Empirical Software Engineering (2025) 30:131
https://doi.org/10.1007/s10664-025-10689-z

(In)Security of mobile apps in developing countries: a systematic literature review

Alioune Diallo[1] · **Jordan Samhi**[1] · **Tegawendé F. Bissyandé**[1] · **Jacques Klein**[1]

Accepted: 17 June 2025 / Published online: 1 July 2025

Abstract
In developing countries, several key sectors, including education, finance, agriculture, and healthcare, mainly deliver their services via mobile app technology on handheld devices. These regions often face unique challenges such as limited cybersecurity infrastructure, lower digital literacy rates, and higher incidences of cyber threats targeting mobile platforms. Consequently, mobile app security has emerged as a paramount issue in developing countries, where the impact of security breaches can be more severe due to these vulnerabilities. In this paper, we performed a systematic literature review to identify studies on mobile app security in developing countries. We identified 25 primary studies and analysed the existing research directions taken, the different security concerns addressed, and the techniques used by researchers to highlight or address app security issues. Our main findings are: (1) the literature includes only a few studies on mobile app security in the context of developing countries (only 25 publications found); (2) among the different security concerns that researchers study, vulnerability detection appears to be the leading research topic; and (3) FinTech apps are revealed as the main target in the relevant literature. Overall, our work highlights that there is largely room for developing further specialized techniques addressing mobile app security in the context of developing countries.

Keywords Mobile application · Vulnerability · Security issue · Malware · Developing country · Literature review

Jordan Samhi, Tegawendé F. Bissyandé and Jacques Klein contributed equally to this work.

Communicated by: Daniel Méndez

✉ Alioune Diallo
alioune.diallo@uni.lu

Jordan Samhi
jordan.samhi@uni.lu

Tegawendé F. Bissyandé
tegawende.bissyande@uni.lu

Jacques Klein
jacques.klein@uni.lu

[1] TruX/SnT, University of Luxembourg, Kirchberg, Luxembourg

1 Introduction

Technological advancement has radically changed our daily lives in recent decades, providing tools such as tablets and smartphones. Mobile use worldwide has seen rapid adoption in the last decade (Olson et al. 2022; Turner 2023a). In particular, with 255 billion app downloads in the world (Turner 2023b), smartphones have become ubiquitous and used for various tasks.

A developing country, also known as an underdeveloped, low-income, or middle-income country, is generally defined as a country that has not yet achieved full maturity in terms of economic and industrial development (Review 2023). The United Nations Development Programme (UNDP) utilizes the Human Development Index (HDI)[1] score to assess whether a country falls into the category of developing or developed. In developing countries, mobile technology has enabled leapfrogging for mass adoption of critical digital services such as mobile money, e-health, e-agriculture, etc. Studies even forecast the adoption of smartphones in Sub-Saharan Africa to 87% by 2030[2].

While the popularity of smartphones worldwide has brought numerous opportunities and benefits (Keyideas 2017), it also comes with challenges and concerns due to the risks that they carry (Sheldon 2019). Mobile security threats and app vulnerabilities can pose significant risks in the critical services used.

On the one hand, mobile apps process sensitive data such as user credentials, financial data, medical information, user's location, etc. (Alaiad et al. 2019; Pentina et al. 2016). This makes users vulnerable to targeted attacks (Pentina et al. 2016). On the other hand, individuals are developing malicious apps that specifically target developing countries. This is justified by the fact that most of the ten countries in 2022 mostly affected by mobile malware are developing countries (Statica 2023). Additionally, mobile malware affects more than 10% of developing country mobile devices (Carter 2017).

Developing countries face unique challenges in many domains, particularly in the digital ecosystem (Lazović and Duričković 2014), which directly impacts mobile app security. These challenges include:

- Limitations in connectivity, which hinder systematic software updates and lead developers to implement unsafe workarounds such as naive, local, and insecure authentication.
- Persaviness of low-cost, but insecure, devices, which are often infected with viruses right out of the box (Kaminsky 2023).
- Low computing literacy and education, which creates awareness issues with security best practices in app development and usage.

These challenges contribute to an elevated level of digital security risks. Indeed, when developing mobile apps, developers may unintentionally leave security gaps that malicious actors can exploit, and outdated technology usage can compound security issues. For example, in developing countries, mobile financial applications face numerous security challenges, including those related to encryption, authentication, management of keys, credentials, and other secrets (approov 2023). There are also some frauds related to mobile financial

[1] https://hdr.undp.org/data-center/human-development-index#/indicies/HDI

[2] Source: http://www.osiris.sn/En-Afrique-subsaharienne-le-taux-d.html

services, such as theft of mobile money customer data using malware, account hijacking with Subscriber Identity Module (SIM) swap and changing Mobile Station International Subscriber Directory Number (MSISDN) linked to the mobile money account, technical attacks such as Denial of Service (DoS) attack and transmission data interception via man in the middle targeting mobile money systems, and Short Message Service (SMS) Spoofing (Osman et al. 2017; Castle et al. 2016).

Considering these challenges and the security aspects mentioned above, the security of mobile apps is a critical concern in developing countries. Focusing on mobile app security in these contexts is vital for improving knowledge and enhancing defense against privacy violations, threats, and cyberattacks.

Several secondary studies have been performed in the context of developing countries. Hoque et al. (2020) performed a review of studies related to mobile health applications by evaluating the quality of evidence reporting in mobile health literature, using the mobile health Evidence Reporting and Assessment (mERA) checklist as recommended by the World Health Organization (WHO). In this study, authors reveal a low level of familiarity with the mERA checklist among researchers in developing countries, and most mHealth studies do not adequately meet the essential criteria for evidence reporting. Msweli and Mawela (2020) reviewed the existing literature about the adoption of mobile banking services among the elderly in developing countries, focusing on the enablers and barriers. The paper highlights that while mobile banking has become prevalent in both developed and developing nations, research focusing on its adoption among the elderly is limited. The main barriers identified include security concerns, trust and privacy issues, a lack of personalization, and limited technical knowledge among the elderly. On the other hand, significant enablers include the perceived ease of use of mobile banking applications, perceived value, convenience, and consumer attitudes. Malik (2020) reviewed empirical research on Internet and mobile banking adoption in developing countries. The review focuses on the factors influencing the adoption of these technologies and the methodologies used in the studies. It also discusses the variables that have been extended in the Unified Theory of Acceptance and Use of Technology (UTAUT) model. In the study, the author highlights the directions, the most used analysis tools, and the main indicators of behavioral intention used in the publications.

Other studies exist to investigate the security of mobile apps. For instance, Martínez-Pérez et al. (2015) evaluate the current state of privacy and security in mobile health (mHealth) apps, focusing on reviewing existing laws regulating privacy and security in the European Union (EU) and the United States (USA), analyzing the corresponding academic literature, and proposing recommendations for app designers to ensure compliance with current security and privacy legislation. The review identified several research lines, including secure systems proposals, authentication techniques, and privacy aspects in Body Sensor Networks (BSNs). Key findings in this study highlighted the need for better security mechanisms in mHealth apps and the importance of user consent and data protection. Other authors reviewed existing literature to identify and analyze the security issues associated with the use of mobile educational apps (Mkpojiogu et al. 2021). The goal is to highlight the security challenges and propose ways to address these issues to enhance the security and usability of mobile educational apps. Their review identified several key security aspects in the use of mobile educational apps, including reliability, integrity, trust, privacy/confidentiality, and availability. They suggested several ways to address these security challenges.

Despite all the works performed to tackle the security of mobile apps in developing countries (Koala et al. 2020; Ibrar et al. 2017; Bassolé et al. 2020; Osho et al. 2019), we have identified five secondary studies that investigate the security of mobile apps, but none of them focus on this context. This indicates that a study is needed that provides a comprehensive overview of the current state of knowledge in this domain.

To address this gap, we conducted a systematic literature review (SLR). Our primary goal is to examine existing works on mobile app security specifically targeting mobile apps in developing countries. This study aims to provide actionable and impactful information for those addressing mobile application security issues in regions where resources are scarcer and challenges more pronounced. In this study, we have excluded countries with high and very high HDI and focused solely on those with medium and low HDI, based on the classification provided by the UNDP in its Human Development Report[3]. This focus ensures that our findings are relevant to contexts where the need for robust mobile app security measures is most critical. Our work aims to identify current research directions and highlight gaps in the literature, thereby pinpointing areas that require further investigation. Through systematically identifying existing studies, we offer an exhaustive survey of the field. This covers a broad range of pertinent research, thereby establishing a robust groundwork for future investigations. By doing so, we hope to contribute to developing more secure mobile applications in developing countries.

The main contributions of this study are as follows:

- We perform a systematic review of the literature on the security of mobile apps in developing countries: By following a systematic process, we identify relevant studies, extract data, and synthesize findings.
- We report on the type of research conducted. We categorize the studies based on their research focus (e.g., user study, app analysis, study of the development framework, app security testing, or study that focuses on proposing design & implementation solution). This analysis clarifies the methodological landscape and guides future research directions.
- We report on the security concerns addressed. We report the specific vulnerabilities and threats explored in the literature. By highlighting the security issues most relevant to developing countries, our review helps prioritize research efforts and tailor solutions to local challenges.
- We report on the type of analysis performed. We classify the methods used to assess mobile app security. This provides a valuable reference for researchers and practitioners seeking effective evaluation approaches.
- We identify research directions that must be followed to contribute to delivering more secure mobile apps in developing countries. By suggesting specific areas for improvement, we guide future research efforts. This encourages the development of specialized techniques that directly address the needs of these regions.

By combining these elements, we provide a good and non-existent resource for researchers, practitioners, and policymakers aiming to enhance mobile app security in regions with unique challenges.

[3] https://hdr.undp.org/sites/default/files/2021-22_HDR/HDR21-22_Statistical_Annex_HDI_Table.xlsx

Paper Organization The rest of this paper is organized as follows. Section 2 presents the background. Section 3 introduces the detailed methodology followed in this SLR. Section 4 reports the findings. Section 5 discusses explored and unexplored research directions, publication trends, and future challenges, Section 6 presents the threat that can compromise the validity of this study. Section 7 lists the related works. And finally, Section 8 concludes this paper.

2 Background

This section introduces terms and concepts related to our SLR on mobile app security in developing countries.

2.1 Mobile App Security

Mobile app security pertains to the measures implemented to safeguard mobile apps from various forms of threats, including hacking, mobile malware, data breaches, privacy violations, and other malicious activities[4]. In practical terms, mobile app security includes various aspects integrated during the app design process, such as:

- Ensuring that only authorized users can access the app by verifying their identity (e.g., using passwords, biometrics, or two-factor authentication).
- Controlling users' actions within the app based on their roles and permissions.
- Ensuring APIs used by the app are secure (e.g., validating input, using tokens).
- Protecting against API abuse and unauthorized access.
- Avoiding hardcoding secrets in the source code.
- Securing data transmitted between the app and servers using secure protocols such as HTTPS.
- Encrypting sensitive data when storing on the device.
- Storing sensitive data (such as passwords, tokens, or keys) securely within the app
- Implementing runtime security controls (e.g., obfuscation, anti-tampering mechanisms) to prevent reverse engineering and code modification.
- Keeping the app up-to-date with security patches and bug fixes.

Ignoring these aspects can lead to various security risks, including data breaches, privacy violations, and mobile malware attacks. Specifically, a data breach in the context of mobile apps refers to a security incident where unauthorized parties gain access to sensitive or confidential information stored within the app, including personally identifiable information, credit card numbers, and medical records (proofpoint 2024). Privacy violations in mobile apps refer to instances where an app mishandles sensitive user data, potentially compromising user privacy. Besides, mobile malware is malicious software that can exploit vulnerabilities to compromise the user's data security and privacy on the device or other installed apps. Mobile apps can contain exploitable risks and unsecured entry points that threat actors, including malware, can leverage.

[4] https://fraudwatch.com/blog/what-is-mobile-app-security-including-8-application-security-tips/

Given that mobile apps often handle sensitive information, such as financial records, personal health data, and location data. Numerous security concerns, including insecure communication, insecure data storage, improper usage of cryptography, and improper platform usage (ValueMentor 2022), can compromise the security of this information, leading to identity theft, financial losses, or reputational damage.

Adversaries can exploit these security issues using various methods, including man-in-the-middle attacks, authentication attacks, device theft, SMS interception, and more (Castle et al. 2016).

2.2 Standards and Initiatives Focused on Mobile Security

Several standards and initiatives aim to improve the security of mobile apps. The Open Web Application Security Project (OWASP) is a worldwide recognized non-profit organization dedicated to improving software security. OWASP plays a pivotal role in the field of mobile application security by providing a comprehensive set of guidelines, tools, and resources that aim to help developers and security professionals create secure mobile applications through the OWASP Mobile Application Security Project (OWASP 2024). This project provides a comprehensive standard for mobile app security, including the OWASP Mobile Application Security Verification Standard (MASVS) and the OWASP Mobile Application Security Testing Guide (MASTG). The MASVS serves as a framework for developing secure mobile applications. It provides a set of security requirements that architects and developers can use to ensure that their applications meet a high-security standard. The MASTG is a comprehensive manual for mobile application security testing. It covers various topics, from mobile OS internals to advanced reverse engineering techniques. It performs comprehensive security assessments, identifying and addressing all potential vulnerabilities. Developers, security testers, and organizations worldwide adopt these standards.

There is also a widely recognized standard for information security management systems, such as **ISO/IEC 27001** (ISO 2022). This standard offers comprehensive guidance for organizations of any size and in all sectors on establishing, implementing, maintaining, and continuously improving their information security management systems. Performing compliance with ISO/IEC 27001 means that an organization has implemented a systematic approach to managing risks associated with the security of the data it owns or handles. This approach adheres to the best practices and principles defined by this International Standard (ISO 2022). ISO/IEC 27001 could be applied to mobile security to manage data handled by mobile applications.

Furthermore, **NIST SP 800-124 Rev. 2** (Howell et al. 2023) offers guidelines for managing the security of mobile devices in enterprise environments. It offers comprehensive recommendations for the secure deployment, use, and disposal of mobile devices throughout their life cycle. NIST SP 800-124 Rev. 2 covers various topics, including mobile devices, centralized device management, and endpoint protection technologies. It addresses both organizational-provided and personally owned (bring your own device) deployment scenarios, as well (Howell et al. 2023).

These standards are highly relevant in mobile app security since they contribute to enforcing the security and securely protecting data handled and processed by mobile app.

2.3 Common Security Issues Faced by Mobile Apps

Worldwide, cybercriminals increasingly target mobile apps due to their widespread use and the sensitive data they handle. The OWASP Mobile security standard (OWASP 2024) grouped the most common security issues into ten (10) categories:

- **Improper Credential Usage.** This involves poor management of user credentials, such as storing passwords insecurely, using weak authentication methods, or hardcoded credentials. For example, an attacker could easily use existing open-source tools to reverse-engineer the app to retrieve the hardcoded credentials and use them for malicious purposes, leading to significant impacts.
- **Inadequate Supply Chain Security.** An attacker could introduce malicious code into the app code or modify the app to use third-party components or libraries containing malicious code during the build process. This could allow the attacker to control the app or the device and to gain unauthorised access to the user's information.
- **Insecure Authentication/Authorization.** Weaknesses in the mechanisms that verify user identity and control access to resources. When an app has this issue, the attacker may exploit it to bypass the authentication process and gain access to the resource. This issue is prevalent and can have serious impacts.
- **Insufficient Input/Output Validation.** The failure to properly validate data input and output can lead to injection attacks such as command injection, SQL injection, and cross-site scripting (XSS) attacks.
- **Insecure Communication.** This occurs when there is a lack of adequate encryption for data transmitted between the app and the server. This common issue could be exploited by intercepting the network traffic or installing malware on the device.
- **Inadequate Privacy Controls.** A poor handling of user data can lead to leaking data such as Personally Identifiable Information (PII). This information may allow the attacker to commit fraud by impersonating the user or damaging the user's data.
- **Insufficient Binary Protections.** Lack of protections against reverse engineering and tampering of the app's binary code could compromise user security. For example, when an app is not protected by reverse engineering, an attacker can decompile it, add malicious code, rebuild it, and distribute it to a third-party app store.
- **Security Misconfiguration.** This involves incorrect or default configurations that leave the app vulnerable to attacks, such as man-in-the-middle attacks, session hijacking, and allowing the theft of sensitive data. This could be exploited by malware installed on the device or by gaining access to the physical device.
- **Insecure Data Storage.** Storing sensitive data without or with weak encryption on the device makes it easier to access. This can lead to data breaches, unauthorized access, and reputation damage.
- **Insufficient Cryptography.** This involves using weak or flawed cryptographic methods that can be easily broken. Cryptographic methods are often used to protect sensitive data. Using insufficient cryptography can lead to unauthorized access to sensitive data, data breaches, financial losses, etc.

In addition to these issues, researchers have identified problems related to mobile apps:

- **Phishing and Smishing.** Attackers use fake messages to trick users into revealing personal information or installing malware (Mishra and Soni 2020).
- **Malicious Apps.** Apps that appear legitimate but contain harmful code (Madwanna et al. 2021).

These security issues concern mobile applications worldwide. However, the security of mobile apps in developing countries presents unique challenges (Nations 2023) compared to developed countries, including:

- A less reliable internet connectivity and outdated technological infrastructure.
- Limited financial and technical resources to implement robust security measures.
- A low digital literacy rate.
- And inconsistent or weak regulatory frameworks to enforce security standards.

2.4 Collaboration for Improving Mobile App Security

Improving mobile app security in developing countries requires collaboration among various stakeholders, including service providers, standardization bodies, government institutions, and educational institutions within developing countries. Stakeholders should understand the unique and specific challenges that developing countries face, and then efforts to develop collaboration strategies should focus on addressing these challenges. For example, a collaboration could be implemented with a banking institution that could explain why the low digital literacy rate imposes the use of specific apps' features (e.g., more pictures than text) targeted at developing countries. Due to the limited access to modern technology (the Unconnected 2023), several users rely on outdated technologies to access services. Stakeholders could collaborate to facilitate access to modern technologies and develop applications targeting only these technologies.

By promoting these collaborations, stakeholders can effectively contribute to ensuring the security of mobile apps, address challenges in developing countries, and also contribute to their overall development.

3 Methodology

In this study, we have followed the systematic literature review guideline proposed by Keele et al. (2007).

The research process, as depicted in Fig. 1, can be broken down as follows:

- We initiated the process by formulating precise research questions, serving as a foundation for identifying relevant publications.
- Guided by our research questions, we identified pertinent keywords.
- Previous keywords were instrumental in pinpointing a substantial body of relevant studies, culminating in constructing a comprehensive search string.
- Leveraging the search string developed in the prior step, we conducted systematic searches in four reputable digital libraries: IEEE Xplore, ACM Digital Library, Springer, and ScienceDirect.

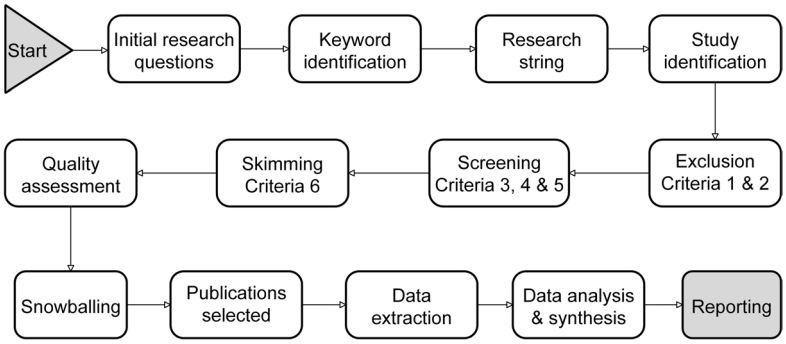

Fig. 1 Overview of the methodology followed in this SLR

- Having gathered publications from the digital libraries, we applied predefined exclusion criteria to filter out the most relevant publications.
- To further refine our selection, we meticulously reviewed the titles and abstracts of each paper, adhering to specific criteria. Only studies meeting these criteria were retained.
- We established a list of criteria to assess the quality of publications by removing poor-quality publications.
- We also employed backward and forward snowballing of selected publications to identify any potentially missed relevant ones.
- We extracted data from selected publications, allowing us to answer research questions.
- Then, we based on the data extracted to perform data analysis to guide the interpretation of the results.
- The final step reports our findings to the research community.

3.1 Research Questions

To provide an understanding of the publications produced by researchers to address the specific challenges of mobile app security, we have formulated a set of research questions (RQs). These RQs serve as the backbone of our investigation, and each sheds light on key aspects of this research field.

RQ0: In which venues are these studies published? Understanding where these studies are published provides a better understanding of the spread of knowledge about mobile app security in developing countries. This question overviews the conferences and journals where researchers have published their work.

RQ1: What are the research directions around mobile app security in developing countries? Mobile app security research can take various directions. Investigating these directions in developing countries points out the areas where researchers have chosen to concentrate their efforts. This knowledge informs us about the prevailing concerns and priorities in this context.

RQ2: What are the security concerns addressed in the literature? The security of mobile apps is a fundamental concern worldwide. As the use of mobile apps continues to grow in

developing countries, understanding the specific security issues that researchers address becomes crucial. This question unveils the most frequent security concerns relevant to mobile apps in these regions.

RQ3: Which apps are covered in the literature? This research question enables us to identify which of the multitude of application categories available are covered in the literature for developing countries. Recognizing the categories publications have focused on helps identify the gaps and areas needing further exploration.

RQ4: What techniques are used to detect security issues? Researchers employ various techniques to detect security issues in mobile apps. By unveiling these techniques, we gain insights into the strategies employed to identify security issues in the context of developing countries.

RQ5: What are the specific characteristics of malware and the techniques used to compromise devices? This research question aims to identify the various types of Android malware targeting developing countries. This will not only categorize the types of malware, but will also examine the techniques and procedures used, the active threat actors in these regions, the malware payloads, the most targeted information assets, and the attacks vectors.

RQ6: What motivated researchers to investigate mobile app security in developing countries? This question elucidates the various motivations mentioned in the literature, providing an understanding of the factors that have inspired researchers to investigate mobile app security in developing countries.

Each research question plays a key role in clarifying the multifaceted landscape of mobile app security in developing countries, contributing to a more informed and comprehensive understanding of this critical field.

3.2 Search Strategy

Getting relevant publications began by crafting a search string and executing our search across four well-regarded repositories.

Search string. Our search string was constructed based on a list of keywords derived from our previous research questions. These keywords were categorized into three groups, as displayed in Table 1: "Device," "Security," and "Target." Each line in the table represents a category with multiple corresponding keywords. For each category, we created a string, denoted as c_i(with *i* representing the category number), using a disjunction of its keywords, such as $c_1 = k_1$ OR k_2 OR k_3 OR ... OR k_n. We obtained three strings (c_1, c_2, c_3). We combined these three strings in our search string as a conjunction, resulting in the final search string, i.e., final_string = c_1 AND c_2 AND c_3. This final string was used in online repositories for our systematic search.

Well-known repositories. We conducted our SLR across four repositories: IEEE Xplore, ACM Digital Library, ScienceDirect, and Springer. The choice of these repositories is motivated by the fact that they are the most important and widely used in the scientific community. We employed Advanced Search for the first three repositories to refine our results,

Table 1 Keywords used in this SLR

Category	Search keywords
	android; mobile; smartphone; ”smart phone”; iphone; ios;
Device	”portable device”; app*
	security; malware; vulnerabilit*; weak*; exploit; flaw; breach; leak*; malicious;
Security	phishing; ransomware; trojan; attack; compliance; crypto*; forensic;
	”reverse engineering”; encryption; threat; hack*; ”privacy violation”
	”developing countr*”; ”developing world”; ”low-income countr*”;
Target	”middle-income countr*”; ”low and middle-income countr*”; Africa*;
	”south Asia*”; ”least-developed countr*”; **Country names**[a]

[a] Egypt; Libya; Angola; Benin; Botswana; ”Burkina Faso”; Burundi; Cameroon; ”Cabo Verde”; ”Central African Republic”; Chad; Comoros; Congo; ”Democratic Republic of the Congo”; ”Ivory coast”; Djibouti; ”Equatorial Guinea”; Eritrea; Eswatini; Ethiopia; Gabon; Gambia; Ghana; Guinea; ”Guinea Bissau”; Kenya; Lesotho; Liberia; Madagascar; Malawi; Mali; Mauritania; Mauritius; Mozambique; Namibia; Niger; Nigeria; Rwanda; ”St. Helena”; ”Sao Tome & Principe”; Senegal; ”Sierra Leone”; Somalia; ”South Sudan”; Sudan; Tanzania; Togo; Uganda; Zambia; Zimbabwe; Albania; Armenia; Azerbaijan; Belarus; ”Bosnia & Herzegovina”; Georgia; Kosovo; Macedonia; Moldova; Montenegro; Serbia; Ukraine; Belize; ”Costa Rica”; Cuba; Dominica; ”Dominican Republic”; ”El Salvador”; Grenada; Guatemala; Haiti; Honduras; Jamaica; Montserrat; Nicaragua; Panama; ”St. Lucia”; ”St. Vincent and the Grenadines”; Bolivia; Ecuador; Guyana; Paraguay; Peru; Suriname; Venezuela; Afghanistan; Bhutan; Cambodia; Kyrgyzstan; ”Lao People’s Democratic Republic”; Maldives; Mongolia; Myanmar; Nepal; Pakistan; Tajikistan; ”Timor Leste”; Turkmenistan; Uzbekistan; Jordan; Lebanon; ”Syrian Arab Republic”; ”West Bank and Gaza Strip”; Yemen; ”Cook Islands”; Fiji; Kiribati; ”Marshall Islands”; Micronesia; Nauru; Niue; Palau; ”Papua New Guinea”; Samoa; ”Solomon Islands” ; Tokelau; Tonga; Tuvalu; Vanuatu; ”Wallis & Futuna”; Philippines; Morocco; Bangladesh; India

focusing on each publication title and abstract. In Springer, we cannot focus our search on the title or the abstract; we performed a classic search across all metadata and filtered the results to computer science publications. To account for specific constraints related to search fields, we subdivided the main search string into multiple strings before executing the search. Notably, IEEE Xplore allows a maximum of 25 keywords in one clause. ScienceDirect restricts string searches to a maximum of 8 boolean operators. While ACM Digital Library and Springer did not explicitly describe these constraints in their documentation, we opted to apply the same limitations as IEEE Xplore to ensure optimal results.

Handling large results. Situations occur where our searches returned more than 1,000 items, exceeding Springer’s display limit. We employed a Python script to scrape all findings. Additionally, Python script-based verification was used. As mentioned above, in IEEE Xplore and ACM DL, we specifically focused our search on publication titles and abstracts to refine the results. However, in Springer, we couldn’t narrow down to titles and abstracts directly. Therefore, we initially conducted a general search, yielding numerous publications. Subsequently, we refined our search by targeting the titles and abstracts of the retrieved publications, ensuring consistency in the filtering process. In our Python script-based verification, we constructed a search string similar to the one used in IEEE Xplore. For titles, the search string looked like this: **((’android’ in title.lower() or ’mobile’ in title.lower() or ...) and (’security’ in title.lower() or ’malware’ in title.lower() or ...) and (’Country_1’ in title or ’Country_2’ in title or ...))**. For abstracts, the search string was as follows: **((’android’ in abstract.lower() or ’mobile’ in abstract.lower() or ...) and (’security’ in abstract.lower() or ’malware’ in abstract.lower() or ...) and (’Country_1’ in abstract or ’Country_2’ in abstract or ...))**. Unlike IEEE Xplore and ACM DL, ScienceDirect’s search may include publications that do not contain the complete search string in the title or

abstract, This also requires the Python script-based verification for additional checking to filter results effectively.

By employing these methods, we ensured comprehensive coverage and accuracy in our search across these repositories.

3.3 Exclusion Criteria

Following our search across cited repositories, we encountered a multitude of publications, including many irrelevant to our SLR due to the use of generic keywords. To curate a consistent dataset of relevant publications, we applied a set of exclusion criteria:

1. **Remove duplicate publications.** We employed a Python script to identify and remove duplicated entries based on title, abstract, author names, and year of publication. We found around 58 212 of duplicated publications that we removed.
2. **Exclude books, thesis reports, and non-English written papers**. Our search on ACM Digital Library returned several books and thesis reports that were not aligned with our SLR objectives, as well as publications that were not written in English. Therefore, we removed these entries (around 414), focusing on journal articles and conference papers.
3. **Filter out unrelated publications**. Some keywords in our search string yielded papers unrelated to mobile apps. We manually reviewed the remaining publications' titles and abstracts, excluding those deemed irrelevant. This step further refined our dataset, discarding approximately 98% of the results.
4. **Exclude non-security-focused publications.** Our dataset contains publications exclusively discussing mobile apps without addressing security. During the manual review of publications' titles and abstracts, we removed those publications.
5. **Remove non-developing-country papers.** During the manual review, we excluded publications that did not explicitly mention "developing country or related terms (e.g., "low-income countries," "emerging economies", name of a developing country, etc.). After this step, we have 88 remaining publications.
6. **Comprehensively review each paper.** We ensured each publication explicitly focuses on mobile application security in developing countries by reviewing each paper entirely. The authors have discussed any publication and decided to exclude 62 irrelevant publications when a consensus was reached.

By implementing these exclusion criteria, we systematically filtered and refined our dataset, ensuring that the publications included in our SLR were directly related to mobile app security in developing countries. At this stage, our dataset contains 26 publications. Figure 2 presents an overview and offers a clearer picture of the publication selection process.

3.4 Quality Assessment

Given that there is no universally accepted definition for 'quality' in the context of a study, the assessment of a study's quality can vary significantly depending on the purpose of the study (Kitchenham et al. 2009; Yang et al. 2021). The quality assessment process serves as an additional layer of scrutiny after applying general exclusion criteria. This step is crucial in mitigating biases that may arise from studies of low quality. In our study, we perform the

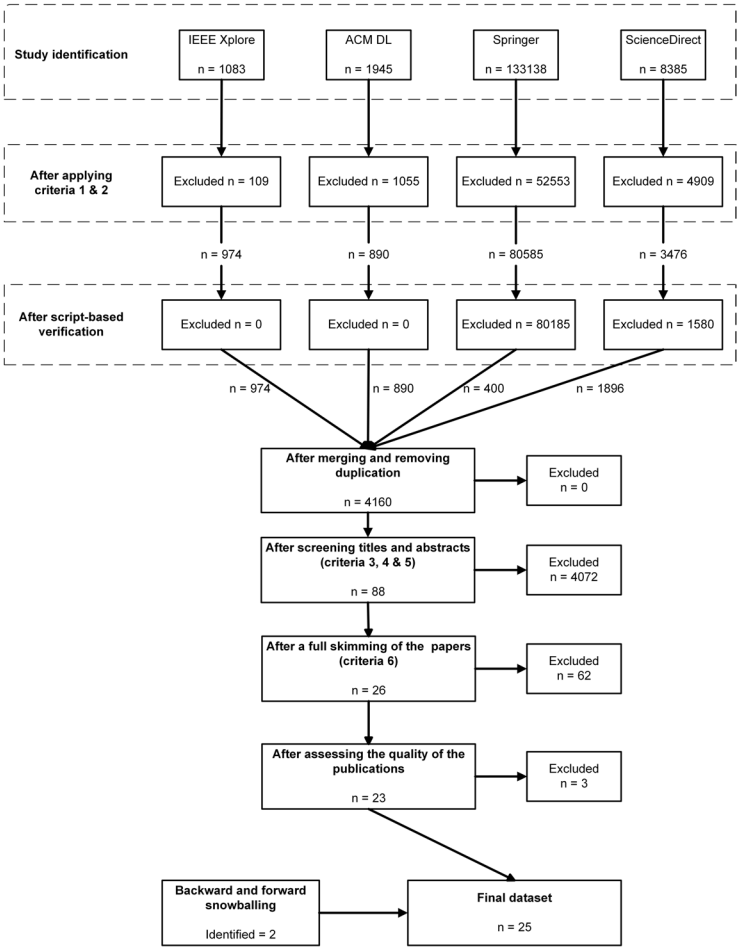

Fig. 2 Process of publication selection

quality assessment to provide a better quality of publications. This enables us to address the research questions more effectively and guides the analysis and interpretation of the results. Based on Kitchenham et al. (2009) and Yang et al. (2021), we have defined 5 quality assessment (QA) criteria that help us ensure optimal publication quality. These criteria are detailed in Table 2. We restrict our consideration to those publications that fulfill at least 3 of these QA criteria. As a result of this selection process, we have excluded 3 from the 26 remaining publications. These 3 papers indeed only fulfill 2 of the criteria listed in Table 2.

3.5 Snowballing

Since we have focused on the most important and widely used repositories in the scientific community, we could probably miss relevant publications published in other repositories. To deal with that, we initiated a backward and a forward snowballing process once we identified the primary publications relevant to our SLR. This involved a combination of auto-

Table 2 Criteria used for assessing the quality of the publications

	Assessment criteria
QA1	Is the paper clearly motivated?
QA2	Are the objectives of the paper clearly stated?
QA3	Does the paper provide a detailed description of the procedures used?
QA4	Are the results of the paper clearly presented and interpreted in the context of the objectives?
QA5	Does the paper discuss the key contributions?

mated scripts and manual efforts to collect references from these publications (backward snowballing) and publications having cited our dataset publications (forward snowballing). Using these collected publications, we utilized scripts to verify and remove any publications that did not align with the focus of our SLR.

Following this initial screening, we manually reviewed the remaining publications. If we encountered relevant publications that were not part of our originally selected primary studies, we incorporated them into our dataset. This iterative process ensured the comprehensive inclusion of pertinent literature in our SLR. We retrieved two additional publications from the backward snowballing.

Table 3 presents the full list of the selected paper.

3.6 Data Extraction

In this section, we present the information extracted to address the research questions mentioned earlier. Table 4 provides an overview of the data extracted from the selected publications. To answer RQ0, we collected metadata for each publication from the repository websites where they were published. These repositories offer comprehensive information about the publications. The extracted data include details related to the venues and the authors' affiliations. Next, we thoroughly read each publication to extract relevant information. Specifically:

- For RQ1, we identified the types of contributions conducted by researchers.
- To address RQ2, we examined the security concerns they tackled.
- For RQ3, we categorized the apps they focused on.
- To answer RQ4, we analyzed the various techniques used to detect and address security issues in these apps.
- Finally, to answer RQ5, we analyzed publications and extracted information related to the malware types, their payloads, the techniques and procedures used to compromise the phones, the active threat actors, and the information assets that are attacked the most in this region.

We have decided to group the selected publications into types of contributions after reading and getting results from the extraction of data. More details have been provided about these extracted data in the next section.

Table 3 The full list of the primary publications selected

Year	Venue type	Venue	Publication title
2023	Conference	ICOEI	Effective Security Testing of Mobile Applications for Building Trust in the Digital World (Kant Kamal et al. 2023)
2023	Conference	ACM SIGCAS/SIGCHI	Evaluating Mobile Banking Application Security Posture Using the OWASP's MASVS Framework (Chiboora et al. 2023)
2022	Conference	IEEE S&P	"Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya (Munyendo et al. 2022)
2022	Journal	HPT	Adoption of Covid-19 contact tracing app by extending UTAUT theory: Perceived disease threat as moderator (Chopdar 2022)
2022	Conference	ICKES	User's Perception on Security and Privacy in Using Crypto Currency Trading Application in India (Vakare et al. 2022)
2022	Conference	ICCCNT	State of Survey: Advancement of Knowledge Environmental Sustainability in Practicing Administrative Apps (Bandan et al. 2022)
2021	Journal	HPT	Understanding digital contact tracing app continuance: Insights from India (Prakash et al. 2021)
2021	Journal	RCS	Determining factors and impacts of the intention to adopt mobile banking app in Cameroon: Case of SARA by afriland First Bank (Kala Kamdjoug et al. 2021)
2021	Conference	ICSCCC	Security Issues of Unified Payments Interface and Challenges: Case Study (Madwanna et al. 2021)
2021	Conference	CT-RSA	Mesh Messaging in Large-Scale Protests: Breaking Bridgefy (Albrecht et al. 2021)
2020	Conference	AFRICOMM	Analysis of the Impact of Permissions on the Vulnerability of Mobile Applications (Koala et al. 2020)
2020	Conference	InterSol	Vulnerability Analysis in Mobile Banking and Payment Applications on Android in African Countries (Bassolé et al. 2020)
2020	Conference	COMPASS	We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh (Al-Ameen et al. 2020)
2020	Conference	COMS2	Signature Based Malicious Behavior Detection in Android (Sihag et al. 2020)
2020	Conference	USENIX Security	Security Analysis of Unified Payments Interface and Payment Apps in India (Kumar et al. 2020)
2019	Conference	ICSIoT	A Comparative Study of User Data Security and Privacy in Native and Cross Platform Android Mobile Banking Applications (Ansong and Synaepa-Addision 2019)
2019	Conference	ICCSA	Forensic Analysis of Mobile Banking Apps (Osho et al. 2019)
2019	Journal	MAT	Forensic analysis of mobile banking applications in Nigeria (Uduimoh et al. 2019)
2018	Conference	RTEICT	Integrating OAuth and Aadhaar with e-Health care System (Khatoon and Umadevi 2018)

Table 3 (continued)

Year	Venue type	Venue	Publication title
2017	Conference	ICTD	A Study of Static Analysis Tools to Detect Vulnerabilities of Branchless Banking Applications in Developing Countries (Ibrar et al. 2017)
2017	Journal	TOPS	Mo(Bile) Money, Mo(Bile) Problems: Analysis of Branchless Banking Applications (Reaves et al. 2017)
2017	Conference	ICEEG	Side-Effects of Permissions Requested by Mobile Banking on Android Platform: A Case Study of Morocco (Latifa et al. 2017)
2017	Conference	NSysS	Vulnerability detection in recent Android apps: An empirical study (Shezan et al. 2017)
2016	Conference	ANTS	On the MitM vulnerability in mobile banking applications for android devices (Kaka et al. 2016)
2016	Conference	ACM DEV	Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World (Castle et al. 2016)

Table 4 The list of the data extracted in the selected publications

Extracted information	Description	Corresponding RQ
Venue name	The name of the venue where the paper has been published.	
Venue Type	The type of the venue where the paper has been published.	RQ0
Venue location	The location where the venue held.	
Type of contribution	The type of contribution researchers performed.	RQ1
Secuirty issues	The issues of security researchers addressed in their publications.	RQ2
Category of app	The categories (according to GooglePlay) of app researchers studied in their works.	RQ3
Issue detection technique	The techniques and methods used to detect issues on the apps.	RQ4
Malware characteristics	The types of malware identified, their procedure and compromise techniques, their payloads, threat actors and targeted information assests	RQ5

3.7 Data Analysis and Synthesis

In the previous section, we extracted several data to address research questions. Based on these data, our analysis involves systematically addressing each research question with the appropriate analysis technique.

3.7.1 Quantitative Analysis

In this section, we particularly focus on quantifying the data extracted from the previous section. We use descriptive statistics to summarize the metadata. For example, we count the number of publications per venue type, geographical distribution of venues, and frequency of publications from different institutions. We then create frequency distributions and visualizations to see the prevalence of each type of contribution, each detection technique, and the distribution of app categories. Finally, we quantify the occurrence of different security aspects and malware types, techniques, and threat actors.

3.7.2 Open Coding (Qualitative Analysis)

To apply open coding, we read through the papers, identified key concepts (e.g., security), and assigned "labels" (e.g., permissions, or cryptography) to these concepts. Then, we grouped similar "labels" into broader categories (e.g., security concerns). To ensure that they accurately represent the data, we reviewed and refined the categories. By applying this process to the papers, we identified several key categories, including app categories, geographic focus, contribution types, analysis methods, security concerns, and analysis focus. This process helps in organizing and interpreting the data, making it easier to draw meaningful insights and address the RQs.

4 Results

In this section, we present and interpret the study results and answer the research questions. The study consists of identifying research works concerning the security of mobile apps used in the context of developing countries. We have identified 25 publications investigating mobile app security. We provide a summary, the strengths, and the limitations of each study presented in these 25 papers in Appendix A.

All have, indeed, investigated mobile apps used in developing countries. In Table 5, we map publications with the context of the study to show where the apps addressed are used.

4.1 Publication Venue and Paper

This section details the distribution of publications according to venue type, geographic origin, and conference locations. In this study, a paper is considered to originate from a specific place if all authors' affiliations match that location. As illustrated in Fig. 3, 76% of publications come from a developing country.

We have found that 80% (20 out of 25) of the publications are presented at conferences, with the remaining 20% in journals, as illustrated in Fig. 4. Almost every venue accounts for one publication, except one journal venue for two.

Given the preponderance of conference publications in the literature, it is noteworthy that researchers often present their work at conferences held in the country of their institutions or in a developing country. Indeed, approximately 75% of conference publications (corresponding to 15) originate from developing country institutions. Among these publications, three (Osho et al. 2019; Chiboora et al. 2023; Latifa et al. 2017) were not presented at con-

Table 5 Mobile app origin area (**N.S**: Not Specified)

Paper	App country origin	Contient
Castle et al. (2016)	N.S	Dev. countries
Koala et al. (2020)	Burkina Faso	Africa
Ibrar et al. (2017)	N.S	Dev. countries
Bassolé et al. (2020)	N.S	Africa
Osho et al. (2019)	Nigeria	Africa
Kant Kamal et al. (2023)	India	Asia
Chiboora et al. (2023)	N.S	Africa
Munyendo et al. (2022)	Kenya	Africa
Chopdar (2022)	India	Asia
Vakare et al. (2022)	India	Asia
Bandan et al. (2022)	Bangladesh	Asia
Prakash et al. (2021)	India	Asia
Kala Kamdjoug et al. (2021)	Cameroon	Africa
Madwanna et al. (2021)	India	Asia
Albrecht et al. (2021)	Belarus, Zimbabwe	Africa, Europe
Al-Ameen et al. (2020)	Bangladesh	Asia
Sihag et al. (2020)	India	Asia
Kumar et al. (2020)	India	Asia
Ansong and Synaepa-Addision (2019)	Ghana	Africa
Uduimoh et al. (2019)	Nigeria	Africa
Khatoon and Umadevi (2018)	India	Asia
Reaves et al. (2017)	N.S	Dev. countries
Latifa et al. (2017)	Morocco	Africa
Shezan et al. (2017)	Bangladesh	Asia
Kaka et al. (2016)	India	Asia

ferences held in developing countries, as illustrated in Table 6. Conversely, non-developing countries contribute a few conference publications (Castle et al. 2016; Munyendo et al. 2022; Albrecht et al. 2021; Al-Ameen et al. 2020; Kumar et al. 2020), with one taking place in a developing country (Castle et al. 2016).

Among the journal publications, one is identified as non-developing countries' contribution (Reaves et al. 2017).

Answer to RQ0

Most studies have been presented at conferences held in developing countries. Nevertheless, mobile app security in developing countries has attracted the interest of developers located outside these countries.

4.2 Types of Contributions

This section outlines the types of contributions performed by researchers examining mobile app security in developing countries. As presented in Table 7, the literature primarily focuses on five main types: user studies, development framework study (DFS), app analysis, app security testing, and designing & implementing solutions (D&I Solution).

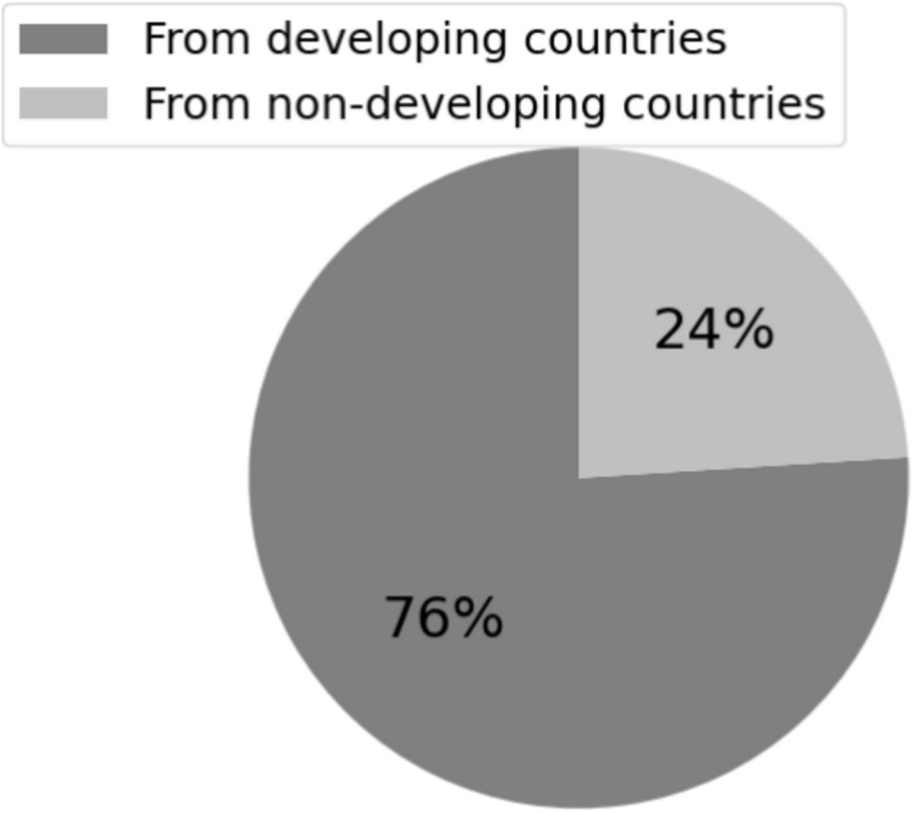

Fig. 3 Publications frequencies from different areas

User study. Security's impact on the adoption of mobile applications in developing countries is a central concern. Around 36% of publications utilize surveys and interviews to gauge this impact. Some of these studies do not exclusively focus on the security of mobile apps but explore broader factors influencing app adoption. For instance, researchers employed models such as the Unified Theory of Acceptance and Use of Technology (UTAUT), the Health Belief Model (HBM), and the Expectation-Confirmation Model (ECM) to understand the factors influencing the adoption and the continuance to adopt mobile health apps in India (Chopdar 2022; Prakash et al. 2021). Similarly, studies in Cameroon leveraged the UTAUT2 framework, the Technology Acceptance Model (TAM), and the Protection Motivation Theory (PMT) to examine the factors influencing users' decisions to adopt mobile banking apps (Kala Kamdjoug et al. 2021). The studies incorporate additional factors, including perceived security and privacy, ease of use, trust in technology, user satisfaction, and perceived usefulness. The Partial Least Squares Structural Equation Modeling (PLS-SEM) is utilized to analyze user questionnaire responses. These studies focused on specific app users and found the factors mentioned above significantly impact the adoption of mobile banking and health apps. Other user study-focused publications concentrate specifically on mobile app security. For example, authors investigated security and privacy perceptions related to cryptocurrency trading apps in India by using supervised

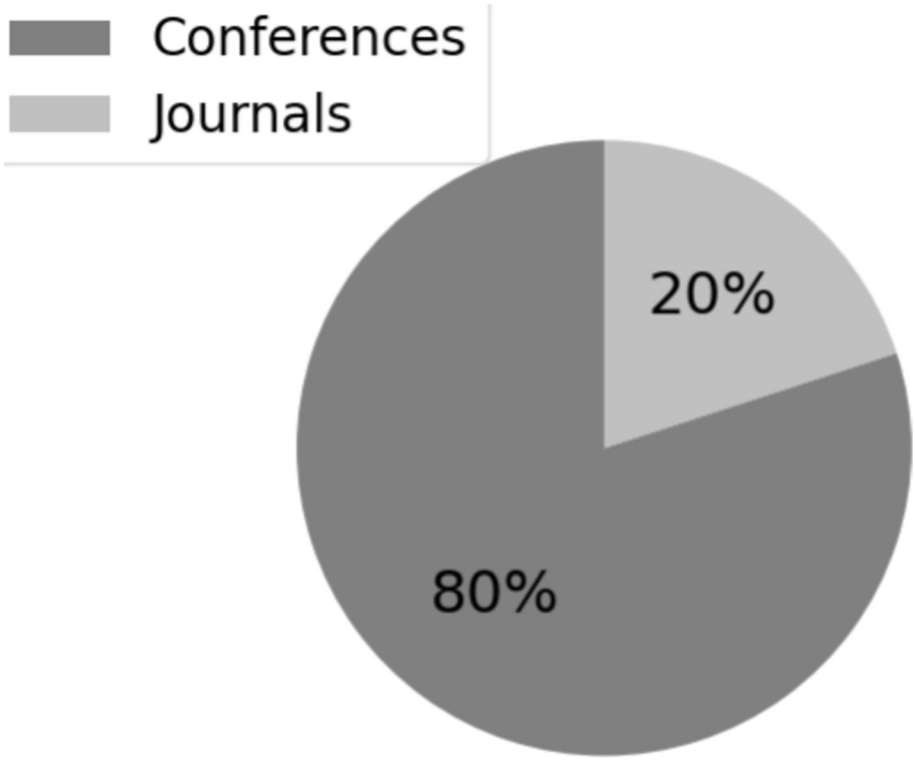

Fig. 4 Publications per venue type

machine learning algorithms (such as Random Forest and Logistic Regression) to analyze user reviews and sentiments (Vakare et al. 2022). In Kenya and Bangladesh, researchers explored user perceptions, behaviors, and privacy concerns associated with data collected by mobile apps (Munyendo et al. 2022; Al-Ameen et al. 2020). The studies reveal that some users recognized the necessity of data collection for app functionality, while others expressed fear or indifference.

App analysis. Most works performed in developing country contexts, approximately 60%, are dedicated to detecting vulnerabilities and privacy violations through app analysis. App analysis involves examining various aspects of a mobile app to understand its performance, security, and user behavior. A subset of the publications combines user studies with app analysis to measure the capacity of developers in implementing protection and ensuring users' security and privacy (Castle et al. 2016; Chiboora et al. 2023). However, the majority of the works have exclusively focused on app analysis, which predominantly centers on static, dynamic, forensic analysis, and a combination of static and dynamic analysis (see more details in Section 4.5). Despite the security challenges mobile applications face in developing countries (approov 2023), most publications do not use specialized approaches to deal with these challenges. However, few studies have developed app analysis approaches specifically for the context of developing countries. For instance, knowing that developing countries face numerous threats in mobile financial services, Castle et al. (2016) have focused on the features and development practices of mobile financial apps in this context.

Table 6 Overview of publications and venues

Year	Paper	Venue	Location	VHIDC *	1st author's institution	ILIDC **	Co-authors' institutions (# of authors)
Conference							
2019	Ansong and Synaepa-Addision (2019)	ICSIoT	Accra, Ghana	Yes	Kwame Nkrumah Univ. of Sci. and Tech., Kumasi, Ghana	Yes	Kwame Nkrumah Univ. of Sci. and Tech., Kumasi, Ghana (1)
2017	Ibrar et al. (2017)	ICTD	Lahore, Pakistan	Yes	Information Technology University, Pakistan	Yes	Information Technology University, Pakistan (2) University of Washington, USA (1)
2019	Osho et al. (2019)	ICCSA Russia	Saint Petersburg,	No	Federal University of Technology, Minna, Nigeria	Yes	Federal University of Technology, Minna, Nigeria (3) Covenant University, Ota, Nigeria (1)
2016	Castle et al. (2016)	ACM DEV	Nairobi, Kenya	Yes	University of Washington, USA	No	University of Washington, USA (3) Cornell University, New York, USA (1) University of Dhaka, Bangladesh (1)
2020	Al-Ameen et al. (2020)	COMPASS	Ecuador	No	Utah State University, USA	No	Jadavpur University, India (1) Utah State University, USA (1) University of Toronto, Canada (2)
2020	Bassolé et al. (2020)	InterSol	Nairobi, Kenya	Yes	Université Joseph Ki-Zerbo, Ouagadougou, Burkina Faso	Yes	Université Joseph Ki-Zerbo, Ouagadougou, Burkina Faso (3)
2022	Munyendo et al. (2022)	IEEE S&P	San Francisco, CA, USA	No	Geoge Washington University, Washington, DC, USA	No	Geoge Washington University, Washington, DC, USA (2)
2019	Koala et al. (2020)	AFRI-COMM	Porto-Novo, Benin	Yes	Université Joseph Ki-Zerbo, Ouagadougou, Burkina Faso	Yes	Université Joseph Ki-Zerbo, Ouagadougou, Burkina Faso (4)

Table 6 (continued)

Year	Paper	Venue	Location	VHIDC *	1st author's institution	ILIDC **	Co-authors' institutions (# of authors)
2017	Latifa et al. (2017)	ICEEG	Turku, Finland	No	University Cadi Ayyad, Marrakesh, Morocco	Yes	University Cadi Ayyad, Marrakesh, Morocco (2)
2022	Vakare et al. (2022)	ICKES	Chickballapur, India	Yes	Symbiosis University, Indore, India	Yes	Symbiosis University, Indore, India (2)
2016	Kaka et al. (2016)	ANTS	Bangalore, India	Yes	University of Hyderabad, Hyderabad, India	Yes	Centre for Mobile Banking, IDRBT, Hyderabad, India (2)
2017	Shezan et al. (2017)	NSysS	Dhaka, Bangladesh	Yes	Bangladesh University of Engineering and Technology	Yes	Bangladesh University of Engineering and Technology (2)
2022	Bandan et al. (2022)	ICCCNT	Kharagpur, India	Yes	Daffodil International University, Dhaka, Bangladesh	Yes	Daffodil International University, Dhaka, Bangladesh (4)
2023	Kant Kamal et al. (2023)	ICOEI	Tirunelveli, India	Yes	Centre for Development of Advanced Computing (C-DAC), Mumbai, India	Yes	C-DAC, Mumbai, India (2) Ministry of Electronics and Information Technology (MeitY), Delhi, India (1)
2023	Chiboora et al. (2023)	ACM SIGCAS /SIGCHI	Cape Town, South Africa	No	Cylab-Africa/Upanzi Network Kigali, Rwanda	Yes	Cylab-Africa/Upanzi Network Kigali, Rwanda (3)
2021	Madwanna et al. (2021)	ICSCCC	Jalandhar, India	Yes	NIT, Karnataka, Surathkal, Mangalore, India	Yes	NIT, Karnataka, Surathkal, Mangalore, India (2)
2018	Khatoon and Umadevi (2018)	RTEICT	Bangalore, India	Yes	B.M.S. College of Engineering, Bengaluru, India	Yes	B.M.S. College of Engineering, Bengaluru, India (1)

Table 6 (continued)

Year	Paper	Venue	Location	VHIDC *	1st author's institution	ILIDC **	Co-authors' institutions (# of authors)
2020	Sihag et al. (2020)	COMS2	Gujarat, India	Yes	Sardar Patel University of Police, Jodhpur, India	Yes	Sardar Patel University of Police, Jodhpur, India (1) National Institute of Technology, Raipur, India (2)
2021	Albrecht et al. (2021)	CT-RSA	Virtual Event	-	University of London, London, UK	No	University of London, London, UK (3)
2020	Kumar et al. (2020)	USENIX Security	USA	No	University of Michigan	No	University of Michigan (3)
Total			13		15		
Journal							
2021	Kala Kamdjoug et al. (2021)	RCS	-	-	Catholic University of Central Africa, Yaoundé, Cameroon	Yes	University of Grenoble, Grenoble Cédex 9, France (1) Catholic University of Central Africa, Yaoundé, Cameroon (1) Toulouse Business School, Toulouse, France (1)
2017	Reaves et al. (2017)	TOPS	-	-	University of Florida, FL, USA	No	University of Florida, FL, USA (5) University of Illinois at urbana-champaign, USA (1)
2019	Uduimoh et al. (2019)	MAT	-	-	Federal University of Technology, Minna, Nigeria	Yes	Federal University of Technology, Minna, Nigeria (2) Clemson University, Clemson, SC, USA (1)

Table 6 (continued)

Year	Paper	Venue	Location	VHIDC *	1st author's institution	ILIDC **	Co-authors' institutions (# of authors)
2022	Chopdar (2022)	HPT	-	-	Indian Institute of Management, Shillong, India	Yes	-
					Indian Institute of Technology Kharagpur,		Indian Institute of Technology Kharagpur,
2021	Prakash et al. (2021)	HPT	-	-	West Bengal, India	Yes	West Bengal, India (1)
							Manipal Academy of Higher Education, KA,
							India (1)

* Venue held in a developing country.

** Institution located in a developing country

Table 7 Overview of the types of research

Publication	User study	App analysis	DFS	App security testing	D&I solution
Albrecht et al. (2021)		✗			
Al-Ameen et al. (2020)	✗				
Ansong and Synaepa-Addision (2019)			✗		
Bandan et al. (2022)	✗				
Bassolé et al. (2020)		✗			
Castle et al. (2016)	✗	✗			
Chiboora et al. (2023)	✗	✗			
Chopdar (2022)	✗				
Ibrar et al. (2017)		✗			
Kaka et al. (2016)		✗			
Kala Kamdjoug et al. (2021)	✗				
Kant Kamal et al. (2023)				✗	
Khatoon and Umadevi (2018)					✗
Koala et al. (2020)		✗			
Kumar et al. (2020)		✗			
Latifa et al. (2017)		✗			
Madwanna et al. (2021)		✗			
Munyendo et al. (2022)	✗				
Osho et al. (2019)		✗			
Prakash et al. (2021)	✗				
Reaves et al. (2017)		✗			
Shezan et al. (2017)		✗			
Sihag et al. (2020)		✗			✗
Uduimoh et al. (2019)		✗			
Vakare et al. (2022)	✗			✗	
Number of publication	**9 (36%)**	**15 (60%)**	**1 (4%)**	**2 (8%)**	**2 (8%)**

In other studies, authors have used approaches to specifically uncover vulnerabilities in UPI1.0 apps that banks from India used (Kumar et al. 2020; Madwanna et al. 2021).

Development framework study. This type of study delves into the usage of development platforms and their security guidelines in developing countries. Several studies show that Android apps often request more permissions than they need or use, impacting the security and privacy of the users' apps (Khatoon and Corcoran 2017; Alenezi and Almomani 2017). Researchers, such as Ansong and Synaepa-Addision, think that stems from the development frameworks used (Ansong and Synaepa-Addision 2019). Aiming to ensure better user data privacy and security in mobile banking apps, they provide in their study a case in point, exploring mobile app security by comparing different development frameworks, including native and cross-platform, used to develop mobile banking apps in Ghana. Development frameworks for developing mobile apps are not specific to the context of developing countries. Indeed, cross and native development frameworks are used worldwide. Authors found that cross-platform apps tend to use more of the requested permissions compared to native apps.

App security testing. App security analysis often involves penetration testing. It simulates attacks on the mobile app to identify and address security vulnerabilities that could be exploitable, helping in enhancing the overall security posture of the app (bertolis 2022). As they feel the need to address security issues on the apps, some researchers test the security posture of mobile apps from a specific AppStore in India's mSeva AppStore) using existing automated analysis tools for several security concerns (Kant Kamal et al. 2023). Their regressive testing methods focus on evaluating multiple facets of mobile apps before hosting in the Inda AppStore, emphasizing the critical need for robust security testing procedures. Similarly, others delve into India's mobile-based cryptocurrency trading apps' security and privacy aspects using penetration testing techniques (Vakare et al. 2022). In this work, authors use the OWASP mobile security testing framework to conduct a security analysis on the apps and identify several vulnerabilities. However, all these security testing approaches are not specific to the unique context of developing countries.

Designing & implementing solution. Proposing sophisticated techniques is pivotal in fortifying the security of mobile apps worldwide. Some authors recognized this necessity by designing and implementing specialized solutions. However, these solutions did not specifically target the concerns of developing countries. Indeed, the authors proposed a system that focuses on identifying malicious behaviors that could lead to several security concerns by analyzing system-generated logs during the execution of the app (Sihag et al. 2020). The main goal is to provide a more dynamic and insightful detection method compared to existing techniques. Besides, Khatoon and Umadevi have considered the problems facing developing country app users by creating a solution to ensure secure access, authentication, and authorization for Indian stakeholders within sensitive domains like healthcare (Khatoon and Umadevi 2018). In their study, they integrate a known secure protocol for access delegation (OAuth 2.0) and the Aadhaar identification system of India into e-Health apps to enhance their security, offering secure access to health data and facilitating efficient interaction between patients and healthcare providers. The proposed system ensures the users' registration, login, and authentication and allows access without an Internet connection.

Answer to RQ1

Our review highlights that the research on mobile app security in developing countries is broad, ranging from user studies to the design & implementation of technical solutions. It is noteworthy, however, that most works have focused on app analysis.

4.3 Security Concerns

This section enumerates the key security concerns of mobile apps in developing countries addressed in the literature.

This information underscores the importance of addressing these concerns to mitigate the associated risks, such as privacy data leaks, unauthorized access, remote command execution, data interception, insecure data protection, etc. As illustrated in Table 8, most of the publications have addressed security issues related to data storage, permissions, network communication, and cryptography.

Several studies reveal that apps insecurely store sensitive data in memory (Uduimoh et al. 2019), log sensitive data clear text or with poor encryption (Castle et al. 2016; Reaves et al. 2017), or allow data backup and enable other apps to read log files (Ibrar et al. 2017). This issue can easily compromise users' security since tools, such as ADB, can be used, for example, to do complete backups of the apps containing sensitive data (Argudo et al. 2017).

Permissions in mobile apps help users to protect restricted access such as users' information, system state, audio/camera record, and connecting to a paired device (Android 2023a). However, one could use them to collect users' sensitive data (Munyendo et al. 2022). Studies reveal that various apps request permissions to access resources, such as for writing and reading data in the external storage (Castle et al. 2016; Koala et al. 2020), and abuse permissions, which most are categorized as risky (Bassolé et al. 2020; Ansong and Synaepa-Addision 2019).

Android uses the SSL/TLS protocol to secure communication by protecting the app's data in the network. Several trusted Certificate Authorities in Android provide certificates for many servers. In communication between a server, the app should verify the trustworthiness of the server by checking the certificate (Android 2023b). Unfortunately, this is not the case in some apps. Indeed, studies reveal that several apps do not implement or properly use SSL/TLS certification validation (Ibrar et al. 2017; Reaves et al. 2017). Occasionally, apps use insecure protocols, such as HTTP, for certain communication (Castle et al. 2016; Reaves et al. 2017). Even if this communication does not transport sensitive data, it can be used by attackers for man in a man-in-the-middle attack or by a phishing attack.

Studies reveal that cryptography is poorly used in several mobile apps. Some apps use custom cryptography or poorly implemented cryptographic mechanisms (Reaves et al. 2017). While others use insecure cipher modes such as ECB, outdated cryptographic protocols like MD5, SHA1, and DES, and hard-coded cryptographic keys to encrypt data (Ibrar et al. 2017; Chiboora et al. 2023).

Beside that, some concerns are not commonly addressed in the literature. For example, there are security concerns related to code quality and resilience. Code quality addresses coding vulnerabilities originating from external sources, including app data entry points, the OS, and third-party software components (OWASP 2024a). For instance, Android debug mode enables the transfer of data from the app to a computer and vice versa, as well as installing and uninstalling apps on the device, reading logcat memory, etc. The developer can enable this mode on the app for testing purposes. However, if it is not disabled before its deployment, the app could allow attackers to inject code for malicious activities, access sensitive data, etc. In some studies, researchers found that this mode is enabled in several apps (Shezan et al. 2017; Chiboora et al. 2023). The resilience aspect covers vulnerabilities leading to app reverse-engineering, tampering, device jailbreak, etc. It verifies that the app operates on a trusted platform, prevents runtime tampering, and maintains the integrity of the intended app functionality (OWASP 2024b). Some authors have analyzed apps for resilience and found that several apps try to have root access on the device, do not implement any obfuscation methods, and do not prevent reverse-engineering (Kant Kamal et al. 2023; Chiboora et al. 2023).

Table 8 The security concerns addressed in the literature

Publication	Data Storage	Cryptography	Permission	Access Control	Network Comm.	IPC	3rd-party Library	WebView	Malware	Code Quality and Build	Re-sil-ience
Albrecht et al. (2021)		✗	✗	✗	✗						
Ansong and Synaepa-Addi-sion (2019)			✗								
Bassolé et al. (2020)	✗		✗						✗		
Castle et al. (2016)	✗		✗	✗	✗		✗				
Chiboora et al. (2023)	✗	✗	✗		✗					✗	✗
Ibrar et al. (2017)	✗	✗			✗	✗		✗			
Kaka et al. (2016)					✗						
Kant Kamal et al. (2023)	✗	✗			✗						✗
Koala et al. (2020)			✗								
Kumar et al. (2020)			✗	✗							
Latifa et al. (2017)			✗								
Madwanna et al. (2021)									✗		
Munyendo et al. (2022)			✗								
Osho et al. (2019)	✗										
Reaves et al. (2017)	✗	✗		✗	✗						
Shezan et al. (2017)	✗					✗	✗	✗		✗	
Sihag et al. (2020)									✗		
Uduimoh et al. (2019)	✗										
Vakare et al. (2022)	✗	✗			✗						
Number of publication	**10 (40%)**	**6 (24%)**	**9 (36%)**	**4 (16%)**	**8 (32%)**	**2 (8%)**	**2 (8%)**	**2 (8%)**	**3 (12%)**	**2 (8%)**	**2 (8%)**

These concerns affect mobile apps worldwide. However, some studies addressed them by focusing on security challenges in developing countries (Castle et al. 2016).

Answer to RQ2

In most publications, investigations are related to data storage, permissions, network communication, and cryptography, concerns that are not specific to developing countries. A few studies, however, have addressed various security concerns by focusing on specific challenges in developing countries.

4.4 Categories of Apps

As shown in Table 9, the SLR illustrates the primary interest in financial applications, particularly mobile banking and money apps. Financial apps receive substantial attention from researchers. Some researchers analyzed the security vulnerabilities of mobile banking and payment apps within African countries aiming to create awareness among users, businesses, and governments about potential security threats (Bassolé et al. 2020), to assess how these apps handle sensitive user information, and to identify potentially exploitable vulnerabilities (Osho et al. 2019). Others provide a comprehensive security analysis of the Unified Payments Interface used by some mobile payment apps in India, aiming to identify vulnerabilities and propose a more secure UPI for payment apps (Madwanna et al. 2021; Kumar et al. 2020). This can be motivated by the fact that they are relatively more sensitive to security compared to other categories of non-financial applications in developing countries (Bassolé et al. 2020), and studies talk about the numerous security challenges they face (approov 2023) and the types of frauds related to mobile financial services in these regions (Osman et al. 2017). Mobile apps related to Health&Fitness receive the attention of researchers in the context of the COVID-19 pandemic through interviews and surveys to determine the factors that influence the adoption and the continuance intentions of usage of contact tracing apps (Chopdar 2022; Prakash et al. 2021). Aiming to provide secure access to health data and facilitate efficient interaction between patients and healthcare providers, some authors implement solutions integrating OAuth 2.0 and the Aadhaar identification system into Indian e-health apps (Khatoon and Umadevi 2018). Communicational apps are studied less frequently, as well as Educational, Travel & Local, and Medical apps. Several studies do not mention the category of apps they focused on. We have grouped those apps in the Generic category.

Answer to RQ3

In the developing country context, researchers primarily focus on financial mobile apps, such as mobile banking and mobile money apps.

4.5 Security Issue Detection Techniques

This section explores the techniques employed to detect security concerns on mobile apps in developing countries. Numerous methods exist for identifying vulnerabilities in these apps, with static and dynamic analysis being the most prevalent. Static analysis involves

examining software without its execution, while dynamic analysis involves the examination of software during runtime. These two techniques are applied based on specific needs. To enhance analysis efficiency, researchers frequently integrate static and dynamic analysis to create a hybrid approach.

As illustrated in Table 10, the literature indicates a predominant reliance on static and hybrid analysis to address app security issues in developing countries.

Additionally, dynamic analysis is occasionally utilized, along with forensic analysis, which entails investigating an app's traces in the device's memory.

The results show that most publications have only used off-the-shelf techniques and tools to uncover security issues (Ibrar et al. 2017; Bassolé et al. 2020; Osho et al. 2019; Kant Kamal et al. 2023; Chiboora et al. 2023). Others have combined those tools with specialized techniques to look for features leading to data leakage (Castle et al. 2016), to analyze the communication flows between server and mobile apps (Castle et al. 2016; Reaves et al. 2017), and the registration and transaction processes (Madwanna et al. 2021; Kumar et al. 2020).

Answer to RQ4

Researchers predominantly have employed static and hybrid analysis methodologies to scrutinize mobile apps for potential security issues. Nevertheless, most did not specifically adapt their works to the specific concerns of developing countries.

4.6 Malware Characteristics

The literature review revealed only three publications, i.e., Bassolé et al. (2020), Madwanna et al. (2021), and Sihag et al. (2020), that identified malicious apps through the exploration and analysis of mobile applications. In these publications, authors found mobile trojans to be the most prevalent type of mobile malware among the apps they studied. More specifically, in the first identified paper, Bassolé et al. (2020) explored malware detection and identified five malware instances in a set of 53 mobile banking apps, including three trojans, using VirusTotal. In the second paper, Madwanna et al. (2021) develop a Trojan to assess the security level of an app leveraging the Indian payment system named Unified Payments Interface (UPI). The Trojan tries to exploit vulnerabilities present in UPI. More specifically, the Trojan disables client-side security and creates a command and control (C&C) server. The authors show that the malicious app can collect users' phone numbers from all the phones it is installed on and send them to the attacker via SMS. Finally, in the third paper, Sihag et al. (2020) identified several malicious apps when applying their dynamic analysis approach to a set of apps, including those that attempted to jailbreak the phone, root the device, and use superuser commands. Their approach focused on detecting malicious behaviors by collecting and inspecting system-generated logs.

These studies mainly focused on apps that are used in the financial domain (Bassolé et al. 2020; Madwanna et al. 2021) and in other categories of apps such as social networks, games, productivity, messaging, etc. (Sihag et al. 2020). However, the studies did not mentioned the information assets that are attacked the most and the attack vectors.

Table 9 The categories of apps addressed in the literature

Publication	Finance	Health & Fitness	Education	Communication	Travel & Local	Medical	Generic
Albrecht et al. (2021)				✗			
Al-Ameen et al. (2020)							✗
Ansong and Synaepa-Addision (2019)	✗						
Bandan et al. (2022)	✗		✗	✗	✗	✗	
Bassolé et al. (2020)	✗						
Castle et al. (2016)	✗						
Chiboora et al. (2023)	✗						
Chopdar (2022)		✗					
Ibrar et al. (2017)	✗						
Kaka et al. (2016)	✗						
Kala Kamdjoug et al. (2021)	✗						
Kant Kamal et al. (2023)							✗
Khatoon and Umadevi (2018)		✗					
Koala et al. (2020)							✗
Kumar et al. (2020)	✗						
Latifa et al. (2017)	✗						
Madwanna et al. (2021)	✗						
Munyendo et al. (2022)	✗						
Osho et al. (2019)	✗						
Prakash et al. (2021)		✗					
Reaves et al. (2017)	✗						
Shezan et al. (2017)							✗
Sihag et al. (2020)							✗
Uduimoh et al. (2019)	✗						
Vakare et al. (2022)	✗						
Number of publication	**16 (64%)**	**3 (12%)**	**1 (4%)**	**2 (8%)**	**1 (4%)**	**1 (4%)**	**5 (20%)**

Answer to RQ5

The literature revealed very few studies on detecting mobile malware in developing countries. These studies mainly identified malware such as trojans, jailbroken apps, and apps that attempt to root devices or use superuser commands. These malware target mainly app categories, such as finance, social networks, games, productivity, and messaging. There are no specific details on the payloads used, the threat actors involved, the attack vectors, and the most targeted information assets.

Table 10 Summary of the techniques used to detect security issues

Publication	Static	Dynamic	Hybrid	Forensic
Albrecht et al. (2021)		✗		
Ansong and Synaepa-Addision (2019)	✗			
Bassolé et al. (2020)			✗	
Castle et al. (2016)	✗			
Chiboora et al. (2023)			✗	
Ibrar et al. (2017)	✗			
Kaka et al. (2016)	✗			
Kant Kamal et al. (2023)			✗	
Koala et al. (2020)	✗			
Kumar et al. (2020)			✗	
Latifa et al. (2017)	✗			
Madwanna et al. (2021)			✗	
Osho et al. (2019)				✗
Reaves et al. (2017)	✗			
Shezan et al. (2017)			✗	
Sihag et al. (2020)		✗		
Uduimoh et al. (2019)				✗
Vakare et al. (2022)			✗	
Number of publication	**7 (28%)**	**2 (8%)**	**7 (28%)**	**2 (8%)**

4.7 Motivations for Research

With Smartphones becoming increasingly popular in developing countries[5], a surge in mobile app usage has raised awareness about security issues among researchers. Researchers motivate their studies by mentioning the growing concerns regarding mobile app security that impact many users in developing countries. They aim to encourage practitioners to enhance user protection and security measures, especially in the case of mobile financial services. The dearth of studies on security issues in developing countries inspires researchers to fill this gap. Furthermore, examining the relatively low adoption rates of certain mobile apps also fuels researchers' curiosity. This curiosity prompted investigations into whether mobile app security plays a role in influencing adoption patterns.

In certain instances, researchers strive to reassure users, mitigate the threat posed by malicious apps, and address the unique security challenges prevalent in their respective regions. This multifaceted approach reflects a commitment to understanding, confronting, and ultimately improving the landscape of mobile app security in the context of developing countries.

Answer to RQ6

Researchers generally motivate their papers by the increased adoption of smartphones coupled with a significant increase in mobile app usage, the growing concerns surrounding mobile apps, and the lack of studies in developing countries.

[5] Source: http://www.osiris.sn/En-Afrique-subsaharienne-le-taux-d.html

5 Discussion

This section discusses various aspects of mobile app security in developing countries. We address unexplored research directions, emerging trends, and issues related to vulnerabilities and outline future challenges.

5.1 Researches Performed and Needs

In the domain of mobile app security in developing countries, several uncharted research directions hold the potential to drive innovation and enhance security practices. Certain avenues have been much more explored.

Explored Research Directions The identified papers investigate a few relevant research avenues that could help develop more secure apps.

Several research papers have conducted user studies through interviews and surveys, which offer useful insights into user behavior and perceptions when using mobile apps, and their intentions to use certain mobile apps. This type of contribution provides a deep understanding of user experiences and sentiments. It also guides the development of more secure apps since it has allowed researchers to provide actionable recommendations and guidelines for developers and policymakers, as well as app markets. Researchers use advanced methods and frameworks such as machine learning algorithms, UTAUT, and PLS-SEM to provide robust analysis. However, we observed that they often use a limited sample size. The sample size used could be representative, taking into account gender diversity and geographic area, to provide stronger results. We have noticed that researchers primarily explore the adoption of financial and healthcare apps. This is understandable since they are two crucial domains. Nevertheless, the scope could be extended, allowing it to cover other domains.

Researchers have mainly focused on app analysis approaches, such as static, dynamic, hybrid, and forensic analysis. Their work is primarily based on using off-the-shelf automated security detection tools, among which some have limited capabilities to detect specific vulnerabilities (Ibrar et al. 2017). Each study's focus is on specific security aspects according to the category of apps it addresses. We have noticed that financial apps have received more attention from researchers than other categories of apps. This attention is not driven by the fact that financial apps are the most used in developing countries, so researchers should attach importance to mobile apps in other domains, including healthcare, gaming, and social media, since the security of these apps could affect millions of users.

Researchers have also minimally addressed app security testing (Kant Kamal et al. 2023; Vakare et al. 2022). This type of study is useful since it not only allows the identification of vulnerabilities statically but also provides a runtime analysis of vulnerabilities, raising awareness in users as well as developers side. According to the threats targeting mobile apps in developing countries (Statica 2023; approov 2023; Osman et al. 2017), there is a pressing need for specialized solutions to deal with these problems. Unfortunately, only a single study has been provided proposing a context-specific tool to ensure secure access, authentication, and authorization within the healthcare domain in India (Khatoon and Umadevi 2018). Another work has proposed a system that collects and evaluates behavioral activity for malicious intent from targeted apps (Sihag et al. 2020). However, these approaches are

not specific to developing countries. The existing literature has not mentioned any security testing tools specifically tailored for mobile apps in developing countries. Researchers typically use pre-existing open-source tools developed for a global context, even for app analysis, rather than creating region-specific solutions.

We have noticed a significant lack of research into the security of mobile applications in developing countries. More studies should be proposed, ranging from considering more app categories to proposing solutions adapted to developing countries. Many approaches exist in the literature worldwide. However, applying them in the developing country context can lead to miss interesting findings because the types of functionality and errors in mobile apps could be different.

Unexplored Research Directions Additionally, there is a domain that deserves to be more explored. Mobile malware detection should be explored in greater depth. Indeed, mobile phone users across the globe are increasingly falling victim to a rising tide of mobile malware infections (Baur-Yazbeck et al. 2019). These infections disproportionately impact users in developing countries. According to Carter (2017), the top ten countries most severely affected by mobile malware are developing countries, meaning that it deserves important attention from researchers. Despite this, we have found only two studies focusing on mobile malware detection in these regions. The one designed a system that analyzes real-time app interactions for malicious behavior (Sihag et al. 2020), while the other one conducted a vulnerability analysis using VirusTotal for malware detection (Bassolé et al. 2020). While several advanced malware detections exist, using AI techniques such as machine learning and deep learning, these studies primarily leveraged dynamic analysis techniques to address mobile malware (Sihag et al. 2020). Apart from these two works, no other studies have delved into the critical issue of mobile malware detection. It is noteworthy that researchers tend to focus on analyzing mobile apps for security vulnerabilities rather than proactively addressing the issue of mobile malware detection despite the escalating threat posed by mobile malware in developing countries.

Another research direction could be to explore proofs-of-concept allowing the exploitation of vulnerabilities found in mobile apps. This can help to improve its security. In our study, we have identified only one paper in which authors have outlined hypothetical attacks on mobile money apps without demonstrating how these attacks could be executed (Castle et al. 2016). This hesitancy may be attributed to the constraints inherent in conducting proof-of-concept experiments. In fact, various factors, such as governmental regulations, resource constraints, or the requisite access to specific accounts, can hinder the practical exploitation of vulnerabilities. However, presenting straightforward use cases can potentially address these issues. Despite these challenges, investigating how adversaries can exploit vulnerabilities remains crucial for improving mobile app security in developing countries.

5.2 Research Trends

We were surprised by the few papers we have identified in this SLR. Indeed, we have identified twenty-five publications, and the first appeared in 2016 (Castle et al. 2016). In general, there is an average of three relevant publications annually until 2023, indicating the scarcity of research in this area. To resolve this problem, more comprehensive work is needed to

address the numerous security issues in the ever-growing mobile app landscape in developing countries. In Section 5.4, we proposed several future types of research identified when analyzing publications to help researchers fill the gap.

5.3 Comparison with Existing Secondary Studies

In the literature, we have identified several secondary studies, each with a different focus compared to our SLR. For instance, a state-of-the-art survey on mobile banking analyzed and classified the challenges and security issues of mobile banking services in Uzbekistan (Abdullaev et al. 2019). This study concentrated on the Wireless Application Protocol (WAP) used for data encryption, the authentication process, SMS banking, and virus attacks. Similarly, another survey focused on identifying the issues and challenges faced by customers using mobile banking services (Rahman et al. 2020). Additionally, researchers conducted a literature review on mobile government (m-government), analyzing studies that presented the challenges, benefits, and success factors for implementing m-government (Azeez and Lakulu 2019). The similarities between these studies and our study are that they investigated the security problems faced by mobile banking and mobile government in developing countries. Some of these security problems are linked to network communication and cryptography, security concerns that we also identified in RQ2 of our study. However, they did not primarily focus on mobile applications as our study does.

Other studies have examined mobile apps in developing countries and various other areas. For example, reviews of mobile health apps (mHealth) have explored the application of recommendations and security and privacy regulations (Hoque et al. 2020; Martínez-Pérez et al. 2015), the current state of the mHealth market (Hsu et al. 2016), and the security challenges of mobile educational apps (Mkpojiogu et al. 2021). Each of these studies focused on specific categories of apps. The main similarities we noticed in these studies are that they (1) focused on the categories of apps we considered, i.e., mHealth and educational apps, and (2) explored security concerns related to cryptography, access control, network communication, and data storage (Martínez-Pérez et al. 2015).

In addition to these specific apps' categories, our SLR considers security problems across all categories of mobile apps. We categorize the publications by types of contributions to highlight future research directions. Furthermore, we explore the types of issues identified in the apps and the methods researchers used to identify these issues.

5.4 Future Challenges

Our discussion highlights perspectives from the existing literature and presents new challenges that need to be addressed to enhance mobile app security in developing countries.

Challenges from the Literature The authors of the papers listed in our SLR have identified several open challenges to extend research or explore new directions. The identified perspectives include:

1. *Investigating development frameworks.* Authors explored some app development frameworks to understand the impacts they have on the security of the apps. They argue that certain frameworks allow the development of more secure apps than others. The

study focuses on two development frameworks, and the authors suggested extending it by considering more frameworks.
2. *Reducing the requested permissions*. Some studies investigated mobile app security by focusing on permissions. The authors found that some apps abuse users by requesting unnecessary permissions, which could have an impact on their security. These authors suggest investigating and proposing solutions to reducing the permissions requested by apps to protect user privacy.
3. *Developing alert tools.* There are also perspectives to develop tools to alert users and administrators about potentially dangerous permissions used by apps.
4. *Expanding studies.* When performing interviews and surveys, researchers used a small number of participants and focused on specific areas and institutions. To have more comprehensive results, they suggested expanding the studies by covering diverse contexts, institutions, and participants.
5. *Focusing on specific aspects.* To refine the analysis results, researchers suggested carrying out studies that focus on specific aspects of financial apps, such as password reset procedures and accountless money transfers.

Future Research Directions Based on the insufficiently explored research directions mentioned above and the need for more specific approaches, we have identified, in addition to the challenges in the literature, the following future research directions:

1. Investigate unexplored research areas on mobile app security analysis targeting developing countries' specific challenges.
2. Extend applications of state-of-the-art research results to explore security concerns beyond fintech apps to other critical categories, such as health and education apps.
3. Investigate malware targeting developing countries. In particular, the types of malware used, the payload of these malware, the techniques and procedures used by attackers to compromise devices in these regions, the active threat actors, and the information assets that are attacked the most as well, should be explored. Furthermore, analysis techniques should be developed that are suited for (1) pre-installed apps in low-cost devices and (2) available and still-in-use insecure technologies (e.g., USSD).

Mobile app security in developing countries is an evolving field with numerous opportunities for research and improvement. Addressing these research directions and challenges is essential to enhance the security of mobile apps and protect users in these regions.

6 Threat to Validity

Our primary objective was to assemble publications discussing mobile app security in developing countries. However, there are potential threats to the validity of this study.

Internal validity. We established exclusion criteria to eliminate irrelevant publications during the selection process. Notably, we excluded books and thesis reports, as we deemed them less relevant, assuming that pertinent information would likely be found in conference or journal papers. The authors reached a consensus to remove certain publications after reviewing them and determining their irrelevance to our study. We also modified our search

keywords to capture more relevant publications than in our initial attempt. However, this adjustment may have led to the omission of some pertinent publications.

External validity. Our study did not take into account works published from 2024 onwards, as we completed our data collection before this date. Consequently, publications released after our cutoff date were not considered, which means the results and arguments presented in this study may not apply to these newer publications.

Construct validity. To streamline our search on the Springer digital library, we performed a general search and applied filters to select publications within the field of Computer Science. We then narrowed our focus to conference papers, articles, and papers written in English. Since some developing countries have French as an official language rather than English, we may have missed relevant publications written in French. Additionally, we used a Python script to refine the results by targeting the titles and abstracts of the collected publications. This script constructs the search string based on a list of keywords and searches for this string in the titles and abstracts. However, this method may inadvertently exclude some relevant publications. We found no irrelevant publications when verifying the results we obtained after running the script. All publications we obtained contain our search string; thus, no false positives have been found. However, we did not exclude the possibility of having false negatives, that is, the exclusion of relevant publications. Our script is publicly available to the research community in our replication package (Diallo et al. 2024) for transparency and verification. Furthermore, we excluded some publications when assessing their quality. This exclusion was not because the publications did not investigate mobile app security in developing countries. We excluded them because they did not meet our quality criteria, which could potentially include biases in our dataset.

While these actions were intended to refine our results, they may have inadvertently excluded some potentially relevant publications. Consequently, we acknowledge the possibility of biases in our study. This means we might have missed publications that should have been included or excluded. However, during our data analysis, we did not identify any additional publications to exclude, as each one helped us address at least one of our research questions.

7 Related Works

To our knowledge, no systematic literature review focuses on mobile app security in developing countries. However, several reviews, investigations, and surveys have been performed on other topics in the context of developing countries.

Hsu et al. (2016) gave an overview of Chinese mobile health (mHealth) apps in December 2015 by investigating the most downloaded apps from Android and iOS. In their study, authors aimed to understand the current state of the Chinese mHealth market, focusing on medical-related apps categorized by ten different medical initiatives rather than general health apps. For each app, they analyzed the main service offered, mHealth initiative, disease and specialty focus, app cost, target user, Web app availability, and emphasis on information security. The findings revealed that the primary mHealth initiatives targeted by the apps reflect Chinese patients' demand for access to medical care. Disease-specific apps are also representative of disease prevalence in China, with the most common disease-specific apps focusing primarily on diabetes, hypertension, and hepatitis management. Most apps

were found to be free and available on both iOS and Android platforms. The paper also underlines the lack of information about users' data security since developers did not mention the purposes for which users' data could be used.

Latif et al. (2017) presented a study that underlines the factors hindering the use of mobile health in developing countries by reviewing various mobile health initiatives, their impacts, and their healthcare challenges. The review highlights several challenges that hinder the successful deployment of mHealth, including infrastructural limitations, the need for strategic partnerships, and cultural and language issues. The authors emphasized the importance of leveraging emerging technologies such as the Internet of Things (IoT) and artificial intelligence (AI) to enhance mHealth adoption. Additionally, the paper features a case study on Pakistan to validate the findings and illustrate the practical implications of mHealth in a specific context. This case study demonstrates that tailored approaches, considering local cultural contexts, are essential for effective mHealth implementation.

Abdullaev et al. (2019) performed a state-of-the-art survey of mobile banking. They aimed to classify and analyze mobile banking services' challenges and security issues in Uzbekistan. They explored the security issues related to the Wireless Application Protocol (WAP). With this protocol, customers can use bank services through the Internet. However, data is not well encrypted at one stage of the communication using WAP. They also identified other risks and issues related to the authentication process, SMS banking, and virus attacks, in which attackers can use many techniques to steal users' sensitive information. They presented many security risks that can compromise the mobile banking system. In their study, authors also found that 60% of customers do not use mobile banking technology.

Azeez and Lakulu (2019) performed a literature review on mobile government (m-government) in developing countries focusing on identifying the benefits, challenges, and critical success factors for the successful implementation of m-government from both government and citizen perspectives. The authors analyzed various studies on the success of m-government and categorized the success factors based on their impact on the successful implementation of m-government. The findings reveal increased efficiency of governmental activities, cost reduction in organizations, and accessibility of government services as benefits of m-government, as well as the offer of real-time information and improvement of citizen participation in governmental activities. However, the study identified several m-government challenges, including security and privacy, technical limitations, infrastructure limitations, and interoperability. The paper concluded that while m-government offers significant opportunities for improving government services in developing countries, it also presents several challenges that need to be addressed to ensure successful implementation.

Hoque et al. (2020) present a review of studies related to mobile health applications between 2013 and 2018. Through this review, they aimed to evaluate the quality of evidence reporting by using mobile health Evidence Reporting and Assessment (mERA), a checklist developed by the World Health Organization (WHO). This review highlights the application level of evidence reporting as recommended by WHO. Authors found that researchers and mobile health intervention designers from developing countries have limited familiarity with the mobile health Evidence Reporting and Assessment checklist. They also noticed that the majority of studies fail to meet the essential evidence-reporting criteria outlined in the checklist. Furthermore, design science-based methods and theory-based frameworks are rarely applied in the development of mobile health interventions. Finally, they found that most mobile health interventions are not prepared for interoperability or integration

into existing health information systems. Overall, the study reveals that most studies do not properly apply WHO's recommendations.

There is also another state-of-the-art in which Rahman et al. (2020) explore the current situation of mobile banking in Bangladesh. The research objectives are to identify the problems and challenges that customers face in mobile banking services and to observe the future prospects of mobile banking in the country. The paper identified several problems related to security (financial loss across virus attacks, fraudulent activities, privacy leakage, etc.), time (because of late payments or any other reason, there is time lost), network (poor network), performance (server break down), financial (lose of money because of mistakes made during money transaction), and lack of banking knowledge. Authors also argued that issues may arise because of compatibilities (difficulty to operate with another device when the first breaks down, unable to access service in some places because of poor internet connection). According to them, trusting mobile banking is an important factor that may give issues such as fairness, capability, and beneficence. Despite these challenges, the paper highlighted the prospects of mobile banking, including benefits for phone operator companies, increasing job scopes, no service charge, increased purchasing power, and easy money transfer. The authors concluded that if these issues can be solved in the future, mobile banking will lead to a greater impact on the banking economy of Bangladesh.

Msweli and Mawela (2020) provided a study that explores the enablers and barriers to mobile banking and mobile commerce among the elderly, particularly in developing countries, by reviewing the existing literature focusing on literature from 2009 to 2019. The findings reveal that there are significant gaps in research concerning the elderly and mobile banking, particularly in developing countries. Key barriers identified include security concerns, lack of trust, and limited technical knowledge among older adults, which hinder their adoption of mobile banking services. Conversely, enablers such as the perceived ease of use and the potential for improved quality of life through mobile commerce were noted. The study concludes that there is a pressing need for further research to address these gaps and to develop tailored mobile banking solutions specifically to the needs of the elderly, thereby enhancing their financial inclusion in the digital era. Similarly, Pankomera and van Greunen (2019) systematically reviewed the opportunities, barriers, and adoption factors of mobile commerce (m-commerce) services for the informal sector in Africa. This paper seeks to provide comprehensive insights into how m-commerce can benefit the informal sector, the challenges faced, and the factors influencing its adoption. The study identified several barriers, including the limited network coverage and broadband infrastructure, high costs of mobile devices and services, resistance due to illiteracy, lack of trust and traditional business practices, and finally, a lack of legal and regulatory frameworks to support m-commerce. The adoption factors identified from the literature include network coverage and availability of electricity, knowledge of m-commerce and its benefits, perceived usefulness and ease of use, affordability of m-commerce solutions, confidence in the security of m-commerce transactions, accessibility of financial services, the impact of social and cultural factors on adoption, and government policies and regulations promoting m-commerce. Furthermore, the authors identified several benefits and opportunities of m-commerce, such as the creation of new services, increased revenue, reduced operational costs, and enhanced productivity and market access, particularly in the agriculture and fishing sectors.

Malik (2020) performs a review article in which he studies publications that talk about Internet and mobile banking adoption from 2015 to 2020 using the Unified Theory of

Acceptance and Use of Technology (UTAUT) model in developing countries. This study highlights the directions, the most used analysis tools, and the main indicators of behavioral intention used in the publications. It also reveals that most publications focused on factors affecting Internet banking adoption (54%). This study argues that the extended UTAUT model is mostly used in publications. Indeed, as presented, this model is used by 67% of the publications among the 54% internet banking and by 70% among the 46% mobile banking publications. This is similar to the study that reviews the literature regarding mobile health adoption in developing countries (Aljohani and Chandran 2021). In this study, Aljohani et al. identify the methodologies used in existing research, the significant factors influencing adoption, and the gaps in the literature, particularly regarding the use of qualitative and mixed methods. The authors conducted a systematic review of the literature by evaluating various studies published between 2010 and 2020. The findings revealed a limited number of studies on m-health adoption in developing countries, with a notable concentration of research in China and Bangladesh. The Technology Acceptance Model (TAM) was frequently used, focusing primarily on technological and individual factors, while other health-related factors and theories were underexplored. Furthermore, most studies employed quantitative methodologies, with only one study utilizing a qualitative approach and none using mixed methods. The authors emphasized the need for more qualitative and mixed-method studies to provide richer insights into the adoption of m-health applications and to better understand the cultural and health impacts of these technologies.

All of these mentioned studies are completely different from ours because we have mainly focused on investigating studies that have been conducted in this area.

8 Conclusion

This SLR has delved into mobile app security in developing countries. We meticulously examined 25 publications from various conference and journal venues throughout this process. Our goal was to shed light on the diverse research directions, security concerns, categories of apps addressed, investigation techniques, and researcher motivations in the domain of mobile app security within developing countries. Key findings from this SLR include:

1. **Lack of studies**. The literature on mobile app security in developing countries is relatively scarce, highlighting a significant research gap in this crucial area. This suggests a pressing need for more focused research on mobile app security tailored to the unique context of developing countries.
2. **Limited research directions**. Most studies focus on user studies and app analyses. A critical area, such as malware detection, is significantly underexplored. This limited scope restricts the development of comprehensive security strategies and tools that could better serve local needs since mobile malware is increasingly targeting developing countries. Other promising directions, such as the development framework study and app security testing, remain also underexplored.
3. **Focus on financial apps**. The literature focuses mainly on mobile apps related to finance. This points out a prioritization of economic concerns, while sectors such as health and education, which are equally vital in developing regions, receive comparatively little

attention. This imbalance presents an opportunity for future research to diversify and address a broader range of societal needs.

4. **Lack of specific analyses**. Notably, there is a lack of in-depth and context-specific analyses, highlighting the need for more sophisticated methodologies that take into account the unique challenges facing developing countries. Without such tailored approaches, existing research may not offer actionable insights or scalable solutions.

Taken together, these findings point out the importance of expanding and diversifying mobile app security research in developing countries. By identifying these gaps and trends, this SLR provides a foundation for future work that can better align with local realities and global security goals. It contributes to both academic research and practical application by mapping the current landscape, highlighting critical gaps, and proposing directions for future research. It serves as a reference for researchers, developers, and policy makers aiming to improve the security of mobile apps in these regions, supporting more secure and inclusive digital ecosystems.

It is essential to acknowledge that this study is limited to developing countries, excluding emerging ones. Future SLRs may expand on this work by including emerging countries, providing a more comprehensive perspective on mobile app security in diverse socio-economic contexts.

Appendix A: Summary of the Selected Publications

Paper Title & Reference *Effective Security Testing of Mobile Applications for Building Trust in the Digital World* (Kant Kamal et al. 2023)

Type of Study: App Security Testing

Summary: The paper discusses the security testing procedures and features of India's first indigenous AppStore, "mSeva AppStore". It tests the security of 300 apps from this AppStore, for improper platform usage, insecure coding practices, insecure communication, and more, using several tools such as MobSF, Appium, Drozer, and Robotium. The test reveals common issues, including insecure communication, insufficient cryptography, and insecure data storage.

Strengths:

- Provides a detailed methodology for security testing.
- Provides useful insights and results.
- Offers a classification of common security issues.
- Highlights the importance in ensuring mobile app security.

Limitations:

- Limit scope (AppStore and OS).
- Sample size is not broad.

Paper Title & Reference *User's Perception on Security and Privacy in Using Crypto Currency Trading Application in India* (Vakare et al. 2022)

Type of Study: App Security Testing and User study

Summary: The paper investigates the security and privacy perceptions of users regarding cryptocurrency trading apps in India. It focuses on the top 6 cryptocurrency trading apps and examines their security profiles using various penetration testing techniques. In this study, authors use supervised machine learning algorithms like Random Forest and Logistic Regression to analyze user reviews and sentiments, and the OWASP mobile security testing framework to conduct a security analysis on the apps to identify common vulnerabilities. The study identifies several vulnerabilities related to data stoarge, cryptography, and network communication. Authors' sentiment analysis reveals a mix of positive and negative sentiments towards the security and privacy of these apps. Users' perceptions of security and privacy are influenced by their awareness and knowledge of potential threats.

Strengths:

- Provides a comprehensive analysis.
- Uses machine learning algorithms to analyze user sentiments.
- The findings have practical implications for developers and users.
- Highlights areas for improvement in app security and user education.
- Provide a clear understanding of the security issues in these apps.

Limitations:

- App sample size may not be representative.
- Limit scope (OS and geography).
- Dependence on user reviews from app stores.

Paper Title & Reference *Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya* (Munyendo et al. 2022)

Type of Study: User study

Summary: The paper investigates the usage, privacy concerns, and user behavior associated with mobile loan applications in Kenya. These apps, which offer quick and easy access to small loans, often at high interest rates, collect sensitive user data through permissions. The study uses semi-structured interviews with 20 users to explore their concerns and trade-offs between privacy and the need for loans.

Strengths:

- Provides useful insights into user behavior and concerns.
- Offers a deep understanding of user experiences and privacy concerns.
- Provides recommendations for regulators, developers, and app markets to improve user privacy and security.

Limitations:

- Limit scope (App category and geography).
- Does not use a representative sample.

Paper Title & Reference *Adoption of Covid-19 contact tracing app by extending UTAUT theory: Perceived disease threat as moderato* (Chopdar 2022)

Type of Study: User study

Summary: The study proposes a research model based on the Unified Theory of Acceptance and Use of Technology (UTAUT), Health Belief Model (HBM), perceived privacy risk, and perceived security risk to understand the adoption of contact tracing applications. An online survey was conducted among 307 users of the 'Aarogya Setu' app. The data was analyzed using Partial Least Squares Structural Equation Modelling (PLS-SEM). The study provides insights into both the drivers and barriers to the adoption of contact tracing apps. In particular, findings revealed that perceived privacy and security risks were significant barriers to the adoption.

Strengths:

- Integrates multiple theoretical frameworks (UTAUT, HBM) and perceived risks, providing a robust model.
- The use of PLS-SEM provides strong empirical support for the proposed hypotheses.
- Provides useful insights for app developers and policymakers.
- Highlights the moderating role of perceived disease threat in the adoption of contact tracing apps.

Limitations:

- Limit scope (App category, geography, etc.).
- Limits on the ability to capture changes in user behavior over time.
- The sample size may not be representative.

Paper Title & Reference *State of Survey: Advancement of Knowledge Environmental Sustainability in Practicing Administrative Apps* (Bandan et al. 2022)

Type of Study: User study

Summary: The paper presents a survey of government mobile apps in Bangladesh, focusing on user satisfaction and the factors contributing to the popularity or unpopularity of these apps. The survey was conducted with 310 participants to gather insights on their experiences and opinions regarding government apps. The findings indicate a general dissatisfaction among users, primarily due to issues related to security, content quality, design, and the presence of bugs.

Strengths:

- Focuses on user feedback.
- Clearly identifies key areas of dissatisfaction.
- Offers actionable suggestions for enhancing app features.

Limitations:

- The sample size may not be representative.

- Limit scope ((App category and geography).
- Potential bias in responses.
- Does not account for changes in user perceptions or app performance over time.

Paper Title & Reference *Understanding digital contact tracing app continuance: Insights from India* (Prakash et al. 2021)

Type of Study: User study

Summary: The paper investigates the factors influencing the continuance intentions of users regarding digital contact tracing (DCT) apps in India, particularly in the context of the COVID-19 pandemic. It extends the Expectation-Confirmation Model (ECM) by incorporating additional factors such as trust in technology and perceived security and privacy. The study employs a quantitative approach, utilizing a survey distributed to users of the "Aarogya Setu" app, and analyzes the data using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings reveal that user satisfaction, trust in the DCT app, and trust in the government are significant determinants of users' intentions to continue using the app.

Strengths:

- The use of PLS-SEM allows for a robust analysis of the relationships between constructs.
- Adheres to established guidelines for assessing measurement and structural models.
- Offers recommendations for policymakers and app developers to improve user engagement and trust.

Limitations:

- Sample bias (demography).
- Does not account for changes in user intentions or behaviors over time.
- Limit scope (geography).
- Focus on intentions rather than actual usage behavior.

Paper Title & Reference *Determining factors and impacts of the intention to adopt mobile banking app in Cameroon: Case of SARA by afriland First Bank* (Kala Kamdjoug et al. 2021)

Type of Study: User study

Summary: The paper investigates the adoption and use of mobile banking apps, specifically focusing on the SARA app by Afriland First Bank in Cameroon. It employs various theoretical frameworks, including the Technology Acceptance Model (TAM), Protection Motivation Theory (PMT), and the Unified Theory of Acceptance and Use of Technology (UTAUT2), to understand the factors influencing users' decisions to adopt mobile banking technology. The study utilizes a structured questionnaire with a Likert scale to gather data from users, analyzing responses through Partial Least Squares Structural Equation Modeling (PLS-SEM). findings indicate that factors such as perceived ease of use, perceived usefulness, and security concerns significantly impact users' intentions to adopt mobile banking apps.

Strengths:

- Integrates multiple established theories to create a comprehensive model.
- Focuses on gender differences.
- The findings help mobile banking service providers to meet user needs and enhance adoption rates.

Limitations:

- Limit scope (App and geography).
- The sample size may not be representative.
- Lack of qualitative exploratory research.

Paper Title & Reference *We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh* (Al-Ameen et al. 2020)

Type of Study: User study

Summary: The paper investigates the perceptions of users in urban Bangladesh regarding data collection by smartphone apps. It highlights the varying attitudes towards privacy, ranging from indifference to fear, and examines how local infrastructure and social practices influence these perceptions. The study is based on interviews with 32 participants from diverse backgrounds in Dhaka, Bangladesh. The findings reveal that participants were aware of privacy issues but had mixed feelings about data collection. Some saw it as beneficial or necessary, while others felt indifferent or fearful. Apps are seen as essential for navigating city life, despite privacy concerns. Language barriers and the complexity of privacy policies hinder users' understanding and ability to make informed decisions.

Strengths:

- Provides useful insights into privacy perceptions.
- Captures a broad spectrum of perspectives by including participants from various age groups, literacy levels, and professions.
- Proposes recommendations to improve privacy awareness and practices tailored to the local context of Bangladesh.
- Integrates perspectives from human-computer interaction, security, and social sciences.

Limitations:

- A small sample of participants.
- Limit scope (Area and language).
- The reliance on self-reported data may introduce biases.

Paper Title & Reference *Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World* (Castle et al. 2016)

Type of Study: User study and App analysis

Summary: The paper investigates the security challenges of mobile money services in the developing world. includes a large-scale analysis of 197 Android apps and interviews with 7 developers from Africa and South America. The authors propose a systematic threat model to assess potential attacks and evaluate current security practices. The security analysis reveals that many apps have vulnerabilities, but service providers generally make security-conscious decisions.

Strengths:

- Provides a comprehensive analysis supported by both app analysis and qualitative insights from developer interviews.
- Proposes a systematic threat model, helping in identifying potential attacks on DFS applications.
- Offers recommendations to improve security practices, including the use of standard encryption and better training for developers.

Limitations:

- Limit scope (Android OS).
- Sample size for interviews limited.
- The insights from developer interviews rely on self-reported data, which may be subject to bias or inaccuracies.
- Regulatory constraints.

Paper Title & Reference *Evaluating Mobile Banking Application Security Posture Using the OWASP's MASVS Framework* (Chiboora et al. 2023)

Type of Study: User study and App analysis

Summary: The paper presents an analysis of 18 mobile banking apps from various financial institutions in Africa. The study aims to assess the security posture of these apps using the OWASP Mobile App Security Verification Standard (MASVS) v2.0 framework. It combines manual and automated testing to analyze app source code and performs developer surveys. The paper identifies several security vulnerabilities in the tested apps, including issues with data storage, cryptography, network communication, permissions, code quality, and resilience. It also highlights the challenges developers face in implementing security measures, such as lack of expertise, time constraints, and complexity.

Strengths:

- Use of comprehensive framework (OWASP MASVS).
- Analyzes apps from various financial institutions across different regions in Africa.
- Provides a detailed breakdown of the security issues found in each category of the MASVS framework.
- Highlights the practical challenges faced by developers in implementing security measures.

Limitations:

- Focuses solely on unauthenticated client-side testing.
- A larger sample size could provide more generalizable results.
- Limit scope (geography and app category).
- Limited profiling of respondents for the surveys.

Paper Title & Reference *Analysis of the Impact of Permissions on the Vulnerability of Mobile Applications* (Koala et al. 2020)

Type of Study: App analysis

Summary: The paper investigates the security risks associated with permission management in Android applications, particularly focusing on apps developed in Burkina Faso. It aims to identify permission abuses and propose measures to enhance data protection for users, developers, and administrators. The study involves statically analyzing a sample of 40 apps developed in Burkina Faso, covering various categories available on Google Play. The findings reveal that despite existing security measures, many apps still exhibit vulnerabilities related to permission management. The paper emphasizes the need for developers to improve their UID allocation systems, limit the number of signatures per app, and ensure that apps with similar features use consistent permission groups.

Strengths:

- Analyzes a diverse sample of apps across various categories.
- Identifies specific permission abuses and their potential impact on user data.
- Provides actionable recommendations for developers and users' awareness to mitigate risks.

Limitations:

- Limit scope (geography).
- Limited sample size.
- Lack of User Perspective.

Paper Title & Reference *A Study of Static Analysis Tools to Detect Vulnerabilities of Branchless Banking Applications in Developing Countries* (Ibrar et al. 2017)

Type of Study: App analysis

Summary: The paper investigates the effectiveness of static analysis tools in identifying security vulnerabilities in Android Digital Financial Services (DFS) apps. It focuses on apps used in developing countries and compares them with those from developed countries. The authors used 3 static analysis tools: MobSF, Qark, and AndroBugs, to analyze 10 DFS apps. They found higher vulnerability in DFS apps in developing countries than in developed countries and argued that off-the-shelf static analysis tools have limitations, especially for DFS-specific vulnerabilities. They identified common vulnerabilities such as insecure inter-process communication, insecure data storage, inadequate use of cryptography, insecure network communication, and WebView vulnerabilities.

Strengths:

- Provides a comprehensive analysis.
- Provides comparative study by comparing apps from developing and developed countries.
- Offers insights for developers and policymakers to enhance the security of DFS apps, particularly in developing countries.
- Identifies specific categories of vulnerabilities, providing a clear focus for future improvements.

Limitations:

- Inherits tool limitations in detecting SSL/TLS misconfigurations and runtime issues.
- The sample may not be representative.
- Limit scope (Android OS).

Paper Title & Reference *Vulnerability Analysis in Mobile Banking and Payment Applications on Android in African Countries* (Bassolé et al. 2020)

Type of Study: App analysis

Summary: The paper assesses the security vulnerabilities of mobile banking and payment apps specifically on Android platforms within African nations, identifying risks related to privacy and data confidentiality. It aims to create awareness among users, businesses, and governments about potential security threats while encouraging the integration of robust security measures in the development of mobile apps.

Strengths:

- Provides a detailed examination of vulnerabilities, focusing on access permissions and code vulnerabilities.
- Gives awareness to stakeholders about the risks.
- Offers insights for developers and users to enhance security.

Limitations:

- Limit scope (App and geography).

Paper Title & Reference *Forensic Analysis of Mobile Banking Apps* (Osho et al. 2019)

Type of Study: App analysis

Summary: In this paper, the authors investigate the security and forensic aspects of mobile banking apps, particularly focusing on popular Android banking apps in Nigeria. The study aims to assess how these apps handle sensitive user data and to identify potential vulnerabilities that could be exploited by attackers. The authors conducted a thorough analysis of twelve mobile banking apps, examining their data storage practices, security measures, and overall resilience against common threats.

Strengths:

- Proposes a detailed forensic analysis of multiple apps.
- Can guide developers in enhancing the security features of mobile banking apps.
- Highlights specific vulnerabilities in the apps.

Limitations:

- Limit scope (App and geography).
- Limited sample

Paper Title & Reference *Security Issues of Unified Payments Interface and Challenges: Case Study* (Madwanna et al. 2021)

Type of Study: App analysis

Summary: The paper provides an in-depth analysis of the Unified Payments Interface (UPI), focusing on its operational framework, security vulnerabilities, and enhancements over time. It outlines how UPI facilitates mobile banking transactions through a user-friendly interface, utilizing Virtual Private Addresses (VPAs) and Payment &Service Providers (PSPs). The paper discusses the architecture of UPI, comparing it with the Immediate Payment Service (IMPS), and highlights the security loopholes present in earlier versions, particularly BHIM UPI 1.0. It also addresses the improvements made in UPI 2.0 to mitigate these vulnerabilities and introduces the concept of offline UPI transactions.

Strengths:

- Provides a thorough explanation of how UPI works.
- Highlights significant security issues and vulnerabilities in UPI, particularly in earlier versions.
- Discusses UPI 2.0 and the measures taken to enhance security.
- Discusses real-world implications of UPI's security issues.

Limitations:

- Lack of comprehensive security analysis for UPI 2.0.
- Limit context and scope.
- Lack of empirical evidence of the current security landscape for UPI.

Paper Title & Reference *Mesh Messaging in Large-Scale Protests: Breaking Bridgefy* (Albrecht et al. 2021)

Type of Study: App analysis

Summary: The paper provides a comprehensive analysis of the security vulnerabilities associated with Bridgefy, a mesh messaging application used in protest scenarios. In this work, authors reverse-engineered the Bridgefy platform using the Jadx tool, and they per-

formed a dynamic inspection using the Frida toolkit to identify several critical weaknesses that undermine its security claims and its effectiveness in facilitating secure communication during protests. The paper details various avenues for tracking users and building social graphs, as well as the lack of effective authentication mechanisms, which could lead to impersonation and man-in-the-middle (MITM) attacks. Authors demonstrated how certain attacks, including variants of Bleichenbacher's attack, can break confidentiality using chosen ciphertexts. They argued that the use of a "zip bomb" could disable the mesh network, highlighting the risks of relying on Bridgefy in critical situations.

Strengths:

- Provides a thorough examination of the Bridgefy application, including reverse engineering and vulnerability assessment.
- The focus on the application's use in protest scenarios makes the findings particularly relevant.
- Outlines the responsible disclosure process.
- Presents concrete examples of attacks that can be executed against the app.

Limitations:

- Limited analysis to a specific version of the app.
- Not include empirical data on how users interact with the app.
- Findings may not be generalizable to all mesh messaging apps.

Paper Title & Reference *Security Analysis of Unified Payments Interface and Payment Apps in India* (Kumar et al. 2020)

Type of Study: App analysis

Summary: In this paper, the authors present a comprehensive security analysis of the UPI protocol, which is widely used in India for digital payment apps. They focus on identifying vulnerabilities within the UPI system and the associated payment apps. The study involved reverse engineering the UPI protocol through various apps, as the protocol details were not publicly available. It uncovered significant weaknesses in the multi-factor authentication workflow of UPI 1.0, which could lead to severe security implications for users. Authors responsibly disclosed their findings and noted that subsequent updates to UPI 2.0 addressed some of the identified vulnerabilities, although several underlying issues remained.

Strengths:

- Provides a detailed security analysis of the UPI 1.0 protocol.
- Addresses a critical area of concern.
- Employes a principled approach to reverse-engineer the UPI protocol.
- The vulnerabilities identified are responsibly disclosed to encourage updates to UPI 2.0.

Limitations:

- Limited sample size.
- The security defenses in the apps prevent the use of automated analysis techniques.

- Limit scope (OS, app category, and geography).

Paper Title & Reference *Forensic Analysis of Mobile Banking Applications in Nigeria* (Uduimoh et al. 2019)

Type of Study: App analysis

Summary: The paper focuses on the forensic examination of five Android-based mobile banking applications used in Nigeria. The primary objectives are to assess the amount of user data generated and retained by these applications after user registration and transactions and to determine if this data can be utilized to identify user actions or transactions. Findings reveal significant insights into the types of sensitive user data retained by these applications, which raises concerns about user privacy and data security.

Strengths:

- Addresses a gap in the literature regarding mobile banking apps in Nigeria.
- Provides a broader understanding of the data retention practices across different platforms.
- Findings are relevant for stakeholders.

Limitations:

- The sample size is not representative.
- Limit scope (OS, app category, and geography).

Paper Title & Reference *Mo(Bile) Money, Mo(Bile) Problems: Analysis of Branchless Banking Applications* (Reaves et al. 2017)

Type of Study: App analysis

Summary: The paper evaluates the security of mobile money applications, particularly focusing on their vulnerabilities and the overall state of security in the mobile money ecosystem. The authors conducted a follow-up analysis nearly a year after their initial study to assess whether the security of these applications had improved. They found that the security of mobile money apps for Android had not significantly improved since 2015: many mobile money applications remained vulnerable to TLS man-in-the-middle attacks at a rate four times higher than normal apps. Nearly half of the apps contacted servers with insecure TLS configurations, and critical vulnerabilities identified in previous analyses had not been addressed, despite ongoing development of non-security features. The authors emphasize the need for collaboration among researchers, regulators, and developers to enhance the security of mobile money apps.

Strengths:

- Provides a thorough examination of mobile money applications.
- Provides a longitudinal study.
- Proposes collaboration with stakeholders.

Limitations:

- Limit scope (OS and app category).
- Limitations in resources to reanalyze apps after vendors made changes.
- Vendor response variability, which may impact the reliability of the findings.

Paper Title & Reference *Side-Effects of Permissions Requested by Mobile Banking on Android Platform: A Case Study of Morocco* (Latifa et al. 2017)

Type of Study: App analysis

Summary: The paper investigates the security issues about the permissions requested by mobile banking applications on the Android platform, focusing on Morocco as a case study. It highlights the potential dangers of these permissions, their effects on sensitive user data, and their relationship with the attack called "Man in the Middle" and its different forms. The authors analyze the permissions requested by the BaridBank Mobile application, comparing it with another banking application, Attijari Mobile, which requests no permissions. The paper also presents the results of an analysis of 100 mobile banking applications using a tool called "PerUpSecure".

Strengths:

- Provides a comprehensive analysis of the permissions requested by mobile banking apps.
- Uses a real-world case study (BaridBank Mobile), making the research relevant and applicable.
- The use of the PerUpSecure tool to analyze a large set of applications adds credibility to the findings.

Limitations:

- Limit scope (OS, app category, and geography).
- Analysis based on permissions requested, not how they are used or misused in practice.
- Does not propose specific solutions or strategies to mitigate the identified risks.

Paper Title & Reference *Vulnerability detection in recent Android apps: An empirical study* (Shezan et al. 2017)

Type of Study: App analysis

Summary: The paper investigates the security vulnerabilities present in Android apps, particularly those developed by individual developers in Bangladesh. The authors conducted an empirical study by selecting a range of applications from a local app store and the Google Play Store and testing them with three different vulnerability detection tools. The study aimed to identify common vulnerabilities, understand their causes and suggest countermeasures to enhance app security. Findings reveal a high prevalence of vulnerabilities, particularly WebView vulnerabilities, which were found in 13 out of 19 tested apps, and other common vulnerabilities such as issues related to advertisement and storage access.

Strengths:

- Employs an empirical approach to analyze apps.
- Selects apps from both local and popular sources.
- Use of multiple tools to ensure a thorough examination of the apps.
- Raises awareness regarding security practices.

Limitations:

- Focus on a small number of apps.
- Limit scope (geographical focus).
- Lack of in-depth analysis of the vulnerability implications.

Paper Title & Reference *On the MitM vulnerability in mobile banking applications for android devices* (Kaka et al. 2016)

Type of Study: App analysis

Summary: The paper discusses the security vulnerabilities in mobile banking applications, specifically focusing on the Man-in-the-Middle (MitM) attack. The authors tested 19 mobile banking applications deployed by public sector banks in India. They found that most of these apps were highly vulnerable to MitM attacks, even those using HTTPS for connection establishment. This indicates a poor implementation of the SSL framework in these applications. The paper also discusses associated attacks such as denial of service, session prediction, account lockout, and HTTP request smuggling.

Strengths:

- Provides a comprehensive analysis of the security vulnerabilities in mobile banking apps.
- Covers a range of associated attacks for the identified vulnerabilities.
- Provides suggestions about the requirements of addressing the basic security flaws.

Limitations:

- Limit scope (geography and app category).
- Not provide specific recommendations or strategies for improving the app security.
- The testing requires actual user credentials, which might raise ethical and privacy concerns.

Paper Title & Reference *Signature Based Malicious Behavior Detection in Android* (Sihag et al. 2020)

Type of Study: App analysis and D&I solutions

Summary: The paper presents a behavior-based approach for detecting Android malware by analyzing system-generated logs during the runtime of apps. The authors focus on identifying malicious behaviors that could lead to information leakage, privilege escalation, and unauthorized access to critical permissions. The proposed system aims to provide a more dynamic and insightful detection method compared to traditional static analysis tech-

niques. It was tested on a variety of applications, including those flagged as malicious by the government of India.

Strengths:

- Proposes a runtime analysis for more accurate detection of malicious activities.
- The system generates signatures based on various malicious behaviors.
- The approach is effective, according to its high accuracy rates.
- The detection system is scalable.

Limitations:

- Dependance on the system logs (which may vary across devices and versions).
- Limited scope of testing (further testing on a broader dataset may be necessary).
- The evasion techniques employed by sophisticated malware are not addressed.

Paper Title & Reference *Integrating OAuth and Aadhaar with e-Health care System* (Khatoon and Umadevi 2018)

Type of Study: D&I solutions

Summary: The paper explores the integration of OAuth 2.0 (a secure protocol for access delegation) and Aadhaar (India's unique identification system) authentication into e-Health apps in India to enhance security and streamline user authentication. The primary goal is to provide secure access to electronic health records (EHR) and facilitate efficient interaction between patients and healthcare providers. The paper outlines the implementation of the proposed system, including authentication, registration, and login flows. It also discusses offline access and the use of big data tools for analytics.

Strengths:

- Provides a robust authentication mechanism.
- Aadhaar-based authentication simplifies the registration and login processes.
- Covers various aspects of eHealth applications, from different types of apps to the roles of stakeholders.
- The system is scalable with the use of cloud infrastructure and big data tools.

Limitations:

- Dependency on Aadhaar.
- The implementation complexity may be a barrier for smaller healthcare providers.
- Use of centralized storage.
- The extent of the offline access functionality is not fully detailed.

Paper Title & Reference *A Comparative Study of User Data Security and Privacy in Native and Cross Platform Android Mobile Banking Applications* (Ansong and Synaepa-Addision 2019)

Type of Study: DFS

Summary: The study investigates the security and privacy of user data in Android mobile banking applications, based on permissions requested and used. The objective is to determine which development framework (native or cross-platform) ensures better user data privacy and security in mobile banking applications. The study focuses on 22 mobile banking apps from Ghanaian banks and identifies the development frameworks and permissions they requested/used. The findings reveal that cross-platform apps tend to use more of the permissions they request compared to native apps, which use fewer of the requested permissions. Consequently, cross-platform frameworks are recommended for mobile banking apps.

Strengths:

- Provides a detailed comparison of permissions requested and used by both native and cross-platform apps.
- The use of specific tools and a structured approach adds credibility to the findings.
- Offers recommendations for developers and banks to enhance security and privacy in mobile banking apps.

Limitations:

- The AVC UnDroid tool could not analyze apps larger than 14MB.
- The sample size may be not representative.
- Limit scope (geography and app category).
- Focus only on Apache Cordova for cross-platform apps.

Author Contributions The idea for this article comes from Jacques Klein. The conceptualization, methodology, investigation, formal analysis, literature search, and data analysis were performed by Alioune Diallo. The first draft of the manuscript was written by Alioune Diallo, and all authors commented on previous versions of the manuscript. All authors critically reviewed, edited, read, and approved the final manuscript. The work was supervised by Jacques Klein and Tégawendé F. Bissyandé.

Funding This work is supported by the Luxembourg Ministry of Foreign and European Affairs through their Digital4Development (D4D) portfolio under the project LuxWAyS (Luxembourg/West-Africa Lab for Higher Education Capacity Building in CyberSecurity and Emerging Topics in ICT4Dev.)

Data Availibility The datasets used in the current study are available in our online repository (Diallo et al. 2024).

Declarations

Ethical approval not applicable.

Informed consent not applicable.

Conflicts of interest The authors declare that they have no conflict of interest.

References

Abdullaev A, Al-Absi MA, Al-Absi AA, Sain M, Lee Y-S, Lee HJ (2019) Security challenge and issue of mobile banking in republic of uzbekistan: a state of art survey. In: 2019 21st international conference on advanced communication technology (ICACT). IEEE, pp 249–255

Alaiad A, Alsharo M, Alnsour Y (2019) The determinants of m-health adoption in developing countries: an empirical investigation. Appl Clin Inform 10(05):820–840

Al-Ameen MN, Tamanna T, Nandy S, Ahsan MAM, Chandra P, Ahmed SI (2020) We don't give a second thought before providing our information: Understanding users' perceptions of information collection by apps in urban bangladesh. In: Proceedings of the 3rd ACM SIGCAS conference on computing and sustainable societies. COMPASS '20. Association for Computing Machinery, New York, NY, USA, pp 32–43. https://doi.org/10.1145/3378393.3402244

Albrecht MR, Blasco J, Jensen RB, Mareková L (2021) Mesh messaging in large-scale protests: breaking bridgefy. In: Paterson KG (ed) Topics in Cryptology – CT-RSA 2021. Springer, Cham, pp 375–398

Alenezi M, Almomani I (2017) Abusing android permissions: a security perspective. In: 2017 IEEE jordan conference on applied electrical engineering and computing technologies (AEECT). IEEE, pp 1–6

Aljohani N, Chandran D (2021) The adoption of mobile health applications by patients in developing countries: a systematic review. Int J Adv Comput Sci Appl

Android (2023a) Permissions on android. https://developer.android.com/guide/topics/permissions/overview

Android (2023b) Security with network protocols. https://developer.android.com/training/articles/security-ssl

Ansong ED, Synaepa-Addision TQ (2019) A comparative study of user data security and privacy in native and cross platform android mobile banking applications. In: 2019 international conference on cyber security and internet of things (ICSIoT), pp 5–10. https://doi.org/10.1109/ICSIoT47925.2019.00007

approov (2023) Security challenges of financial mobile apps in Africa. https://approov.io/info/security-challenges-of-financial-mobile-apps-in-africa

Argudo A, López G, Sánchez F (2017) Privacy vulnerability analysis for android applications: a practical approach. In: 2017 fourth international conference on eDemocracy & eGovernment (ICEDEG), pp 256–260. https://doi.org/10.1109/ICEDEG.2017.7962545

Azeez ND, Lakulu MM (2019) Review of mobile government at developing countries: benefits and challenges. Int J Econ Bus Manag Res 3(2):198–219

Bandan SS, Rahman Ajmain M, Rejuan AR, Farhana Khatun M, Khushbu SA (2022) State of survey: advancement of knowledge environmental sustainability in practicing administrative apps. In: 2022 13th international conference on computing communication and networking technologies (ICCCNT), pp 1–8. https://doi.org/10.1109/ICCCNT54827.2022.9984416

Bassolé D, Koala G, Traoré Y, Sié O (2020) Vulnerability analysis in mobile banking and payment applications on android in african countries. In: Thorn JPR, Gueye A, Hejnowicz AP (eds) Innovations and interdisciplinary solutions for underserved areas. Springer, Cham, pp 164–175

Baur-Yazbeck S, Frickenstein J, Medine D (2019) Cyber security in financial sector development. CGAP Background Documents 5(2)

bertolis (2022) A step-by-step android penetration testing guide for beginners. https://www.hackthebox.com/blog/intro-to-mobile-pentesting

Carter W (2017) Forces shaping the cyber threat landscape for financial institutions. SWIFT Institute Working Paper

Castle S, Pervaiz F, Weld G, Roesner F, Anderson R (2016) Let's talk money: evaluating the security challenges of mobile money in the developing world. ACM DEV '16. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3001913.3001919

Chiboora TH, Chacha L, Byagutangaza T, Gueye A (2023) Evaluating mobile banking application security posture using the owasp's masvs framework. In: Proceedings of the 6th ACM SIGCAS/SIGCHI conference on computing and sustainable societies, pp 99–106

Chopdar PK (2022) Adoption of covid-19 contact tracing app by extending utaut theory: perceived disease threat as moderator. Health Policy Technol 11(3):100651. https://doi.org/10.1016/j.hlpt.2022.100651

Diallo A, Samhi J, Bissyandé T, Klein J (2024) (In)Security of mobile apps in developing countries: a systematic literature review - dataset. https://github.com/liounea/Dataset-for-the-SLR-in-mobile-app-security

Hoque MR, Rahman MS, Nipa NJ, Hasan MR (2020) Mobile health interventions in developing countries: a systematic review. Health Informatics J 26(4):2792–2810

Howell G, Franklin JM, Sritapan V, Souppaya M, Scarfone K (2023) Guidelines for managing the security of mobile devices in the enterprise. Technical report, National Institute of Standards and Technology

Hsu J, Liu D, Yu YM, Zhao HT, Chen ZR, Li J, Chen W (2016) The top chinese mobile health apps: a systematic investigation. J Med Internet Res 18(8):222

Ibrar F, Saleem H, Castle S, Malik MZ (2017) A study of static analysis tools to detect vulnerabilities of branchless banking applications in developing countries. ICTD '17. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3136560.3136595
ISO (2022) ISO/IEC 27001:2022. https://www.iso.org/standard/27001
Kaka S, Sastry VN, Maiti RR (2016) On the mitm vulnerability in mobile banking applications for android devices. In: 2016 IEEE international conference on advanced networks and telecommunications systems (ANTS), pp 1–6. https://doi.org/10.1109/ANTS.2016.7947811
Kala Kamdjoug JR, Wamba-Taguimdje S-L, Wamba SF, Kake IB (2021) Determining factors and impacts of the intention to adopt mobile banking app in cameroon: case of sara by afriland first bank. J Retail Consumer Services 61:102509. https://doi.org/j.jretconser.2021.102509
Kaminsky S (2023) The hidden risks of cheap android devices. https://www.kaspersky.com/blog/how-to-avoid-threats-from-budget-android-devices/49565/
Kant Kamal K, Joshi P, Bang A, Bhatia K (2023) Effective security testing of mobile applications for building trust in the digital world. In: 2023 7th international conference on trends in electronics and informatics (ICOEI), pp 550–556. https://doi.org/10.1109/ICOEI56765.2023.10125814
Keele S et al (2007) Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, ver. 2.3 ebse technical report. ebse
Keyideas (2017) Impact of smartphones over society. https://www.keyideasinfotech.com/blog/impact-of-smartphone-on-society/
Khatoon A, Corcoran P (2017) Privacy concerns on android devices. In: 2017 IEEE international conference on consumer electronics (ICCE). IEEE, pp 149–152
Khatoon A, Umadevi V (2018) Integrating oauth and aadhaar with e-health care system. In: 2018 3rd IEEE international conference on recent trends in electronics, information & communication technology (RTEICT), pp 1681–1686. https://doi.org/10.1109/RTEICT42901.2018.9012487
Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering-a systematic literature review. Inf Softw Technol 51(1):7–15
Koala G, Bassolé D, Zerbo/Sabané A, Bissyandé TF, Sié O (2020) Analysis of the impact of permissions on the vulnerability of mobile applications. In: Zitouni R, Agueh M, Houngue P, Soude H (eds) e-Infrastructure and e-Services for developing countries. Springer, Cham, pp 3–14
Kumar R, Kishore S, Lu H, Prakash A (2020) Security analysis of unified payments interface and payment apps in india. In: 29th USENIX security symposium (USENIX Security 20). USENIX Association, ???, pp 1499–1516. https://www.usenix.org/conference/usenixsecurity20/presentation/kumar
Latif S, Rana R, Qadir J, Ali A, Imran MA, Younis MS (2017) Mobile health in the developing world: review of literature and lessons from a case study. IEEE Access 5:11540–11556
Latifa E-r, Ahemed EKM, Mohamed EG (2017) Side-effects of permissions requested by mobile banking on android platform: a case study of morocco. In: Proceedings of the 1st international conference on E-Commerce, E-Business and E-Government. ICEEG '17. Association for Computing Machinery, New York, NY, USA, pp 76–81. https://doi.org/10.1145/3108421.3108433
Lazović V, Duričković T (2014) The digital economy in developing countries-challenges and opportunities. In: 2014 37th international convention on information and communication technology, electronics and microelectronics (MIPRO), pp 1580–1585. https://doi.org/10.1109/MIPRO.2014.6859817
Madwanna Y, Khadse M, Chandavarkar BR (2021) Security issues of unified payments interface and challenges: case study. In: 2021 2nd international conference on secure cyber computing and communications (ICSCCC), pp 150–154. https://doi.org/10.1109/ICSCCC51823.2021.9478078
Malik M (2020) A review of empirical research on internet & mobile banking in developing countries using utaut model during the period 2015 to April 2020. J Internet Bank Commer 25(2):1–22
Martínez-Pérez B, De La Torre-Díez I, López-Coronado M (2015) Privacy and security in mobile health apps: a review and recommendations. J Med Syst 39:1–8
Mishra S, Soni D (2020) Smishing detector: A security model to detect smishing through sms content analysis and url behavior analysis. Future Gener Comput Syst 108:803–815. https://doi.org/10.1016/j.future.2020.03.021
Mkpojiogu EO, Hussain A, Agbudu MO (2021) Security issues in the use of mobile educational apps: a review. Int J Interactive Mobile Technol 15(6)
Msweli NT, Mawela T (2020) Enablers and barriers for mobile commerce and banking services among the elderly in developing countries: a systematic review. In: Responsible design, implementation and use of information and communication technology: 19th IFIP WG 6.11 conference on e-Business, e-Services, and e-Society, I3E 2020, Skukuza, South Africa, April 6–8, 2020, Proceedings, Part II 19. Springer, pp 319–330
Munyendo CW, Acar Y, Aviv AJ (2022) "desperate times call for desperate measures": user concerns with mobile loan apps in kenya. In: 2022 IEEE symposium on security and privacy (SP), pp 2304–2319. https://doi.org/10.1109/SP46214.2022.9833779

Nations U (2023) Widening digital gap between developed, developing states threatening to exclude world's poorest from next industrial revolution, speakers tell second committee. https://press.un.org/en/2023/gaef3587.doc.htm

Olson JA, Sandra DA, Colucci ÉS, Al Bikaii A, Chmoulevitch D, Nahas J, Raz A, Veissière SP (2022) Smartphone addiction is increasing across the world: a meta-analysis of 24 countries. Comput Hum Behav 129:107138

Osho O, Mohammed UL, Nimzing NN, Uduimoh AA, Misra S (2019) Forensic analysis of mobile banking apps. In: Misra S, Gervasi O, Murgante B, Stankova E, Korkhov V, Torre C, Rocha AMAC, Taniar D, Apduhan BO, Tarantino E (eds) Computational science and its applications – ICCSA 2019. Springer, Cham, pp 613–626

Osman F, Hassan2 WH, Yamada Y, Goudarzi4 S (2017) Challenges of mobile money to mobile transaction service on policy regulation and security frauds in east africa. In: ASIA international multidisciplinary conference 2017

OWASP (2024) OWASP mobile application security. https://mas.owasp.org/

OWASP (2024) OWASP Mobile Top 10. https://owasp.org/www-project-mobile-top-10/

OWASP (2024a) MASVS-CODE: code quality. https://mas.owasp.org/MASVS/10-MASVS-CODE/#masvs-code-code-quality

OWASP (2024b) MASVS-RESILIENCE: resilience against reverse engineering and tampering. https://mas.owasp.org/MASVS/11-MASVS-RESILIENCE/#masvs-resilience-resilience-against-reverse-engineering-and-tampering

Pankomera R, Greunen D (2019) Opportunities, barriers, and adoption factors of mobile commerce for the informal sector in developing countries in africa: a systematic review. Electron J Inf Syst Dev Countries 85(5):12096. https://doi.org/10.1002/isd2.12096. https://onlinelibrary.wiley.com/doi/pdf/10.1002/isd2.12096. e12096 ISD-RA-0111.R3

Pentina I, Zhang L, Bata H, Chen Y (2016) Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Comput Hum Behav 65:409–419

Prakash AV, Das S, Pillai KR (2021) Understanding digital contact tracing app continuance: insights from india. Health Policy Technol 10(4):100573. https://doi.org/10.1016/j.hlpt.2021.100573

proofpoint (2024) What is a data breach? https://www.proofpoint.com/us/threat-reference/data-breach

Rahman M, Tazim MZ, Das S, Islam L (2020) State of the art of mobile banking services and future prospects in developing countries. In: 2020 IEEE 9th international conference on communication systems and network technologies (CSNT). IEEE, pp 145–149

Reaves B, Bowers J, Scaife N, Bates A, Bhartiya A, Traynor P, Butler KRB (2017) Mo(bile) money, mo(bile) problems: analysis of branchless banking applications. ACM Trans Priv Secur 20(3). https://doi.org/10.1145/3092368

Review WP (2023) Developing countries 2023. https://worldpopulationreview.com/country-rankings/developing-countries

Sheldon R (2019) Advantages and disadvantages of mobile devices in business. https://www.techtarget.com/searchmobilecomputing/feature/Discover-the-benefits-of-mobile-devices-in-the-enterprise

Shezan FH, Afroze SF, Iqbal A (2017) Vulnerability detection in recent android apps: an empirical study. In: 2017 international conference on networking, systems and security (NSysS), pp 55–63. https://doi.org/10.1109/NSysS.2017.7885802

Sihag V, Swami A, Vardhan M, Singh P (2020) Signature based malicious behavior detection in android. In: Chaubey N, Parikh S, Amin K (eds) Computing science, communication and security. Springer, Singapore, pp 251–262

Statica (2023) Percentage of mobile users who have fallen victim to mobile malware infections in 3rd quarter 2022, by country. https://www.statista.com/statistics/325201/countries-share-of-malicious-attacks/

Turner A (2023a) How many smartphones are in the world? https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#1579705085743-b3697bdb-9a8f

Turner A (2023b) How many apps are there in the world. https://www.bankmycell.com/blog/number-of-mobile-apps-worldwide

Uduimoh A, Idris I, Osho O, Abdulhamid S (2019) Forensic analysis of mobile banking applications in nigeria. i-manager's J Mobile Appl Technol 6:9–20. https://doi.org/10.26634/jmt.6.1.15704

Unconnected IC (2023) Digital divide in developing countries: why we need to close the gap. https://ctu.ieee.org/blog/2023/01/23/digital-divide-in-developing-countries-why-we-need-to-close-the-gap/

Vakare G, Rautela D, Shobharam Lamkuche H (2022) User's perception on security and privacy in using crypto currency trading application in india. In: 2022 international conference on knowledge engineering and communication systems (ICKES), pp 1–8. https://doi.org/10.1109/ICKECS56523.2022.10060666

ValueMentor (2022) Top 10 mobile app security vulnerabilities banks should avoid! https://valuementor.com/mobile-app-security-testing/top-10-mobile-app-security-vulnerabilities-banks-should-avoid/

Yang L, Zhang H, Shen H, Huang X, Zhou X, Rong G, Shao D (2021) Quality assessment in systematic literature reviews: a software engineering perspective. Inf Softw Technol 130:106397

Alioune Diallo is a Ph.D. student at the TruX research group from the SnT (Interdisciplinary Centre for Security, Reliability, and Trust) of the University of Luxembourg. He received her engineering diploma in computer science in 2019 from Gaston BERGER University (UGB) of Saint-Louis, in Senegal. He joined the TruX under the LuxWays initiative, which is a project developed by the University's Interdisciplinary Centre for Security, Reliability, and Trust (SnT) with three participating universities: the University of Cheikh Anta Diop from Senegal, the University of Joseph Ki-Zerbo and the Virtual University, both from Burkina Faso. This project aims to allow students at the partnering universities in West Africa to participate in cybersecurity PhD programs in Luxembourg. This will eventually allow them to return to their home universities to teach students about issues related to cybersecurity, such as FinTech systems and Artificial Intelligence. Alioune Diallo is interested in cybersecurity and is currently working on mobile application security in developing countries as PhD project.

Jordan Samhi is a research scientist in the TruX research group within the Interdisciplinary Center for Security, Reliability, and Trust (SnT) at the University of Luxembourg. He pursued his Ph.D. and then became a postdoc at the TruX research group and at CISPA in Germany in Software Security and Software Engineering, where he contributed to the software research group's ongoing efforts in this field. He received an Excellent Doctoral Thesis Award at the University of Luxembourg. Dr. Jordan Samhi's research focuses on harnessing the power of static code analysis to automate software security, with a keen interest in enhancing the comprehensiveness of software analysis to ensure the utmost security and reliability of software systems. Currently, his work focuses on Android systems, seeking innovative ways to protect and optimize these platforms. He has published and contributed to several research papers in computer science and related topics in top-tier venues, including ACM/IEEE ICSE, IEEE ESEC/FSE, IEEE/ACM MOBILESoft, etc.

Tegawendé F. Bissyandé is a Chief Scientist (Professor) affiliated with the SnT Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg. He received his Ph.D. in Computer Science from the University of Bordeaux (France) in 2013 after earning an engineering degree in Telecom software engineering in 2009. He is currently an ERC Starting Grant holder on natural program repair based on Artificial Intelligence. Prof. Bissyandé is the Principal Investigator of a cooperation project with Canada to establish an Interdisciplinary Centre of Excellence in Artificial Intelligence for Development in Burkina Faso, where research and innovation projects in various domains, such as agriculture, are being investigated in light of the power of Artificial Intelligence. Prof. Bissyandé also coleads the Trustworthy Software Engineering (TruX) Research Group at SnT with Prof. Klein, where his research interests span across several topics, including mainly: (0) application of machine learning to software engineering, (1) program repair; (2) software security, i.e., mobile static security analysis, vulnerability detection, and malware detection; (3) software analytics, i.e., code search, clone detection, and repository mining. Prof. Bissyandé's research is funded through several research grants and by prominent industry partners. He has published around 100 research papers in computer science and related topics in top-tier venues, including AAAI, ACM/IEEE ICSE, IEEE/ACM ASE, IEEE ESEC/FSE, IEEE TSE, ACM TOPS, IEEE TIFS, ACM TOSEM, EMSE, KDD, etc. He has also served his research community as a Program Committee member of several conferences, including ASE, ISSTA, ICSME, and ICSE.

Jacques Klein is a researcher and professor in software engineering and software security who develops innovative approaches and tools for helping the research and practice communities build trustworthy software. He is a member of the Interdisciplinary Centre for Security, Reliability, and Trust (SnT) at the University of Luxembourg. Prof. Klein co-leads the Trustworthy Software Engineering (TruX) Research Group there. He received a Ph.D. degree in Computer Science from the University of Rennes, France, in 2006. His main areas of expertise are threefold: (1) Software Security (Malware detection, prevention and dissection, Static Analysis for Security, Vulnerability Detection, etc.); (2) Software Reliability (Software Testing, Semi-Automated and Fully-Automated Program Repair, etc.); (3) Data Analytics (Multi-objective reasoning and optimization, Model-driven data analytic, Time Series Pattern Recognition, etc.). He has published over 150 research papers in computer science and related topics in top-tier venues, including AAAI, ACM/IEEE ICSE, IEEE/ACM ASE, IEEE ESEC/FSE, ACM CSUR, ACM TOSEM, etc. He has also served his research community as a Program Committee member of several conferences, including ASE, ISSTA, ICSME, and ICSE. In addition to academic achievements, Prof. Klein also has long-standing experience and expertise in successfully running industrial projects with several industrial partners in various domains by applying data analytics, software engineering, information retrieval, etc., to their research problems.