International Journal of Safety and Security Engineering
Vol. 16, No. 6, June, 2026, pp. 1297-1308
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Risk Exposure and Civilian Financial Safety in Digital Payment Systems During Armed Conflict: Evidence from Sudan

Mustafa ElGili[1*], Ahmed ELtayeb[2], Ahmed Abaker[1], Mohamed Mamoun[3]

[1] Applied College-Huraymila, Computer Programs, Imam Muhammad Ibn Saud Islamic University, Huraymila 15432, Saudi Arabia
[2] College of Science and Humanities-Dawadmi, Shaqra University, Dawadmi 17431, Saudi Arabia
[3] Information Technology Department, Alzaiem Alazhari University, Khartoum 11119, Sudan

Corresponding Author Email: meelmogadem@imamu.edu.sa

https://doi.org/10.18280/ijsse.160612

Received: 23 May 2026
Revised: 16 June 2026
Accepted: 23 June 2026
Available online: 30 June 2026

Keywords:
armed conflict, civilian financial safety, Cybersecurity Risk Exposure, digital payment systems, infrastructure instability, security engineering

ABSTRACT

Digital payment systems have become essential for civilians in conflict-affected environments where conventional banking and financial services have been disrupted. This study investigates Cybersecurity Risk Exposure (CRE) associated with the use of digital payments during armed conflict and examines its impact on Perceived Financial Safety (PFS) among civilians affected by the Sudan conflict. A quantitative cross-sectional survey was conducted using a structured questionnaire administered to 173 respondents. The data were analyzed using descriptive statistics, reliability and validity analyses, supportive one-sample t-tests and Chi-square tests, and regression-based hypothesis testing. The findings show that respondents demonstrated relatively high levels of cybersecurity awareness and protective practices, while also experiencing substantial Cyber Threat Exposure (CTE) and elevated CRE. The regression results indicate that CTE significantly increased CRE, whereas Advanced Privacy Protection (APP) and Cybersecurity Awareness and Security Practices (CASP) were negatively associated with CRE, while perceived cybersecurity Training Need (TN) also showed a significant negative association that should be interpreted as an inverse statistical relationship rather than causal risk reduction. CRE also had a significant negative effect on PFS. This study contributes a civilian-centered socio-technical perspective and highlights the need for conflict-sensitive cybersecurity strategies to strengthen digital resilience during crises.

1. INTRODUCTION

Digital payment systems have expanded rapidly alongside the growth of financial technologies (FinTech), enabling more accessible and efficient financial transactions worldwide. In fragile and conflict-affected states, these systems become essential when traditional banking infrastructure is disrupted. However, although digital payments enhance financial access, they also introduce significant cybersecurity risks, including fraud, phishing, and data breaches [1, 2].

Existing research highlights the importance of trust, perceived security, and usability in FinTech adoption [3]. However, these models have largely been developed in stable environments and assume the presence of reliable infrastructure and institutional support. In conflict settings, such assumptions may not apply. Infrastructure disruption, banking collapse, and limited access to cash may force civilians to rely on digital payments out of necessity, thereby increasing their exposure to cyber threats.

The current literature presents several limitations. Cybersecurity studies are often technology-centric, focusing on detection systems while giving limited attention to user vulnerability and environmental constraints [4]. FinTech adoption research emphasizes trust and risk but often overlooks necessity-driven usage in crisis contexts [5]. Meanwhile, humanitarian studies on digital payments mainly focus on efficiency and financial inclusion, with limited attention to cybersecurity risks and financial safety outcomes [6, 7].

Compared with prior work, this study provides a more comprehensive understanding by linking technology, user behavior, and conflict conditions, offering a novel and practically relevant perspective on cybersecurity risks in digital payment systems.

Therefore, this study investigates how cybersecurity awareness, Cyber Threat Exposure (CTE), Advanced Privacy Protection (APP), and Training Needs (TN) influence Cybersecurity Risk Exposure (CRE) and Perceived Financial Safety (PFS) among civilians using digital payment systems during the Sudan conflict.

2. LITERATURE REVIEW AND THEORETICAL FOUNDATION

2.1 Cybersecurity in digital payment systems

Digital payment technologies have transformed financial

services by improving transaction speed, accessibility, and financial inclusion, particularly in developing and resource-constrained contexts [1, 8]. However, their rapid expansion has also increased cybersecurity risks, including phishing, malware, ransomware, denial-of-service attacks, identity theft, account compromise, and authentication vulnerabilities [1, 2]. Phishing remains a particularly serious threat because it exploits users' trust to obtain sensitive financial and personal information [9].

Existing studies have proposed data mining, machine learning, deep learning, and decentralized fraud detection approaches to enhance fraud detection and strengthen platform security. However, most of this research remains system-centered and assumes stable infrastructure, reliable connectivity, and strong institutional support [1, 10-14]. As a result, there is limited understanding of user-centered cybersecurity risks in fragile and conflict-affected environments.

In humanitarian and armed conflict settings, civilians often depend on digital payment systems under unstable conditions, including infrastructure disruption, internet instability, displacement, and weak institutional protection. These conditions increase user vulnerability and reduce the effectiveness of conventional cybersecurity safeguards. Therefore, cybersecurity in digital payment systems should be understood not only as a technical issue but also as a socio-technical challenge shaped by technology, user behavior, and environmental instability.

2.2 Digital payments in conflict and humanitarian contexts

Digital payment systems have become important tools in humanitarian response because they enable faster assistance, lower transaction costs, improved transparency, and better access to financial support for vulnerable populations affected by displacement, poverty, and armed conflict [6, 15]. Prior studies show that digital cash assistance can improve aid delivery, household welfare, and food security during crises [6, 16].

In fragile and conflict-affected environments, digital payments become especially important when banking infrastructure, communication systems, and formal financial services are disrupted [17]. Evidence from Sudan shows that digital cash transfers can support vulnerable households and reduce food insecurity, while humanitarian reports indicate growing reliance on digital wallets and electronic financial tools among displaced and crisis-affected populations [7, 18]. Thus, digital payment systems function not only as FinTechbut also as mechanisms that support resilience and survival during humanitarian crises.

However, these systems depend on stable infrastructure, connectivity, identification mechanisms, regulation, and institutional support, all of which may be weakened during conflict [6, 19]. Such instability can increase exposure to cybercrime, fraud, misinformation, identity misuse, and unauthorized access, particularly among displaced populations with limited digital literacy and weak cybersecurity support [20, 21]. In Sudan, disruptions to banking systems, internet infrastructure, and public services since 2023 have increased reliance on digital payments, creating both humanitarian benefits and new forms of CRE [22, 23].

2.3 Financial technologies adoption, trust and security

FinTech has transformed financial services by introducing mobile payments, e-wallets, online banking, peer-to-peer payment systems, and other digital financial applications that enhance convenience, efficiency, cost reduction, and financial inclusion [3, 8]. In this context, trust, perceived security, privacy, and financial risk are key factors influencing users' adoption and continued use of digital FinTech [3, 5, 24].

Previous studies show that users are more likely to adopt digital payment systems when they believe that these platforms protect personal information, ensure transaction integrity, and provide reliable security mechanisms, such as encryption, authentication, and privacy safeguards [3, 24, 25]. Trust also mediates the relationship between perceived usefulness (PU), ease of use, and technology adoption, while institutional and regulatory trust further influence FinTech acceptance [25, 26].

However, most FinTech adoption studies have been conducted in stable environments where users voluntarily evaluate benefits, risks, and trust before adoption [3, 24-26]. In conflict-affected settings, these assumptions may not fully apply because banking disruption and limited financial alternatives may force civilians to use digital payments despite low trust and high cybersecurity risk [20]. This creates a trust-behavior disconnect, where technology use continues due to necessity rather than confidence, highlighting the need to study FinTech adoption in humanitarian and armed conflict contexts.

2.4 Theoretical foundation

2.4.1 Technology Acceptance Model

The Technology Acceptance Model (TAM), developed by Davis [27], is one of the most widely used frameworks for explaining technology adoption behavior. TAM proposes that technology acceptance is primarily influenced by PU and perceived ease of use (PEOU), which shape users' attitudes and behavioral intentions toward technology use. The model has been extensively applied in mobile banking, digital payment, and FinTech studies because of its strong ability to explain technology adoption behavior [25, 28]. Previous studies have found that trust, perceived security, and privacy significantly influence users' willingness to adopt digital FinTech [3, 24, 25].

Later extensions of TAM incorporated additional factors, such as trust, perceived risk, and security perceptions, to better explain technology use decisions [29]. However, conventional TAM assumptions may be limited in conflict environments, where technology adoption is driven by necessity rather than voluntary choice. In contexts such as Sudan, disruptions to banking systems and financial infrastructure may force civilians to rely on digital technologies regardless of trust or usability considerations [22, 23]. Therefore, this study extends TAM by integrating Cybersecurity Awareness and Security Practices (CASP), APP, and PFS to explain digital payment behavior under conditions characterized by instability, cybersecurity threats, and constrained technological alternatives.

2.4.2 Protection Motivation Theory

Protection Motivation Theory (PMT), developed by Rogers [30], explains how individuals respond to perceived threats and adopt protective behaviors. The theory proposes that individuals evaluate risks through threat appraisal, including perceived severity and vulnerability, and coping appraisal, including response effectiveness and self-efficacy. Together,

these appraisals influence adaptive protective actions. PMT has been widely applied in cybersecurity and information security research because it explains why individuals adopt security practices and protective behaviors [31, 32].

Previous studies indicate that greater threat perception and stronger coping capabilities increase individuals' likelihood of adopting cybersecurity measures, such as privacy protection, secure practices, and risk mitigation behaviors [33, 34]. In digital environments, users increasingly face cybersecurity threats, including phishing, fraud, malware, misinformation, and identity-related risks [1, 2]. In conflict settings, these risks become more severe because of instability, weakened infrastructure, and greater dependence on digital technologies.

The proposed framework aligns with PMT by incorporating CTE as a threat-related dimension, while CASP and APP are treated as protective behavior dimensions. Perceived Cybersecurity TN is examined separately as an indicator of respondents' perceived need for cybersecurity education, rather than as evidence of completed training or existing preparedness. Accordingly, greater threat exposure is expected to be positively associated with CRE, whereas stronger awareness and privacy protection practices are expected to be negatively associated with CRE. TN is examined as a non-directional correlate because higher perceived TN may reflect either greater vulnerability awareness or a proactive orientation toward cybersecurity support.

2.4.3 Socio-Technical Systems theory

Socio-Technical Systems (STS) theory explains that technological outcomes emerge through interactions between social and technical components rather than from technology alone [35]. The theory argues that system performance depends on the relationships among users, technologies, organizational structures, and environmental conditions. STS has been widely applied in information systems and cybersecurity research because it provides a broader understanding of how social, technical, and environmental dimensions jointly shape security outcomes in complex systems [36]. Recent cybersecurity studies emphasize that effective cyber resilience requires a balanced consideration of behavioral, technological, and contextual factors rather than a focus on technology alone.

This perspective is particularly relevant in conflict environments, where technological systems operate under unstable conditions characterized by infrastructure disruption, communication instability, institutional breakdown, and increased dependence on alternative digital services. Unlike traditional cybersecurity approaches that assume stable infrastructure, STS recognizes that cybersecurity outcomes are shaped by both human behavior and environmental conditions.

The proposed framework aligns with STS by integrating the social and technical dimensions that affect cybersecurity vulnerability. CASP and TN represent behavioral dimensions, APP reflects technical safeguards, and CTE captures environmental pressures and cyber risks. These factors collectively influence CRE, which subsequently affects PFS. STS also supports the study's concept of a behavior-vulnerability gap, suggesting that strong protective behaviors alone may not sufficiently reduce cyber risks when broader socio-technical environments remain unstable.

2.5 Research gap

Existing studies have significantly contributed to understanding cybersecurity, digital payment adoption, fraud detection, trust, and financial technology behavior [1-5]. Similarly, recent humanitarian and conflict-related studies highlight the increasing role of digital technologies and payment systems in supporting vulnerable populations and maintaining financial access during crises [6, 7, 15, 16, 18, 21]. However, several limitations remain.

First, most cybersecurity and FinTech studies have been developed in stable environments that assume reliable infrastructure and institutional support [1, 3, 5]. These assumptions may not apply to conflict settings characterized by infrastructure instability and disrupted services. Second, previous studies often examine cybersecurity dimensions independently, such as awareness, trust, or protective behavior, which limits understanding of how these factors interact under humanitarian conditions [33-35]. Third, existing research frequently emphasizes technical solutions, including authentication systems and fraud detection models, while overlooking civilian-centered vulnerabilities and socio-technical conditions [10-14, 37]. Finally, limited empirical evidence exists regarding cybersecurity experiences among conflict-affected populations, particularly in Global South contexts such as Sudan [6, 7, 16].

To address these limitations, this study proposes a conflict-sensitive and civilian-centered framework that integrates CASP, CTE, APP, TN, CRE, and PFS. The study further introduces the concept of a behavior-vulnerability gap, suggesting that civilians may demonstrate strong protective behaviors while remaining exposed to substantial cyber risks under conflict conditions. Thus, this research extends the cybersecurity literature by providing empirical evidence from Sudan and offering a broader socio-technical understanding of cybersecurity vulnerability during armed conflict.

2.6 Conceptual framework and hypothesis development

The model proposes that CASP and APP are negatively associated with CRE, whereas CTE is positively associated with it. Perceived Cybersecurity TN is examined as a non-directional correlate of CRE because higher scores may reflect either greater vulnerability awareness or a proactive orientation toward cybersecurity support.

The hypotheses were developed based on the proposed conceptual framework and supported by PMT and STS. PMT explains how individuals respond to cyber threats through protective behaviors, whereas STS highlights the interaction among users, technology, and environmental conditions. In the context of the Sudan conflict, cybersecurity vulnerability is shaped by both digital risks and conflict-related instability. Therefore, the hypotheses examine how cybersecurity awareness, privacy protection, TN, and CTE influence CRE and PFS.

H1: CASP negatively influence CRE.
H2: CTE positively influences CRE.
H3: APP negatively influences CRE.
H4: Perceived Cybersecurity TN is significantly associated with CRE.
H5: CRE negatively influences PFS.

Collectively, these hypotheses establish the empirical structure of the proposed conceptual framework and explain how cybersecurity awareness, privacy behaviors, CTE, and perceived cybersecurity TN interact to influence cybersecurity vulnerability and financial safety among civilians during armed conflict. These relationships are illustrated in Figure 1 and are subsequently tested through statistical analysis.

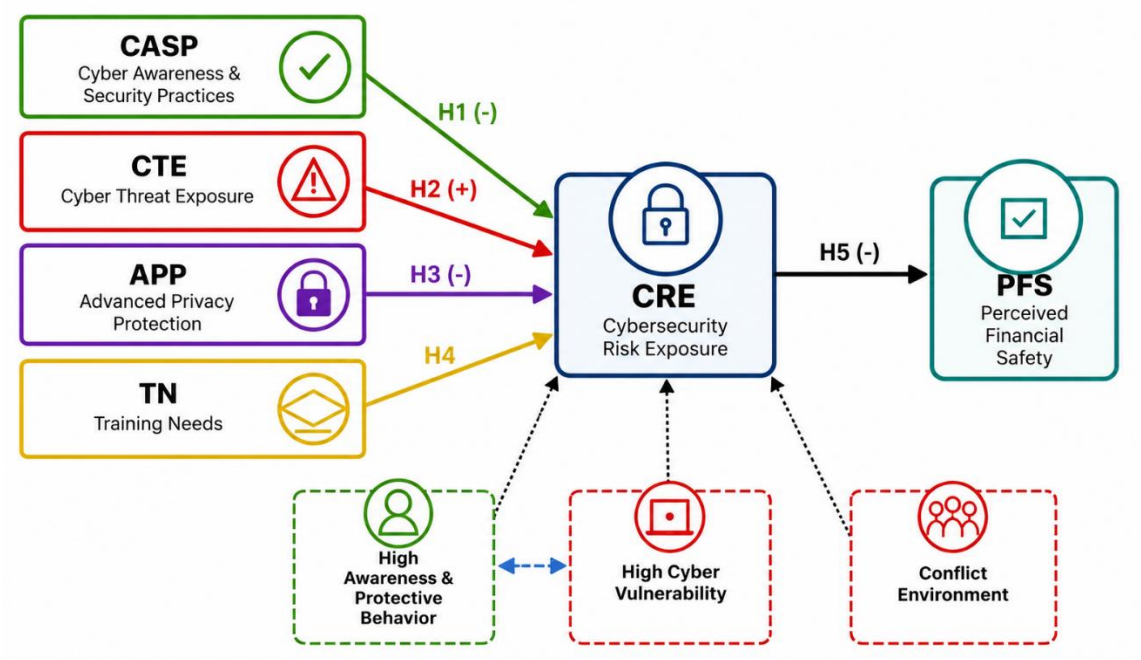

Figure 1. Conflict-sensitive socio-technical framework for cybersecurity vulnerability and financial safety

3. METHODOLOGY

3.1 Research design and study context

This study adopts a quantitative, cross-sectional research design to examine cybersecurity risks associated with digital payment systems during armed conflict. A structured survey approach was used to collect primary data from civilians affected by the Sudan conflict. The quantitative design enables statistical testing of relationships between variables and supports hypothesis-driven analysis.

The study is conducted in the context of the ongoing armed conflict in Sudan (2023-2026), where traditional banking infrastructure has been significantly disrupted. In this environment, civilians increasingly rely on digital payment systems, including mobile banking, e-wallets, and informal digital financial platforms. This context provides a unique opportunity to investigate cybersecurity risks under extreme and unstable conditions.

3.2 Sampling procedure and data collection

The study included conflict-affected Sudanese civilians aged 18 years or older who had used or attempted to use digital payment services during the conflict. Given the insecurity, displacement, communication disruptions, and absence of a reliable sampling frame, purposive and snowball sampling were used to recruit participants through online platforms, community networks, conflict-affected groups, and participant referrals.

Among the respondents, 69 (39.9%) remained in their original hometowns, 36 (20.8%) were internally displaced, 63 (36.4%) were outside Sudan, and 5 (2.9%) provided other or unclassified responses. Although broad conflict-related residence categories were recorded, the questionnaire did not capture precise locations, specific payment platforms, frequency of use, or duration of digital payment experience.

The sample is not nationally representative. Online purposive and snowball recruitment may have overrepresented digitally connected and highly educated respondents while underrepresenting civilians with limited internet access, low digital literacy, or severe displacement-related constraints. Therefore, the findings should be interpreted as context-specific evidence from digitally reachable, conflict-affected respondents rather than generalized to the entire Sudanese population.

3.3 Measurement instrument, reliability, and validity

The questionnaire was designed based on established literature in cybersecurity, FinTech, and digital payment systems, and was adapted to the conflict context.

3.3.1 Constructs and items

As shown in Table 1, the study uses six constructs to measure cybersecurity vulnerability and financial safety. CASP capture respondents' knowledge and routine protective behaviors, while CTE measures experiences with threats such as phishing, fraud, malware, misinformation, and identity-related risks. APP assesses stronger security behaviors, including privacy management, secure authentication, data protection, and device security. TN reflect the need for cybersecurity education and digital literacy support. CRE represents perceived vulnerability to cyber threats, financial risks, data exposure, and identity compromise, while PFS measures trust and confidence in digital financial environments. Together, these constructs operationalize the socio-technical framework and support the empirical analysis of cybersecurity risk and financial safety during armed conflict.

CTE and CRE represent related but distinct concepts. CTE measures respondents' exposure to external cyber threats, including suspicious communications, fraud attempts, fake applications, and the broader threat environment. In contrast, CRE captures respondents' perceived vulnerability and anticipated personal, financial, or identity-related consequences when using digital payment systems. Thus, CTE represents an external threat antecedent, whereas CRE

represents an internal risk appraisal and perceived outcome.

TN measures respondents' perceived need for and value of cybersecurity education rather than completed training or existing preparedness. Higher scores indicate stronger recognition of training requirements and may reflect either greater awareness of vulnerability or a proactive orientation toward cybersecurity support. Therefore, H4 was specified as non-directional.

The complete wording of all measurement items is provided in Appendix.

Table 1. Constructs and item codes

Construct	Code	Items
Cybersecurity Awareness and Security Practices	CASP	A1-A5
Cyber Threat Exposure	CTE	B1-B4
Advanced Privacy Protection	APP	C1-C5
Training Need	TN	D1-D4
Cybersecurity Risk Exposure	CRE	E1-E4
Perceived Financial Safety	PFS	F1-F5

3.3.2 Reliability and validity

Reliability was assessed using Cronbach's Alpha (α). All constructs demonstrated excellent internal consistency, with values ranging from 0.887 to 0.926. The overall reliability was $\alpha = 0.923$, exceeding the recommended threshold of $\alpha \geq 0.70$.

Content validity was ensured through a review of the relevant literature and expert evaluation. Construct validity was achieved by aligning the measurement items with the theoretical frameworks, including TAM, PMT, and cybersecurity models. Convergent validity was assessed using Composite Reliability (CR) and Average Variance Extracted (AVE). All constructs exceeded the recommended thresholds of CR > 0.70 and AVE > 0.50, indicating satisfactory convergent validity.

3.4 Ethical considerations

Ethical considerations were carefully observed throughout the study. Participation was voluntary, and informed consent was obtained electronically before respondents completed the questionnaire. The survey was anonymous, and no names, identity numbers, phone numbers, precise locations, financial account details, or other personally identifiable information were collected. All data were used only for academic research purposes and reported in aggregate form.

Because the study involved conflict-affected civilians, additional precautions were taken to reduce potential risk. Respondents were informed that they could decline participation, skip any question, or withdraw before submitting the questionnaire without consequences. The questionnaire avoided politically sensitive questions, military information, precise displacement routes, and details that could identify individuals, families, organizations, or communities. The questions focused only on perceptions and experiences related to digital payment use, cybersecurity awareness, CTE, and PFS.

Formal ethics committee approval was not obtained because the study was an anonymous, non-interventional, low-risk survey that did not collect personally identifiable information and did not involve clinical procedures, biological samples, financial account records, or experimental manipulation. Nevertheless, the study followed standard ethical safeguards for voluntary participation, informed consent, anonymity, confidentiality, and the protection of vulnerable conflict-affected respondents.

Accordingly, no ethics committee approval number or approval date was issued.

4. RESULTS

4.1 Sample characteristics

4.1.1 Demographic profile of respondents

This study analyzed data from 173 valid respondents affected by the Sudan conflict. The demographic characteristics of the sample were summarized in terms of gender, age, and internet access, as these variables are important for understanding digital payment usage and cybersecurity exposure.

4.1.2 Gender distribution

The gender distribution of respondents is presented in Table 2. The results indicate that male participants constituted the majority of the sample (59.0%), while female respondents accounted for 41.0%.

This distribution suggests that males were more represented among digital financial service users in the conflict-affected sample, which may reflect existing gender disparities in access to technology and financial systems.

Table 2. Gender distribution

Gender	Frequency	Percentage (%)
Male	102	59.0%
Female	71	41.0%
Total	173	100%

4.1.3 Age distribution

The age distribution of respondents is summarized in Table 3. The majority of participants were in the 26-35 age group (38.7%), followed by those aged 18-25 years (27.7%), while older age groups represented a smaller proportion of the sample.

This indicates that younger and middle-aged individuals were the primary users of digital payment systems in the study sample. These groups are generally more familiar with digital technologies, which may influence both their level of usage and their cybersecurity awareness.

Table 3. Age distribution

Age Group	Frequency	Percentage (%)
18–25 years	48	27.7%
26–35 years	67	38.7%
36–45 years	36	20.8%
46 years and above	22	12.7%
Total	173	100%

4.1.4 Internet access

Table 4 shows that internet access among respondents was largely unstable. More than half of the respondents reported unstable or intermittent access (51.4%), while only 31.2% had stable connectivity and 17.3% had very limited or no access. These results highlight serious infrastructure challenges during the conflict and support the view that internet instability affects both CRE and digital payment reliability.

Table 4. Internet access

Internet Access Type	Frequency	Percentage (%)
Stable access	54	31.2%
Unstable / intermittent access	89	51.4%
Very limited / no access	30	17.3%
Total	173	100%

4.1.5 Discussion of demographics

The demographic profile shows that digital payment usage during the Sudan conflict was mainly concentrated among younger and middle-aged respondents, who are generally more digitally active. It also suggests that gender differences may affect access to digital financial services and exposure to cybersecurity risks. In addition, unstable internet access highlights infrastructure instability as an important factor influencing digital payment reliability and security. Overall, age, gender, and internet access provide important context for understanding CRE and financial vulnerability under conflict conditions.

4.2 Reliability analysis

To evaluate the internal consistency and reliability of the measurement instrument, Cronbach's Alpha analysis was conducted for all constructs included in the revised conceptual framework. The analysis assessed the extent to which items within each construct consistently measured the same underlying concept.

Table 5 shows that the revised measurement model demonstrated strong reliability. All constructs exceeded the recommended Cronbach's Alpha threshold of 0.70, with values ranging from 0.887 to 0.926. APP recorded the highest reliability ($\alpha = 0.926$), followed by CRE ($\alpha = 0.918$), CASP ($\alpha = 0.914$), and PFS ($\alpha = 0.903$). Although CTE had the lowest value ($\alpha = 0.887$), it still demonstrated good internal consistency. Overall, the full instrument achieved excellent reliability ($\alpha = 0.923$), confirming its suitability for validity assessment and hypothesis testing.

Table 5. Cronbach's Alpha reliability test per construct

Construct	Number of Items	Cronbach's Alpha (α)	Reliability Interpretation
CASP	5	0.914	Excellent
CTE	4	0.887	Good
APP	5	0.926	Excellent
TN	4	0.901	Excellent
CRE	4	0.918	Excellent
PFS	5	0.903	Excellent
Overall Instrument	27	0.923	Excellent

4.3 Convergent validity results (Average Variance Extracted and Composite Reliability)

Table 6 confirms acceptable convergent validity for the measurement model. All constructs recorded CR values above 0.70 and AVE values above 0.50, meeting the recommended thresholds. APP showed the highest AVE (0.670), followed by CRE (0.661) and PFS (0.628), indicating that their indicators adequately represented the intended constructs. Overall, the results support the reliability and validity of the model for hypothesis testing and regression analysis.

Table 6. Convergent validity results (Average Variance Extracted (AVE) and Composite Reliability (CR))

Construct	Number of Items	Cronbach's Alpha	CR	AVE
CASP	5	0.914	0.886	0.609
CTE	4	0.887	0.872	0.631
APP	5	0.926	0.901	0.670
TN	4	0.901	0.859	0.603
CRE	4	0.918	0.889	0.661
PFS	5	0.903	0.871	0.628

4.4 Measurement model assessment

Table 7 presents the adequacy tests and exploratory factor analysis results for the measurement model. The KMO value of 0.910 indicates excellent sampling adequacy, while Bartlett's test of sphericity was statistically significant ($\chi^2 = 3411.052$, $df = 351$, $p < 0.001$), confirming that the correlation matrix was suitable for factor analysis. The exploratory factor analysis retained six factors corresponding to the six theoretical constructs and explained 76.84% of the total variance. These results provide additional support for the factorial validity of the measurement model.

Table 7. Kaiser-Meyer-Olkin (KMO), Bartlett's test, EFA, and explained variance

Measurement Test	Result	Interpretation
KMO measure	0.910	Excellent sampling adequacy
Bartlett's test of sphericity	$\chi^2 = 3411.052$	Correlation matrix suitable for factor analysis
Degrees of freedom	351	Adequate for 27 measurement items
Significance level	$p < 0.001$	Statistically significant
Extraction method	Principal component / exploratory factor analysis	Used to assess the factor structure
Rotation method	Varimax rotation	Used to clarify factor interpretation
Number of retained factors	6	Matches the six theoretical constructs
Total variance explained	76.84%	Strong explanatory power of the measurement model

Table 8 reports the rotated factor loadings for the 27 measurement items. The results show that all items loaded most strongly on their intended constructs, supporting the six-factor structure of the measurement model. The factor loadings ranged from 0.822 to 0.856 for CASP, 0.800 to 0.867 for CTE, 0.834 to 0.868 for APP, 0.845 to 0.865 for TN, 0.678 to 0.715 for CRE, and 0.718 to 0.794 for PFS. These results indicate acceptable item-level convergent validity and support the distinctiveness of the six constructs.

Tables 9 and 10 present the discriminant validity results using the Fornell-Larcker criterion and HTMT ratios. The Fornell-Larcker results show that the square root of AVE for each construct was greater than its correlations with other constructs, supporting discriminant validity. In addition, all HTMT values were below the conservative threshold of 0.85, with the highest value observed between CRE and PFS

(HTMT = 0.739). These results indicate that the six constructs are empirically distinct and that the measurement model demonstrates acceptable discriminant validity.

Table 8. Rotated factor loadings

Item	CASP	CTE	APP	TN	CRE	PFS
A1	0.856	-0.061	0.055	0.123	-0.093	0.119
A2	0.846	0.021	0.037	0.011	-0.134	0.202
A3	0.843	0.030	0.168	-0.003	-0.052	0.134
A4	0.822	0.031	0.007	0.057	-0.149	0.081
A5	0.845	0.027	-0.040	0.109	-0.149	0.029
B1	-0.047	0.800	-0.050	-0.019	0.278	-0.147
B2	0.053	0.857	-0.031	0.027	0.069	-0.082
B3	0.030	0.867	-0.025	-0.045	0.090	-0.226
B4	0.014	0.858	0.041	0.009	0.175	-0.079
C1	0.064	-0.056	0.834	0.137	-0.135	0.140
C2	0.036	0.056	0.841	0.171	-0.167	0.145
C3	0.058	-0.027	0.844	0.033	-0.114	0.243
C4	0.016	-0.021	0.855	-0.013	-0.158	0.139
C5	0.044	-0.029	0.868	0.088	-0.140	0.054
D1	0.060	-0.047	0.074	0.863	-0.086	0.120
D2	0.029	-0.023	0.058	0.845	-0.184	0.101
D3	0.117	0.045	0.141	0.861	-0.034	0.130
D4	0.050	-0.013	0.080	0.865	-0.148	0.077
E1	-0.201	0.214	-0.272	-0.255	0.691	-0.323
E2	-0.196	0.285	-0.333	-0.155	0.694	-0.241
E3	-0.214	0.230	-0.281	-0.216	0.715	-0.280
E4	-0.267	0.289	-0.265	-0.147	0.678	-0.330
F1	0.146	-0.150	0.108	0.093	-0.152	0.794
F2	0.109	-0.177	0.268	0.127	-0.188	0.760
F3	0.160	-0.064	0.132	0.105	-0.321	0.718
F4	0.123	-0.125	0.178	0.140	-0.167	0.786
F5	0.184	-0.253	0.248	0.165	-0.187	0.738

Table 9. Fornell-Larcker criterion

Construct	CASP	CTE	APP	TN	CRE	PFS
CASP	0.780					
CTE	-0.022	0.794				
APP	0.151	-0.090	0.819			
TN	0.176	-0.061	0.232	0.777		
CRE	-0.414	0.464	-0.523	-0.400	0.813	
PFS	0.338	-0.361	0.426	0.322	-0.672	0.792

Table 10. HTMT ratios

Construct	CASP	CTE	APP	TN	CRE	PFS
CASP						
CTE	0.061					
APP	0.162	0.108				
TN	0.195	0.083	0.255			
CRE	0.451	0.510	0.567	0.440		
PFS	0.372	0.401	0.467	0.357	0.739	

4.5 Common method bias assessment

Because all variables were collected from the same questionnaire at a single point in time, common method bias was assessed using Harman's single-factor test. The unrotated factor solution showed that the first factor explained 34.34% of the total variance, which is below the commonly used 50% threshold. This suggests that common method bias was unlikely to dominate the results. In addition, procedural measures were used to reduce response bias, including voluntary participation, anonymous responses, informed consent, and the non-collection of personally identifiable information. Nevertheless, because the study relied on self-reported, same-source, cross-sectional survey data, common method variance cannot be completely ruled out and is acknowledged as a limitation.

4.6 Descriptive statistics per construct

To provide an overview of respondents' perceptions of the major constructs included in the revised conceptual framework, descriptive statistical analysis was conducted. The analysis included calculating mean values and standard deviations for all study constructs. Mean values were used to indicate the overall level of agreement, while standard deviations measured variability in participants' responses.

Table 11 shows that respondents reported high levels of APP (M = 4.05), CRE (M = 4.02), CASP (M = 3.88), and CTE (M = 3.84). This indicates that civilians adopted protective behaviors while still experiencing substantial cybersecurity risks during the Sudan conflict. TN showed a moderate-to-high mean score (M = 3.49), reflecting continued demand for cybersecurity education. In contrast, PFS recorded the lowest mean score (M = 2.74), suggesting weak confidence in digital financial security. Overall, the findings support the behavior–vulnerability gap, where strong cybersecurity awareness and protective practices coexist with high cyber risk exposure and reduced financial safety.

Table 11. Descriptive statistics per construct

Construct	Mean	Standard Deviation	Interpretation
CASP	3.88	1.21	High
CTE	3.84	1.28	High
APP	4.05	1.18	High
TN	3.49	1.35	Moderate-High
CRE	4.02	1.19	High
PFS	2.74	1.21	Low
Overall Mean	3.67	1.24	Moderate-High

4.7 Descriptive and response pattern analysis

To provide supportive descriptive evidence, one-sample t-tests and Chi-square tests were conducted. These tests were not used to test the hypothesized relationships among constructs. Instead, they were used to examine whether construct-level responses differed from neutral benchmark values and whether response distributions showed systematic patterns rather than random variation.

4.7.1 One-sample t-test results

To determine whether respondents' perceptions significantly differed from a neutral benchmark, a one-sample t-test was conducted for all constructs included in the revised conceptual framework. Following common practice in Likert-scale studies, the midpoint value of 3 was used as the test value, representing a moderate or neutral perception level. Because construct scores were aggregated from multiple items, the benchmark values were adjusted according to the number of items in each construct.

The test examined whether respondents' observed mean values significantly differed from the expected moderate levels.

Table 12 shows that all constructs differed significantly from their neutral benchmark values. CASP, APP, CTE, CRE, and TN all showed significant positive differences, indicating strong awareness, protective behavior, threat exposure, perceived vulnerability, and a continued need for cybersecurity education. In contrast, PFS showed a significant

negative difference, reflecting low confidence in digital financial security during the Sudan conflict. Overall, the t-test results support the proposed framework and confirm the behavior-vulnerability gap, where strong protective practices coexist with high cyber risk exposure and reduced financial confidence.

Table 12. One-sample t-test results

Construct	Mean	Test Value	T-Value	p-Value
CASP	19.40	15	4.217	0.000
CTE	15.36	12	5.681	0.000
APP	20.25	15	6.024	0.000
TN	13.96	12	2.853	0.005
CRE	16.08	12	8.534	0.000
PFS	13.70	15	−3.741	0.000

4.7.2 Chi-square (χ^2) results

To further examine response distributions across the questionnaire constructs, a Chi-square (χ^2) goodness-of-fit test was conducted. The purpose of this analysis was to determine whether respondents' answers differed significantly from an equal or random response distribution. Significant Chi-square values indicate that participants demonstrated meaningful response patterns rather than random selection behavior.

Table 13 shows that all Chi-square results were statistically significant ($p < 0.001$), indicating that respondents' answers reflected meaningful and systematic perceptions rather than random patterns. APP recorded the highest Chi-square value, showing strong agreement regarding the use of privacy and device protection practices. CASP also showed strong agreement, indicating active awareness and safe digital behavior among civilians. CRE and CTE confirmed consistent experiences of vulnerability, phishing, fraud, misinformation, and cyber-enabled threats. Although TN and PFS recorded lower values, both remained statistically significant. Overall, these results provide descriptive support for the observed response patterns but do not directly test the hypothesized relationships among constructs.

Table 13. Chi-square (χ^2) results per construct

Construct	χ^2	Degrees of Freedom (df)	p-Value
CASP	389.524	4	0.000
CTE	275.762	3	0.000
APP	451.143	4	0.000
TN	146.905	3	0.000
CRE	337.810	3	0.000
PFS	121.571	4	0.000

4.8 Regression-based hypothesis testing

To further examine the predictive relationships proposed in the conceptual framework, two regression models were developed. Consistent with the revised theoretical structure, CRE was treated as an intermediate dependent construct influenced by cybersecurity awareness, threat exposure, privacy protection practices, and perceived cybersecurity TN. Subsequently, PFS was modeled as an outcome variable influenced by CRE.

4.8.1 Predictors of Cybersecurity Risk Exposure

The first regression model examined the effects of CASP, CTE, APP, and TN on CRE. The regression coefficients for Model 1 are presented in Table 14, while the corresponding model fit statistics are reported in Table 15.

The results show that the model was statistically significant and explained 61.0% of the variance in CRE, indicating strong explanatory power. CTE was the strongest positive predictor, suggesting that higher self-reported exposure to phishing, fraud, malware, and other cyber-enabled threats was associated with greater perceived cybersecurity vulnerability.

CASP and APP were significantly and negatively associated with CRE, indicating that stronger cybersecurity awareness and privacy protection practices were linked to lower perceived cybersecurity risk exposure. TN was also significantly and negatively associated with CRE ($\beta = -0.244$, $p = 0.001$). This inverse relationship may indicate that respondents who recognized a greater need for training were also more risk-aware or more receptive to protective support. However, because TN measures perceived training need rather than completed training, this finding should not be interpreted as evidence that training needs causally reduce vulnerability.

Table 14. Multiple regression results (model 1)

Independent Variable	β (Beta)	Std. Error	T-Value	p-Value
CASP	−0.312	0.071	−4.394	0.000
CTE	0.421	0.067	6.284	0.000
APP	−0.381	0.065	−5.861	0.000
TN	−0.244	0.074	−3.297	0.001

Table 15. Model fit statistics for model 1

Statistic	Value
R	0.781
R^2	0.610
Adjusted R^2	0.597
F-value	41.822
Sig. (F-test)	0.000

4.8.2 Effect of Cybersecurity Risk Exposure on Perceived Financial Safety

The second regression model examined the effect of CRE on PFS.

The second regression model examined the effect of CRE on PFS, as shown in Table 16. The model was statistically significant ($F = 73.561$, $p < 0.001$) and explained 44.6% of the variance in PFS ($R^2 = 0.446$), as reported in Table 17.

Table 16. Simple regression results (model 2)

Independent Variable	β (Beta)	Std. Error	T-Value	p-Value
CRE	−0.446	0.052	−8.577	0.000

Table 17. Model fit statistics for model 2

Statistic	Value
R	0.668
R^2	0.446
Adjusted R^2	0.442
F-value	73.561
Sig. (F-test)	0.000

CRE was significantly and negatively associated with PFS ($\beta = -0.446$, $p < 0.001$), indicating that increased vulnerability to cyber threats substantially reduced respondents' confidence in digital financial environments.

This finding suggests that perceived exposure to cyber risks

is associated with lower trust, weaker security perceptions, and reduced financial confidence under conflict conditions.

The regression analyses were used to evaluate the proposed hypotheses, as summarized in Table 18. The findings indicate that all hypothesized relationships were statistically supported. CASP and APP were negatively associated with CRE, while CTE was positively associated with CRE. TN also showed a significant association with CRE, and CRE was negatively associated with PFS.

Table 18. Hypothesis-testing summary

Hypothesis	Relationship	β	p-Value	Decision
H1	CASP → CRE	−0.312	<0.001	Supported
H2	CTE → CRE	0.421	<0.001	Supported
H3	APP → CRE	−0.381	<0.001	Supported
H4	TN → CRE	−0.244	0.001	Supported as significant association
H5	CRE → PFS	−0.446	<0.001	Supported

5. DISCUSSION

The findings indicate that civilians affected by the Sudan conflict demonstrated relatively high levels of CASP and APP, reflecting adaptive protective behaviors such as phishing awareness, secure authentication, and privacy management. Consistent with previous studies, cybersecurity awareness supports protective actions [27, 36]. However, despite these stronger practices, respondents simultaneously experienced high CTE and CRE, supporting the existence of a behavior–vulnerability gap, in which protective behaviors coexist with considerable cyber risks [1, 36].

From a theoretical perspective, these findings partially support PMT [30, 31]. While stronger awareness and coping behaviors contributed to reducing vulnerability, conflict-related conditions appear to weaken the effectiveness of individual protective actions. This suggests that, in unstable environments, environmental threats may outweigh personal coping capabilities. Similarly, the findings extend TAM assumptions [27-29], indicating that digital payment usage during armed conflict may be driven more by necessity and survival needs than by conventional factors such as trust or PU.

The results also support STS [36], emphasizing that cybersecurity experiences emerge through interactions among user behavior, cyber threats, and environmental instability rather than through technological factors alone. The findings suggest that cybersecurity vulnerability during armed conflict emerges not only from technological threats but also from the interaction between environmental instability and constrained adaptive capacity. Even when individuals demonstrate protective behaviors, unstable conflict conditions may reduce the effectiveness of these coping mechanisms.

From a safety and security engineering perspective, the findings suggest that digital payment systems in conflict environments should be treated as critical socio-technical infrastructures rather than ordinary financial applications. CRE is not only a technical security issue but also a civilian safety concern because it affects financial confidence, access to essential resources, and crisis resilience. Therefore, digital payment platforms used in humanitarian and conflict settings require risk-aware design, resilient communication infrastructure, user-centered security controls, and continuous cybersecurity education.

The study's major contribution is its introduction of the behavior-vulnerability gap, demonstrating that stronger protective behaviors alone may not sufficiently reduce cyber risks in conflict environments. Therefore, strengthening civilian digital resilience requires not only individual awareness but also broader institutional, infrastructural, humanitarian, and security-engineering support mechanisms. This interpretation reinforces the need for conflict-sensitive cybersecurity strategies that combine technical safeguards, user education, infrastructure resilience, and civilian-centered protection policies.

6. LIMITATIONS AND FUTURE WORK

This study has several limitations that should be considered when interpreting the findings. First, the study employed a purposive and snowball sampling approach, which may limit the generalizability of the findings beyond the conflict-affected populations included in this research. Second, the study focused exclusively on the Sudan conflict context; therefore, the findings may reflect country-specific social, technological, and institutional conditions. Third, the cross-sectional design captured perceptions at a single point in time and may not reflect changes in cybersecurity experiences across different stages of conflict.

Fourth, the study relies on self-reported perceptions rather than objective cybersecurity records. The survey did not collect verified evidence of actual fraud incidents, financial losses, account compromise, platform security breaches, transaction failures, or digital payment system logs. Therefore, the findings should be interpreted as evidence of perceived CRE and PFS, rather than as direct evidence of actual cybersecurity incidents or technical platform performance. Future research should combine survey data with objective indicators, such as verified fraud reports, transaction failure records, platform incident data, or institutional cybersecurity logs.

Fifth, because all variables were collected from the same respondents using the same questionnaire at a single point in time, the findings may be affected by common method variance. Although Harman's single-factor test suggested that common method bias was not severe, future research should use multiple data sources, temporal separation, objective incident records, or longitudinal designs to reduce this risk.

Future research may extend this work by conducting comparative studies across multiple conflict-affected regions, employing longitudinal approaches to examine changes in cybersecurity experiences over time, and validating the proposed framework using larger samples and advanced analytical techniques, such as Structural Equation Modeling (SEM). Future studies may also examine additional factors influencing digital resilience, including institutional trust, infrastructure resilience, and humanitarian technology interventions.

7. RECOMMENDATIONS

Based on the findings, several recommendations are proposed to enhance cybersecurity resilience and financial

safety among civilians in conflict-affected environments.

(1) Strengthen cybersecurity awareness and education programs. Humanitarian organizations and digital service providers should implement targeted cybersecurity awareness initiatives focusing on phishing detection, secure authentication practices, privacy protection, and safe digital payment behaviors.

(2) Develop conflict-sensitive cybersecurity strategies. Conventional cybersecurity approaches designed for stable environments may not adequately address conflict-related conditions. Policymakers should develop adaptive cybersecurity frameworks that consider infrastructure instability and crisis-related vulnerabilities.

(3) Improve infrastructure resilience. Reliable internet connectivity, communication systems, and digital infrastructure should be prioritized because infrastructure instability can amplify cybersecurity vulnerabilities and reduce financial safety.

(4) Integrate cybersecurity into humanitarian digital programs. Organizations delivering digital cash transfers and humanitarian assistance should incorporate cybersecurity risk assessment and civilian protection mechanisms into program design.

(5) Provide continuous cybersecurity training and support. The finding on Perceived Cybersecurity TN indicates that respondents recognize the importance of continued cybersecurity education. Therefore, humanitarian organizations, digital service providers, and policymakers should strengthen conflict-sensitive cybersecurity training programs focusing on phishing detection, fraud prevention, secure authentication, privacy protection, and safe digital payment practices.

(6) Support civilian-centered digital protection policies. Governments, financial institutions, and humanitarian agencies should adopt policies that emphasize civilian digital safety, privacy protection, and secure access to FinTech.

8. CONCLUSION

This study investigated cybersecurity risks associated with digital payment usage among civilians during the Sudan conflict. It examined the effects of CASP, CTE APP, and TN on CRE and PFS.

Regression analysis showed that APP and CASP were significantly and negatively associated with CRE, whereas CTE was significantly and positively associated with it. TN also demonstrated a significant negative association with CRE; however, this finding should not be interpreted as evidence that perceived TN causally reduce vulnerability.

The study contributes theoretically by integrating TAM, PMT, and STS within a conflict-sensitive framework and introducing the concept of a behavior-vulnerability gap, in which civilians exhibit strong protective behaviors but remain highly vulnerable because of conflict-related environmental instability. The findings emphasize that cybersecurity in conflict settings should be understood as a broader socio-technical issue requiring civilian-centered resilience strategies.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications, 241: 122697. https://doi.org/10.1016/j.eswa.2023.122697

[2] Laxman, V., Ramesh, N., Prakash, S.K.J., Aluvala, R. (2025). Emerging threats in digital payment and financial crime: A bibliometric review. Journal of Digital Economy, 3: 205-222. https://doi.org/10.1016/j.jdec.2025.04.002

[3] Jafri, J.A., Amin, S.I.M., Rahman, A.A., Nor, S.M. (2024). A systematic literature review of the role of trust and security on FinTech adoption in banking. Heliyon, 10(1): e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

[4] Chen, Y.S., Zhao, C.Q., Xu, Y.X., Nie, C.H., Zhang, Y.X. (2025). Deep learning in financial fraud detection: Innovations and challenges, and applications. Data Science and Management, 9(2): 100162. https://doi.org/10.1016/j.dsm.2025.08.002

[5] Kaur, S., Arora, S. (2021). Role of perceived risk in online banking and its impact on behavioral intention: Trust as a moderator. Journal of Asia Business Studies, 15(1): 1-30. https://doi.org/10.1108/JABS-08-2019-0252

[6] Juntunen, E.A., Kalla, C., Widera, A., Hellingrath, B. (2023). Digitalization potentials and limitations of cash-based assistance. International Journal of Disaster Risk Reduction, 97: 104005. https://doi.org/10.1016/j.ijdrr.2023.104005

[7] Abay, K.A., Abdelfattah, L.A., Abushama, H., Kirui, O.K., Nigus, H.Y., Siddig, K. (2025). Can digital cash transfers serve those in active conflict? Evidence from a randomized intervention in Sudan. FPRI Discussion Paper 2374. Washington, DC, International Food Policy Research Institute. https://hdl.handle.net/10568/177655.

[8] Ozili, P.K. (2021). Financial inclusion research around the world: A review. Forum for Social Economics, 50: 457-479. https://doi.org/10.1080/07360932.2020.1715238

[9] Yuspin, W., Putri, A.O., Fauzie, A., Pitaksantayothin, J. (2024). Digital banking security: Internet phishing attacks, analysis and prevention of fraudulent activities. International Journal of Safety and Security Engineering, 14(6): 1699-1706. https://doi.org/10.18280/ijsse.140605

[10] Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y.J., Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review. Decision Support Systems, 50(3): 559-569. https://doi.org/10.1016/j.dss.2010.08.006

[11] Dal Pozzolo, A., Caelen, O., Johnson, R.A., Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. In 2015 IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, pp. 159-166. https://doi.org/10.1109/SSCI.2015.33

[12] Fiore, U., De Santis, A., Perla, F., Zanetti, P., Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card

fraud detection. Information Sciences, 479: 448-455. https://doi.org/10.1016/j.ins.2017.12.030
[13] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., Beling, P. (2018). Deep learning detecting fraud in credit card transactions. In 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, pp. 129-134. https://doi.org/10.1109/SIEDS.2018.8374722
[14] AbouGrad, H., Sankuru, L. (2025). Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations. Mathematics, 13: 2110. https://doi.org/10.3390/math13132110
[15] Burton, J. (2020). Doing no harm in the digital age: What the digitalization of cash means for humanitarian action. International Review of the Red Cross, 102(913): 43-73. https://doi.org/10.1017/S1816383120000491
[16] Callen, M., Fajardo-Steinhäuser, M., Findley, M.G., Ghani, T. (2025). Can digital aid deliver during humanitarian crises? Management Science, 71(11): 9730-9748. https://doi.org/10.1287/mnsc.2024.06469
[17] World Bank. (2024). Financial inclusion. https://www.worldbank.org/ext/en/topic/financial-sector/financial-inclusion.
[18] United Nations High Commissioner for Refugees (UNHCR). (2024). Cash Assistance in 2023: Main Outcomes from Post-Distribution Monitoring. Geneva, UNHCR, pp. 1-9. https://www.unhcr.org/sites/default/files/2024-05/cash-assistance-in-2023-main-outcomes-from-post-distribution-monitoring.pdf.
[19] McLean, C., Egemi, O. (2025). Political Economy of Cash and Markets in Sudan. Nairobi, Rift Valley Institute, pp. 1-26. https://riftvalley.net/wp-content/uploads/2026/02/RVI-20260227-PEA-cash-markets-Sudan_final.pdf.
[20] Ozili, P. (2026). Role of digital financial services in war and armed conflict. Conflict Resolution Quarterly. https://doi.org/10.1002/crq.70028
[21] FSD Africa. (2022). Supporting digital payments in cash programming in Sudan. Nairobi, Kenya, Financial Sector Deepening Africa. https://fsdafrica.org/publication/supporting-digital-payments-in-cash-programming-in-sudan/.
[22] World Bank. (2025). Sudan Economic Update, May 2025: The Economic and Social Consequences of the Conflict-Charting a Path to Recovery. Washington, DC, USA, World Bank. https://doi.org/10.1596/43314
[23] World Bank. (2024). Macro Poverty Outlook for Sudan. Washington, DC, USA, World Bank. http://documents.worldbank.org/curated/en/099346410152441879.
[24] Aljaradat, A., Shukla, S.K. (2025). Trust and cybersecurity in digital payment adoption: Socioeconomic insights from India. Journal of Business and Socio-economic Development, 5(4): 372-386. https://doi.org/10.1108/JBSED-04-2025-0119
[25] Oliveira, T., Thomas, M., Baptista, G., Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Computers in Human Behavior, 61: 404-414. https://doi.org/10.1016/j.chb.2016.03.030
[26] Amnas, M.B., Selvam, M., Raja, M., Santhoshkumar, S., Parayitam, S. (2023). Understanding the determinants of FinTech adoption: Integrating UTAUT2 with trust theoretic model. Journal of Risk and Financial Management, 16(12): 505. https://doi.org/10.3390/jrfm16120505
[27] Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3): 319-340. https://doi.org/10.2307/249008
[28] Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3): 425-478. https://doi.org/10.2307/30036540
[29] Venkatesh, V., Davis, F.D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2): 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926
[30] Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91: 93-114. https://doi.org/10.1080/00223980.1975.9915803
[31] Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In Social Psychophysiology: A Sourcebook, pp.153-176.
[32] Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2): 254-268. https://doi.org/10.1287/isre.1090.0260
[33] Malaika, M., Soderberg, G., Zhabska, K. (2025). Payment Resilience in Fragile and Conflict-Affected States: Lessons for Central Bank Digital Currency (CBDC). Financial Technologies Notes, 2025/009. https://www.imf.org/-/media/files/publications/ftn063/2025/english/ftnea2025009a.pdf.
[34] Bakar, M.H., Yahaya, S.N., Ramli, N.N. (2025). Cyber security awareness among digital banking users in Malaysia. International Journal of Research and Innovation in Social Science, 9(10): 433-445. https://doi.org/10.47772/IJRISS.2025.910000038
[35] Ifinedo, K. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory. Computers & Security, 31(1): 83-95. https://doi.org/10.1016/j.cose.2011.10.007
[36] Malatji, M., von Solms, S., Marnewick, A. (2019). Socio-technical systems cybersecurity framework. Information & Computer Security, 27(2): 233-272. https://doi.org/10.1108/ICS-03-2018-0031
[37] Omogbeme, A., Atoyebi, I., Soyele, A., Ogunwobi, E. (2024). Enhancing fraud detection and prevention in FinTech: Big data and machine learning approaches. World Journal of Advanced Research and Reviews, 24(2): 2301-2319. https://doi.org/10.30574/wjarr.2024.24.2.3617

APPENDIX

Table A1. Measurement items

Cybersecurity Awareness and Security Practices (CASP)	
Item Code	Measurement item
A1	I can recognize suspicious links, messages, or calls that may attempt to steal my digital payment information.
A2	I verify the identity of unknown senders before responding to messages related to money transfers or banking services.
A3	I avoid sharing passwords, PIN codes, verification codes, or banking information with others.
A4	I use strong passwords, screen locks, or secure login methods to protect my digital payment accounts.
A5	I regularly follow safe practices when using mobile banking, e-wallets, or digital payment applications.
Cyber Threat Exposure (CTE)	
Item Code	Measurement item
B1	I have received suspicious messages, links, or calls related to digital payments or financial assistance during the conflict.
B2	I have been exposed to fraud attempts involving mobile banking, e-wallets, money transfers, or digital financial services.
B3	I have encountered fake pages, fake applications, or misleading information related to financial transactions or aid payments.
B4	I believe that civilians using digital payments during the conflict are highly exposed to cyber threats.
Advanced Privacy Protection (APP)	
Item Code	Measurement item
C1	I use privacy settings to limit access to my personal and financial information on digital platforms.
C2	I avoid saving sensitive payment information, passwords, or verification codes in unsafe places on my phone.
C3	I use secure authentication methods, such as two-factor authentication, when available.
C4	I delete suspicious or unnecessary applications that may expose my data, location, or digital identity.
C5	I avoid sharing live location, personal documents, or financial screenshots through unsafe digital channels.
Perceived Cybersecurity Training Need (TN)	
Item Code	Measurement item
D1	Civilians using digital payments during the conflict need more training on how to detect phishing and fraud.
D2	I need more practical guidance on how to protect my digital payment accounts and personal data.
D3	Cybersecurity awareness programs would help civilians use digital financial services more safely during conflict.
D4	Training on safe digital payment practices is important for reducing cyber risks during the Sudan conflict.
Cybersecurity Risk Exposure (CRE)	
Item Code	Measurement item
E1	I feel vulnerable to cyber fraud or account misuse when using digital payment systems during the conflict.
E2	I worry that my personal or financial information may be exposed when using digital payment services.
E3	Poor internet access, weak infrastructure, or unstable services increase my cybersecurity risk when using digital payments.
E4	I believe that using digital payments during the conflict may expose civilians to financial or identity-related risks.
Perceived Financial Safety (PFS)	
Item Code	Measurement item
F1	I feel safe when using digital payment systems for financial transactions during the conflict.
F2	I trust digital payment platforms to protect my money and transaction information.
F3	I believe digital payment systems allow me to conduct financial transactions securely during the conflict.
F4	I feel confident that my digital payment account is protected from fraud or unauthorized access.
F5	Overall, I believe digital payment systems provide a safe financial option for civilians during the Sudan conflict.

Note: All items were measured using a five-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree. Higher scores indicate stronger agreement with the measured construct. No reverse coding was applied.