Information Systems Frontiers
https://doi.org/10.1007/s10796-022-10280-7

Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective

Ben Krishna[1] · **Satish Krishnan**[1] · **M. P. Sebastian**[1]

Accepted: 13 April 2022

Abstract
Cyberattacks can be considered one of the fundamental challenges that paralyze the progress of digital payment usage (DPU) progress among citizens, as consumers shun away from using digital banking services due to increased concern over information security. National Cybersecurity Commitment (NCSC) has emerged as a preventive cybersecurity mechanism for countries to tackle such cybersecurity threats. Previous studies have shown that a country's NCSC positively impacts the business and economy of the country. This study examines the effect of NCSC on digital payment usage (DPU) across nations by grounding our discussion on the institutional trust theory. As trusting belief in security measures is a culturally embedded characteristic, we also examine the moderating role of national culture through Hofstede's cultural dimensions. We use multilevel models to analyze publicly available archives of repeated cross-sectional data covering 76 countries to test the proposed relationships. Our findings indicate that NCSC has a positive influence on DPU. Further, our results highlight that the relationship between NCSC and DPU in a country is contingent on cultural dimensions. Overall, the evidence suggests that a competent cybersecurity environment compatible with cultural values can influence the speedy diffusion of digital payments in a country. Implications of our findings for research and practice are also discussed.

Keywords Cybersecurity commitment · Digital payment · Preventive security · National culture · Institutional trust

1 Introduction

State-led and private-led cyber-attacks like denial of e-services, data integrity breaches, financial frauds, and data confidentiality breaches threaten national infrastructure and systems, as well as private companies, households, and citizens (Lee et al., 2018). Financial institutions are considered one of the most vulnerable institutions in a country as they are prone to frequent cyberattacks (Gurung et al., 2008; Huang et al., 2011). Consumers of digital financial services shun away from using digital banking services due to increased concern over information security (Kimani et al., 2019). Thus, cyberattacks can be considered one of the fundamental challenges that paralyze the progress of digital payment usage (DPU) progress among citizens (Moon & Kim, 2017; Mukhopadhyay et al., 2019; Traynor et al., 2017). Consumers are increasingly aware of the various security threats they are likely to face in the digital space, and many of them shun away from electronic transactions. Potential digital payment users often lack information on the process (e.g., what is happening to data and money during transactions?) and the outcome (e.g., whether the data or money is getting shared with other parties?). Reports from Cisco (2017) and European Commission Brussels (2016) suggest that 27% of internet users have shown an unwillingness to conduct electronic transactions because of concerns regarding online payment security. Currently, users rely on self-defence cybersecurity systems (e.g. anti-virus software, cyber hygiene) to counter malicious attacks. However, sources of anonymous cyberattacks are difficult to trace and take longer to mitigate because of the sophistication of offender and enabler networks. Information systems security research stresses

✉ Satish Krishnan
satishk@iimk.ac.in

Ben Krishna
benkrishna12fpm@iimk.ac.in

M. P. Sebastian
sebasmp@iimk.ac.in

[1] Information Systems Area, Indian Institute of Management Kozhikode, Kozhikode, Kerala, India

Published online: 07 May 2022

the necessity of preventive security measures and platforms to overcome the above limitations (Lee et al., 2020). For instance, the Bright Internet initiative (www.brightinternet.org) stresses the necessity of preventive measures. Lee et al. (2018) defined the Bright Internet as "the Internet that can pre-emptively reduce origins of cybersecurity threats by having the capability of identifying malicious origins and deliverers on a global scale while maintaining the freedom of anonymous expression and a legitimate level of privacy protection for innocent netizens." (p. 64). To achieve the goals of the Bright Internet initiative, several behaviour studies should be conducted at the individual and country-level to understand netizens' perceptions about preventive cybersecurity measures (Lee et al., 2018). In this regard, our study is positioned as one of the prior studies investigating the role of preventive security mechanisms in influencing the trust of netizens in using digital services and hence, contributes to the preventive security paradigm research.

Accordingly, in the current study, we use national cybersecurity commitment as a proxy for preventive security measures implemented by various public institutions in a country. The need for national cybersecurity commitment stems from the fact that every nation needs to protect critical digital infrastructure and systems from boosting trust and confidence among citizens and hence pave the way for economic development (Shukla, 2016; Milian et al., 2019). National cybersecurity commitment stresses the improvement of five cybersecurity pillars- Legal, Technical, Organizational, Capacity building, and Cooperation- to reduce cyberattacks on firms and the public (ITU Arner et al., 2015; Cyber, 2018). In theory and practice, national cybersecurity commitment can bring many positive changes in society, and it helps establish citizens' trust in various initiatives within the country (ITU Cyber, 2018). Krishna & Sebastian (2021) posited that improving cybersecurity measures in a country would drive ICT usage in firms and improve macroeconomic conditions. We believe that seemingly competent preventive cybersecurity measures (here, national cybersecurity commitment) would help overcome individuals' information security concerns in using digital payment services. Accordingly, this study conceptualizes national cybersecurity commitment contingent on digital payment usage. We establish this relationship using the institutional trust theory (Zucker, 1986), which characterizes public institutions as trustworthy and citizens as truster. This relationship is based on the degree of belief the citizens place on institutional structures such as law, regulations, etc. Various studies (e.g., Gai et al., 2016; Kim & Hong, 2016) have explored the question, 'How to guarantee the secrecy and privacy of information during digital transactions?' Researchers currently focus on micro-level variables related to security, privacy, and trust (Patil et al., 2020). Only a few studies have looked into the macro aspect of building trust via an institution-based trust mechanism (through government interventions) to understand digital payment usage (e.g., Zhang et al., 2016). While we acknowledge the significance of those studies, it is noteworthy to investigate the macro-level factors synthesizing the concept of institution-based trust. Hence, we pose the first research question:

RQ1: *What is the role of national cybersecurity commitment in explaining digital payment usage in a country?*

Preventive cybersecurity mechanisms may not always automatically reduce cybersecurity concerns regarding digital payment usage. We argue that the direction and magnitude of the effects of national cybersecurity commitment on digital payment usage depend on a country's social context, especially national culture. Privacy and security concerns are culturally embedded characteristics influencing digital payment usage (Mombeuil, 2020). Prior literature examined the moderating role of national culture on technology diffusion and has found compelling evidence regarding the effect of culture (Leidner & Kayworth, 2006). One of the criticisms of those studies was that national culture as a variable is best suited for analyzing the breadth of diffusion (longitudinal effect) and not well suited for one-time adoption studies (Leidner & Kayworth, 2006). In this regard, most of the studies in the prior literature related to the adoption of digital payment usage were built on cross-sectional samples (e.g., Baptista & Oliveira, 2015). Research related to the cultural impact on digital payment usage is in the fledgling stage because of the lack of longitudinal studies. Moreover, we still lack an in-depth understanding of why citizens' trust in actors and institutions of government varies across countries. A restricted cross-sectional sample may fail to capture the true essence of national culture. Thus, a longitudinal cross-country analysis helps provide a more comprehensive view and more generalizability to the findings (Srivastava & Teo, 2010). Accordingly, we pose the second research question:

RQ2: *What is the role of national culture in influencing the relationship between national cybersecurity commitment and digital payment usage in a country?*

This study synthesizes institutional trust theory and literature on national culture to answer the above research questions. It presents the implications of the relationship between national cybersecurity commitment, cultural dimensions, and digital payment usage. Thus, our objective is to address the following literature gaps: (1) lack of studies on the impact of macro-level variables on the digital payment usage at cross-country level (2) lack of studies examining varying patterns of within-country and between-country processes accounting for temporal effect. To achieve these,

we utilize hierarchical (multilevel) modelling that distinguishes between different levels of analysis. We show significant implications can be derived by separating within-country and between-country processes. To fully evaluate the institutional trust theory and maximize the robustness of results, we use publicly available archives of repeated cross-sectional data covering 76 countries to test the proposed relationship. Accordingly, we contribute to the knowledge base of Fintech literature and behavioural information system security literature in two broad ways. First, our study is instrumental in understanding the positive impact of national cybersecurity commitment on the digital payment usage of citizens across countries. And second, drawing on the institutional trust theory and cultural dimensions, our study proposes a framework for analyzing the relationships between national culture and various technological interventions in a country, which we believe will serve as a reference framework for future research.

Section 2 discusses the digital payment environment and the theoretical background of institutional trust used in this study. We then explore the role of culture in the formation of institutional trust. Section 3 describes the research model and hypothesis. Section 4 explains the data, variables, and the multilevel model. Section 5 presents the results, and Section 6 discusses the findings. Section 7 presents the contributions and implications of the research for theory and practice, and Section 8 concludes the paper.

2 Theoretical and Empirical Background

2.1 Digital Payments Literature

Digital payment usage can be summarized as a process where financial transactions are securely conducted over computers, smartphones, or other mobile devices using the internet or various wireless technologies (Bluetooth, NFC, RFID, among others) (Liu et al., 2015; Slade et al., 2013). Financial transactions involve individual-to-individual transactions, individual-to-banks transactions, payments for goods, services, and bills in both offline and online channels. Previous studies were focused on various theories and related constructs to identify the determinants of digital payment adoption and usage (Kapoor et al., 2014). The major theories[1] include innovation diffusion theory (IDT), technology acceptance model (TAM), theory of planned behaviour (TPB), unified theory of acceptance and use of technology (UTAUT), and extended UTAUT (UTAUT 2) (Patil et al., 2020). The majority of the researchers focussed on the constructs from TAM such as perceived usefulness (Kim et al., 2016), perceived ease of use (Koenig-Lewis et al., 2015); constructs from UTAUT such as performance expectancy (Morosan & DeFranco, 2016), effort expectancy (Slade et al., 2015); constructs from IDT such as relative advantage (Lu et al., 2011), frequently. Besides these technology-based constructs, several other variables like habit (UTAUT 2), hedonic motivation (UTAUT 2), and social influence(UTAUT) have been used to predict an individual's behavioural intention to use digital /mobile payment usage (Patil et al., 2020). The rationale behind the more frequent use of these theories was to examine technology-based factors (usability, compatibility and connivence) and individual-based antecedents(e.g. habit) in the initial adoption process.

However, to explore the continuous DPU, various researchers have looked into the security and privacy concerns of the consumers (Cao et al., 2018). Existing research underscores the importance of perceived information security (PIS) as an essential determinant of digital payment usage (Mohr & Walter, 2019; Mtaho, 2015). Major constructs include perceived information security (PIS) (Dzidzah et al., 2020; Oliveira et al., 2016; Semerikova, 2020), privacy concerns (Morosan & DeFranco, 2016), trust and risk (Phonthanukitithaworn et al., 2015; Qasim & Abu-Shanab, 2016; Slade et al., 2015). Chellappa and Pavlou (2002) define PIS as ''the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage or by inappropriate parties, in a manner consistent with their confident expectations'' (p.359). PIS captures an individual's anticipation rather than an objective measure of information security and is often termed as a trusting belief in information security measures (Hinde, 1998; Mohr & Walter, 2019; Mukundan & Sai, 2014; Stewart & Jürjens, 2018). In addition, from the consumer's perspective, the concern for security, risk, and privacy are highly related to the trust in the products and service providers (Gefen, 2002; Gefen & Straub, 2004; Gefen et al., 2003; Kim et al., 2008). Trust is an important factor when related closely to financial transactions, primarily when the transactions are conducted through a network (Qasim & Abu-Shanab, 2016); consequently, trust can be a robust construct in predicting the usage behaviour of digital payment services. Trust become crucial to mitigate uncertain technology environment, develop long-term relationships and encourage future transactions (Mcknight & Chervany, 2001; Zheng et al., 2017). Thus, to protect themselves, consumers transfer their trust in the formal institutional structures and mechanisms (here, the cybersecurity commitment of the nation) to accept unknown entities (McAllister, 1995). In sum, earlier studies have shown conclusive evidence that security concerns are significant inhibitors in the adoption of digital technologies

[1] We explain various theoretical lenses in this section and next section. We thank Reviewer#1 for this thought.

where money and personal information are involved and trusting belief in secure environments reduce such security concerns (Bélanger & Crossler, 2011; Chang, 2014; Kalinic et al., 2019; Mtaho, 2015; Pal et al., 2021b; Patil et al., 2020; Pavlou et al., 2007).

2.2 Diverse Theoretical Foundations and Application of Institutional Trust in the Unique Digital Payments Environment

Previous literature on trust has discussed several theoretical lenses to explain the trust-building process, including deterrence-based trust, calculus-based trust, relational trust, institution-based mechanism, and trust transfer mechanism (Rousseau et al., 1998; McKnight et al., 2002; Wang et al., 2013; Cao et al., 2018). Deterrence-based trust emphasizes utilitarian consideration, where trust between parties is formed because of the costly sanctions. Calculus-based trust is developed based on rational choice, where trust between parties are created based on deterrence and credible information on the intention and competence of parties involved. Relational trust is formed over repeated interaction between parties and is often called affective trust or identity-based trust. The trust transfer mechanism explains transferring trust from a known entity to an unknown entity (e.g. transfer trust from a known brick-and-mortar entity to an online entity) (Stewart, 2003). Institution-based trust incorporates above trust dimensions from an institutional perspective. Institutional factors warranty intention and competition and sustain for a more extended time, enabling risk-taking and trust behaviour among parties. However, understanding which theoretical lens works better requires further consideration of the research context. DPU context is characterized by vulnerable financial institutions and platforms (internet banking systems) because of cybersecurity breaches affecting confidentiality, integrity, and customer data privacy. Thus, the perception formed out of the cybersecurity threat potentially interferes with the user's decision process regarding digital payment usage. In this situation, the linkage between the decision process and the concerns about security breaches may play an essential role in the trust-building process. Growing knowledge of the cybersecurity threat could be a driver that could potentially influence customers' perception of the acceptance and retention of new technology. Since the underlying concept, national cybersecurity commitment in the research theme denotes the structural mechanism that protects against consequences (negative effect) regarding the use of internet environment transcend to the user's decision of the DPU. Therefore, we propose to view the DPU decision from an institution-based perspective as other theoretical lenses do not capture institutional factors; instead, they capture interpersonal or intergroup phenomena. The role of structural assurance in influencing DPU has also been discussed in prior studies (Pal et al., 2021a; Thakur & Srivastava, 2014; Yu, 2012; Zhou et al., 2010).

We consider institutional trust the specific type of trust relationship where a citizen is the truster, and the institution is trustworthy (Smith, 2010). Various definitions of institutional trust are explored in the literature (see Appendix Table 12). According to Smith (2010), institutional trust can be defined as "truster places trust in the rules, roles, and norms of an institution independent of the people occupying those roles" (p.226). More precisely, it refers to the citizen's faith that they place in the institutions not to act in ways that will harm them. In her seminal work, Zucker (1986) highlighted that institutional trust was one of the vital trust-building mechanisms which are instrumental in instilling trust in citizens in an impersonal economic environment where similarity and familiarity do not exist. In a similar vein, Shapiro (1987) explained institutional trust as the belief that a truster has about the security of a situation because of the various guarantees, safety nets, and other performance structures.

Over the years, several compelling empirical findings have been put forward in support of institutional trust theory to understand positive expectations of individuals in various relationships (Cerić et al., 2021; McKnight et al., 2002; Offe, 1999; Pavlou & Gefen, 2004; Sha, 2009). Existing research underscores the importance of institutional trust as it is an essential ingredient of long-term transactional engagements between actors. One of the significant contributions to the E-commerce research stream was identifying the role played by institutional trust in e-commerce success (Ratnasingam, 2004). Further, McKnight and Chervany (2001) described institutional trust as a critical part of internet transactions and introduced two dimensions of Institutional trust. First, structural assurances refer to the belief that a favourable outcome is likely to happen because of the contextual structures, such as regulations and formal policies. Second, situational normality, which refers to the success of a transaction, is anticipated because the situation is normal. Consistent with this argument, we conceptualize institutional trust through the structural assurance dimension (McKnight et al., 2002; Pavlou & Gefen, 2004). Structural assurance can be defined as "consumers' beliefs about the available protection from institutional structures and mechanisms" (Sha, 2009, p.43). These structures and mechanisms reflect trustworthiness cues (Smith, 2010), which give assurance to consumers, and thus, trust is developed (Gefen et al., 2005, 2006). Individuals look for trustworthiness cues (signs) that display trustworthy properties (trustworthy's competence and motivations) when they make trust judgments (Bacharach & Gambetta, 2001; Sztompka, 1999). Indeed, citizens cannot fully apprehend the trustworthy properties through the trustworthiness cues (Offe, 1999). However, the trust-building mechanism depends on the quality of information: credibility, clarity,

salience, memorability, visibility, and clarity (Sztompka, 1999).

The idea of trust in the formal institutional structures and mechanisms was particularly evident in the mid-1800s to the early-1900s to expedite business transactions in the absence of familiarity (Zucker, 1986). The lack of familiarity in the early-1900s was caused by the frequent and massive domestic migrations, the presence of bankrupt companies, and the rapidly growing immigrant population. As a result, various business organizations and citizens relied on formal institutional structures to facilitate the transaction of money and goods (Zucker, 1986). The characteristics of digital payments closely resemble the mid-1800s to the early-1900s period. First, similar to unfamiliarity between actors in the previous periods, there is also significant unfamiliarity between consumers, banks, or intermediaries in the current situation. Digital payment, being an innovative technology-oriented financial service, individuals develop increased concern over security, trust, and risk in using digital payment services. Additionally, digital banking reduces the human-to-human interaction activities inherent in traditional banking or shopping. Furthermore, cybersecurity threats such as denial of e-services, data integrity breaches, and data confidentiality breaches are significant challenges for the progress of digital banking. According to the official annual report (2019) on cyber-dependent crime, Steve Morgan, the Editor in chief of Cybersecurity Ventures, commented, "Cybercriminal activity is one of the biggest challenges humanity will face in the next two decades." In addition, the budget for preventing cybercrimes will hit $6 trillion by 2021. Under these circumstances, building a stable, trusting relationship with the banks and intermediaries becomes very difficult. Transactional parties chose to rely on formal institutional structures and mechanisms in the volatile mid-1800s to the early-1900s. Today's customers might need to depend on formal institutional structures and mechanisms as their safety net to have a sense of confidence, assurance, and protection when they conduct digital transactions.

Objects of institutional trust vary from abstract to something concrete. Examples include local government, legal system, political parties, political leaders, police, and policies. In this study, we focus on the cybersecurity commitment of government institutions in a country as the object of trust. National cybersecurity commitment emphasizes the need to have cybersecurity structures, best practices and risk management approaches, a secure cyber environment, guarantees, and policies to protect the country and its citizens from cyber intrusions. Building on existing theoretical and empirical research on institutional trust, we define trust in national cybersecurity commitment as "the subjective probability by which citizens believe that the underlying formal institutional structures and mechanisms are capable of facilitating electronic transactions according to their confident expectations." Accordingly, we propose that cybersecurity solutions, policies, and frameworks provide impersonal assurances to citizens in a country that contributes towards their positive expectations, intentions, and behaviours in digital banking relationships. Various studies have looked into this aspect of trust in government institutions to understand the positive influence on the usage of digital services. For example, in one of the studies, Srivastava and Teo (2009) demonstrated that citizens build trust through government and technology. Similarly, Bélanger and Carter (2008) showcased that trust in government and trust in the internet turned out to be positively influencing the intention to adopt e-government services. In another study, Zhang et al. (2016) demonstrated that the governments' role in developing and enforcing contracts, agreements, and regulations and providing guidance and information positively influences the likelihood of increasing customers developing trusting belief towards sustainable consumption.

Only a few studies have investigated the influence of institutional trust on digital payment usage. In one of the studies, Yeh (2020) analyzed the impact of public policy on mobile payment usage behaviour. The author argued that government plays a vital role in building secure infrastructure, reducing transaction costs, and instilling confidence in citizens to use digital payment services. Further, Xin et al. (2013) investigated the characteristics of mobile technology on mobile payment adoption using constructs like perceived structural assurance and perceived environmental risks. They found that perceived structural assurance positively impacted the trusting belief in the adoption of mobile payments. Similar studies were conducted concerning mobile-commerce adoption where structural assurance positively impacted consumers' trust in mobile banking (Chandra et al., 2010; Dahlberg et al., 2015; Kim et al., 2009a, b; Liu et al., 2009; Yang & Mao, 2011). Siau and Shen (2003) emphasized that technology-related risks like the failure of infrastructure, security failures, server downtime during the transaction, loss of money due to a technical error, etc., would reduce the level of trust among consumers. Further, Luo et al. (2010) found that consumers who have a trusting belief in structural assurance (government law, regulation, and proper infrastructure) will automatically believe that their money and data are safe during the transaction.

2.3 Cultural Differences as a Moderator

Values and norms of the citizens play an independent role in shaping institutional trust (Verba & Almond, 1963; Inglehart, 1999; Putnam, 1992). In other words, individuals from different cultures react differently to the same stimuli as they assign their specific values to the events (Inglehart, 1999; Shi, 2001). Prior empirical findings emphasized that citizens with similar value orientation with institutions have a firm,

trusting belief in institutions (Devos et al., 2002). National culture is the shared values and norms among individuals in a social grouping like a country (Walsham, 2002). ‘‘the collective programming of the mind distinguishes the members of one group or category of people from another’’ (Hofstede, 2001, p. 9). It is also noteworthy that the macro–micro level interaction studies used Hofstede’s cultural dimensions (Leung & Bond, 2004; Migliore et al., 2022; Oyserman et al., 2002). Hofstede (2001) and Hofstede et al. (2010) identified five dimensions of national culture: Power distance (PD), uncertainty avoidance (UA), individualism/collectivism (IDV), masculinity/femininity, and long versus short term orientation (LTO). Prior works suggest that PD, UA, and IDV are the three dimensions used extensively in the technology adoption and diffusion literature (Leidner & Kayworth, 2006). We omitted the power distance (PD) dimension because digital payments are not based on top-down decisions. Therefore, we believe that these two cultural dimensions, IDV and UA, may affect the relationship between national cybersecurity commitment and digital payment usage and focus on this study.

The individualism/collectivism dimension explains the difference in value between individualistic and collectivist societies. In a collectivist society, individuals believe that “from birth onwards, they are integrated into strong, cohesive in-groups, which throughout people’s lifetimes continue to protect them in exchange for unquestioning loyalty” (Chien et al., 2018, p.29:6). Individuals from high individualistic cultures focus on self-achievements rather than group goals. They are more likely to seek information from direct and formal resources and separate themselves from the social group. A person's self-worth is intrinsically derived and not conferred by others in society. Thus, individualistic culture manifests individual independence and prioritizes choosing one’s own goals (Schwartz, 1994). The context surrounding individual interaction is egalitarian, consisting of individuals who focus on personal goals, supported by an efficient legal system that enforces contracts and rights (Leung & Cohen, 2011). These characteristics will lead to quick technology adoption of incredibly innovative technologies to effectively help individuals achieve personal goals (Chien et al., 2018). Thus, we propose that individuals from collectivist cultures have lower usage of digital payment services than individualistic cultures. In addition, Doney et al. (1998) postulate that the IDV dimension affects how people develop trust. Individuals from collectivist cultures are likely to form trust through the transference process, whereas trust is created through the calculative process in individualistic cultures. Trust transfers from the trustor (known entity) to another individual or group in the transference process. To establish trust through the transference process, trustors must find trusted entities (e.g., public institutions) to transfer the trust. In the absence of prior experience, individuals from collectivist cultures establish trust through transference (Milliman & Fugate, 1988). For example, individuals from collectivist societies are more likely to rely on the approval of institutional entities in the society and act accordingly. Further, under the calculative process, trust is established through calculating cost or benefit in the relationship. People in individualistic cultures evaluate the technology uncertainty against the benefits of using digital payment. In a situation where the benefits of using digital payments outweigh the cost, they are likely to engage in digital payments. Considering these two processes, we propose that individuals from both societies (especially collectivist cultures) have higher digital payment usage at the higher level of national cyber security commitment.

The uncertainty avoidance dimension can be defined as “the extent to which the members of a culture feel threatened by uncertain or unknown situations” (Chien et al., 2018, p.29:6). In a strong UA culture, individuals are programmed to feel uncomfortable in unstructured circumstances. These circumstances are often unknown or novel. Individuals from strong UA cultures try to minimize the possibility of such circumstances by following strict rules and processes (Bankole & Bankole, 2017). As discussed, the digital payments environment inherently involves an uncertain environment compared to offline transactions. Further, sharing data or money with unknown entities like e-vendors and transferring money through mobile payments represent a total change in lifestyle for individuals. Prior research has also shown that high UA societies show increased resistance to change than weak UA societies (Kale & Barnes, 1992). Therefore, it is reasonable to expect that individuals in strong UA cultures are more likely to resist digital payments than individuals in weak UA cultures. Thus, we infer that digital payments will be higher in weak UA cultures than in strong UA cultures. In addition, individuals from strong UA cultures have higher needs for formal structure and a stronger faith in institutions (e.g., public) than in weak UA cultures (Doney et al., 1998). Individuals from strong UA cultures are more likely to be uncomfortable in ambiguous environments. Their trust in a formal structure reduces uncertainty in those ambiguous environments (Harris et al., 2005). Privacy data breaches or financial data breaches have been the most pressing issues in recent years and continue to impact the trust in digital payment usage. Thus, at higher levels of national cybersecurity commitment, people in strong UA societies are more likely to rely on formal institutional structures to protect their data and money. Hence, we propose that digital payment usage be higher for countries with strong UA culture at a higher level of national cybersecurity commitment. To summarize, culture moderates the trusting belief between individuals and institutions (Gefen et al., 2005; Gefen & Heart, 2006; Miltgen & Peyrat-Guillard, 2014). The overall conceptual framework is shown in Fig. 1.

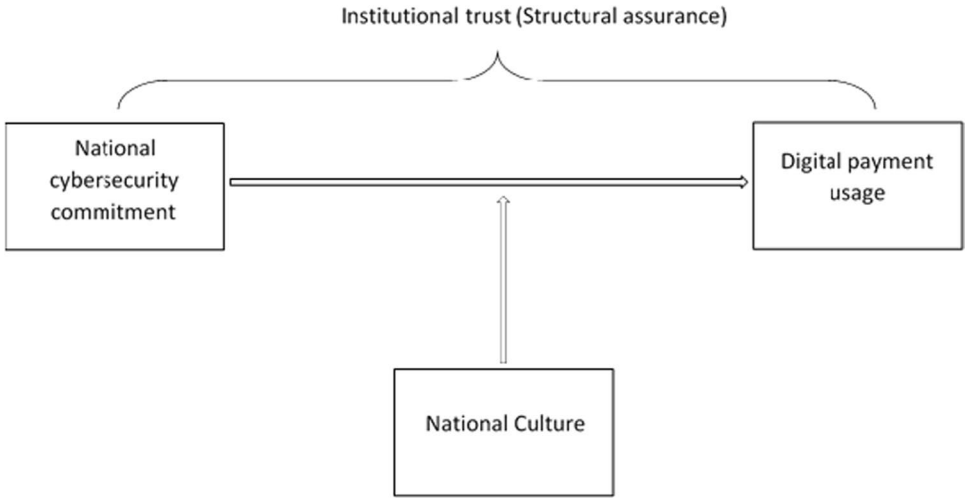

Fig. 1 The conceptual framework used in this study

The impact of Hofstede's national cultural dimensions on technology diffusion has been an interesting topic among practitioners and academicians (Straub, 1994; Walsham, 2002; Bagchi et al., 2004; Leidner & Kayworth, 2006; Takieddine & Sun, 2015). Several empirical findings underscore the moderating role of culture on technology usage (Bellman et al., 2004; Bélanger & Crossler, 2011; Zhang et al., 2012; Miltgen & Peyrat -Guillard, 2014). In addition, the perceived information security concerns (or trusting belief in security measures) are culturally embedded characteristics that will influence digital payment usage (Mohr & Walter, 2019; Mombeuil, 2020). Various studies have looked into this aspect as well. Fan et al. (2018) empirically investigated how digital payment adoption significantly varies across the USA and China concerning perceived security and trust. The findings suggest that UA positively impacts perceived security and trust, leading to a positive attitude towards digital payment adoption. Further, Al-Okaily et al. (2020) studied the moderating effect of culture on the Jordanian citizens' adoption of mobile payment services and found it insignificant. In addition, citizens from higher individualistic culture countries, like the USA, have higher institutional trust and are more likely to use online payments and purchases than countries like Italy, where citizens have lower individualistic culture (Dinev et al., 2006). Takieddine and Sun (2015) studied internet banking diffusion across 33 European countries and found that national culture moderated internet banking diffusion and internet access across countries. Inclusion of the culture moderator improved the explanation power of the model by 13%, which shows the analytical superiority of including culture-related variables (Baptista & Oliveira, 2015). Tam and Oliveira (2019) shed light on the moderating role of UA on the impact of task technology fit (mobile banking payment services are appropriate for me) on individual performance (mobile banking payment services help me to accomplish tasks more efficiently). Similarly, IDV positively moderates the impact of task technology fit on digital payment usage. Few other studies demonstrated the indirect influence of national culture on mobile payment adoption through trust and privacy concerns (Bankole & Bankole, 2017). In sum, digital payment usage is contingent on individuals' cultural values.

3 Research Model and Hypotheses

We adopt institutional trust theory as the theoretical foundation to conceptualize the linkage between national cybersecurity commitment and digital payment usage. Further, to understand whether the cultural differences inhibit or facilitate digital payment usage, we conceptualize culture through two prominent Hofstede cultural dimensions. We believe that digital payment usage varies significantly across UA and IDV dimensions based on cultural differences. These cultural differences moderate the institutional trust relationship between national cybersecurity commitment and digital payment usage. The research model is shown in Fig. 2, which explains how the diffusion of digital payment usage is contingent upon the national cybersecurity commitment and the two prominent cultural dimensions according to the conceptual framework proposed.

3.1 National Cybersecurity Commitment and Digital Payment Usage

National cybersecurity commitment is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organization and user's assets" (ITU Cyber, 2018). In the absence of reasonable cybersecurity measures, cyber intrusion will impair

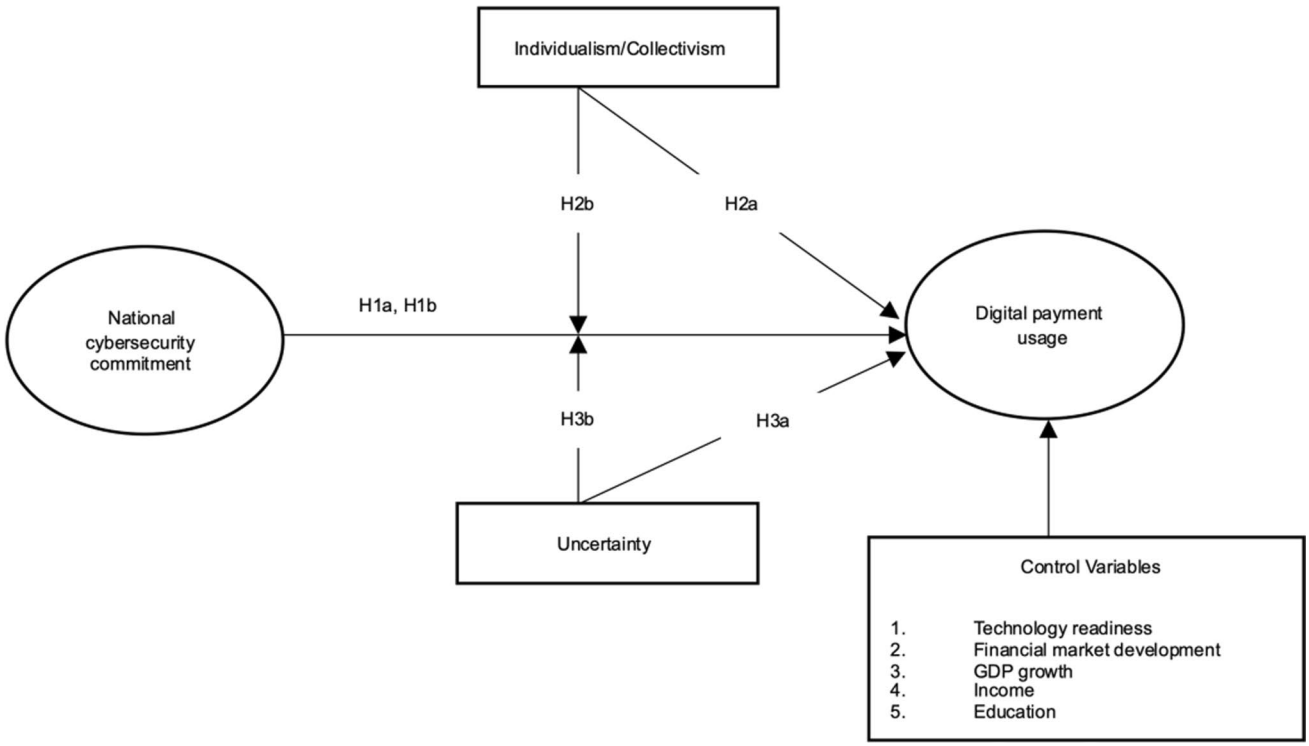

Fig. 2 Research model

the various services, especially business services and ICT infrastructure in a country (Halchin, 2004). Despite multiple advantages in ICT, cybersecurity threats play a crucial role in the adoption and continued use of technology-related products and services (Kimani et al., 2019; Tyagi, 2019). More and more consumers of financial institutions and banks are now aware that they are more vulnerable to cyberattacks and data breaches because hackers can access bank information and steal money (Gurung et al., 2008; Huang et al., 2011; Kimani et al., 2019). Confidentiality, integrity, and availability (CIA) of the data are the major concerns for the individuals while using digital payment services (Berghel, 2000; Kim et al., 2016; Safa et al., 2015; de Gusmão et al., 2018). For example, in the case of a digital banking transaction, personal and bank account information must be kept under secrecy (confidentiality), must not be modified by unauthorized parties (integrity), and there should be unrestricted access of information to the authorized parties (availability). Apart from conventional methods like stealing mobile phones or skimming through passwords, technical methods like phishing/spoofing, impersonation, hacking, and malware like spyware, Trojan, or worms affect the CIA of data (Lai et al., 2012).

Individual's perception of these information security threats can influence their belief, attitude, and behaviour towards the risk associated with the internet environment (Tsiakis & Sthephanides, 2005). This negative perception is primarily because of two reasons (1) consumers' incomplete knowledge about the information security measures to protect data and money (2) lack of trust in the uncertain digital environment due to the absence of human-to-human interaction (Manoj, 2011). This creates trust issues, and consumers must take a leap of faith in the preventive information security measures to accept unknown entities (McAllister, 1995). It captures the individual's subjective belief rather than an objective information security measure. For example, as an objective measure, hackers have a probability of one in 2^{128} to crack 128-bit encrypted data. Still, an average consumer who uses digital payment services is unlikely to assess this probability. In uncertain threat situations, individuals might not separately evaluate the issue of information security; instead, they mainly transfer their trust in the ecosystem, which forms a trusting belief that their information and money are secure (Lu et al., 2011; Mohr & Walter, 2019). Thus, the growing knowledge of cyber security threats becomes a driver for consumers' technology-related decision making, specifically in electronic transactions. Hence, trust in the preventive cybersecurity measure like the nation's cybersecurity commitment will help consumers cope with cybersecurity threat concerns and make them more likely to use digital payments. Thus, we hypothesize that.

H1a: *National cybersecurity commitment is positively associated with digital payment usage within a country.*

H1b: *Between countries, a persistent difference in national cybersecurity commitment predicts a difference in digital payment usage.*

3.2 Cultural Dimension and Digital Payment Usage

From the cultural perspective, innovation diffusion is not just a technical phenomenon but embedded in social and cultural contexts (Lee et al., 2013). This study considers digital payments as an innovative product. Digital payment is a personal or individual activity where consumers use personal devices to conduct transactions for their benefit. Thus, digital payments aim to complete an electronic transaction anywhere and anytime with utmost privacy. An individual from a society with an individualistic culture who gives prime importance to self-goals will be influenced by the perceived usefulness of digital payments (Bankole & Bankole, 2017) more than individuals from a collectivist culture. Further, digital payment systems such as mobile banking applications or e-vendor websites were designed to support the individualistic nature of online transactions. Features such as saving different credit card information, hassle-free interface, quick pay, QR code, etc., were introduced to increase the ease of using payment systems. As the individualistic culture manifests individual independence and prioritises choosing one's own goals over others, such culture promotes innovative products like digital payments that will help individuals achieve personal goals effectively. Thus, we hypothesize that

H2a: *Digital payment usage rates are lower for collectivist (low IDV) than individualist (high IDV) countries.*

Similarly, trust in public institutions varies across different countries as the notion of institutional trust varies across cultures (Kim, 2008). Individuals who have been brought up in similar cultures (e.g., similar values and belief systems) may have different perceptions about the cybersecurity of digital payment systems than individuals from different cultures. As discussed, individuals from highly individualistic cultures have swift trust assumptions and technology diffusion with minimal structural assurance. They have a more universalistic view of others and have higher propensities to trust than to distrust those in collectivist culture (Huff & Kelley, 2003). On the contrary, institutional trust among individuals in a collectivist society happens through transference. Moreover, there is a slow trust assumption in these cultures, and mainly trust is governed by social interactions (Leung & Cohen, 2011). Therefore, if the institutions exhibit higher commitment (high trustworthiness cues) towards protecting digital transactions from cyber security threats, individuals from collectivist societies are more likely to choose digital payments. Thus, we hypothesize that

H2b: *Higher levels of national cybersecurity commitment amplify the effect of the IDV dimension on digital payment usage. Countries with collectivist cultures have higher rates of digital payment usage at higher levels of national cybersecurity commitment.*

Uncertainty avoidance measures how society manages the fact that the future is uncertain. People from weak UA societies accept higher levels of risk and therefore do not try to control the uncertainty regarding the future (Hofstede, 1980). Alternatively, individuals in strong UA cultures attempt to control uncertain events and reduce risk. Although the probability of cyberattack against data and money is predominantly higher in digital payments, individuals from weak UA cultures are conditioned to accept it. As discussed, people from strong UA are resistant to change, presumably because change often involves uncertainty (Lim et al., 2004). On the contrary, people from weak UA exhibit lower resistance to change. Digital payment inherently involves various technology uncertainties, making it less appealing to individuals in strong UA culture. Thus, we hypothesize that

H3a: *Digital payment usage rates are higher for countries with relatively lower uncertainty avoidance levels.*

Weak uncertainty avoidance culture is associated with less regard for stability and permanence in the relationship. As a result, it may be difficult for individuals in these cultures to trust an individual or institution. Also, considering the high tolerance for opinions different from their own, individuals in weak UA culture may be less willing to judge others to be similar. Thus, it is difficult for individuals in weak UA cultures to identify trusted sources (Doney et al., 1998). Strong uncertainty avoidance culture is associated with the following societal norms and values: (1) need for structure (formal rules and regulations), (2) strong faith in institutions, (3) belief in experts and knowledge, and (4) high regard for stability (Doney et al., 1998). This belief system permits individuals to develop trust in institutions. It is thus expected that people in countries with strong uncertainty avoidance levels would generally view digital payments more favourably at higher levels of national cyber security commitment. Therefore, we hypothesize that

H3b: *Higher levels of national cybersecurity commitment attenuate the negative effect of UA dimension on digital payment usage. Countries with strong uncertainty avoidance have higher rates of digital payment usage at higher levels of national cybersecurity commitment.*

4 Research Methodology

4.1 Data Analysis

4.1.1 Data Source and Variables

We tested our hypotheses using archival data collected from the Global Findex database, World Economic Forum, Hofstede's national culture, and the World Bank database. Specifically, we used repeated cross-section (RCS) data of household *digital payment usage* collected from the Global Findex database aggregated at the country level. Further, we also explored the moderating effect of culture in building trust using Hofstede's national cultural dimensions at the country level. All the values of the variables are collected for the years 2011, 2014, and 2017 which constitute a pseudo panel data set (cross-sectional at level 1, time-series at level 2) for this study.

The primary reason for collecting data from the secondary database is because of the nature of the study. This is a cross-country study where data is collected in repeated cross-sections, nested at the country level. Collecting primary data is constrained by the time and resources in such extensive studies. Further, secondary data adds additional benefits of statistical generalization, robustness to common method bias, and easy replication (Krishnan et al., 2013). The dependent variable in this study is *digital payment usage*, which was operationalized using the measure 'use of at least two buckets of digital financial services by the individual' (see Table 1) collected from the Global Findex database. Global Findex database is one of the comprehensive global datasets of adults' financial inclusion, including their account holding pattern how individuals save, borrow, make payments, or send money. This survey covers more than 150,000 national representatives accounting for more than 1000 samples (adults above 15 years of age) from every 140 countries. In the Global Findex survey, respondents were asked questions like" whether they received government transfers through mobile phone" or used mobile phone internet services to pay utility bills." It was assessed using the scale 0 and 1, which indicates nonuser and user. Based on the nature of the questions, we grouped the services conducted by individuals into five buckets (see Table 2) in reference to the Global Fintech Adoption Index published by EY (GFAI, 2019). We operationalized the *digital payment usage* using the scale 0 and 1, where 0 indicates an individual using less than two buckets of digital payment service and 1 indicates an individual using two or more buckets of digital payment service. Then, we pooled the observations at the occasion and country level. For example, in 2014, in Finland, the country-level digital payment usage rate was 72%, where higher usage was among individuals in the age group 35–44 (95%), income level richest (96%), and education tertiary or more (98%). *National cybersecurity commitment* was operationalized using the measure "global cybersecurity index." This composite index focuses on five pillars: legal, technical, organizational, capacity building, and cooperation assessed using a continuous scale ranging from 0 to 1. The sample items include the quality of cybersecurity regulation, the use of the cloud for cybersecurity, educational awareness programs, and bilateral agreements. The moderating variable in this study is national culture, which was operationalized using Hofstede's national cultural dimensions: uncertainty avoidance and individualism/collectivism. The countries used for the analysis are listed in Appendix Table 10.

This study also used macro-level and micro-level control variables. Micro-level control variables include education level and household income. These represent the usage of digital payment at a given time and country among various socio-demographic profiles. We captured these factors as an aggregate and explained their effect on the digital payment usage rate. Macro-level control variables include technology readiness, financial market development, and GDP growth. Table 1 reports the variables used, their operationalization, and data sources.

4.1.2 Multilevel Model

Our goal was to create a complete picture of the relationship between national cybersecurity commitment, culture, and digital payment usage. To achieve this, we adopted a multilevel[2] or hierarchical modelling approach from a nuanced perspective that distinguishes different levels of analysis. Country-level data are nested within multiple, sequential time points in a repeated cross-sectional design. Multilevel models are suited for this type of data structure as countries embedded within the year where the specific cross-section was collected (DiPrete & Grusky, 1990; Lebo & Weber, 2015). Figure 3 presents a schematic of our multi-level analysis. Our data structure consists of year-wise observations nested within country-level units. Our variables are measured for multiple occasions at level 1, and those multiple occasions are produced within multiple countries, which serve as nesting units at level 2. Over the last years, the varying cybersecurity intervention levels across countries have unfolded. It is essential to ask if these interventions have affected digital payment usage in our basic model. Multilevel modelling on such hierarchical data structures allows us to account for both within-country and between-country variations by including fixed effects for the predictors and specific random effects (variability across years

[2] We thank Reviewers #1 & #2 for this suggestion.

Table 1 Variables and operationalization

Variables	Operationalization	Data sources
DPU	This is defined as the aggregate usage of digital payment services in the country. At the country level, it can be referred to as the proportion of citizens using digital payment usage according to the sample collected for each country's occasion. Digital payment services refer to finance solutions' technology-enabled or digitalization process (Wang et al., 2019). To improve compatibility with Global Fintech Adoption Index published by EY (GFAI, 2019), this study also introduces the concept of "buckets" or "categories" and groups similar services together. Therefore, digital payment usage can be called true for someone who used two or more service buckets. This study uses five categories: basic access to financial services, money transfer and payments, E-commerce trade/utility bills, budgeting, financial planning, borrowing, and insurance. Buckets and related services are explained in Table 2	Global financial inclusion index (GFI, 2011, 2014, 2017)
Independent variable		
NCSC	The global cybersecurity index focuses on the five pillars: legal, technical, organizational, capacity building, and cooperation. Even though the reports were published later, actual data collection was in alignment with the Global Findex survey. A detailed description is given in Table 9 in Appendix	International Telecom Union (ITU Cyber, 2011, 2014, 2018)
Moderator variable		
UAI IDV	Hofstede's cultural dimensions have been employed to differentiate two cultural dimensions	Hofstede et al. (2010); Hofstede (2021)
Control Variables		
EDU INC	Household income (INC) is a nominal variable with five different groups ranging from the poorest 20% to the richest 20%. Education (EDU) is a nominal variable with three levels ranging from primary to tertiary and more. This is a proxy for human capital	Global financial inclusion index (GFI, 2011, 2014, 2017)
TR PCT GDP	*TR:* The technological readiness pillar measures the agility with which an economy adopts existing technologies to enhance the productivity of its industries, with specific emphasis on its capacity to fully leverage information and communication technologies (ICT) in daily activities and production processes for increased efficiency and competitiveness *PCT:* Financial market development explains the availability and accessibility of financial resources to the firms to develop the financial market. It is measured using private credit to GDP *GDP:* GDP growth explains the year-wise GDP growth of a country. GDP growth was used to account for the faster economic growth episodes in the country, which would influence financial inclusion and financial industry development	World Economic Forum (ITU, 2011, 2014, 2017) World bank data (WBD, 2020)

Note. *DPU* Digital payment usage, *NCSC* National cybersecurity commitment; *GDP* GDP growth rate, *PCT* Private credit to GDP, *TR* Technology readiness, *CUL* National culture, *EDU* educational qualification Tier, *INC* Household income quantile tiers

Table 2 Categories and services which explain digital payment usage

Categories/buckets	Services
Basic access to financial services	Access account through internet or mobile
Money transfer and payments	Send or receive digital remittances or E-money (e. g., wages, school fees, government transfers, agricultural services, self-employment through mobile and money transfer services)
E-commerce trade/utility bill	Purchase and payment through e-commerce applications using mobile or Internet. Pay bills or online brokerage (through mobile or internet)
Budgeting and financial planning	Use of financial tools for financial planning and pension management
Borrowing and Insurance	Online loan or insurance request and access to the financial or non-financial institution and brokerage services

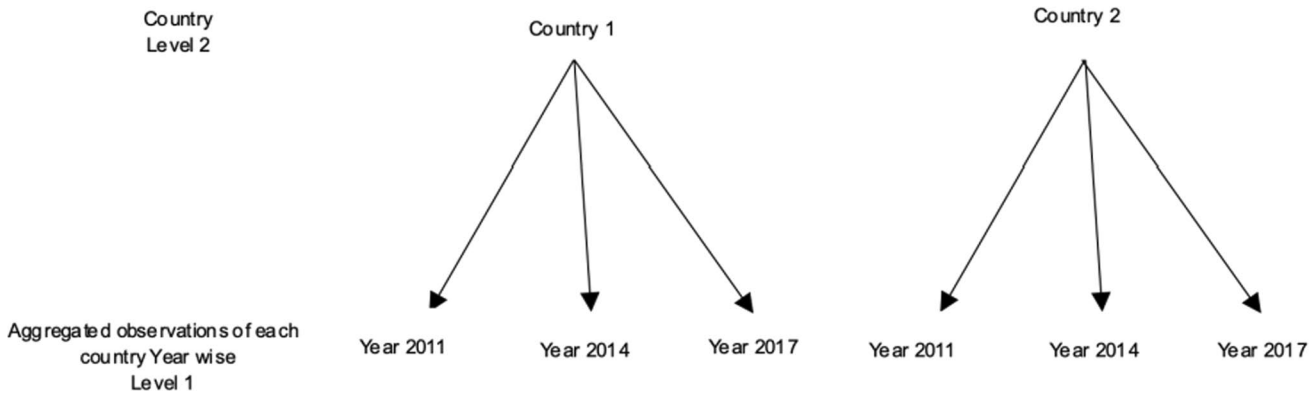

Fig. 3 Schematic of multi-level analysis

and countries). To fully evaluate the relationships and maximize the robustness of our findings, we analyzed time-series cross-sectional data, covering 76 countries from 2011 to 2017, which produced 228 observations (3 occasions per country).

In this study, we conflated the two independent processes (1) a lower-level process that happens within country (within-country effect) and (2) a higher-level process that happens across countries (between-effect). We argue that a between-country effect refers to a long-term and persistent process that characterizes digital payment usage compared to other countries. However, the within-country effect refers to a short-term process of relative change within a country. These effects might produce the same pattern, but they speak to different mechanisms. There is interdependence among occasions generated in a country, as these occur in their contexts. This process varies largely across countries. Multilevel modelling on our hierarchical data allowed us to simultaneously infer both between-country and within-country processes without confusing the two. To conduct multilevel modelling, we followed the procedure described by Kusano and Kemmelmeier (2020).

The first step is analyzing model 1, which decomposes variance into occasions and country. This analysis shows why the between-country and the within-country processes should be separated. The other models explain varying longitudinal processes by analyzing both within-country and between-country processes, accounting for country-specific effects. We created an additional model (Appendix Table 11) to increase the robustness, where we used data regarding digital payment usage directly from the source rather than using the concept of the bucket. The multilevel model was analyzed using full information maximum-likelihood estimation by *'xtmixed'* in Stata 14 software. The two-level model is as follows:

$$Digpayusage_{it} = \beta_0 + \beta_1 Year_{it} + \beta_2^W Cybcomm_{it} + \beta_3^B CUL_i + \beta_4^W IND_{it} + \beta_5^W COU_{it} + \beta_6^B Cybcomm_{it} + \beta_7^B COU_{it} + \beta_8 Cybcomm_{it} * CUL_i + \{\mu_0 + \mu_1 Year_{it} + \mu_2 Cybcomm_{it}\} + e_{it}$$
$$\begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \end{pmatrix} \sim N\left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} \sigma_{u0}^2 & & \\ \sigma_{u01} & \sigma_{u1}^2 & \\ \sigma_{u02}^2 & \sigma_{u12}^2 & \sigma_{u2}^2 \end{bmatrix}\right), \quad (1)$$
$$e_{it} \sim N(0, \sigma_e^2)$$

Table 3 Descriptive statistics and correlations

Variable name	M	DPU	NCSC	GDP	PCT	TR	IDV	UAI	EDU	INC
DPU	0.41	1								
NCSC	0.56	0.56	1							
GDP	3.52	-0.03	-0.01	1						
PCT	4.09	0.41	0.40	-0.22	1					
TR	4.42	0.63	0.63	-0.17	0.65	1				
IDV	0.40	0.51	0.48	-0.13	0.44	0.65	1			
UAI	0.69	-0.30	-0.21	-0.24	-0.23	-0.10	-0.26	1		
EDU	1.94	0.50	0.44	-0.18	0.49	0.72	0.54	0.02	1	
INC	3.19	-0.06	-0.07	-0.07	-0.12	-0.09	0.11	0.05	-0.01	1

Note. *DPU* Digital payment usage, *NCSC* National cybersecurity commitment, *GDP* GDP growth rate, *PCT* Private credit to GDP, *TR* Technology readiness, *IDV* Individualism/collectivism, *UAI* Uncertainty avoidance index, *EDU* educational qualification Tier, *INC* Household income quantile tiers, N = 76, *M* Mean

$Digpayusage_{it}$ is the aggregated usage of digital payment services in country i at time t. β_0 is the intercept of digital payment usage, allowed to vary by country (μ_0). β_1 estimates the linear slope of Year on digital payment usage. It corresponds to a deviation relative to the underlying trajectory of the dependent variable. In addition, the slope of Year is allowed to vary by country, and its random effect is estimated by μ_1. Our within-between random-effects regression model expresses the target predictors using within-country and between-country predictors. We, firstly, group mean centre a series of time-variant level-1 predictors by subtracting country-specific average scores. This procedure generates variables representing predictors' temporal fluctuations around the country-specific means. This also removes any between-country variability inherent in the time-variant level-1 predictors. Therefore, β_2^W, β_4^W and β_5^W represent fixed effects of the level-1 time-variant predictors: national cybersecurity commitment, micro-level control variables (education level, and household income level), and country-level control variables (technological readiness, financial market development, and GDP growth), respectively. These effects correspond to level-1 within-country effect – the degree to which a change in cybersecurity commitment and other control variables affect digital payment usage within any given country. The within-country effects are also allowed to vary by country, and these random effects are captured by μ_2. β_3^B, β_6^B and β_7^B represent the fixed effects of time-invariant level-2 predictors: national cybersecurity commitment, cultural dimensions, and country-level control variables (technological readiness, financial market development, and GDP growth). These estimates represent level-2 between-country effect, i.e., the country's historical characteristics of each predictor- the degree to which a predictor affects digital payment usage at the between-country level on the average across the entire period under consideration. By using different coefficients to capture between-country and within-country effects, this approach solves the endogeneity problem by removing potential collinearity between level-1 and level-2 predictors (Bell et al., 2019). We explore cross-level interactions to estimate the moderating effect between cyber security commitment and cultural dimensions. β_8 estimates the interaction effect between time-variant cyber security commitment and time-invariant level-2 cultural dimension predictors. Level 1 variance is σ_e^2.

5 Results

5.1 Summary Statistics

We restricted our sample to 76 countries. We dropped countries where the data regarding variables used in this study are not available. Our final sample consisted of 228 observations from 76 countries, collected from different waves in 2011, 2014, and 2017, forming pseudo panel data for this study. Table 3 shows the descriptive statistics and correlations for all variables in our study. Descriptive statistics indicate that one-third of the individuals use digital payments in the given sample. However, the average level of financial market development and technological readiness is higher

Table 4 Likelihood ratio test comparing the two-level model with the single-level model

Digital Payment usage (model 1)	Single-level model	Two-level model
σ_e^2	0.231*** (0.010)	0.193*** (0.018)
σ_u^2		0.127*** (0.007)
Log-likelihood	10.09	67.25[a]
Observations	228	228

[a]Significant model improvement if the new model was superior to the immediate left at $p < 0.001$

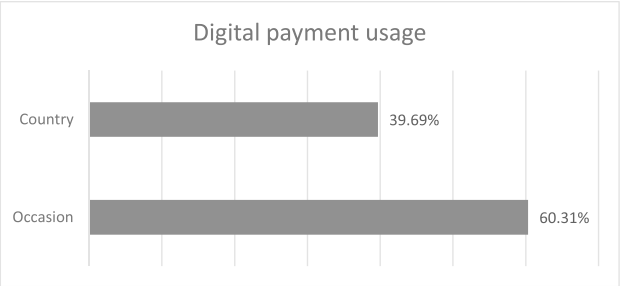

Fig. 4 The proportion of variance present at two levels (expressed in percentage)

among the countries in the current sample. The correlation matrix indicates a positive relationship between digital payment usage and country-level variables. Further, the strength of the association between independent variables is low to moderate (< 0.8), which is indicative of minimal multi-collinearity (Hair et al., 2006).

5.2 Analyzing the Trajectory of Digital Payment Usage

To illustrate the multi-level nature of data, we first present a variance-component model (null model). Table 4 summarizes the likelihood ratio tests comparing null models at each level. There is a significant improvement in the goodness of fit between models, thereby justifying the need for building a multi-level model. Figure 4 explains the proportion of variance present at two levels (expressed in percentage) and thus confirms hierarchical data structure. Occasion corresponds to the level-1 residual variance (σ_e^2) and reflects longitudinal variation. Country corresponds to the level-2 residual variance (σ_u^2) and reflects the country-level variation. This suggests that digital payment usage varies more longitudinally than cross-sectionally. Further, to improve the accuracy of the results, we clustered the error at country and year level, which established that the results were robust to heteroscedasticity. We ran different models to increase the robustness of the results. Different models are reported in Table 5 and Appendix Table 7. Model 2 examined the longitudinal pattern of digital payment usage. The significant coefficient, with b = 0.027, SE = 0.002, and $p < 0.001$, suggested that, on average, there is a predictive increase of 0.027 in digital payment usage on successive occasions (see Model 2 in Table 5). Model 2 with only the Year as predictor reduced the variance previously attributable to the occasion-level residual in Model 1 from 0.19 to 0.1, by 46%. Further, when the slope for Year and NCSC are allowed to vary by country, the resulting random slope models (Model 4 and Model 5) produce a significantly better fit than the fixed-effect model. A critical insight derived from our models is that individual trajectories of digital payment usage among countries are rather heterogeneous. The rest of the models are discussed in detail in the next section.

5.3 Analysis of within-Country and between-Country Effects

Building on the two-level model, this section explains the within-country and between-country effects. Model 3 examined the within-country impact by including the time-variant level-1 predictors. Model 3 in Table 5 suggests that the within-country effect of national cybersecurity commitment was positive, with b = 0.140, SE = 0 0.078, and $p < 0.1$, indicating that an increase in digital payment usage within any given country corresponds to an increase in national cybersecurity commitment. Adding these time-variant level-1 predictors in Model 3 reduced the variance previously attributable to the occasion-level residual in Model 3 from 0.1 to 0.093. Therefore, fixed-effects of these time-variant level-1 predictors alone explained an additional 7% of the occasion-level variance, unexplained by the previous model. Models 4 and 5 examined the within-country and between-country effect by including the time-variant level-1 predictors, time-invariant level-2 predictors, and interaction terms. Our results suggest that national cybersecurity commitment produces a mixed pattern that varies by level of analysis. The within-country effect of NCSC corresponds to a longitudinal process. The within-country effect of NCSC turned out to be negative in Model 4 and Model 5. However, the standard error pertaining to this coefficient is large enough to render this effect unreliable. By contrast, the between-country effect of NCSC represents the degree to which a persistent difference in NCSC between countries predicts a difference in DPU between countries. Model 4 in Table 5 suggests that the between-country effect of NCSC was positive, with b = 0.23, SE = 0.130, and $p < 0.1$, indicating that across countries, an increase in digital payment usage corresponds to an increase in national cybersecurity commitment. There is enough evidence from Model 3 and Model 5 to suggest that the relationship between national cybersecurity commitment and digital payment usage is significant and positive, thus supporting H1a and H1b. Overall, the between-country effect of NCSC is predominantly higher and positive, indicating that a 1-unit increase in NCSC between countries predicts a 0.23-unit increase in digital payment usage.

The uncertainty avoidance index (UAI) exhibits similar effects in Models 4 and 5. The between-country effect of UA was negative, with b = -0.202, SE = 0.089, and $p < 0.05$, meaning that countries with high uncertainty avoidance culture would have lower digital payment usage, thus supporting H3a. However, the path coefficient of the moderating effect of the UA on the relationship between national cybersecurity commitment and digital payment usage is significant and positive, with b = 0.376, SE = 0.176, and $p < 0.05$.

Table 5 Impact of national cybersecurity commitment and culture on digital payment usage

Dependent Variable: DPU	Model 2	Model 3	Model 4	Model 5	Hypothesis supported
Fixed parts					
Year	0.027*** (0.002)	0.014** (0.004)	0.034*** (0.007)	0.035 *** (0 0.006)	
Within-effects					
NCSC		0.140* (0 0.078)	-0.094 (0.150)	-0.096 (0.144)	H1a supported
GDP		0.002 (0.003)	0.020** (0.008)	0.021** (0.009)	
PCT		-0.022 (0.062)	-0.016 (0.065)	-0.007 (0.077)	
TR		0.079** (0.033)	-0.012 (0.045)	-0.018 (0.040)	
EDU		0.109 (0.165)	0 0.059 (0 0.102)	0.042 (0.157)	
INC		-0.001 (0.0347)	-0.037 (0.054)	-0.046 (0.049)	
Between-effects					
NCSC			0.23* (0.130)	0.226* (0.132)	H1b supported
IDV			0 0.104 (0 0.101)	0.112 (0.110)	H2a not supported
UAI			-0.205** (0.091)	-0.202** (0.089)	H3a supported
GDP			-0.017** (0 0.008)	-0.018** (0.007)	
PCT			0.004 (0.035)	0.007 (0.047)	
TR			0.105** (0.030)	0.104 *** (0.032)	
within × between interaction					
NCSC x IDV				-0.057 (0.267)	H2b not supported
NCSC x UAI				0.376** (0.176)	H3b supported
random parts					
Level 2: country					
0. (intercept)σ^2_{u0}	0.198** (0.013)	0.191** (0.017)	0.127** (0.015)	0.124 ** (0.021)	
1. (Year) σ^2_{u1}			0.0005 (0.0002)	0.0003 (0.008)	
2. (NCSC) σ^2_{u2}			0.232** (0.128)	0.208** (0.216)	
Level 1: Occasion					
σ^2_e	0.1 ** (0.008)	0.093** (0.005)	0.089** (0.005)	0.078** (0 0.009)	
Log pseudolikelihood	108.6	115.72	140.55	146.86	
Observations	228	228	228	228	
countries	76	76	76	76	
Wald chi2	90.57	151.16	227.41	513.22	

Values in the bracket represent robust standard error

Note. Significance level $*p<0.10$, $**p<0.05$, $***p<0.001$, *DPU* Digital payment usage, *NCSC* National cybersecurity commitment, *GDP* GDP growth rate, *PCT* Private credit to GDP, *TR* Technology readiness, *IDV* Individualism/collectivism, *UAI* Uncertainty avoidance Index, *EDU* educational qualification Tier, *INC* Household income quantile tiers

This implies that the negative effect of UA on digital payment usage is lower among countries with higher cyber security commitment, thus supporting H3b. To further dig into the nature of moderations, it was necessary to plot the moderation effects. Accordingly, simple slope analysis was conducted using the margin command in STATA. Figure 5

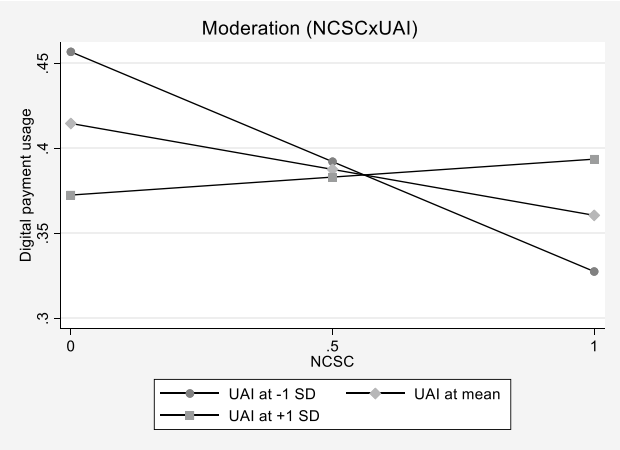

Fig. 5 Moderation effect of UA on the relation between NCSC and DPU

shows the moderating effect of the UAI on the relationship between national cybersecurity commitment and digital payment usage. Digital payment usage at a low level (-1 SD) and a high level (+ 1 SD) of UAI showed a considerable difference when national cybersecurity commitment was low and high. Countries with high uncertainty avoidance cultures have higher digital payment usage when there is a higher national cybersecurity commitment. However, at its mid ranges, the difference was more minor. At weak UA and higher NCSC, digital payments are lower, to our surprise. This finding is exciting and explained in the next section.

Regarding the effects of the control variables, as shown in Table 5, the within-country effect of GDP was positive, with b = 0.021, SE = 0.009, and $p < 0.05$, meaning that any increase in GDP growth within-country was linked to a modest increase in digital payment usage. The significant between-country effect of GDP, with b = -0.018**,** SE = 0.007, and $p < 0.05$, suggests that a 1-unit difference in GDP growth between countries predicts a 0.018-unit decrease in digital payment usage. This implies that a persistent difference in GDP growth between countries negatively predicts a persistent difference in digital payment usage. The between-country effect of technology readiness was positive, with b = 0.104, SE = 0.032, and $p < 0.001$, meaning that any increase in technology readiness was linked to a modest increase in digital payment usage. Given the interdependence between countries, it is worthwhile to investigate regional implications for the observed effects of national cybersecurity commitment. For instance, countries in a particular region might drive the observed effects entirely. Thus, we investigated an additional model to increase the robustness of the results. Here, we allowed the intercept to vary by region; this allowed us to test whether adding a third level would cause variability in observed effects. Model 6 of Appendix Table 7 summarizes the coefficients of this model. Our findings are often confirmed, as shown in Appendix Table 7. The region corresponds to the level-3 residual variance (σ_k^2) and reflects region-level variation. We observed that there is region-level variation in digital payment usage. We emphasize that the third level (regional analysis) model is somewhat exploratory, and further research needs to be conducted to identify region-specific relationships.

6 Discussion

In response to the research questions- what are the roles of national cybersecurity commitment and national culture in explaining digital payment usage within and between countries, this study proposed a research model that allowed the investigation of these factors through hierarchical modelling. The analysis revealed that national cyber security commitment's within-country and between-country effects positively influenced digital payment usage. However, one of the cultural dimensions, IDV, yielded no significant results. Meanwhile, the UA cultural dimension was the most important factor concerning digital payment usage among citizens across countries.

6.1 National Cybersecurity Commitment on Digital Payment Usage

A citizen's use of technological innovations is primarily based on two prerequisites: first, the need for the service, and second, the capability of technology solutions to fulfil that need (Srivastava & Teo, 2009). Digital payments are electronic transactions that involve the transference of personal and financial information where individuals have lesser control over the technology platform. This enforces individuals to trust the technology and the enabler of technology (political and public institutions). A situation where citizens trust both technology and capabilities of public institutions in delivering those technologies as an enabler will lead to a scenario where there is a collaborative effort from both ends in the diffusion of innovation (Srivastava & Teo, 2009). This will lead to the successful implementation of the technology initiatives. This study used national cybersecurity commitment as the proxy for preventive cybersecurity measures. We studied its positive impact on the diffusion of technological innovation, i.e. digital payment usage among citizens. Institutional trust theory was used as defining principle for many social and economic interactions (Mayer et al., 1995). We used institutional trust theory to explain the role of national cybersecurity commitment on digital payment usage behaviour. Findings from this study underscore the level of confidence that citizens have in both political and public institutions to 'do the right thing,' 'to act diligently and appropriately' on behalf of the public in the

matter of cybersecurity. The findings emphasized that trust in institutions has a more significant influence on usage decisions, and we discuss how this trust can be enhanced through various commitment efforts. Findings are consistent with prior results on the role of facilitating conditions on digital payment usage (Thakur & Srivastava, 2014; Yu, 2012; Zhou et al., 2010). A recent study revealed that a lack of facilitating conditions in a country hurts the actual usage of mobile payment services (Pal et al., 2021a). Further, the significant and negative effect of lack of facilitating conditions on the future intention to use digital payments brings out the relevance of institutions' commitment towards cybersecurity.

To dig deeper, we analysed all pillars of national cybersecurity commitment as significant trust enablers on digital payment usage. Appendix Table 8 displays the effect of different pillars of cybersecurity commitment on digital payment usage. Results indicate that digital payment usage is mainly driven by the cooperation measures implemented by the countries (b = 0.248, SE = 0.1431, $p < 0.1$). This suggests that cooperation measures are taken by the government enrich citizens' trusting belief towards the government's abilities to minimize cybersecurity threats. Further, this is also an indication that the trustworthiness cues demonstrated by the government in terms of their commitment towards cooperation measures are accepted by the citizens and reflected in their trust in the institution. Greater cooperation among institutions within-country and between countries can enable the development of much more robust cybersecurity capabilities, helping to deter repeated and persistent cybersecurity threats and allow better investigation of cybercrimes and apprehension and prosecution of malicious offenders. Participation in various international forums is strong among nations to better cybersecurity within the country. However, most countries have lesser bilateral/ multilateral agreements, inter-agency partnerships, and public–private partnerships (ITU Cyber, 2018). This indicates that more and more efforts are needed from countries to increase the cooperation efforts to minimize cyber threats. However, various countries have done well in their cooperation efforts. For instance, Estonia was one of the first countries to create a cybersecurity strategy in 2008. Currently, their efforts intend to formalize existing ties and enhance R&D activities in the cybersecurity field in Estonia. Similarly, Hungary actively engages with partners within the Global Forum on Cyber Expertise and shares information and best practices on cyber incidents, critical information infrastructure protection, etc. Singapore is a prime example of establishing a partnership with other countries to establish channels for information exchange on cyber threats and incidents. Association of Southeast Asian Nations (ASEAN) Cyber Capacity Programme is an example of an approach towards cybersecurity cooperation measures between countries (ITU Cyber, 2018).

Cybersecurity commitment exercised by the nations through legal measures has a negative effect on digital payment usage. A possible explanation for this result could be that signals of trustworthiness cues related to the execution of legal efforts by the government are weak. For instance, the objective of the legislative framework is to harmonize practices at the national/international level and combat cybercrimes. Even though countries have strong cybercrime legislation, most of the time, the law becomes ineffective, and offenders are not prosecuted (Park, 2019). This makes citizens lose faith in cybersecurity legislation. It is interesting to note that other pillars turned out to be non-significant in explaining the institutional trust mechanism. We offer two major explanations for these insignificant results. First and foremost, information cues regarding organizational, capacity building and technical measures are less visible to the citizens even though government makes those efforts. The second explanation is the number of resources spent on these measures is limited in countries. This is evident in the measures of the other pillars reported in the global cybersecurity index. Most countries have low values for these indices or have not been measured (ITU Cyber, 2018).

6.2 Moderation Effect of Culture

It is essential to understand the role of cultural dimensions on digital payment usage because citizens' acceptance and use of digital technologies contribute to financial inclusion and economic progress within a country. However, the value systems ingrained in the individuals shape the usage of such novel technologies and thereby act as a barrier or facilitator. Our findings partially support this claim. To elaborate, the direct and moderating impact of the IDV dimension on the proposed relationship was insignificant. The lack of support for the direct and moderation effect of IDV on digital payment usage may lie in the system's characteristics. It may be possible that the IDV dimension is more readily manifest in the case of collaborative technologies acceptance (e.g., internet forums, project management systems) rather than standalone systems such as Apple Pay and mobile banking (Srite & Karahanna, 2006). This is primarily because of interdependence in collaborative technologies where the trust factor gains considerably more salience. We also offer an alternative explanation that few countries with high IDV have lower digital payment adoption. For instance, France has a higher GCI (0.918) and IDV (71), but digital payment adoption was comparatively lower (34%) as compared to the United Kingdom (GCI: 0.931, IDV: 89, digital payment adoption: 71%) (ITU Cyber, 2018; GFAI, 2019). These concerns also call for future studies to explore cultural effects at a deeper level.

The hypothesized main effect of uncertainty avoidance is significant. This suggests that uncertainty avoidance plays a dominant role in explaining digital payment usage rates across cultures. This pattern could be attributed to their tolerance for the uncertainty associated with digital payments. Individuals from weaker UA cultures accept a higher level of risk and do not attempt to control uncertainty, which results in the acceptance of newer technologies. This is termed as the innovation effect and is more evident in weak UA culture (Lee et al., 2013). Innovation effect stems from the individual's perception, and they choose to adopt an innovation at the early stages of diffusion. However, higher UA cultural societies formulate ways to control future events to reduce uncertainty and thus accept technologies after risk acceptance has disappeared (Lee et al., 2013). This was called the 'imitation effect,' which stems from social interaction. In one study, Baptista & Oliveira (2015) used a sample from Mozambique (weak UA) and found that UA positively impacts mobile banking usage. UA's positive and significant moderation effect on the relation between national cybersecurity commitment and digital payment usage suggests that there is higher adoption of digital payment usage at a higher level of cybersecurity commitment. As discussed earlier, citizens trust the institution in case of uncertainties, especially in digital payment systems, where they have less control over the technology platform. Members of strong UA culture have more interdependence tendencies, want more structural ways of controlling risk, and are influenced by group norms and opinions. Moreover, trust is formed through the transference process. Thus, transference-based trust determinants such as referral, word of mouth, intermediate institution's review, and recommendation are more positively related to consumer trust in digital payment systems in a strong UA culture than a weak UA culture (Kim, 2008). In other words, transference-based trust determinants like national cybersecurity commitment play a more decisive role in building consumer trust in digital payments in a strong UA culture. It is interesting to note that digital payments are lower at lower levels of UA and higher NCSC. This is primarily because of the disparity between countries used in the dataset. To elaborate, few countries with low UA have lower digital payment usage. For instance, in 2014, a country like Singapore had a lower usage rate than the United Kingdom, both having weak UA and higher NCSC. Another possible explanation is that people from weak UA culture use the internet for collecting information for their offline purchases rather than directly involved in online shopping (GFAI, 2019; Lim et al., 2004). Further, there is evidence in previous literature regarding the difficulty for individuals in weak UA to identify with trusted sources (Doney et al., 1998). However, more extensive longitudinal data should be considered for future research to assess the complete picture.

6.3 The Impact of Control Variables on Digital Payment Usage

Results displayed in Table 5 indicate that technology readiness is an essential predictor of digital payment usage. As expected, the ICT development in a country will improve cybersecurity measures. Furthermore, age is one of the important determinants of digital payment usage. These results are consistent with previous studies (Krishna & Krishnan, 2020). However, there are two major insignificant results worth mentioning. The first is the negative impact (weaker) of GDP growth rate (between-country effect) on digital payment usage. It is reasonable to expect that a country with higher GDP growth will have better ICT infrastructure, which results in more increased proliferation and use of digital payment systems. However, it is interesting to note that the digital payment adoption rate of countries with lower GDP is more significant than most developed nations (GFAI, 2019). For Instance, countries like India (87%) and South Africa (82%) have higher digital payment adoption than developed countries like the Netherlands (73%) or the United Kingdom (71%). One of the reasons for this reverse trend is the availability of financial institutions in remote villages, forcing citizens to rely on digital payment systems like mobile money transfer services (e.g., M-Pesa). The second was the statistical insignificance of financial market development on digital payment usage. It was expected to get a significant positive relationship with digital payment usage since it automatically increases credit access to financial firms and thus flourishes Fintech industries (Léon & Zins, 2020). However, to reflect the growth of the financial market in digital payment usage, there must be an integration of Fintech services into different categories such as borrowing, insurance, budget, and financial planning. Some countries regulate or restrict investing in equity crowdfunding or peer-to-peer lending, which slows the diffusion process. Further, reaching out to various demographic groups of customers like women, the older generation, and consumers in rural areas is always challenging (GFAI, 2019). For instance, usage of digital services in the savings and planning category is lower for women (27%) than for men (40%).

7 Contributions and Implications

7.1 Theoretical Contributions

This study makes three significant contributions to the literature of Fintech and behavioural information system security research. First, drawing on the institutional trust theory, this research is instrumental in broadening our current understanding of national cybersecurity commitment by identifying its positive impact on digital payment usage

among citizens in a country. This study also underscores the moderating role of national culture on the above relationship. By conducting multilevel modelling using repeated cross-sectional (RCS) data, this study uncovered a complex, dynamic pattern of netizens' trust in preventive cybersecurity measures. In doing so, this study answers Bright Internet research's call for studies to assess individuals' perceptions about national cybersecurity (Lee et al., 2018). This study also heeds to Leidner and Kayworth's (2006) observation that national culture is best suited to capture the breadth of technology diffusion at the country level. Second, our review of prior literature reveals that extant studies examining the impact of structural assurance on digital payments are mostly focused on general policy-related effects (Luo et al., 2010; Yeh, 2020), ICT development, or characteristics of mobile technology (Xin et al., 2013). Acknowledging the significance of those studies, in line with the foundation of institutional trust theory, this study conceptualizes the national cybersecurity commitment as one of the structural assurance factors that have positive implications on digital payment usage among the citizens in the country. Further, drawing on the literature on Hofstede's cultural dimensions, this study extends the boundary condition of institutional trust theory by emphasizing the role of cultural dimensions in shaping the institutional trust mechanism. As shown in our research model (Fig. 2), IDV and UA dimensions shape individual technology-related decision-making, especially regarding digital payment usage. The role of cultural dimensions alters our understanding regarding instilling institution-based trust in individuals and makes it a frame of reference for future scientific exploration. And third, in line with the Global Fintech Adoption Index published by EY (GFAI, 2019), we introduce the concept of "buckets" or "categories" and bring conceptual clarity to the definition of digital payment usage. In doing so, we extend and enrich the Fintech literature (1) by defining digital payment user as someone who uses two or more "buckets" or "categories" of digital services (see Tables 1 and 2) and (2) by identifying national cybersecurity commitment as an important determinant of the digital payment usage. In sum, by introducing the concept of institutional trust from the discipline of social psychology, our study provides a robust theoretical foundation for understanding the phenomenon of digital payment usage driven by national cybersecurity commitment and explaining the variation in trust mechanisms through different cultural dimensions thereby contributing to interdisciplinary research.

7.2 Practical Implications

From a practical standpoint, our study offers three critical implications. First, through a cross-country analysis, our study provides empirical evidence on the impact of the national cybersecurity commitment on digital payment usage, thereby sensitizing policymakers, especially those operating in cybersecurity, to incorporate cybersecurity measures to solicit citizen's trust in the government's ability and commitment towards protecting the money and personal information. We suggest that policymakers reduce their country's cybersecurity vulnerability by benchmarking cybersecurity practices employed by higher commitment countries. Cybersecurity measures should be implemented in all five pillars (see Appendix Table 9). However, our findings suggest that the legal framework should be strengthened and support citizens to use digital transactions without perceived risk. For example, Russia has a robust legal framework to implement and drive the national cybersecurity strategy. Their cybercrime law integrated a large arsenal of procedural measures to ensure compliance. In addition, their entire financial system has been digitally enhanced to instil confidence in using digital payment systems among citizens. Cybersecurity cooperation measures positively impact digital payment usage, suggesting that trustworthiness cues of cooperation measures are more visible, and citizens perceive less risk while they transact digitally. For example, in Malaysia, an internet banking task force has been developed with the help of financial institutions, Malaysian police, and the cybersecurity wing of Malaysia to combat online banking fraud. Even though our findings did not significantly impact other pillars (technical, organizational, and capacity building), it is imperative to assume that these pillars have a larger role to play. For instance, capacity-building measures ensure that proper awareness regarding cybersecurity threats and how to prevent them can be communicated to the citizens. This is important because social engineering attacks are more common in digital transactions involving money and confidential information (Salahdine & Kaabouch, 2019).

Second, we firmly believe that our conceptual framework (Fig. 1) can serve as a contingency model for policymakers to speed up the diffusion of digital payment services by developing tailor-made cybersecurity measures about cultural differences. Such a model could help them accurately decide what kind of trustworthiness cues are needed to instil institutional trust among citizens to increase the digital payment diffusion process. Findings from the current study suggest that cooperation measures and legal measures must be used to strengthen the belief of UA culture populations, as they start with low trust. Trust calibration in these populations will be highly challenging as they are more likely to fall for false propaganda and less likely to focus on actual measures. Thus, it is important to have increased transparent mechanisms behind highly complex transaction processes. For instance, displaying security banners (e.g., shields, badges, logos, or other trust symbols) in the footer of the digital payment application or payment page so that customers do not miss them. It is to be noted that human trust,

compliance, and reliance tend to drop after encountering a failure, and there are fewer chances of recovery over subsequent failure-free trials (Lee & Moray, 1994). In strong UA culture, once the trust is broken, it takes longer to negotiate or calibrate trust again (Leung & Cohen, 2011). Thus, UA culture policymakers must caution in the implementation of cybersecurity measures as failure leads to loss of trust in the institution and, therefore, has repercussions on digital payment usage. Further, policymakers from countries where UA culture is prominent should pay attention to the mindset of the citizens as the imitation effect is prevalent. The imitation effect reflects social influence (e.g., word of mouth). Accordingly, we suggest that policymakers of these countries take measures for beefing up investments in cybersecurity measures and encourage people to subscribe to digital payment services by providing an adequate guarantee against losses. This will push citizens to calibrate trust and collaborate with financial technology implementation in a country.

And third, research related to preventive security mechanisms is currently surging. It is necessary to extend our view towards understanding the trusting belief of netizens towards the capabilities of the safe cyberspace platform provider. Through this study, we demonstrate that a positive perception among netizens was created through the trustful services offered by the government. As more and more netizens have begun to value the potential benefits of preventive security mechanisms employed by institutions (here, government) in preventing cybersecurity threats, acceptance of advanced social information system platforms like Bright internet are very likely to happen. This study also highlights the positive influence of cooperation measures on the netizens' trusting belief. Thus, we suggest that academicians and policymakers working on the Bright internet initiative should promote trustworthiness cues related to enhanced benefits of technology among netizens using the Bright Internet platform. In addition, we suggest that Bright Internet should make extra effort to emphasize the role of legal measures in fighting cybersecurity threats, as these will boost the trusting belief in an institution like Bright internet. Further, the role of culture is also an essential factor in the acceptance of institutions like Bright Internet. As our study indicates, strong UA culture will result in a slower diffusion rate and is contingent primarily on society (social norms). Thus, it is advisable to carry relevant security mechanisms compatible with culture while implementing the Bright Internet platform in various countries. Table 6 summarizes the bright internet initiative and how this study contributes to the Bright Internet research.

7.3 Limitations and Future Research

Our findings should be interpreted considering the following limitations. First, this study uses archival data to undertake a

Table 6 Contributions to the Bright Internet research initiative

The objective of the Bright Internet approach is to design the future Internet platform to balance preventive cybersecurity measures with privacy protections. Preventive cybersecurity measures address state-led cyberattacks (SLCAs) and private-led cyberattacks (PLCAs) through Bright Internet principles and Internet peace principles		
Goals of the Bright Internet initiative	*Solutions*	*How this study contributes to the Bright Internet initiative?*
Preventive security: "Realize the preventive security infrastructure that can deter the motivation of cybercrime and terror originators" (Lee et al., 2018, p.64)	1. Policy (Legislation) 2. Global collaboration (Governance)	This study intends to make a case for the Bright Internet initiative by highlighting the importance of preventive security. This study helps clarify the prescriptive requirements of netizens for the next-generation Internet platform (i.e., Bright Internet initiative). This study highlights, • Societal perception about preventive security mechanisms (i.e., national cybersecurity commitment) and how it influences digital payment usage • Comparative study about perceptions of preventive security mechanisms (i.e., national cybersecurity commitment) across countries • Role of cooperative measures: Bright Internet acts as a platform for countries to cooperate, reduce cyber-attacks, and increase trust • Importance of legal measures in instilling trust in institutions: Bright Internet initiative acts as a platform where countries can devise policies and legislation, subsequently reducing cyber-attacks and increasing trust • We emphasized the role of culture in instilling trust in institutions

Note. Other two goals (Freedom of expression and Privacy) was omitted as this study does not directly contribute to the goals

study where we have less control in collecting samples and measuring variables. However, our research questions and conceptualization require a large amount of cross-country data where primary data collection is not feasible; the use of secondary data is justified with a limited sample size. Moreover, data was collected from reliable sources, and they have followed stringent guidelines to avoid bias and error in data collection. Previous research has utilised this study's archival sources (e.g., Krishna & Krishnan, 2020; Krishna & Sebastian, 2021). Second, we only analyzed data from 76 countries (see Table 10 in Appendix for a list of countries), consisting of 228 observations. We limited the analysis to these countries as the data for other countries were not available at the analysis point. Nevertheless, given that we are dealing with three variables (excluding control variables), a sample size of 76 is justified. As a rule of thumb, a sample size of 50 is considered an optimum number to avoid degrees of freedom and efficiency problems (Hair et al., 2006). In addition, our use of pseudo-panel data and clustering of standard errors across countries and years give more robustness to the results. And third, we assumed that culture as a variable that remains relatively stable across timeframe of current study. However, a study conducted by Beugelsdijk and Welzel (2018) report that cohorts of people born in over 100 countries from 1900 to 2000 exhibit substantial change in national culture.[3] We recognize this issue as one limitations of the current study and readers should interpret the results with this in mind.

The current study offers various directions for future research. First, this study underscores the role of trust in government institutions as a provider of cybersecurity measures that influence digital payment usage diffusion. Future studies may consider another important construct, 'trust in the security of financial technologies,' to understand how digital payment usage also shapes. Current studies have only considered constructs that explained trust in technology in general. For example, Sharma and Sharma (2019) examined constructs like service quality, information quality, and system quality to understand satisfaction. To conduct research with 'trust in the security of financial technologies,' an initial level of knowledge among the individuals regarding cybersecurity measures should be gauged. Second, by utilising an additional dataset, future research can also add an intermediate variable called 'Agent trust' (Senyo & Osabutey, 2020) by using a supplementary dataset. Agent trust is referred to as the trustworthiness of the intermediary parties. Some trustworthiness cues may be invisible or silent to the citizens, as discussed previously. Agents like Google pay, Apple money, M-Pesa, etc., serve as a touchpoint to customers where they could easily relate. Thus, it would be interesting to understand how agents trust the government and indirectly impact the customers' beliefs. Third, in the current study, we made an implicit assumption that citizens of each country as an aggregate have similar cultural effects. However, it has been understood by various studies that there may be cultural variations within the country (Leung & Cohen, 2011). These cultural variations within the country occur mainly because of the individual differences, interactions, and exchanges of culture. International migration might add to within-country cultural variation, which results in cultural heterogeneity within a country. Future research may consider extending our study to understand how within-country cultural variation impacts digital payment usage. Insights from those studies might be refreshing and could differ from a global study. Further, within-country studies will shed more light on the policy level changes based on the within-country cultural variation. And fourth, future studies may consider extending our pseudo panel study to a proper longitudinal or panel data study when more data becomes available. If longitudinal data is unavailable for most countries, future researchers could work with fewer countries from different cultural types. For instance, one can choose the USA (Dignity culture), Turkey (Honour culture), and Taiwan (Face culture) (Leung & Cohen, 2011), thereby comparing the diffusion of digital payment services among countries to test innovation and imitation effect.

8 Concluding Remarks

Even though the use of self-defensive security mechanisms is a way to defend against cybersecurity threats, with the rise in the effectiveness of preventive cybersecurity mechanisms, it has become agenda for countries to rely on several preventive cybersecurity measures to protect digital information systems. Despite the importance of such preventive measures, there is a dearth of scientific investigation into the positive impacts of preventive security mechanisms on public services since they are the key target groups of such cyberattacks. Drawing on institutional trust theory and literature on cultural dimensions, this study examined one of the preventive security mechanisms, national cybersecurity commitment, and its positive impacts on digital payment usage. As privacy and security concerns are culturally embedded characteristics, this study also investigated the moderating role of national culture and proposed a comprehensive conceptual model to explain how individuals from various cultural dimensions moderate the above-stated relationship. We believe that our study uncovered an exciting phenomenon, theoretical reasoning, and empirical evidence on the influence of structural assurance on digital payment usage, which will enrich the literature on Fintech and behavioural information system security research. In addition, this

[3] We thank Reviewer #1 for this suggestion.

study contributes to the Bright Internet research by assessing the individual's trusting belief in institutions and clarifying the prescriptive requirements of the next generation social information system platform. Further, this study also highlights the role of cybersecurity commitment from countries in achieving the primary goal of the Bright Internet initiative (Shin et al., 2018).

Appendix

Table 7 Three-level model (Regional analysis)

Dependent Variable: DPU	Model 6
Fixed parts	
Year	0.032*** (0.01)
Within-effects	
NCSC	-0.30 (0.165)
GDP	0.02** (0.009)
PCT	-0.012 (0.109)
TR	-0.003 (0.014)
EDU	0.116* (0.06)
INC	-0.048** (0.021)
Between-effects	
NCSC	0.189** (0.085)
IDV	0.10 (0.135)
UAI	-0.21** (0.078)
GDP	-0.017** (0.006)
PCT	0.011 (0.05)
TR	0.078** (0.039)
Within × between interaction	
NCSC x IDV	-0.02 (0.14)
NCSC x UAI	0.37** (0.137)
random parts	
Level 3: Region	
σ_k^2	0.0001 (0.005)
Level 2: country	
σ_u^2	0.128** (0.021)
Level 1: Occasion	
σ_e^2	0.088** (0.006)
Log pseudolikelihood	148.6
Observations	228
countries	76
Wald chi2	234.32

Note. Regions: East Asia & Pacific, Europe & Central Asia, Latin America & Caribbean, Middle East & North Africa, North America, South Asia and Sub-Saharan Africa

Table 8 National cybersecurity commitment pillars and its impact on digital payment usage

Dependent Variable: Digital payment usage	
Legal	-0.188 (-0.113)*
Cooperation	0.248 (0.1431)*
Organizational	0.119 (0.137)
Capacity building	-0.140 (0.139)
Technical	0.045 (0 0.110)
GDPgrow (GDP growth rate)	0.002(0.007)
PrivCredit (Financial market development)	0.191 (0.094)**
techreadines (Technology Readiness)	0.106 (0.056)**
Observations	133

Note. Other control variables are omitted in the table as they show similar results as in Table 4. Values in bracket represent t-statistics; Significance level: $*p<0.10$, $**p<0.05$, $***p<0.001$; Standard errors are adjusted for clustering at the (country year) level. Few observations were dropped owing to data unavailability

Table 9 Cybersecurity sub-indices and their definition

GCI Indices	
Legal	Legal measures ensure that legal institutions set up a basic foundation or response mechanism for prosecuting crimes or imposing sanctions for cybersecurity breaches or violations. This pillar is evaluated based on the number of legal institutions and frameworks that can deal with cybersecurity and cybercrime
Technical	The technical measure is considered as the primary frontier of defense to detect and respond to cyber threats. Countries are required to build at least accepted minimum security protocols and accreditation schemes for web and mobile applications and systems. Technological advancement in cybersecurity is measured on the quantity of practical mechanisms to ensure cybersecurity
Organization	Organizational measures focus on the national strategy, governance model, and supervisory body for the implementation of cybersecurity development
Capacity building	The capacity building focuses on the education and training to raise awareness, build knowledge regarding cybersecurity and promote the development of qualified professionals, as well as building self-awareness among citizens regarding possible cybersecurity threats
Cooperation	Cooperation measures rely on the partnerships and agreements between various government and private agencies. Greater cooperation enables greater cybersecurity capability and measures the number of partnerships, cooperative frameworks, and information-sharing networks

Table 10 List of countries

Australia	Albania	Peru	Argentina
Belgium	Algeria	Poland	Bangladesh
Canada	Austria	Portugal	China
Denmark	Azerbaijan	Romania	Croatia
Estonia	Bolivia	Russia	Czech Republic
Finland	Bosnia	Saudi Arabia	India
France	Brazil	Serbia	Indonesia
Germany	Bulgaria	Slovakia	Japan
Hungary	Chile	Slovenia	Korea
Ireland	Columbia	Tanzania	Latvia
Italy	Dominican Republic	Ukraine	Lithuania
Lithuania	Egypt	United Arab Emirates	Malaysia
Luxembourg	El Salvador	Uruguay	Malta
Netherland	Georgia	Venezuela	Pakistan
New Zealand	Ghana		Philippines
Spain	Greece		Singapore
Sweden	Jordan		South Africa
United Kingdom	Lebanon		Thailand
United States of America	Mexico		Vietnam
	Moldova		Zambia
	Montenegro		

Table 11 Robust analysis

Dependent Variable: DPU	Model 7
Fixed parts	
Year	0.0423*** (0.009)
Within-effects	
NCSC	- 0.084 (0.101)
GDP	0.004* (0.008)
PCT	-0.203* (0.078)
TR	-0.118* (0.07)
EDU	0.146 (0.19)
INC	-0.086 (0.10)
Between-effects	
NCSC	0.855** (0.32)
IDV	0.002* (0.009)
UAI	-0.002**(0.009)
GDP	-0.005* (0.010)
PCT	0.007 (0.047)
TR	0.184 *** (0.025)
within × between interaction	
NCSC x IDV	0.007** (0.003)
NCSC x UAI	0.009** (0.003)
random parts	
Level 2: country	
0. (intercept) σ^2_{u0}	0.09 ** (0.016)
1. (Year) σ^2_{u1}	0.0006(0.002)
2. (NCSC) σ^2_{u2}	0.079**(0.337)
Level 1: Occasion	
σ^2_e	0.129** (0 0.012)
Log pseudolikelihood	107.86
Observations	228
countries	76
Wald chi2	780.85

Table 12 Definitions of institutional trust (adopted from Smith (2010))

Author	Definition of institutional trust
Zucker (1986)	Institutional trust emerges when "formal mechanisms are used to provide trust that does not rest on personal characteristics or on past history of exchange" (Zucker, 1986, p. 61)
Warren (2018)	Trust in democratic institutions is the trust placed in the institutional norms and the effectiveness of accountability mechanisms. This requires three conditions: (1) institutions are defined by norms that both the truster and trusted know and the trusted is expected to follow; (2) the truster can effectively monitor (or know that others are monitoring) the trustee and (3) the institution has effective accountability mechanisms if the trustee diverges from the norms
O'hara (2004)	Trust in institutions comes from a specific and generally inflexible framework of codes of practice and rules (e.g. impartiality) and the credible threat of sanctions, and the institutions that impose sanctions must have sufficient power and authority
Cook et al. (2005)	Trust in institutions is trust in the "quality of the institutional arrangements within which they operate"
Offe (1999)	"It is this implied normative meaning of institutions and the moral plausibility I assume it will have for others which allows me to trust those that are involved in the same institution – although they are strangers and not personally known to me" (p. 70 emphasis in original)
Giddens (2013)	Trust in modern institutions is trust in the correctness of the abstract systems, emphasizing competence (reliability and credentials) rather than motivation (pp. 33–4, 83–7)
Shapiro (1987)	Institutional trust is the belief that a party has about the security of a situation because of guarantees, safety nets, and other performance structures

Declarations

Conflict of Interest The authors declare that they have no conflict of interest.

References

Al-Okaily, M., Lutfi, A., Alsaad, A., Taamneh, A., & Alsyouf, A. (2020). The determinants of digital payment systems' acceptance under cultural orientation differences: The case of uncertainty avoidance. *Technology in Society, 63*, 101–367.

Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm. *Geo. J. Int'l l., 47*, 12–71.

Bacharach, M., & Gambetta, D. (2001). Trust in signs. In M. S. Cook (Ed.), *Trust in society.* Russell Sage Foundation.

Bagchi, K., Hart, P., & Peterson, M. F. (2004). National culture and information technology product adoption. *Journal of Global Information Technology Management, 7*(4), 29–46.

Bankole, F. O., & Bankole, O. O. (2017). The effects of cultural dimension on ICT innovation: Empirical analysis of mobile phone services. *Telematics and Informatics, 34*(2), 490–505.

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior, 50*, 418–430.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165–176.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly, 35*, 1017–1041.

Bell, A., Fairbrother, M., & Jones, K. (2019). Fixed and random effects models: Making an informed choice. *Quality & Quantity, 53*(2), 1051–1074.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313–324.

Berghel, H. (2000). Identity theft, social security numbers, and the web. *Communications of the ACM, 43*(2), 17–21.

Beugelsdijk, S., & Welzel, C. (2018). Dimensions and dynamics of national culture: Synthesizing Hofstede with Inglehart. *Journal of Cross-Cultural Psychology, 49*(10), 1469–1505.

Cao, X., Yu, L., Liu, Z., Gong, M., & Adeel, L. (2018). Understanding mobile payment users' continuance intention: A trust transfer perspective. *Internet Research, 28*(2), 456–476. https://doi.org/10.1108/IntR-11-2016-0359

Cerić, A., Vukomanović, M., Ivić, I., & Kolarić, S. (2021). Trust in megaprojects: A comprehensive literature review of research trends. *International Journal of Project Management, 39*(4), 325–338.

Chandra, S., Srivastava, S. C., & Theng, Y. L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems, 27*(1), 561–588.

Chang, T. (2014). A Secure operational model for mobile payments. *The Scientific World Journal, 2014*, 14.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management 15*(5/6), 358–368. https://doi.org/10.1108/09576050210447046.

Chien, S.-Y., Lewis, M., Sycara, K., Liu, J.-S., & Kumru, A. (2018). The effect of culture on trust in automation: Reliability and workload. *ACM Transactions on Interactive Intelligent Systems, 8*(4), 1–31.

CISCO (2017). Retrieved January, 2021 from https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html. Accessed 1 April 2020.

Cook, K. S., Hardin, R., & Levi, M. (2005). *Cooperation without trust?* Russell Sage Foundation.

Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Contemporary Research on Payments and Cards in the Global Fintech Revolution, 14*(5), 265–284.

Devos, T., Spini, D., & Schwartz, S. H. (2002). Conflicts among human values and trust in institutions. *British Journal of Social Psychology, 41*(4), 481–494.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy

and the United States. *European Journal of Information Systems, 15*(4), 389–402. https://doi.org/10.1057/palgrave.ejis.3000590.
DiPrete, T. A., & Grusky, D. B. (1990). The multilevel analysis of trends with repeated cross-sectional data. *Sociological Methodology, 20*, 337–368.
Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review, 23*(3), 601–620.
Dzidzah, E., Owusu Kwateng, K., & Asante, B. K. (2020). Security behaviour of mobile financial service users. *Information & Computer Security, 28*(5), 719–741.
European Commission Brussels (2016). Retrieved January, 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0108&rid=2. Accessed 1 April 2020.
Fan, J., Shao, M., Li, Y., & Huang, X. (2018). Understanding users' attitude toward mobile payment use. *Industrial Management & Data Systems, 118*(3), 524. Complementary Index.
Gai, K., Qiu, M., Sun, X., & Zhao, H. (2016). Security and privacy issues: A survey on FinTech. In *International Conference on Smart Computing and Communication* (pp. 236–247). Springer.
Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 33*(3), 38–53.
Gefen, D., & Heart, T. H. (2006). On the need to include national culture as a central issue in e-commerce trust beliefs. *Journal of Global Information Management (JGIM), 14*(4), 1–30.
Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega, 32*(6), 407–424.
Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*, 51–90.
Gefen, D., Rose, G. M., Warkentin, M., & Pavlou, P. A. (2005). Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa. *Journal of Global Information Management (JGIM), 13*(1), 54–78.
Gefen, D., Pavlou, P., Benbasat, I., McKnight, H., Stewart, K., & Straub, D. (2006a). ICIS panel summary: Should institutional trust matter in information systems research? *Communications of the Association for Information Systems, 17*(1), 9.
GFAI. (2019). https://www.ey.com/en_gl/ey-global-fintech-adoption-index, last accessed on April 01, 2020.
GFI. (2011) https://globalfindex.worldbank.org/, last accessed on 01 Apr 2020.
GFI. (2014) https://globalfindex.worldbank.org/, last accessed on 01 Apr 2020.
GFI. (2017) https://globalfindex.worldbank.org/, last accessed on 01 Apr 2020.
Giddens, A. (2013). *The consequences of modernity*. Wiley.
Gurung, A., Luo, X., & Raja, M. K. (2008). An empirical investigation on customer's privacy perceptions, trust and security awareness in E-commerce environment. *Journal of Information Privacy and Security, 4*(1), 42–60.
de Gusmão, A. P. H., Silva, M. M., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management, 43*, 248–260.
Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. (2006). Multivariate data analysis. Uppersaddle River.
Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. *Government Information Quarterly, 21*(4), 406–419.
Harris, P., Rettie, R., & Cheung, C. K. (2005). Adoption and usage of m-commerce: A cross-cultural comparison of Hong Kong and the United Kingdom. *Journal of Electronic Commerce Research, 6*(3), 210–224.
Hinde, S. (1998). Privacy and security—The drivers for growth of E-Commerce. *Computers & Security, 17*(6), 475–478.
Hofstede, G. (1980). Culture and organizations. *International Studies of Management & Organization, 10*(4), 15–41.
Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage publications.
Hofstede, G. (2021). National culture: Dimensions of National Culture. Retrieved January, 2021 from https://geert-hofstede.com/national-culture.html. Accessed 1 April 2020.
Hofstede, G., Hofstede, G., & Minkov, M. (2010). Intercultural cooperation and its importance for survival. In *Cultures and organizations: Software of the mind*. McGraw-Hill.
Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies, 69*(12), 870–883.
Huff, L., & Kelley, L. (2003). Levels of organizational trust in individualist versus collectivist societies: A seven-nation study. *Organization Science, 14*(1), 81–90.
Inglehart, R. (1999). *Trust, well-being and democracy. Democracy and trust* (Vol. 88, pp. 88–120). Cambridge University Press.
ITU Cyber. (2011). https://www.itu.int/pub/D-STR-SECU-2015, last accessed on 01 Apr 2020.
ITU Cyber. (2014). https://www.itu.int/pub/D-STR-GCI.01-2017, last accessed on 01 Apr 2020.
ITU Cyber. (2018). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, last accessed on 01 Apr 2020.
ITU. (2011). https://reports.weforum.org/global-information-technology-2011/. last accessed on 01 Apr 2020.
ITU. (2014). http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf, last accessed on 01 Apr 2020.
ITU. (2017). https://networkreadinessindex.org/wp-content/uploads/2020/03/The-Network-Readiness-Index-2019-New-version-March-2020.pdf, last accessed on 01 Apr 2020.
Kale, S. H., & Barnes, J. W. (1992). Understanding the domain of cross-national buyer-seller interactions. *Journal of International Business Studies, 23*(1), 101–132.
Kalinic, Z., Marinkovic, V., Molinillo, S., & Liébana-Cabanillas, F. (2019). A multi-analytical approach to peer-to-peer mobile payment acceptance prediction. *Journal of Retailing and Consumer Services, 49*, 143–153.
Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2014). Innovation adoption attributes: a review and synthesis of research findings. *European Journal of Innovation Management 17*(3), 327–348. https://doi.org/10.1108/EJIM-08-2012-0083.
Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13–45.
Kim, K., & Hong, S. (2016). The data processing approach for preserving personal data in fintech-driven paradigm. *International Journal of Security and Its Applications, 10*(10), 341–350.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2009a). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. *Information Systems Research, 20*(2), 237–257.
Kim, G., Shin, B., & Lee, H. G. (2009b). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information System Journal, 19*(3), 283–311.

Kim, Y., Choi, J., Park, Y. J., & Yeon, J. (2016). The adoption of mobile payment services for "Fintech." *International Journal of Applied Engineering Research, 11*(2), 1058–1061.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection, 25*, 36–49.

Koenig-Lewis, N., Marquet, M., Palmer, A., & Zhao, A. L. (2015). Enjoyment and social influence: predicting mobile payment adoption. *The Service Industries Journal, 35*(10), 537–554.

Krishna, B., & Krishnan, S. (2020). Explaining variation in adoption of FinTech products and services among citizens: A multilevel model. In Sujeet K. Sharma, Y. K. Dwivedi, B. Metri, & N. P. Rana (Eds.), *Re-imagining diffusion and adoption of information technology and systems: A continuing conversation* (Vol. 617, pp. 541–552). Springer International Publishing.

Krishna, B., & Sebastian, M. P. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Information and Computer Security*. https://doi.org/10.1108/ICS-12-2020-0205

Krishnan, S., Teo, T. S., & Lim, V. K. (2013). Examining the relationships among e-government maturity, corruption, economic prosperity and environmental degradation: A cross-country analysis. *Information & Management, 50*(8), 638–649.

Kusano, K., & Kemmelmeier, M. (2020). Multi-level modelling of time-series cross-sectional data reveals the dynamic interaction between ecological threats and democratic development. *Royal Society Open Science, 7*(3), 191804.

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353–363.

Lebo, M. J., & Weber, C. (2015). An effective approach to the repeated cross-sectional design. *American Journal of Political Science, 59*(1), 242–258.

Lee, J. D., & Moray, N. (1994). Trust, self-confidence, and operators' adaptation to automation. *International Journal of Human-Computer Studies, 40*(1), 153–184.

Lee, S.-G., Trimi, S., & Kim, C. (2013). The impact of cultural differences on technology adoption. *Journal of World Business, 48*(1), 20–29.

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the bright internet. *Journal of the Association for Information Systems, 19*(2), 3.

Lee, J. K., Chang, Y., Kwon, H. Y., & Kim, B. (2020). Reconciliation of privacy with preventive cybersecurity: The bright internet approach. *Information Systems Frontiers, 22*(1), 45–57.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly, 30*, 357–399.

Léon, F., & Zins, A. (2020). Regional foreign banks and financial inclusion: Evidence from Africa. *Economic Modelling, 84*, 102–116.

Leung, K., & Bond, M. H. (2004). Social Axioms: A Model for Social Beliefs in Multicultural Perspective. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 36, pp. 119–197). Elsevier Academic Press. https://doi.org/10.1016/S0065-2601(04)36003-X

Leung, A. K. Y., & Cohen, D. (2011). Within-and between-culture variation: Individual differences and the cultural logics of honor, face, and dignity cultures. *Journal of Personality and Social Psychology, 100*(3), 507.

Lim, K. H., Leung, K., Sia, C. L., & Lee, M. K. (2004). Is eCommerce boundary-less? Effects of individualism–collectivism and uncertainty avoidance on Internet shopping. *Journal of International Business Studies, 35*(6), 545–559.

Liu, J., Kauffman, R. J., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. *Electronic Commerce Research and Applications, 14*(5), 372–391.

Liu, Z., Min, Q., & Ji, S. (2009). An empirical study on mobile banking adoption: The role of trust. In 2009 Second International Symposium on Electronic Commerce and Security (Vol. 2, pp. 7–13). IEEE.

Lu, Y., Yang, S., Chau, P. Y., & Cao, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. *Information & Management, 48*(8), 393–403.

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multidimensional trust and multi-faced risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems, 49*(2), 222–234.

Manoj, V. B. (2011). SMS based secure mobile banking. *International Journal of Engineering and Technology, 3*(6), 472–479.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *The Academy of Management Journal, 38*(1), 24–59.

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*(2), 35–59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359.

Migliore, G., Wagner, R., Cechella, F. S., & Liébana-Cabanillas, F. (2022). Antecedents to the Adoption of Mobile Payment in China and Italy: an Integration of UTAUT2 and Innovation Resistance Theory. *Information Systems Frontiers,* 1–24. https://doi.org/10.1007/s10796-021-10237-2

Milian, E. Z., de Spinola, M. D. M., & de Carvalho, M. M. (2019). Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications, 34,* 100833.

Milliman, R. E., & Fugate, D. L. (1988). Using trust-transference as a persuasion technique: An empirical field investigation. *Journal of Personal Selling & Sales Management, 8*(2), 1–7.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103–125.

Mohr, H., & Walter, Z. (2019). Formation of Consumers' Perceived Information Security: Examining the Transfer of Trust in Online Retailers. *Information Systems Frontiers, 21*(6), 1231–1250.

Mombeuil, C. (2020). An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets. *Journal of Retailing and Consumer Services, 55*, 102127.

Moon, W. Y., & Kim, S. D. (2017). Adaptive fraud detection framework for fintech based on machine learning. *Advanced Science Letters, 23*(10), 10167–10171.

Morosan, C., & DeFranco, A. (2016). It's about time: Revisiting UTAUT2 to examine consumers' intentions to use NFC mobile payments in hotels. *International Journal of Hospitality Management, 53*, 17–29.

Mtaho, A. B. (2015). Improving mobile money security with two-factor authentication. *International Journal of Computer Applications, 109*(7), 9–15.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers, 21*(5), 997–1018.

Mukundan, N. R., & Sai, L. P. (2014). Perceived information security of internal users in Indian IT services industry. *Information Technology and Management, 15*(1), 1–8.

Offe, C. (1999). How can we trust our fellow citizens? Democracy and trust, Cambridge University Press, Cambridge, 52, 42-87.

Official Annual Cybercrime Report (2019). Retrieved January, 2021 from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf. Accessed 1 April 2020.

O'hara, K. (2004). *Trust: from Socrates to spin*. Icon Books.

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.

Oyserman, D., Coon, H. M., & Kemmelmeier, M. (2002). Rethinking individualism and collectivism: Evaluation of theoretical assumptions and meta-analyses. *Psychological Bulletin, 128*(1), 3.

Pal, A., Herath, T., & Rao, H. R. (2021a). Why do people use mobile payment technologies and why would they continue? An examination and implications from India. *Research Policy, 50*(6), 104–228.

Pal, A., Herath, T., De, R., & Rao, H. R. (2021b). Is the convenience worth the risk? An investigation of mobile payment usage. *Information Systems Frontiers, 23*(4), 941–961.

Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics, 58*, 132–145.

Patil, P., Tamilmani, K., Rana, N. P., & Raghavan, V. (2020). Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. *International Journal of Information Management, 54*, 102144.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 667–675.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*, 105–136.

Phonthanukitithaworn, C., Sellitto, C., & Fong, M. W. L. (2015). User intentions to adopt mobile payment services: A study of early adopters in Thailand. *Journal of Internet Banking and Commerce, 20*(1).

Putnam, R. D. (1992). *Making democracy work: Civic traditions in modern Italy*. Princeton University Press.

Qasim, H., & Abu-Shanab, E. (2016). Drivers of mobile payment acceptance: The impact of network externalities. *Information Systems Frontiers, 18*(5), 1021–1034.

Ratnasingam, P. (2004). The role of facilitating conditions in developing trust for successful electronic marketplace participation. *Journal of Internet Commerce, 3*(3), 95–110.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393–404. Chicago

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65–78.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89.

Schwartz, S. H. (1994). Beyond individualism/collectivism: New cultural dimensions of values.

Semerikova, E. (2020). What hinders the usage of smartphone payments in Russia? Perception of technological and security barriers. *Technological Forecasting and Social Change, 161*, 120312.

Senyo, P., & Osabutey, E. L. C. (2020). Unearthing antecedents to financial inclusion through FinTech innovations. *Technovation, 98*, 102155.

Sha, W. (2009). Types of structural assurance and their relationships with trusting intentions in business-to-consumer e-commerce. *Electronic Markets, 19*(1), 43–54.

Shapiro, S. P. (1987). The social control of impersonal trust. *American Journal of Sociology, 93*(3), 623–658.

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. *International Journal of Information Management, 44*, 65–75.

Shi, T. (2001). Cultural values and political trust: a comparison of the People's Republic of China and Taiwan. *Comparative Politics, 33*, 401–419.

Shin, Y. Y., Lee, J. K., & Kim, M. (2018). Preventing state-led cyberattacks using the bright internet and internet peace principles. *Journal of the Association for Information Systems, 19*(3), 3.

Shukla, S. K. (2016, January). Cyber security of cyber physical systems: Cyber threats and defense of critical infrastructures. In 2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID) (pp. 30–31). IEEE.

Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM, 46*(4), 91–94.

Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: Extending UTAUT with innovativeness, risk, and trust. *Psychology & Marketing, 32*(8), 860–873.

Slade, E. L., Williams, M. D., & Dwivedi, Y. K. (2013). Extending UTAUT2 to explore consumer adoption of mobile payments. In Proceedings of the Uk academy for information systems conference. Oxford.

Smith, M. L. (2010). Building institutional trust through e-government trustworthiness cues. *Information Technology & People, 23*(3), 222–246.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly, 30*, 679–704.

Srivastava, S. C., & Teo, T. S. H. (2010). E-Government, E-Business, and National Economic Performance. *Communications of the Association for Information Systems, 26*(1), 14.

Srivastava, S. C., & Teo, T. S. (2009). Citizen trust development for e-government adoption and usage: Insights from young adults in Singapore. *Communications of the Association for Information Systems, 25*(1), 31.

Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization Science, 14*(1), 5–17.

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security, 26*(1), 109–128.

Straub, D. W. (1994). The Effect of Culture on IT Diffusion: E-Mail and FAX in Japan and the US. *Information Systems Research, 5*(1), 23–47.

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.

Takieddine, S., & Sun, J. (2015). Internet banking diffusion: A country-level analysis. *Electronic Commerce Research and Applications, 14*(5), 361–371.

Tam, C., & Oliveira, T. (2019). Does culture influence m-banking use and individual performance? *Information & Management, 56*(3), 356–363.

Thakur, R., & Srivastava, M. (2014). *Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India*. Internet Research.

Traynor, P., Butler, K., Bowers, J., & Reaves, B. (2017). FinTechSec: Addressing the security challenges of digital financial services. *IEEE Security & Privacy, 15*(5), 85–89.

Tsiakis, T., & Sthephanides, G. (2005). The concept of security and trust in electronic payments. *Computers & Security, 24*(1), 10–15.

Tyagi, S. (2019). Cybercrime overwhelming online banking: A Project Management approach's alternative1. PM World Journal. http://www.pmworldjournal.net. Accessed 1 April 2020.

Verba, S., & Almond, G. (1963). *The civic culture: Political attitudes and democracy in five nations*. Princeton University Press.

Walsham, G. (2002). Cross-cultural software production and use: A structurational analysis. *MIS Quarterly, 26*, 359–380.

Wang, N., Shen, X. L., & Sun, Y. (2013). Transition of electronic word-of-mouth services from web to mobile context: A trust transfer perspective. *Decision Support Systems, 54*(3), 1394–1403.

Wang, Z., Zhengzhi Gordon, G. U. A. N., Hou, F., Li, B., & Zhou, W. (2019). What determines customers' continuance intention of FinTech? Evidence from YuEbao. *Industrial Management & Data Systems, 119*(8), 1625–1637. https://doi.org/10.1108/IMDS-01-2019-0011

Warren, M. (2018). Trust and democracy. In E. M. Uslaner (Ed), *The Oxford handbook of social and political trust* (pp. 75-94). Oxford University Press

WBD. (2020). https://data.worldbank.org/indicator/NY.GDP.PCAP.CD. last accessed on 01 Apr 2020.

Xin, H., Techatassanasoontorn, A. A., & Tan, F. B. (2013). Exploring the influence of trust on mobile payment adoption. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Jeju Island, Korea.

Yang, G., Mao, Y. (2011). A research on the model of factors influencing consumer trust in mobile business. International Conference on E-Business and E-Government (ICEE), p. 1–5, IEEE.

Yeh, H. (2020). Factors in the ecosystem of mobile payment affecting its use: From the customers' perspective in Taiwan. *Journal of Theoretical and Applied Electronic Commerce Research, 15*(1), 0–0.

Yu, C. S. (2012). Factors affecting individuals to adopt mobile banking: Empirical evidence from the UTAUT model. *Journal of Electronic Commerce Research, 13*(2), 104.

Zhang, J., Liu, H., Sayogo, D. S., Picazo-Vela, S., & Luna-Reyes, L. (2016). Strengthening institutional-based trust for sustainable consumption: Lessons for smart disclosure. *Government Information Quarterly, 33*(3), 552–561.

Zhang, L., Zhu, J., & Liu, Q. (2012). A meta-analysis of mobile commerce adoption and the moderating effect of culture. *Computers in Human Behavior, 28*(5), 1902–1911.

Zheng, X., Lee, M., & Cheung, C. M. (2017). *Examining e-loyalty towards online shopping platforms: The role of coupon proneness and value consciousness*. Internet Research.

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior, 26*(4), 760–767.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior, 8*, 53–111.

Ben Krishna is a doctoral student in the Information Systems Area at the Indian Institute of Management (IIM) Kozhikode. His research interest includes Information Security behavioral research (information security compliance, trust in security and privacy-enhancing systems, cyber hygiene), financial technology and service adoption and usage (financial access and inclusion, linking security behavior and usage of digital payments, security policies and digital payment adoption) and sustainability. He has published in reputed journals such as Information and computer security, International Journal of Management and Enterprise Development, and preeminent conferences, including the Decision Science annual conference, International Federation for Information Processing (IFIP). He has served as a reviewer in journals and conferences such as the Information Systems Frontiers, Internet Research, Government Information Quarterly, Academy of Management (AOM) Annual Conference, International Conference on Information Systems (ICIS), Pacific Asia Conference on Information Systems (PACIS) and IFIP.

Satish Krishnan received his PhD in Information Systems from the National University of Singapore. He is the Chair Associate Professor of Information Systems at the Indian Institute of Management (IIM) Kozhikode. His research includes IT resistance, fake news and disinformation, gender gap, e-government, e-business, virtual social networks, technostresscyberloafing, and cyberbullying. He has published in leading journals, such as the Journal of Applied Psychology, Organizational Behavior and Human Decision Processes, Information and Management, Information Systems Frontiers, Journal of Association for Information Science and Technology, International Journal of Information Management, Computers in Human Behavior, Human Resource Development Review, Journal of Global Information Technology Management, e-Service Journal, and others. He is on the editorial boards of various journals such as Internet Research, Technological Forecasting and Social Change, Information Systems Frontiers, International Journal of Information Management, and Computers in Human Behavior. He also serves at various conferences such as PACIS and ICIS as Track Chair or Review Coordinator or Associate Editor. He won the Outstanding Associate Editor Award for ICIS 2017 and 2019.

M. P. Sebastian is a Professor of Information Systems at the Indian Institute of Management Kozhikode for more than one decade. He received his masters and Ph.D. from the Indian Institute of Science, Bangalore. His research topics include Cybersecurity, AI, Machine learning, Text Analytics, Healthcare IS, and Enterprise Information Systems. He published articles in journals such as Information and Computer Security, Health Policy and Technology, Asia Pacific Journal of Health Management, Clinical Governance, International Journal of Electronic Government Research, Computers and Electrical Engineering, Knowledge and Information Systems, Evolving Systems, etc. He served as a reviewer for journals such as Nature Communications, Government Information Quarterly, and the International Journal of Medical Informatics.