationships. *Educ. Res. (IJMCER)* **2018**, *2*, 1–11.
42. Venkatesan, V. Revolutionary Trends in Mobile Banking Technology and the Influence of Digital Financial Literacy on Consumer Adoption in the United States. *Int. J. High Sch. Res.* **2025**, *7*, 56–64. [CrossRef]
43. Jang, J.M.; Kim, H. Diverging influences of usability in online authentication system: The role of culture (US vs Korea). *Int. J. Bank Mark.* **2022**, *40*, 384–400.
44. Faruk, M.A.A. Safeguarding Citizen Security and Fostering Economic Prosperity in Bangladesh through Digitization. *Econ. Aff.* **2024**, *69*, 469–477. [CrossRef]
45. Razzaq, K.; Shah, M. Machine Learning and Deep Learning Paradigms: From Techniques to Practical Applications and Research Frontiers. *Computers* **2025**, *14*, 93. [CrossRef]
46. Shubham; Sodhi, R.; Kaur, P. Safeguarding mobile ecosystems: A comprehensive examination of cyber-attacks and mobile security. *Int. J. Multidiscip. Trends* **2024**, *5*, 34–39.
47. Karunamurthy, A.; Kiruthivasan, R.; Gauthamkrishna, S. Human-in-the-Loop Intelligence: Advancing AI-Centric Cybersecurity for the Future. *Quing Int. J. Multidiscip. Sci. Res. Dev.* **2023**, *2*, 20–43.
48. Naik, B.; Mehta, A.; Yagnik, H.; Shah, M. The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex Intell. Syst.* **2022**, *8*, 1763–1780. [CrossRef]
49. Omolara, A.E.; Alabdulatif, A.; Abiodun, O.I.; Alawida, M.; Alabdulatif, A.; Arshad, H. The internet of things security: A survey encompassing unexplored areas and new insights. *Comput. Secur.* **2022**, *112*, 102494.
50. German, R.; Barber, K.S. Current Biometric Adoption and Trends. The University of Texas at Austin. Retrieved from Identity. 2017. Available online: https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%20and%20Trends.pdf (accessed on 19 March 2025).

51. Syed, W.K.; Mohammed, A.; Reddy, J.K.; Dhanasekaran, S. Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures. In Proceedings of the 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC), Gwalior, India, 27–28 July 2024.
52. Alwahaishi, S.; Zdrálek, J. Biometric authentication security: An overview. In Proceedings of the 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bengaluru, India, 6–7 November 2020.
53. Agidi, R.C. Biometrics: The future of banking and financial service industry in Nigeria. *Int. J. Electron. Inf. Eng.* **2018**, *9*, 91–105.
54. ALSaleem, B.O.; Alshoshan, A.I. Multi-factor authentication to systems login. In Proceedings of the 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 27–28 March 2021.
55. Singh, G.; Bhardwaj, G.; Singh, S.V.; Garg, V. Biometric Identification System: Security and Privacy Concern. In *Artificial Intelligence for a Sustainable Industry 4.0*; Awasthi, S., Travieso-González, C.M., Sanyal, G., Kumar Singh, D., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 245–264.
56. Stylios, I.; Kokolakis, S.; Thanou, O.; Chatzis, S. Key factors driving the adoption of behavioral biometrics and continuous authentication technology: An empirical research. *Inf. Comput. Secur.* **2022**, *30*, 562–582.
57. Bhagavatula, R.; Ur, B.; Iacovino, K.; Kywe, S.M.; Cranor, L.F.; Savvides, M. *Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption*; Internet Society: San Diego, CA, USA, 2015; Available online: https://ink.library.smu.edu.sg/sis_research/3967 (accessed on 16 March 2025).
58. Hino, H. Assessing factors affecting consumers' intention to adopt biometric authentication technology in e-shopping. *J. Internet Commer.* **2015**, *14*, 1–20. [CrossRef]
59. Akinnuwesi, B.A.; Uzoka, F.-M.E.; Okwundu, O.S.; Fashoto, G. Exploring biometric technology adoption in a developing country context using the modified UTAUT. *Int. J. Bus. Inf. Syst.* **2016**, *23*, 482–521. [CrossRef]
60. Lovisotto, G.; Malik, R.; Sluganovic, I.; Roeschlin, M.; Trueman, P.; Martinovic, I. *Mobile Biometrics in Financial Services: A Five Factor Framework*; University of Oxford: Oxford, UK, 2017.
61. Piotrowska, A. Determinants of consumer adoption of biometric technologies in mobile financial applications. *Econ. Bus. Rev.* **2024**, *10*, 81–100. [CrossRef]
62. Markevych, M.; Dawson, M. *A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI)*; International Conference Knowledge-Based Organization: Sibiu, Romania, 2023.
63. Rangaraju, S. Ai sentry: Reinventing cybersecurity through intelligent threat detection. *EPH-Int. J. Sci. Eng.* **2023**, *9*, 30–35. [CrossRef]
64. Vetrivel, S.; Mohanasundaram, T.; Saravanan, T.; Maheswari, R. Real-Time Analysis of Banking Data with AI Technologies. In *Artificial Intelligence for Risk Mitigation in the Financial Industry*; Wiley: Hoboken, NJ, USA, 2024; pp. 261–288.
65. Asokan, A.; Bhuvanesh, B.; Sandhiya, R. AI-Powered Disaster Data Calculation & SMS Alerting: An Overview. In Proceedings of the 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 23–25 October 2024.
66. Vieira, A.; Sehgal, A. How banks can better serve their customers through artificial techniques. In *Digital Marketplaces Unleashed*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 311–326.
67. Abououf, M.; Singh, S.; Mizouni, R.; Otrok, H. Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. *IEEE Internet Things J.* **2023**, *11*, 3446–3457. [CrossRef]
68. Syed, F.M.; ES, F.K. AI and Multi-Factor Authentication (MFA) in IAM for Healthcare. *Int. J. Adv. Eng. Technol. Innov.* **2023**, *1*, 375–398.
69. Ma, S.; Feng, R.; Li, J.; Liu, Y.; Nepal, S.; Diethelm; Bertino, E.; Deng, R.H.; Ma, Z.; Jha, S. An empirical study of sms one-time password authentication in android apps. In Proceedings of the 35th Annual Computer Security Applications Conference, San Juan, PR, USA, 9–13 December 2019.
70. Zimmermann, V.; Gerber, N. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *Int. J. Hum.-Comput. Stud.* **2020**, *133*, 26–44. [CrossRef]
71. Mehraj, H.; Jayadevappa, D.; Haleem, S.L.A.; Parveen, R.; Madduri, A.; Ayyagari, M.R.; Dhabliya, D. Protection motivation theory using multi-factor authentication for providing security over social networking sites. *Pattern Recognit. Lett.* **2021**, *152*, 218–224. [CrossRef]
72. Abbott, J.; Patil, S. How mandatory second factor affects the authentication user experience. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25–30 April 2020.
73. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. [CrossRef]
74. Shillair, R.; Esteve-González, P.; Dutton, W.H.; Creese, S.; Nagyfejeo, E.; von Solms, B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Comput. Secur.* **2022**, *119*, 102756. [CrossRef]

75. Robles-Gómez, A.; Tobarra, L.; Pastor-Vargas, R.; Hernández, R.; Haut, J.M. Analyzing the users' acceptance of an IoT cloud platform using the UTAUT/TAM model. *IEEE Access* **2021**, *9*, 150004–150020. [CrossRef]
76. Alsyouf, A.; Lutfi, A.; Alsubahi, N.; Alhazmi, F.N.; Al-Mugheed, K.; Anshasi, R.J.; Alharbi, N.I.; Albugami, M. The use of a technology acceptance model (TAM) to predict patients' usage of a personal health record system: The role of security, privacy, and usability. *Int. J. Environ. Res. Public Health* **2023**, *20*, 1347. [CrossRef] [PubMed]
77. Taherdoost, H. Development of an adoption model to assess user acceptance of e-service technology: E-Service Technology Acceptance Model. *Behav. Inf. Technol.* **2018**, *37*, 173–197.
78. Mutahar, A.M.; Daud, N.M.; Ramayah, T.; Isaac, O.; Aldholay, A.H. The effect of awareness and perceived risk on the technology acceptance model (TAM): Mobile banking in Yemen. *Int. J. Serv. Stand.* **2018**, *12*, 180–204.
79. Rahimi, R.A.; Oh, G.S. Beyond theory: A systematic review of strengths and limitations in technology acceptance models through an entrepreneurial lens. *J. Mark. Anal.* **2024**, 1–24. [CrossRef]
80. Rukhiran, M.; Wong-In, S.; Netinant, P. User acceptance factors related to biometric recognition technologies of examination attendance in higher education: TAM model. *Sustainability* **2023**, *15*, 3092. [CrossRef]
81. Buabeng-Andoh, C. Predicting students' intention to adopt mobile learning: A combination of theory of reasoned action and technology acceptance model. *J. Res. Innov. Teach. Learn.* **2018**, *11*, 178–191. [CrossRef]
82. Muñoz-Leiva, F.; Climent-Climent, S.; Liébana-Cabanillas, F. Determinants of intention to use the mobile banking apps: An extension of the classic TAM model. *Span. J. Mark.—ESIC* **2017**, *21*, 25–38. [CrossRef]
83. Zainal, H.Y. Examining the Factors Affecting Users' Cybersecurity Behaviour in Mobile Payment Contactless Technologies: A Hybrid SEM-ANN Approach. Ph.D. Thesis, The British University in Dubai (BUiD), Dubai, United Arab Emirates, 2022.
84. Afzal, M.; Ansari, M.S.; Ahmad, N.; Shahid, M.; Shoeb, M. Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: An integrated model approach. *J. Financ. Serv. Mark.* **2024**, *29*, 1503–1523.
85. Wang, J.S. Exploring biometric identification in FinTech applications based on the modified TAM. *Financ. Innov.* **2021**, *7*, 42.
86. Gusnan, Z.K.; Utomo, R.G. Factors affecting user's acceptance of adopting biometrics technologies using the tam model. *J. Tek. Inform. (Jutif)* **2024**, *5*, 309–320.
87. Fallatah, W.; Kävrestad, J.; Furnell, S. Establishing a Model for the User Acceptance of Cybersecurity Training. *Future Internet* **2024**, *16*, 294. [CrossRef]
88. Hanif, Y.; Lallie, H.S. Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technol. Soc.* **2021**, *67*, 101693. [CrossRef]
89. Sekaran, U. *Research Methods for Business: A Skill Building Approach*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
90. Luo, L.; Wildemuth, B.M. Semistructured interviews. In *Applications of Social Research Methods to Questions in Information and Library Science*; Bloomsbury Publishing: NewYork, NY, USA, 2009; pp. 248–257.
91. Bence, D.; Hapeshi, K.; Hussey, R. Examining investment information sources for sophisticated investors using cluster analysis. *Account. Bus. Res.* **1995**, *26*, 19–26. [CrossRef]
92. Adeoye-Olatunde, O.A.; Olenik, N.L. Research and scholarly methods: Semi-structured interviews. *J. Am. Coll. Clin. Pharm.* **2021**, *4*, 1358–1367. [CrossRef]
93. Chenail, R.J. Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *Qual. Rep.* **2011**, *16*, 255–262.
94. Bulmer, M.; Warwick, D.P. *Social Research in Developing Countries: Surveys and Censuses in the Third World*; Psychology Press: East Sussex, UK, 1993.
95. In, J. Introduction of a pilot study. *Korean J. Anesthesiol.* **2017**, *70*, 601–605. [CrossRef]
96. SBP. Payment Systems Review. 2024. Available online: https://www.sbp.org.pk/psd/pdf/PS-Review-Q3FY24.pdf (accessed on 18 November 2024).
97. Johri, A.; Kumar, S. Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Hum. Behav. Emerg. Technol.* **2023**, *2023*, 2103442. [CrossRef]
98. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Secur. Appl.* **2018**, *42*, 36–45. [CrossRef]
99. Nyimbili, F.; Nyimbili, L. Types of purposive sampling techniques with their examples and application in qualitative research studies. *Br. J. Multidiscip. Adv. Stud.* **2024**, *5*, 90–99. [CrossRef]
100. Rahimi, S. Saturation in qualitative research: An evolutionary concept analysis. *Int. J. Nurs. Stud. Adv.* **2024**, *6*, 100174. [CrossRef] [PubMed]
101. Mocănașu, D.R. Determining the sample size in qualitative research. In *International Multidisciplinary Scientific Conference on the Dialogue Between Sciences & Arts, Religion & Education*; Ideas Forum International Academic and Scientific Association: Târgoviște, Romania, 2020.

102. Creswell, J.W.; Poth, C.N. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*; Sage Publications: Thousand Oaks, CA, USA, 2016.
103. Guest, G.; Bunce, A.; Johnson, L. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* **2006**, *18*, 59–82. [CrossRef]
104. Easterby-Smith, M.; Jaspersen, L.J.; Thorpe, R.; Valizade, D. *Management and Business Research*; Sage: Thousand Oaks, CA, USA, 2021.
105. Saunders, B.; Sim, J.; Kingstone, T.; Baker, S.; Waterfield, J.; Bartlam, B.; Burroughs, H.; Jinks, C. Saturation in qualitative research: Exploring its conceptualization and operationalization. *Qual. Quant.* **2018**, *52*, 1893–1907. [CrossRef]
106. Pope, C.; Mays, N. *Qualitative Research in Health Care*; Wiley-Blackwell: Oxford, UK, 2013.
107. Clarke, V.; Braun, V. Thematic analysis. *J. Posit. Psychol.* **2017**, *12*, 297–298. [CrossRef]
108. Braun, V.; Clarke, V. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qual. Res. Psychol.* **2020**, *18*, 328–352. [CrossRef]
109. Welsh, E. Dealing with data: Using NVivo in the qualitative data analysis process. *Forum Qual. Sozialforschung/Forum Qual. Soc. Res.* **2002**, *3*. [CrossRef]
110. Bree, R.T.; Gallagher, G. Using Microsoft Excel to code and thematically analyse qualitative data: A simple, cost-effective approach. *All Irel. J. High. Educ.* **2016**, *8*. [CrossRef]
111. Allsop, D.B.; Chelladurai, J.M.; Kimball, E.R.; Marks, L.D.; Hendricks, J.J. Qualitative methods with Nvivo software: A practical guide for analyzing qualitative data. *Psych* **2022**, *4*, 142–159. [CrossRef]
112. Nakisa, B.; Ansarizadeh, F.; Oommen, P.; Shrestha, S. Technology Acceptance Model: A case study of palm vein authentication technology. *IEEE Access* **2022**, *10*, 120436–120449. [CrossRef]
113. Tam, C.; Balau, M.; Oliveira, T. What Influences People's Adoption of Cognitive Cybersecurity? *Int. J. Hum. Comput. Interact.* **2024**, *40*, 8295–8312. [CrossRef]
114. Hizam, S.M.; Ahmed, W.; Fahad, M.; Akter, H.; Sentosa, I.; Ali, J. 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)*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 2.
115. Dinev, T.; Hu, Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Inf. Syst.* **2007**, *8*, 23.
116. Alfalah, A.A. The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. *Int. J. Adv. Appl. Sci.* **2023**, *10*, 136–144.
117. Elrayah, M.; Jamil, S. Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness. *Int. J. Cyber Criminol.* **2023**, *17*, 166–187.
118. Ladipo, P.; Dixon-Ogbechi, B.; Enyinnaya, N.; Akeke, O. Influence of technology acceptance model (TAM) on customer adoption of e-banking practice in Lagos state. *J. Soc. Sci.* **2021**, *3*, 124–138.
119. Lesjak, D.; Zwilling, M.; Klein, G. Cyber crime and cyber security awareness among students: A comparative study in israel and slovenia. *Issues Inf. Syst.* **2019**, *20*, 80.
120. Zhang, T.; Yang, L.; Wu, Y. Evaluation of the Multifactor Authentication Technique for mobile applications. In *Intelligent Computing: Proceedings of the 2019 Computing Conference*; Springer: Berlin/Heidelberg, Germany, 2019; Volume 2.
121. Hussaini, B. Risks and Challenges Associated with Biometric Authentication in Multifactor Authentication Systems. Bachelor's Thesis, School of Engineering, Jönköping University, Jönköping, Sweden, 2024. Available online: https://www.diva-portal.org/smash/get/diva2:1901989/FULLTEXT01.pdf (accessed on 16 March 2025).
122. Cadet, E.; Osundare, O.S.; Ekpobimi, H.O.; Samira, Z.; Wondaferew, Y. *AI-Powered Threat Detection in Surveillance Systems: A Real-Time Data Processing Framework*; ResearchGate: Berlin, Germany, 2024.
123. Chirra, D.R. AI-Based Real-Time Security Monitoring for Cloud-Native Applications in Hybrid Cloud Environments. *Rev. Intel. Artif. Med.* **2020**, *11*, 382–402.
124. Colnago, J.; Devlin, S.; Oates, M.; Swoopes, C.; Bauer, L.; Cranor, L.; Christin, N. "It's not actually that horrible" Exploring Adoption of Two-Factor Authentication at a University. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018.
125. Busse, K.; Schäfer, J.; Smith, M. Replication: No one can hack my mind revisiting a study on expert and {Non-Expert} security practices and advice. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, 12–13 August 2019.
126. Jelínek, V. The Usage of Multi-Factor Authentication Amongst University Students. Bachelor's Thesis, Masaryk University, Brno, Czech Republic, 2020.
127. Kendyala, S.H. The Role of Multi Factor Authentication in Securing Cloud Based Enterprise Applications. *Int. Res. J. Mod. Eng. Technol. Sci.* **2020**, *2*, 820–835.
128. Anderson, C. *Study of Deployed Authentication Mechanisms*; Worcester Polytechnic Institute: Worcester, MA, USA, 2024.

129. Basori, A.A.; Ariffin, N.H.M. The adoption factors of two-factors authentication in blockchain technology for banking and financial institutions. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *26*, 1758–1764.
130. Henriksson, A. What Are the Motivations and Barriers for Incorporating Multi-Factor Authentication among IT Students? Available online: https://www.diva-portal.org/smash/get/diva2:1678668/FULLTEXT02 (accessed on 18 March 2025).
131. Albayram, Y.; Khan, M.M.H.; Fagan, M. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *Int. J. Hum. Comput. Interact.* **2017**, *33*, 927–942.
132. Childers, D. *State of the Auth: Experiences and Perceptions of Multi-Factor Authentication*; DuoLabs Report; Duo Labs: Ann Arbor, MI, USA, 2021.
133. Alammari, A.; Albahar, M. Exploring and Adoption of Two Authentication Factors: Formation of Competence. *ASEAN J. Psychiatry* **2022**, *23*, 1.
134. Chanda, K. Password security: An analysis of password strengths and vulnerabilities. *Int. J. Comput. Netw. Inf. Secur.* **2016**, *8*, 23.
135. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of multi-factor authentication for securing advanced IoT applications. *IEEE Netw.* **2019**, *33*, 82–88.
136. Crossler, R.E.; Bélanger, F. The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *J. Inf. Syst. Secur.* **2009**, *5*, 3.