International Journal of Safety and Security Engineering
Vol. 15, No. 4, April, 2025, pp. 631-641
Journal homepage: http://iieta.org/journals/ijsse

# Security of Personal Information in Electronic Payments: A Bibliometric Analysis and Model Extension

Yuqing Guan[1*], Andrea Tick[2]

[1] Doctoral School of Safety and Security Sciences, Obuda University, Budapest 1088, Hungary
[2] Keleti Karoly Faculty of Business and Management, Obuda University, Budapest 1084, Hungary

Corresponding Author Email: guan.yuqing@uni-obuda.hu



https://doi.org/10.18280/ijsse.150401

**Received:** 27 January 2025
**Revised:** 10 April 2025
**Accepted:** 21 April 2025
**Available online:** 30 April 2025

***Keywords:***
*electronic payments, personal information, bibliometric analysis, UTAUT, VOSviewer*

**ABSTRACT**

The global rise in the use of electronic payments highlights the growing importance of personal information security in this domain. Scholars have explored various aspects of this issue, including payment systems, technological implementations, user acceptance, behavior, and psychological factors. This study aims to identify research gaps and future trends in personal information security in electronic payments through bibliometric analysis. Data was sourced from the Scopus and Web of Science databases, covering the period from 1974 to 2023. The dataset was analyzed using VOSviewer and R-Bibliometrix (Biblioshiny) software. The co-occurrence network output indicates that future research should focus on clusters with lower density and central positions, such as user acceptance of new technologies, consumer behavior, user trust, and user satisfaction with electronic payments. The R-Bibliometrix (Biblioshiny) thematic map identified research gaps across four quadrants: motor themes, niche themes, emerging or declining themes, and basic themes. The study proposes potential research areas in personal information security in electronic payments and develops an extended UTAUT (Unified Theory of Acceptance and Use of Technology) model tailored to this field. The study identifies trust and technology acceptance as critical themes and extends the UTAUT model to incorporate personal information security cognition.

## 1. INTRODUCTION

With the acceptance of online banking and online shopping, electronic payment methods have grown significantly in recent years. An electronic funds transfer is the electronic transfer of money between buyers and merchants. Millions of people make online purchases every day [1]. Electronic payment systems improve people's overall quality of life by providing a practical means of conducting transactions [2].

People are facing increasing risks, like identity theft, phishing attacks, and data breaches, as the use of electronic payment increases [3]. In order to obtain sensitive information, swindlers impersonate providers, which may result in fund transfers [4]. They create phishing websites that resemble established official platforms [5]. Cyber attackers usually use different IP addresses to mask their activities [6]. More and more people have increased concerns about private information leaking while using mobile payment applications [7].

Consumers need to know the security measures in electronic payments. So many scholars have started researching problems about privacy and security. This study uses bibliometric analysis to recognize research gaps and finally build a research framework by some key theories as the foundation. The bibliometric analysis can understand the trends of research topics through document metadata, such as authors, keywords, and citations [8, 9]. In this study， we use co-keyword and co-citation analysis to assess research directions and themes. Using this method, we can better understand the development of the research topic [10, 11]. Nowadays, a lot of research areas like social entrepreneurship, crowdfunding, entrepreneurship education, borrower behavior, and SMEs' perceptions of cloud services are using R-Bibliometrix (Biblioshiny) and VOSviewer for bibliometric analysis [12-15].

In order to develop a theoretical model, this study uses bibliometric analysis to identify key topics and trends in the security of personal information in electronic payments. To effectively analyze these publications, we offer the following research questions:

RQ1: Based on the quantity of publications, what are the key topics in personal information security in electronic payments?

RQ2: What are the research trends in personal information security in electronic payments?

RQ3: What theoretical model is finally established?

The study is organized as follows: Section 2 introduces and discusses the research data, methods, and software. Section 3 presents the ten most influential articles. Section 4 showcases the research findings. Section 5 develops the theoretical model. Section 6 provides the discussion. Section 7 presents conclusions and limitations.

## 2. MATERIALS AND METHODS

This study chose bibliometric analysis to investigate research gaps in personal information security in electronic payments. As Osareh [16] suggests, this method can monitor and evaluate the progress in "science" and "technology". VOSviewer and Biblioshiny were used by researchers to examine the most popular journals, topics, authors, institutions, and research areas, as well as overall trends in publication [17, 18].

The Web of Science and Scopus databases were used to gather data for this study because they have a lot of relevant peer-reviewed papers and conference proceedings. They also allow the export of high-quality metadata, including author affiliations, keywords, citations, and abstracts. This data is essential for conducting bibliometric analysis using tools. Since some data appeared in both databases, we reviewed all entries based on title, authors, publication year, and journal source, and removed any duplicates. The preliminary search revealed that literature related to electronic payments and personal information security began to appear in the mid-1970s.

As of 2023, a search using the keywords ("Electronic Payment") OR ("E-payment") OR ("Electronic Commerce" OR "E-commerce") AND ("Personal Information" OR "Personal Info") AND ("Security" OR "Safety") in the Web of Science and Scopus database yielded 5,865 publications. These were downloaded in Tab-delimited, CSV, and BibTeX formats for processing with VOSviewer and Biblioshiny to visualize research trends.

VOSviewer is a visualization tool widely used in bibliometric studies. It helps us efficiently gather literature and establish relationships between selected publications within a chosen scope [19]. VOSviewer constructs networks based on co-authorship, co-occurrence, citation, bibliographic coupling, and co-citation, and displays them using network, overlay, or density views [20, 21]. It enables efficient mapping and clustering of related literature [22].

Biblioshiny, powered by Bibliometrix, offers a user-friendly, web-based interface coded in R. It supports data from Web of Science, Scopus, and Dimensions [18, 23]. Using R-Bibliometrix (Biblioshiny) software allows for a comprehensive assessment of these publications.

One of its features, the Thematic Map, visualizes research themes based on centrality (external connectivity) and density (internal development) [23, 24].

The themes can be written into four groups [25]:

(1) Motor themes (quadrant Q1): The research field's development is driven by central and well-developed themes.

(2) Niche themes (quadrant Q2): Specialized but peripheral topics with limited relevance to the core field.

(3) Emerging or declining themes (quadrant Q3): Underdeveloped themes with low centrality, indicating either new or fading topics.

(4) Basic themes (quadrant Q4): Fundamental but not yet well-developed themes for the field.

The themes in the motor quadrant will be the focus of our research.

## 3. MOST INFLUENTIAL PUBLICATION

The number of citations that a publication obtains influences its impact. To better understand the dynamics that exist in this field, the most influential publications on personal information security in electronic payments. Table 1 shows the top ten most referenced articles in this scientific topic (based on the Web of Science and Scopus downloaded dataset).

**Table 1.** Most cited articles on security of personal information in electronic payments

| Document Title | Ref. | Journal Title | Total Citation |
|---|---|---|---|
| Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model from Bitcoin | [26] | Information Systems Research | 2218 |
| An extended privacy calculus model for e-commerce transactions | [27] | Information Systems Research | 1721 |
| Information privacy research: An interdisciplinary review | [28] | MIS Quarterly: Management Information Systems | 1515 |
| The impact of initial consumer trust on intentions to transact with a web site: a trust building model | [29] | The Journal of Strategic Information Systems | 1081 |
| An overview of online trust: Concepts, elements, and implications | [30] | Computers in Human Behavior | 674 |
| Technology acceptance model for wireless Internet | [31] | Internet Research | 625 |
| The impact of customer trust and perception of security control on the acceptance of electronic commerce | [32] | International Journal of Electronic Commerce | 418 |
| Research report: Richness versus parsimony in modeling technology adoption decisions-understanding merchant adoption of a smart card-based payment system | [33] | Information Systems Research | 322 |
| Beyond concern - a privacy-trust-behavioral intention model of electronic commerce | [34] | Information & Management | 252 |
| An empirical study of customers' perceptions of security and trust in e-payment system | [35] | Electronic Commerce Research and Applications | 235 |

The results show that the article by Malhotra et al. [26] is the most influential, with 2,218 citations. Malhotra et al. [26] identified consumer distrust in information privacy as an important challenge to the development of online commerce. In addition, it proposes the IUIPC framework, which is based on social contract theory, to explain a substantial amount of variation in behavioral intentions and analyzes how online customers behave to several privacy concerns on the web.

Information privacy has drawn increasing attention from stakeholders such as businesses, governments, and consumers. Jeff Smith et al. [28] conducted an interdisciplinary review of 320 articles and 128 books, categorizing existing research into conceptualizations of privacy, its relationships with other constructs, and the links among these factors.

The research by Dinev and Hart [27] aims to understand better the challenging of balancing between privacy risk perceptions and views of trust and temptation, which affect the motivation to provide personal information for transactions on the internet. Dinev and Hart [27] developed a theoretical model based on privacy calculus, analyzing data from 369 respondents.

The study finds that while issues with privacy reduce users' willingness to give personal data, trust as well as perceived benefits can offset these concerns.

Insufficient trust continues to be highlighted as one of the most significant barriers to individuals engaging in e-commerce. Without a pervasive atmosphere of online confidence, the coming days of online shopping will be precarious [30].

Many researchers have begun developing trust models to study the degree of trust people have in participating in e-commerce activities. Harrison McKnight et al. [29] proposed a trust model based on structural assurances (i.e., consumers' views about internet security), seller reputation, and website quality, which are all having a significant influence on buyer trust and engagement in online commerce.

The theory of reasoned action (TRA) has long served as a foundation for forecasting behavioral motives and behaves. Liu et al. [34] examined how individuals' privacy perceptions affect their intention to conduct online transactions.

Articles based on the Technology Acceptance Model (TAM) have also proven important. Lu et al. [31] adapted the Technology Acceptance Model (TAM) to wireless Internet, finding that personal traits, perceived usefulness, and trust in the wireless environment drive adoption. Suh and Han [32] and Plouffe et al. [33] used the TAM model to analyze the consumer acceptance on online shopping and the use of a smart card-based payment system.

It is widely thought that excellent protection can enhance trust and that both high security and a sense of trust will eventually expand the application of online commerce. Customers' opinions of electronic payment system security are now important for the market's success [35].

These ten influential articles analyze people's perception of privacy, their trust in the security of personal information in electronic payments, and their acceptance of technology. These articles show that, as e-commerce, mobile payments, and digital currencies have grown in popularity, there has been an increasing concern in the security of personal information in electronic payments. Current impactful research on personal information security in electronic payments includes studies that use trust models, the Technology Acceptance Model (TAM), and behavioral theories to investigate the willingness of individuals and behavior about the use of electronic payments and e-commerce [36, 37].

## 4. RESULTS OF THE BIBLIOMETRIC ANALYSIS

This section shows the key results from the bibliometric analysis worked on the selected dataset. This analysis covers several dimensions, including publication trends over time, frequently referenced journals and keyword co-occurrence. These findings give an in-depth analysis of the research landscape, highlighting the current trends and future directions in personal information security in electronic payments. Table 2 lists the number of publications for each year.

**Table 2.** Number of publications by year

| Years | Number of Publications |
|---|---|
| 1974-1983 | 2 |
| 1984-1993 | 9 |
| 1994-2003 | 239 |
| 2004-2013 | 1667 |
| 2014-2023 | 3948 |
| Total | 5865 |

As depicted in Figure 1, there has been an exponential trend in the number of publications from 1974 to 2023.

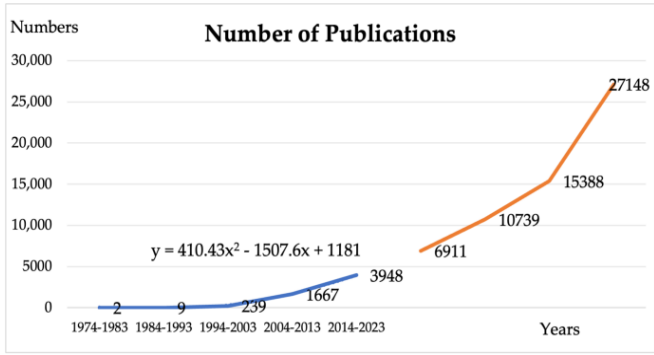


**Figure 1.** Trends in the number of publications

The growth in publications is largely driven by advancements in electronic payment technologies, particularly the rise of mobile payments in the early 21st century [38]. The COVID-19 pandemic further accelerated this trend, as digital payments became mainstream and governments promoted them to support economic recovery and digital transformation [39]. This also motivated researchers to further explore the field, leading to a significant surge in publications. Future publication numbers are expected to keep rising, fueled by technological progress, digitalization, and policy support.

Table 2 shows that the number of publications from 2004 to 2013 is more than doubled from 1974 to 2003. The number of publications from 2014 to 2023 is approximately twice that of the publications from 2004 to 2013. The large increase in the number of publications between 1974 and 2023 shows researcher's' keen interest in the security of personal information in electronic payments. The growth trend observed in Figure 1 suggests that research on the security of personal information in electronic payments will increase from 2024 to 2033, leading to a higher number of publications.

The study investigated various documents related to the security of personal information in electronic payments. Table 3 lists publications on the security of personal information in electronic payments according to document type. Table 3 presents publication types. Articles account for 46%, followed by conference papers at 25%. Other types include editorials, book chapters, notes, books, data papers, and letters.

**Table 3.** Publications by document type

| Document Type | Number of Publications | Percentage of Total Publications (%) |
|---|---|---|
| Article | 2707 | 46 |
| Conference Paper | 1443 | 25 |
| Review | 114 | 2 |
| Other | 1601 | 27 |
| Total | 5865 | 100 |

Figure 2 illustrates the most cited sources related to "the security of personal information in electronic payments". The most cited source is Lecture Notes in Computer Science, with 1083 citations, followed by Management Information Systems Quarterly with 660 citations, Communications of the ACM with 366 citations, and Information Systems with 344 citations. The least cited source is Quantum Information Processing, cited 149 times.

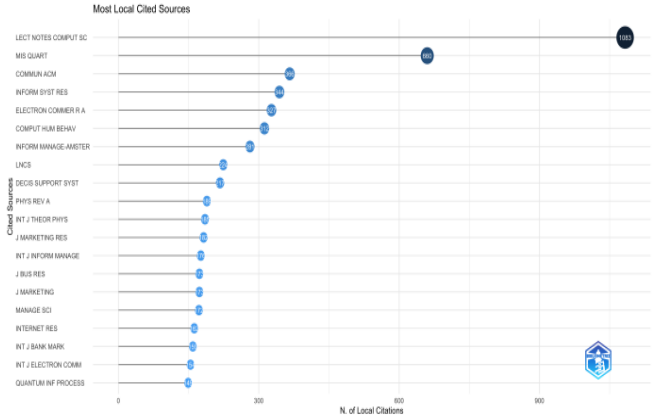


**Figure 2.** Most local cited source

Journal influence on personal information security research is reflected not only by publication count but also by impact, measured through the H-index and visualized using shades of blue in Figure 3. The deeper the blue color in the figure, the greater the journal's impact and H-index. The data reveals that Computers in Human Behavior is a top-tier journal with an H-index value of 45 (as indicated by the deepest blue color). This indicates that this journal has the highest H-index compared to others. Meanwhile, there are two journals with the lowest H-index of 11, as indicated by the lighter blue in Figure 3.

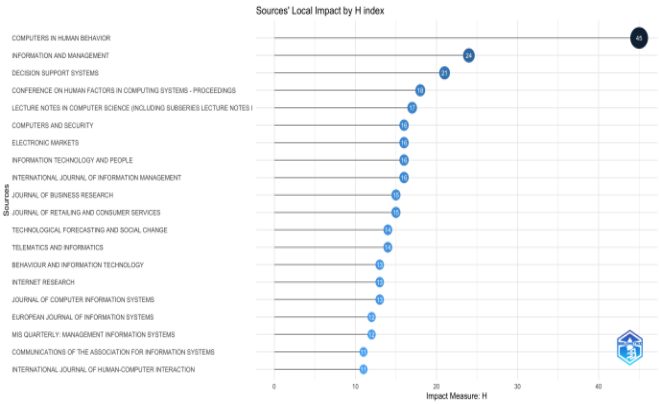


**Figure 3.** Sources' local impact by H-index

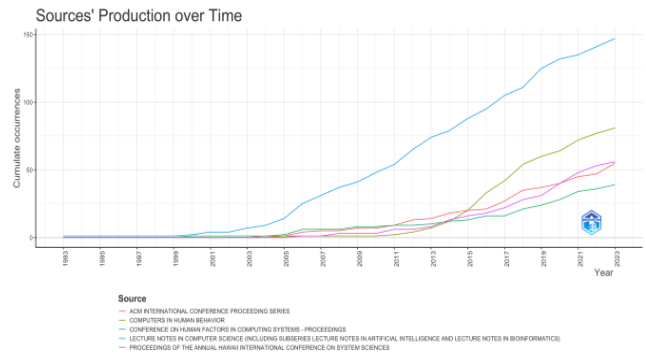


**Figure 4.** Sources' production over time

The growth of journals publishing research on personal information security in electronic payments from 1993 to 2023 is illustrated in Figure 4. The figure depicts the growth of journals over the research period in a curved manner. From Figure 4, a steady rise in publication volume began around 2005. Lecture Notes in Computer Science (blue line) shows the most consistent and rapid growth, followed by Computers in Human Behavior.

Figure 5 illustrates the Scientific Production of various countries regarding "the security of personal information in electronic payments". The USA tops in scientific output, having 2175 publications, represented by the deepest shade of blue in Figure 5. Following closely is China with 1064 publications. Next in rank are the UK (538), Germany (510), and India (346).

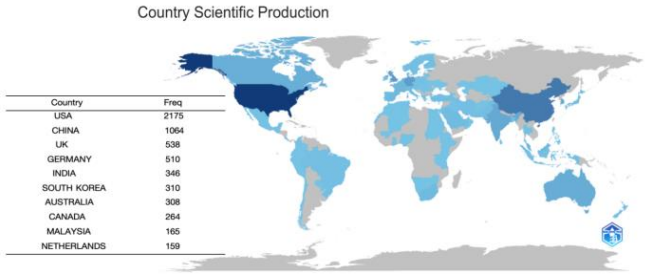


**Figure 5.** Countries' scientific production (Summarized by R-Bibliometrix (Biblioshiny) software)

Using VOSviewer to analyze the Scientific Production of various countries regarding "the security of personal information in electronic payments". Figure 6 shows the correlation of bibliography with countries as a component of analysis. As shown in Figure 6, around 2012, the initial research on the security of personal information in electronic payments was primarily concentrated in European countries like Germany, Switzerland, and the Netherlands. By 2014, China and the USA made significant contributions to the security of personal information in electronic payments.

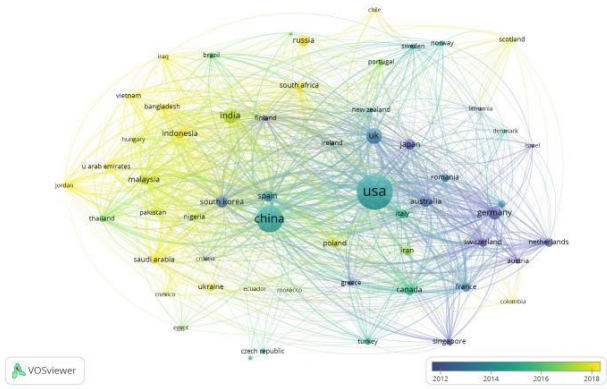


**Figure 6.** The cluster of countries overlay visualization

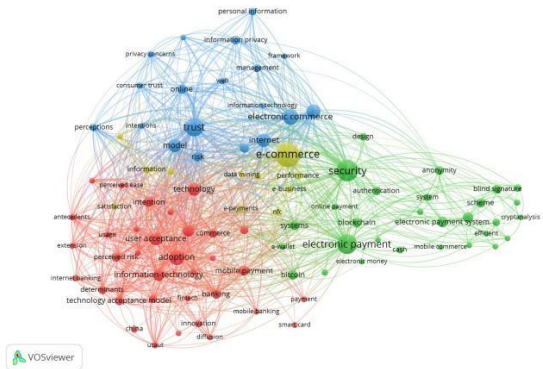


**Figure 7.** The cluster of keywords network visualization

After 2018, research on the security of personal information in electronic payments became prevalent worldwide, with many Asian and European countries joining the research efforts.

Figure 7 represents a network visualization of keyword occurrences in scientific publications. The word cloud displays the frequency with which each keyword appears in the publications, as well as the relationships among keywords. In the network, every keyword can be seen by a circle, the size of which is proportional to the frequency with which the keyword found in publications. Each color represents a cluster of keywords that are merged together, with the length of the curves indicating the approximate connections between keywords, and the thickness of the curves representing the strength of the corresponding topic area or keyword pair. Clusters represent relationships between one topic and another.

The keyword filtering process involved setting a repetition rate to 10, resulting in the selection of 93 keywords from a pool of 4130 keywords, which were then divided into 4 clusters. The colors of the 4 clusters are respectively red, green, blue, and yellow, highlighting different aspects of research within electronic payment security.

Table 4 captures the focus areas of each cluster, emphasizing the role they play in technology acceptance and user behavior in financial technologies, cryptographic security and protocols in electronic payment systems, trust and privacy in information security for electronic payments, and data mining and fraud detection in electronic payment systems.

**Table 4.** Keyword clusters

| Cluster | Color | Keywords | Description |
|---|---|---|---|
| Technology Acceptance and User Behavior in Financial Technologies | Red | Technology Acceptance Model (TAM), UTAUT, perceived usefulness, perceived ease of use, behavior, intention, customer satisfaction, perceived risk, perceived security, FinTech, innovation, mobile payment, online banking, internet banking, mobile banking | This cluster explores electronic payment systems' acceptance, adoption, and user behavior. It covers technology acceptance theories, customer behavior, perceived security, and risk in financial technologies like FinTech, online, and mobile payments. |
| Cryptographic Security and Protocols in Electronic Payment Systems | Green | Cryptography, elliptic curve cryptography, quantum cryptography, blind signature, signcryption, cryptanalysis, anonymity, authentication, electronic cash, electronic money, e-wallet, blockchain, bitcoin, cryptocurrency, security, scheme, protocol | This cluster focuses on the security of electronic payment systems, covering encryption technologies, anonymity, authentication, blockchain technologies, and payment protocols. It emphasizes system design, cryptographic measures, and emerging digital currencies and protocols. |
| Trust and Privacy in Information Security for Electronic Payments | Blue | Consumer trust, privacy, information privacy, personal information, self-disclosure, risk, perceptions, management, information technology, internet, web, framework, model | This cluster centers around trust, privacy, and information security in electronic payments. It deals with user concerns over personal data protection, privacy, and how risks are perceived and managed through security frameworks and technological solutions. |
| Data Mining and Fraud Detection in Electronic Payment Systems | Yellow | Data mining, NFC, fraud detection, attitudes, satisfaction | This cluster addresses the importance of data mining for fraud detection, secure transaction technologies (such as NFC), and maintaining user trust and satisfaction in e-commerce platforms and electronic payment systems. |

Figure 8 highlights the research depth in these areas, with more concentrated colors indicating higher research activity. Key topics include e-commerce, electronic payments, user trust, and the Technology Acceptance Model (TAM).

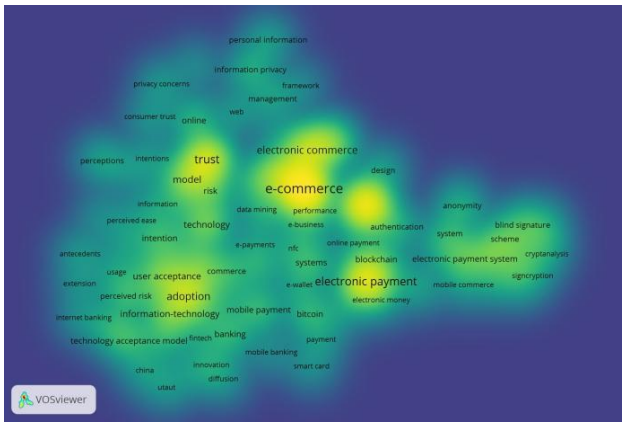


**Figure 8.** The cluster of keywords density visualization

Figure 9 shows the results of the analysis performed with R-Bibliometrix (Biblioshiny). The appearance of topics is represented by the frequency of keywords found in publications related to the security of personal information in electronic payments.

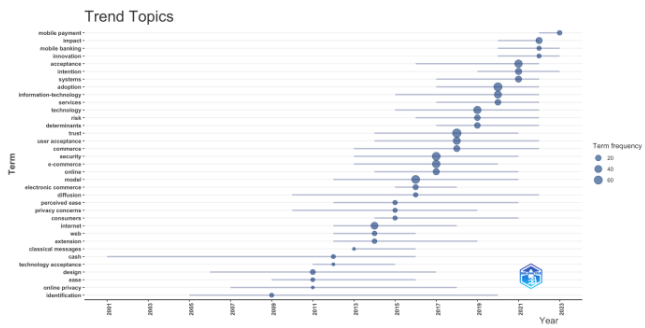


**Figure 9.** Trend topic

A higher number indicates a higher frequency of keyword usage. Additionally, the further right (closer to recent years), the keywords were used more recently. From Figure 9, it can be observed that in 2014, there was a primary discussion about consumers. In 2016, the focus shifted to online. In 2017, discussions cantered around e-commerce and security. In 2020, discussions involved information technology and adoption. By 2023, the discussion turned to mobile payment.

The trend indicates that topics related to human behavior and psychology have been consistently present over these years. For instance, in 2011, publications mainly focused on the theme of technology acceptance [40]. In 2015, the primary discussion revolved around perceived ease [41]. In 2017, the focus shifted to user acceptance [42]. In 2021, the main discussion centered around intention and acceptance [43]. In 2022, the focus was on the impact [44]. The evolution of this range of topics not only reflects a change in research focus but also reveals a continuing focus on key topics in the field of security of personal information in electronic payments. Figure 10 will show the future research direction.

From Figure 10, it can be observed that the motor themes consist of keywords are the focus of future research.

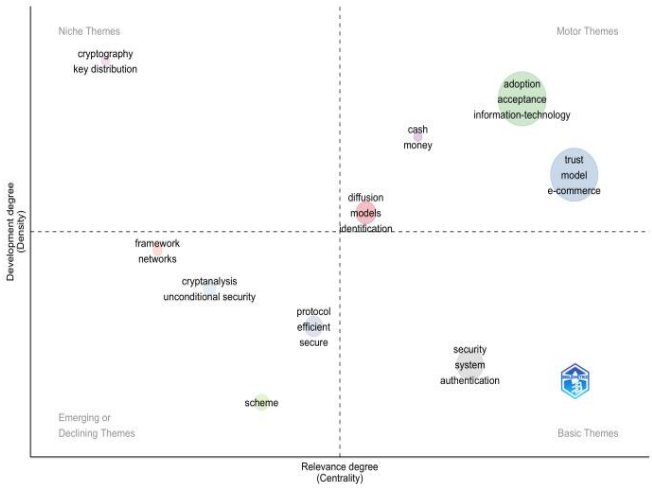


**Figure 10.** Thematic map

## 5. THEORETICAL MODEL

The fundamental UTAUT model by study [45] includes four core constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions, as well as four moderating factors: gender, age, experience, and voluntariness of use, as shown in Figure 11.

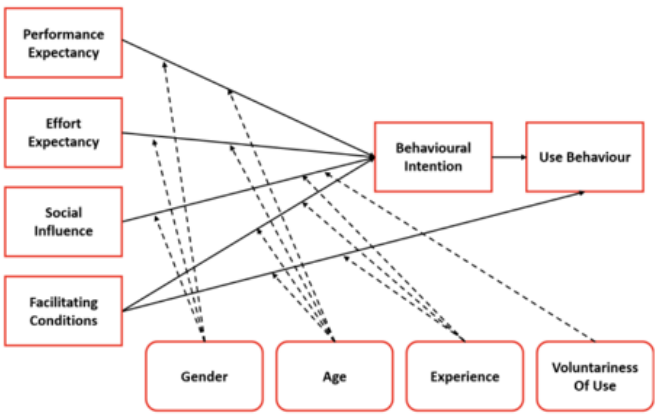


**Figure 11.** UTAUT [45]

UTAUT2 (Figure 12), developed by study [46], is an extension of the original Unified Theory of Acceptance and Use of Technology (UTAUT) model. It includes extra dimensions relating to consumer market factors that influence behavioral intentions to use new technology.

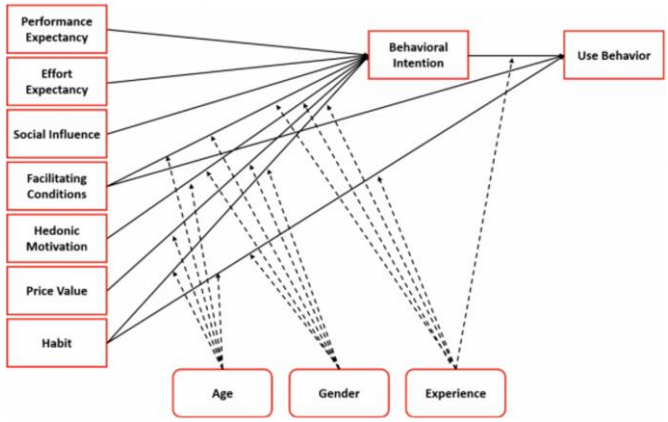


**Figure 12.** UTAUT2 [46]

Although the UTAUT and UTAUT2 models have become commonly employed to explain technology adoption, they have limitations when applied to personal information security in electronic payments. Neither model explicitly includes factors related to users' perceptions of personal information security or privacy risks. These perceptions are crucial in electronic payments, where trust, risk, and data protection are central to user acceptance.

As shown in Figure 12, although UTAUT2 adds factors like hedonic motivation and price value, these relate more to consumer satisfaction and cost perception than to security concerns. Performance expectancy and facilitating conditions also fail to address security-related issues. Users may still reject technologies they perceive as insecure, even if those technologies are high-performing or easy to use [47]. To address this limitation, this study introduces a new factor: Personal Information Security Cognition (PISC), which captures users' awareness, concerns, and trust regarding personal information security in electronic payment systems. This enhancement better shows how security cognition influences user intentions and behaviors.

The link between perceived information security and technology adoption can be understood through various theoretical frameworks. The Technology Acceptance Model (TAM) combines usability and utility with trust and security perceptions. Pavlou [48] argues that perceived security enhances trust, which in turn influences perceived utility and simplicity of use. The Protection Motivation Theory (PMT) explains how motivations to protect against security threats shape behavior, considering perceptions of threat severity, vulnerability, and coping [49, 50]. In this study, PMT takes a theoretical approach to studying how users assess the security of personal information in electronic payment systems and what motivates them to adopt protective measures. The Unified Theory of Acceptance and Use of Technology (UTAUT) incorporates security perception for a moderating variable that influences basic constructs like performance expectancy and effort expectancy [46]. According to research, stronger security perceptions increase the components' favorable impact on behavioral intention to utilize electronic payment systems. An extended UTAUT model will be constructed, as depicted in Figure 13.

In the extended UTAUT model, the key components include:

(1) Performance Expectancy (PE) means users' perceptions of how electronic payment technologies can enhance their professional or personal efficiency.

(2) Effort Expectancy (EE) means how users' perception of the ease or difficulty of using electronic payment technology.

(3) Social Influence (SI) relates to the perceived pressure from others to use electronic payment technology.

(4) Facilitating Conditions (FC) describes users' perception of environmental and resource support when using electronic payment technology.

(5) Habit (HB) relates to users' automatic actions or inertia when using electronic payment technology.

(6) Personal Information Security Cognition (PISC) refers to users' awareness and trust in electronic payment technology to protect their personal information.

(7) Demographic factors such as gender, age, and experience may influence other relationships.

(8) Behavioral Intention relates to the intention to use the technology.

(9) Use Behavior is how the technology truly used.

These components provide a framework for analyzing users' acceptance of electronic payment technology, taking consideration of usability and security perceptions.

Relationships between key components:

(1) Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI) → Behavioral Intention: Perceptions of usefulness, ease of use, and social influence positively affect intention.

(2) Facilitating Conditions (FC) → Behavioral Intention and Usage Behavior: Adequate support leads to increased behavioral intention and usage.

(3) Habit (HB) → Behavioral Intention: Users' regular use of the technology affects their intention to use it.

(4) Behavioral Intention → Usage behavior: Intention leads to actual use.

(5) Personal Information Security Cognition (PISC) → Behavioral Intention: Security awareness and trust affect willingness to adopt the technology.

(6) Age, Gender, Experience: These moderate the strength of other relationships. For instance, younger users may be more influenced by performance expectancy.

In Figure 13, dashed lines indicate moderation effects. For example, age may influence how strongly Performance Expectancy affects intention.

This model seeks to capture the complicated relationships that influence technology acceptance and usage. By understanding these relationships, organizations can better design, implement, and support electronic payment technologies to enhance user acceptance and usage rates.

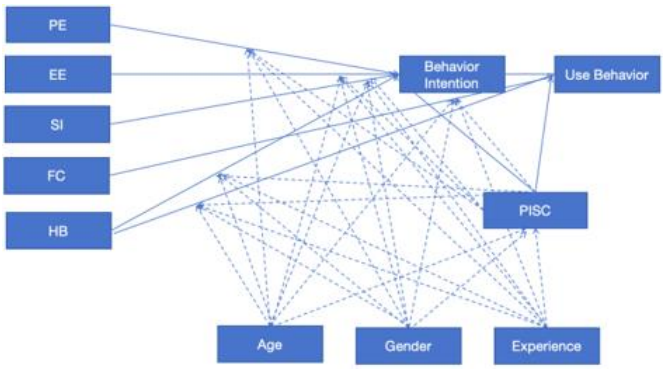


**Figure 13.** Author's extended UTAUT model

This extended model can link the creation of research theories and surveys for upcoming research. A validated questionnaire can be used to assess a users' level of security awareness [51]. The extended UTAUT model integrates theoretical foundations from the Protection Motivation Theory (PMT), the Technology Acceptance Model (TAM), the Theory of Reasoned Action (TRA), and Social Contract Theory (SCT) to create the survey items. A pilot study will then be conducted with a small sample of participants. Their responses will be analyzed, and the reliability of the items will be assessed using Cronbach's alpha. Exploratory Factor Analysis (EFA) or Confirmatory Factor Analysis (CFA) will be employed to verify the components of the UTAUT model. This method provides a deeper understanding of how users' perceptions of security influence their behavior.

## 6. DISCUSSION

The Unified Theory of Acceptance and Use of Technology (UTAUT) used in research on technology adoption across various fields. Venkatesh et al. [52] investigated the adoption of electronic medical records (EMRs) in the United States, emphasizing the roles of facilitating conditions and social influence. Gagnon et al. [53] identified that performance expectancy and effort expectancy significantly influence the adoption of telemedicine by both patients and providers. Šumak et al. [40] found the students' intentions for using E-learning platforms are affected by performance expectancy and effort expectancy, with social influence as a moderating factor. Thomas et al. [54] reported that facilitating conditions and effort expectancy are crucial for adopting mobile learning tools among university students. Zhou et al. [55] applied UTAUT to mobile banking, highlighting performance expectancy and social influence as key predictors. Oliveira et al. [56] emphasized that perceived security and facilitating conditions have a substantial impact on users' intentions for using online payment systems. Shareef et al. [57] indicated that performance expectancy and effort expectancy are essential for citizens' acceptance of e-government services. Luthra et al. [58] found that social influence and facilitating conditions are critical for adopting smart city technologies. Pavlou [48] integrated UTAUT with perceived risk and trust, showing that core UTAUT constructs interact with these factors to influence online shopping behavior. Javornik [59] indicated that performance expectancy and perceived enjoyment are important factors in the adoption of Augmented Reality (AR) in purchasing.

Omar et al. [60] developed a comprehensive UTAUT model for investigating the use of smart tourism technologies, incorporating privacy and security threats as moderators. This study found that performance expectancy, effort expectancy, and facilitating conditions can improve behavioral intention, but the threats of privacy and security can reduce behavioral intention. Rana et al. [61] added the trust and privacy in UTAUT model to study the application of AI in education for undeveloped countries. This study found that privacy and trust influence people's adoption of AI technologies. An extended UTAUT model used by Trkman et al. [62], examing the users' adoption intentions toward proximity tracking apps (PTAs) in e-government. This model showed how privacy concerns and trust in government and technology impacted adoption intentions. Reith et al. [63] used the UTAUT model to study fitness tracker adoption. This study found that privacy concerns are key factors influencing user behavioral intention.

The above studies show that the extended UTAUT model is a good tool for researching technology adoption in various fields. Adding the variables, including trust, perceived security, risk, and enjoyment to the model can flexible investigation of

technology adoption processes.

Nowadays, privacy protections are very important for electronic payment systems. The security of personal data is a key factor in building consumers' trust, because it can improve the adoption of electronic payments [64]. Users avoid electronic payment systems because they fear the risks associated with personal information exposure. Adoption rates decrease when users perceive higher risks [65]. Security measures that are robust help decrease potential threats and boost system adoption rates.

Compliance with privacy regulations, including the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States, is essential. These standards when followed protect user information and make electronic payment systems more trustworthy and widely accepted [66]. Cejas et al. [67] analyzed privacy concerns that emerged from GDPR regulations in mobile applications. The evaluation demonstrated that although GDPR established strict data protection standards numerous mobile applications violate compliance requirements which produces rising user privacy concerns. The gap between regulatory requirements and actual practices affects users' trust and their willingness to adopt new mobile technologies. Awareness and understanding of GDPR provisions influence users' trust in and willingness to engage with digital services. Privacy regulations have a big impact on technology adoption behavior [68]. Therefore, ensuring the security of personal information is a necessary condition for users to embrace and maintain applying electronic payment systems.

## 7. CONCLUSIONS

This study employed bibliometric analysis. The study searched the Web of Science and Scopus databases for works on personal information security in electronic payments from 1974 to 2023. The study, based on 5,865 documents, outlined several aspects including changes in publication counts over the research period, types of documents published, sources of publications, and studies using VOSviewer and R-Bibliometrix (Biblioshiny). This study provides a theoretical foundation for improving privacy protection in electronic payment systems.

In this study, the results of statistical analysis, as well as co-cited articles, authors, and keywords, were used to formulate the responses for the main research questions:

RQ1: Based on the quantity of publications, what are the key topics in personal information security in electronic payments?

Keywords such as e-commerce, electronic payments, user trust in electronic payments, and research on the TAM model have become widely discussed topics. Additionally, the behavior of users using electronic payment systems and user psychology has also become a popular subject of study.

RQ2: What are the research trends in personal information security in electronic payments?

Initially, researchers focused solely on e-commerce, the Internet, and the electronic payment tools themselves. However, with the passage of time and technological advancements, their focus shifted from studying the crucial components that constitute the security of electronic payment systems to investigating user acceptance of new technologies, consumer behavior, user trust, and user satisfaction within electronic payments.

Future study can include exploration in the following areas:

(1) The research on user adoption of electronic payment systems and the cognition of personal information security investigates how consumers' views of personal information security influence their decision to use electronic payments systems.

(2) The development and validation of a trust model examines consumers' trust in electronic payment systems and their influencing elements, with a focus on the impact of personal information security cognition.

(3) The diffusion model is developed by using diffusion models to study the spread and adoption of electronic payment technologies and systems among different user groups, with a focus on the role of personal information security cognition in the dissemination process.

(4) The UTAUT model was developed to provide a explanation of user behavior when adopting electronic payment systems while also considering the influence of individuals cognition of personal information security on this behavior.

RQ3: What theoretical model has finally been established?

An extended UTAUT model can be constructed by blending the Theory of Reasoned Action (TRA) Social Contract Theory (SCT) Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT). Through the integration of these theories, into the UTAUT model framework, a comprehensive understanding of the connections between various factors that impact technology acceptance and usage is achieved. These theories establish a basis for the different elements of the UTAUT model supporting its effectiveness, in elucidating user behavior within the realm of technology adoption.

The Theory of Reasoned Action (TRA) a core component of the UTAUT model incorporates elements, including Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Personal Information Security Cognition (PISC), Behavioral Intention, and Use Behavior. The Social Contract Theory (SCT) supports, like Social Influence (SI), Personal Information Security Cognition (PISC), Behavioral Intention, and Use Behavior. The Technology Acceptance Model (TAM) includes factors, like Performance Expectancy (PE), Effort Expectancy (EE), and Behavioral Intention. Finally, the Protection Motivation Theory (PMT) lays down the groundwork for things like Facilitating Conditions (FC), Habit (HB), Personal Information Security Cognition (PISC) as considering aspects like Gender, Age and Experience when examining Behavioral Intention and Use Behavior.

Understanding these theoretical relationships is very important because they can help to create an electronic payment system with high security and a high usage rate. Future research will provide hypotheses based on the extended UTAUT model and test them through empirical surveys.

The number of publications is growing but our research publications are limited in number. Our analysis focused only on English language publications, not on publications in other languages. Despite these limitations, this study remains valuable as it has found future research directions in the field of personal information security in electronic payments.

## REFERENCES


[1] Hassan, M.A., Shukur, Z., Hasan, M.K., Al-Khaleefa, A.S. (2020). A review on electronic payments security. Symmetry, 12(8): 1344. https://doi.org/10.3390/sym12081344

[2] Oney, E., Guven, G.O., Rizvi, W.H. (2017). The

determinants of electronic payment systems usage from consumers' perspective. Economic Research, 30(1): 394-415. https://doi.org/10.1080/1331677X.2017.1305791

[3] Guan, Y., Tick, A. (2024). Literature review on security of personal information in electronic payments. In 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, pp. 000533-000540. https://doi.org/10.1109/SACI60582.2024.10619864

[4] Kovacs, L., David, S. (2016). Fraud risk in electronic payment transactions. Journal of Money Laundering Control, 19(2): 148-157. https://doi.org/10.1108/JMLC-09-2015-0039

[5] Jain, A.K., Gupta, B.B. (2017). Phishing detection: Analysis of visual similarity based approaches. Security and Communication Networks, 2017(1): 5421046. https://doi.org/10.1155/2017/5421046

[6] Čerget', M., Hudec, J. (2023). Cyber-security threats origins and their analysis. Acta Polytech Hungarica, 20(9): 23-41. https://doi.org/10.12700/APH.20.9.2023.9.2

[7] Cavus, N., Atanda, A. (2022). Security and privacy concerns in mobile payment services. Global Journal of Information Technology: Emerging Technologies, 12: 136-148. https://doi.org/10.18844/gjit.v12i2.8264

[8] Nicolaisen, J. (2010). Bibliometrics and citation analysis: From the science citation index to cybermetrics. Journal of the American Society for Information Science and Technology, 61(1): 205-207. https://doi.org/10.1002/asi.21181

[9] Van Raan, A.F.J. (2005). For your citations only? Hot topics in bibliometric analysis. Measurement: Interdisciplinary Research & Perspective, 3(1): 50-62. https://doi.org/10.1207/s15366359mea0301_7

[10] Köseoglu, M.A., Sehitoglu, Y., Craft, J. (2015). Academic foundations of hospitality management research with an emerging country focus: A citation and co-citation analysis. International Journal of Hospitality Management, 45: 130-144. https://doi.org/10.1016/j.ijhm.2014.12.004

[11] Leung, A., Yan, Z., Fong, S. (2004). On designing a flexible e-payment system with fraud detection capability. In Proceedings of IEEE International Conference on e-Commerce Technology, San Diego, CA, USA, pp. 236-243. https://doi.org/10.1109/ICECT.2004.1319739

[12] Talukder, S.C., Lakner, Z. (2023). Exploring the landscape of social entrepreneurship and crowdfunding: A bibliometric analysis. Sustainability, 15(12): 9411. https://doi.org/10.3390/su15129411

[13] Talukder, S.C., Lakner, Z., Temesi, Á. (2024). Development and state of the art of entrepreneurship education: A bibliometric review. Education Sciences, 14(3): 295. https://doi.org/10.3390/educsci14030295

[14] Mwirigi, D., Fekete-Farkas, M., Lakner, Z. (2024). A bibliometric analysis of borrowers' behavior. Journal of Risk and Financial Management, 17(3): 111. https://doi.org/10.3390/jrfm17030111

[15] Bak, G., Reicher, R. (2023). Small and medium-sized enterprises' perceptions of the use of cloud services. Interdisciplinary Description of Complex Systems, 21(2): 131-140. https://doi.org/10.7906/indecs.21.2.1

[16] Osareh, F. (1996). Bibliometrics, citation analysis and co-citation analysis: A review of literature I. Libri, 46(3): 149-158. https://doi.org/10.1515/libr.1996.46.3.149

[17] Van Eck, N.J., Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2): 523-538. https://doi.org/10.1007/s11192-009-0146-3

[18] Aria, M., Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4): 959-975. https://doi.org/10.1016/j.joi.2017.08.007

[19] Kuzior, A., Sira, M. (2022). A bibliometric analysis of blockchain technology research using VOSviewer. Sustainability, 14(13): 8206. https://doi.org/10.3390/su14138206

[20] Van, E., Waltman, L., Jan, N. (2017). Citation-based clustering of publications using CitNetExplorer and VOSviewer. Scientometrics, 111(2): 1053-1070. https://doi.org/10.1007/s11192-017-2300-7

[21] Arruda, H., Silva, E.R., Lessa, M., Proença Jr, D., Bartholo, R. (2022). VOSviewer and bibliometrix. Journal of the Medical Library Association, 110(3): 392-395. https://doi.org/10.5195/jmla.2022.1434

[22] Effendi, D.N., Anggraini, W., Jatmiko, A., Rahmayanti, H., Ichsan, I.Z., Rahman, M.M. (2021). Bibliometric analysis of scientific literacy using VOSviewer: Analysis of science education. Journal of Physics: Conference Series, 1796(1): 012096. https://doi.org/10.1088/1742-6596/1796/1/012096

[23] Moral-Muñoz, J.A., Herrera-Viedma, E., Santisteban-Espejo, A., Cobo, M.J. (2020). Software tools for conducting bibliometric analysis in science: An up-to-date review. El Profesional de la Información, 29(1): e290103. https://doi.org/10.3145/epi.2020.ene.03

[24] Nazaruddin, L.O., Gyenge, B., Fekete-Farkas, M., Lakner, Z. (2023). The future direction of halal food additive and ingredient research in economics and business: A bibliometric analysis. Sustainability, 15(7): 5680. https://doi.org/10.3390/su15075680

[25] Cobo, M.J., López-Herrera, A.G., Herrera-Viedma, E., Herrera, F. (2011). An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the fuzzy sets theory field. Journal of Informetrics, 5(1): 146-166. https://doi.org/10.1016/j.joi.2010.10.002

[26] Malhotra, N.K., Kim, S.S., Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4): 336-355. https://doi.org/10.1287/isre.1040.0032

[27] Dinev, T., Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1): 61-80. https://doi.org/10.1287/isre.1060.0080

[28] Jeff Smith, H., Dinev, T., Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly: Management Information Systems, 35(4): 989-1015. https://doi.org/10.2307/41409970

[29] Harrison McKnight, D., Choudhury, V., Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. Journal of Strategic Information Systems, 11(3-4): 297-323. https://doi.org/10.1016/S0963-8687(02)00020-3

[30] Wang, Y.D., Emurian, H.H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior, 21(1): 105-125.

https://doi.org/10.1016/j.chb.2003.11.008
[31] Lu, J., Yu, C.S., Liu, C., Yao, J.E. (2003). Technology acceptance model for wireless Internet. Internet Research, 13(3): 206-222. https://doi.org/10.1108/10662240310478222
[32] Suh, B., Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce, 7(3): 135-161. https://doi.org/10.1080/10864415.2003.11044270
[33] Plouffe, C., Hulland, J., Vandenbosch, M. (2001). Research report: Richness versus parsimony in modeling technology adoption decisions—Understanding merchant adoption of a smart card-based payment system. Information Systems Research, 12: 208-222. https://doi.org/10.1287/isre.12.2.208.9697
[34] Liu, C., Marchewka, J.T., Lu, J., Yu, C.S. (2004). Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. Information and Management, 42(1): 127-142. https://doi.org/10.1016/j.im.2004.01.002
[35] Kim, C., Tao, W., Shin, N., Kim, K.S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. Electronic Commerce Research and Applications, 9(1): 84-95. https://doi.org/10.1016/j.elerap.2009.04.014
[36] German Ruiz-Herrera, L., Valencia-Arias, A., Gallegos, A., Benjumea-Arias, M., Flores-Siapo, E. (2023). Technology acceptance factors of e-commerce among young people: An integration of the technology acceptance model and theory of planned behavior. Heliyon, 9(6): e16418. https://doi.org/10.1016/j.heliyon.2023.e16418
[37] Junadi, S. (2015). A model of factors influencing consumer's intention to use e-payment system in Indonesia. International Conference on Computer Science and Computational Intelligence (ICCSCI 2015), 59: 214-220. https://doi.org/10.1016/j.procs.2015.07.557
[38] Dennehy, D., Sammon, D. (2015). Trends in mobile payments research: A literature review. Journal of Innovation Management, 3(1): 49-61. https://doi.org/10.24840/2183-0606_003.001_0006
[39] Acopiado, I.M., Sarmiento, J.M., Romo, G.D., Acuna, T., Traje, A.M., Wahing, G. (2022). Digital payment adoption during the COVID-19 pandemic in the Philippines. Philippine Journal of Science, 151: 1185-1196. https://doi.org/10.56899/151.03.31
[40] Šumak, B., Heričko, M., Pušnik, M. (2011). A meta-analysis of e-learning technology acceptance: The role of user types and e-learning technology types. Computers in Human Behavior, 27(6): 2067-2077. https://doi.org/10.1016/j.chb.2011.08.005
[41] Liébana-Cabanillas, F., Muñoz-Leiva, F., Sánchez-Fernández, J. (2015). Influence of age in the adoption of new mobile payment systems. Review of Business Management, 17: 1390-1407. https://doi.org/10.7819/rbgn.v17i58.1989
[42] Park, E., Cho, Y., Han, J., Kwon, S.J. (2017). Comprehensive approaches to user acceptance of internet of things in a smart home environment. IEEE Internet of Things Journal, 4(6): 2342-2350. https://doi.org/10.1109/JIOT.2017.2750765
[43] Yan, C., Siddik, A.B., Akter, N., Dong, Q. (2021). Factors influencing the adoption intention of using mobile financial service during the COVID-19 pandemic: The role of FinTech. Environmental Science and Pollution Research, 30(22): 61271-61289. https://doi.org/10.1007/s11356-021-17437-y
[44] Mshvidobadze, T.I. (2022). Security issues in next generation mobile payment systems. Economic Bulletin of Dnipro University of Technology, 77: 134-139. https://doi.org/10.33271/ebdut/77.134
[45] Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3): 425-478. https://doi.org/10.2307/30036540
[46] Venkatesh, V., Thong, J.Y.L., Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1): 157-178. https://doi.org/10.2307/41410412
[47] Schnall, R., Higgins, T., Brown, W., Carballo-Dieguez, A., Bakken, S. (2015). Trust, perceived risk, perceived ease of use and perceived usefulness as factors related to m-health technology use. Studies in health technology and informatics, 216: 467-471.
[48] Pavlou, P.A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7(3): 101-134. https://doi.org/10.1080/10864415.2003.11044275
[49] Menard, P., Bott, G.J., Crossler, R.E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. Journal of Management Information Systems, 34(4): 1203-1230. https://doi.org/10.1080/07421222.2017.1394083
[50] Rogers, R., Cacioppo, J., Petty, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social Psychophysiology: A Sourcebook (Guilford), pp. 153-177.
[51] Solic, K., Velki, T., Fosic, I., Vukovic, M. (2024). Study on information security awareness using the behavioral-cognitive internet security questionnaire. Acta Polytechnica Hungarica, 21(4): 49-68. https://doi.org/10.12700/APH.21.4.2024.4.3
[52] Venkatesh, V., Zhang, X., Sykes, T.A. (2011). "Doctors do too little technology": A longitudinal field study of an electronic healthcare system implementation. Information Systems Research, 22(3): 523-546. https://doi.org/10.1287/isre.1110.0383
[53] Gagnon, M.P., Orruño, E., Asua, J., Abdeljelil, A.B., Emparanza, J. (2012). Using a modified technology acceptance model to evaluate healthcare professionals' adoption of a new telemonitoring system. Telemedicine and e-Health, 18(1): 54-59. https://doi.org/10.1089/tmj.2011.0066
[54] Thomas, T.D., Singh, L., Gaffar, K. (2013). The utility of the UTAUT model in explaining mobile learning adoption in higher education in Guyana. International Journal of Education and Development using ICT, 9(3): 71-85. https://www.learntechlib.org/p/130274/
[55] 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. https://doi.org/10.1016/j.chb.2010.01.013

[56] Oliveira, T., Thomas, M., Baptista, G., Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Computers in Human Behavior, 61: 404-414. https://doi.org/10.1016/j.chb.2016.03.030

[57] Shareef, M.A., Kumar, V., Kumar, U., Dwivedi, Y.K. (2011). E-government adoption model (GAM): Differing service maturity levels. Government Information Quarterly, 28(1): 17-35. https://doi.org/10.1016/j.giq.2010.05.006

[58] Luthra, S., Kumar, S., Kharb, R., Ansari, M., Shimmi, S.L. (2014). Adoption of smart grid technologies: An analysis of interactions among barriers. Renewable and Sustainable Energy Reviews, 33: 554-565. https://doi.org/10.1016/j.rser.2014.02.030

[59] Javornik, A. (2016). Augmented reality: Research agenda for studying the impact of its media characteristics on consumer behaviour. Journal of Retailing and Consumer Services, 30: 252-261. https://doi.org/10.1016/j.jretconser.2016.02.004

[60] Omar, A., Tiwari, V., Saad, M. (2025). Smart technology's potential in smart destinations: A comprehensive UTAUT model with privacy and safety risk moderation. Journal of Hospitality and Tourism Technology. https://doi.org/10.1108/JHTT-01-2024-0061

[61] Rana, M.M., Siddiqee, M.S., Sakib, M.N., Ahamed, M.R. (2024). Assessing AI adoption in developing country academia: A trust and privacy-augmented UTAUT framework. Heliyon, 10(18): e37569. https://doi.org/10.1016/j.heliyon.2024.e37569

[62] Trkman, M., Popovič, A., Trkman, P. (2023). The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications. Government Information Quarterly, 40(1): 101787. https://doi.org/10.1016/j.giq.2022.101787

[63] Reith, R., Buck, C., Eymann, T., Lis, B. (2020). Integrating privacy concerns into the unified theory of acceptance and use of technology to explain the adoption of fitness trackers. International Journal of Innovation and Technology Management, 17(7): 20500492. https://doi.org/10.1142/S0219877020500492

[64] Gefen, D., Karahanna, E., Straub, D.W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1): 51-90. https://doi.org/10.2307/30036519

[65] Featherman, M.S., Pavlou, P.A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4): 451-474. https://doi.org/10.1016/S1071-5819(03)00111-3

[66] Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1): 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

[67] Cejas, O.A., Sannier, N., Abualhaija, S., Ceci, M., Bianculli, D. (2024). GDPR-relevant privacy concerns in mobile apps research: A systematic literature review. arXiv:2411.19142. https://doi.org/10.48550/arXiv.2411.19142

[68] Marikyan, D., Papagiannidis, S., Rana, O.F., Ranjan, R. (2023). General data protection regulation: A study on attitude and emotional empowerment. Behaviour & Information Technology, 43(14): 3561-3577. https://doi.org/10.1080/0144929X.2023.2285341