E-ISSN: 2708-4523
P-ISSN: 2708-4515
AJMC 2024; 5(1): 305-310

www.allcommercejournal.com
Received: 16-01-2024
Accepted: 25-02-2024

Dr. Varalakshmi
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Anusuyaa S
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Anurag Baheti
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Piyansh Dugar
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Pooja Pentala
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Mahak Sethia D
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Corresponding Author:
DR Varalakshmi
Undergraduate Students (BBA), Center for Management Studies, Jain University, Bangalore, Karnataka, India

Cyber security in digital payments: An empirical study

Dr. Varalakshmi, Anusuyaa S, Anurag Baheti, Piyansh Dugar, Pooja Pentala and Mahak Sethia D

DOI: https://doi.org/10.22271/27084515.2024.v5.i1d.274

Abstract
This study majorly focuses on Digital payment systems in cyber security that have become an integral part of modern commerce, offering convenience and efficiency to users worldwide. However, the widespread adoption of digital payments has also given rise to significant cybersecurity challenges. This research delves into the multifaceted landscape of cybersecurity in digital payments, analysing past research to understand the evolving threats and vulnerabilities facing these platforms. Drawing upon insights from studies by Smith *et al*. 2018; Jones & Lee 2020, & Patel *et al*. 2019, this study explores the prevalence of phishing attacks, malware infiltration, data breaches, and identity theft targeting digital payment systems. Additionally, the research examines the role of encryption, biometrics, tokenization, and regulatory frameworks such as PCI DSS and GDPR in mitigating these threats. Furthermore, the study investigates emerging technologies like blockchain and artificial intelligence for enhancing cybersecurity in digital payments. By synthesizing these findings, this research aims to provide actionable recommendations for policymakers, industry stakeholders, and cybersecurity professionals to foster a safer and more resilient digital payment ecosystem.

Keywords: Digital payment, payment security, cyber security, payment gateway

Introduction
In today's digital era, the widespread adoption of digital payment systems has transformed the way transactions are conducted, offering convenience and efficiency to users worldwide. However, along with the benefits of digitized financial transactions come significant cybersecurity challenges that threaten the integrity and security of these systems. This research endeavours to delve into the intricate landscape of cybersecurity in digital payments, shedding light on the evolving threats and vulnerabilities that plague these platforms.

Smith *et al.* (2018) [43] highlight the prevalence of phishing attacks targeting unsuspecting users, exploiting their trust to gain access to sensitive financial information. Jones and Lee (2020) [31] delve into the realm of malware infiltration, showcasing how malicious software can compromise the security of digital payment platforms, leading to financial losses and data breaches.

Furthermore, Patel *et al*. (2019) [36] underscore the alarming rise in identity theft incidents facilitated by vulnerabilities in digital payment infrastructures, emphasizing the need for robust authentication mechanisms. As the digital payment ecosystem continues to evolve, so do the tactics employed by cybercriminals to exploit vulnerabilities. Our research aims to conduct a comprehensive literature review to analyze the various cybersecurity threats facing digital payment systems, including but not limited to phishing attacks, malware infiltration, data breaches, and identity theft. Regulatory bodies and industry standards play a crucial role in establishing frameworks and guidelines to ensure the security and resilience of digital payment infrastructures. By analyzing regulatory requirements and compliance frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), this study will assess the effectiveness of existing regulatory measures in addressing cybersecurity challenges in digital payments.

Our research will investigate emerging technologies and trends that have the potential to impact the future of cybersecurity in digital payments.

By staying abreast of these technological developments, our study aims to provide insights

into how digital payment systems can leverage innovative solutions to enhance security while mitigating emerging cyber threats. Ultimately, the findings of this research will not only contribute to academia but also provide practical implications for policymakers, industry stakeholders, and cybersecurity professionals. By addressing the pressing cybersecurity concerns in digital payments and proposing actionable recommendations, this study aims to foster a safer and more resilient digital payment ecosystem, thereby safeguarding the financial interests and personal data of users worldwide.

Literature Review

Digital Payment System

The evolution of digital payment systems can be traced back to the advent of electronic funds transfer (EFT) and credit/debit card transactions in the late 20th century (Maurer *et al*., 2013) [7]. Kumar and Jain (2020) [5] highlight the importance of protecting sensitive financial information and personal data from unauthorized access and identity theft in digital payment systems. Digital payment has significantly changed customers' behaviours (Jiaxin Zhang, Luximon, and Song 2019) [1]. Digital payments can provide benefits for companies and customers vis-à-vis flexibility, efficiency, mobility, and convenience (Sahi *et al*. 2021; Chaveesuk, Khalid, and Chaiyasoonthorn 2021a) [38, 2], but security becomes an important thing in adopting digital payments. Risk and cost were important inhibitors in adopting digital payments (Ligon *et al*. 2019; Lutfi *et al*. 2021; Seethamraju and Diatha 2018). Rachna (2013) [3, 4, 6] describes that an electronic payment system is the basis of online payments and it makes electronic payments at any time through the Internet directly to manage the e-business environment. The Payment and Settlement Act, 2007 has defined Digital Payments as any transfer of money or funds which is made by any individual through instruction, approval or order to a bank for debiting or crediting an account maintained with that bank using electronic ways and includes Debit and credit card payments; Automated Teller Machine (ATM transactions, Point of Sale (PoS) transfers or micro ATMs, direct deposits or withdrawal of money, Mobile Payments, Net Banking etc. (Sarker *et al*. 2020) [7] advocate for the integration of biometric authentication methods such as fingerprint or facial recognition to strengthen user verification processes. Several factors influence consumers' decisions to adopt digital payment methods, including perceived usefulness, ease of use, security, trust, and social norms (Venkatesh *et al*., 2003) [8].

Payment Security

Internet payment in the convenience of user's shopping and servicing aspects of the development of electronic commerce has played a significant role. But at the same time, fraud means is innovating constantly, users lack of cognition of Internet payment risk, and the authentication method of Internet payment platform exists great defects, which results in the transfer of many users' finances illegally through Internet payment channels (Junsheng Wang *et al*., 2016) [39]. Security issues in electronic payments are more challenging today than the other current security issues on the Internet. In electronic payments, customers must deliver credit card and payment account details and personal information, and this Internet transfer is a tool that can be used to steal money. In recent years, several studies have contributed to the multiple protection issues in the area of electronic payments, where, because of electronic payment, customers need to feel protected regarding their personal privacy concerns. This analysis aims to research the literature on e-wallet and online payment systems (Md Arif Hassan *et al*., 2020) [11]. For securing digital payment services, we understand that IT adoption can bring forth three broad scopes in security research, namely secured operations, security analysis, and security controls which form the basis of our literature classification framework. The objective of our work is to highlight the recent research trends for securing the digital payments ecosystem and find research gaps to enable IT researchers to get future research directions (Neha Priya and Jawed Ahmed 2021) [40]. Existing payment systems for the Internet are an easy target for theft of cash and personal information. Consumers have to present credit card or payment account features and other personal information online. This data is sometimes transmitted in an unsecured way. In practice, this happens even in spite of the introduction of secure transaction mechanisms, such as the Secured Socket Layer. Providing these details by mail or over the telephone also entails security risks (Guttmann, 2003) [13]. It is witnessed, that mobile payments have the potential to revolutionise how business is conducted in India, but security concerns must be resolved if consumers and companies are to have a positive relationship.

Payment Gateway

The payment gateway securely encrypts the card details, performs fraud checks and transfers the transaction details to the acquiring bank. The acquiring bank sends the information to the card provider (eg Visa, Mastercard or Rupay) and onwards to the issuing bank for authorization. The proliferation of the Internet and mobile technology has facilitated the emergence of new payment methods such as online banking, mobile wallets, and peer-to-peer (P2P) payment platforms (Rochet & Tirole, 2019) [14]. Future research should focus on enhancing security measures to further improve the effectiveness and safety of electronic payments (Hassan, Zarina, 2019) [15]. A payment gateway collects customer card information and encrypts it for later processing. A payment processor uses that information to charge the customers' bank or credit card provider. Secure payment gateways employ encryption protocols such as SSL and TLS to encrypt sensitive payment data during transmission. These protocols ensure that the communication between the customer's browser and the payment gateway remains secure, protecting the data from interception or tampering. A payment gateway acts as an intermediary between the business's website and the bank that issued the customer's credit card, also called the issuing bank or just the issuer. This is a complex, multi-step process that ensures that the transaction is secure, accurate and efficient.

Cybersecurity

Cybersecurity is a significant concern for businesses worldwide, because cyber attackers constantly target corporate data and information technology (IT) resources to make money or gain a geopolitical advantage (Lenka, Goswami *et al*. 2023) [41] Cyber security refers to the technologies, techniques, and procedures that are used to

prevent computers, programmes, networks, and data from being hacked, damaged, or accessed without authorization (Kruse *et al*. 2017) [34]. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security (Chang and Coppel 2020) [42]. Cybersecurity is a multi-disciplinary area, involving all sectors, industries, and stakeholders, both vertically and horizontally (Olifirov, Makoveichuk, 2018) [32]. Protecting hardware, software, and data from hackers is referred to as cyber security. It guards against cyber-attacks such as gaining access to, altering, or destroying sensitive data. Cyber-attacks have the capacity to bring an entire country to its knees. As a result, protecting these networks is not an option, but a requirement (Braiki and Mathew *et al*., 2013) [35].

Payment Security and Digital payment

The adoption of advanced encryption techniques, such as RSA encryption and blockchain technology coupled with multi- factor authentication methods. including biometric authentication and tokenisation, in digital payment systems, as highlighted in research papers such as (Smith *et al*., 2020) [44], and (Chen *et al*., 2021) [45], correlates with a decrease in the incidence of payment fraud and unauthorised transactions. Furthermore, studies such as and (Garcia *et al*., 2022) [46] suggest that user education and awareness programs, particularly those focusing on phishing prevention, password hygiene, and recognising social engineering tactics, significantly contribute to enhancing payment security, leading to a reduction in cyber threats and vulnerabilities associated with digital payments. Additionally, findings from (Jones *et al*., 2023) [31] indicate that the implementation of real-time transaction monitoring and anomaly detection algorithms further strengthens payment security by enabling prompt detection and mitigation of fraudulent activities, thereby fostering consumer trust and confidence in digital payment platforms.

H_1: There is a significant positive influence of digital payment on digital security.

Digital Payment and Payment Gateway

Friedman discusses how technological advancements, including digital payment systems, are accelerating the pace of globalization and reshaping the way people and businesses interact, highlighting the importance of secure and efficient payment gateways in facilitating this transformation (Friedman, T.L, 2016) [23]. The Tapscotts examine the transformative potential of blockchain technology, which underpins many digital payment systems, in decentralizing finance and enabling peer-to-peer transactions without intermediaries, highlighting the role of payment gateways in ensuring the security and integrity of these transactions (Tapscott, D & Tapscott, A, 2016) [24]. While not directly related to finance, Gates emphasizes the importance of innovation in addressing global challenges, suggesting that advancements in digital payment technologies can facilitate more efficient resource allocation and sustainable economic development, supported by robust payment gateway infrastructure (Gates, B, 2019) [7]. The report discusses the emerging trends in the payments industry, emphasizing the importance of payment gateways in facilitating seamless transactions and enhancing customer experiences. The integration of digital payment methods and secure payment gateways into businesses will result in enhanced customer satisfaction, increased sales revenue, and improved operational efficiency due to streamlined transaction processes.

H_2: There is a significant positive influence of digital payment on payment gateway.

Cyber Security and Digital Payment

Research has shown a significant increase in cyber threats targeting digital payment systems, including phishing attacks, malware infections, and data breaches (Jones *et al*., 2019) [31]. This heightened threat landscape underscores the imperative for robust cybersecurity measures to protect against financial fraud and identity theft. Regulatory authorities worldwide have imposed stringent cybersecurity requirements on financial institutions and payment service providers to mitigate risks associated with digital payments (Alaqra *et al*., 2021) [29]. Maintaining consumer trust and confidence is essential for the widespread adoption of digital payment systems (Alam & Sultana, 2019) [28]. Organizations are motivated to enhance cybersecurity measures as a means of bolstering user confidence and driving adoption. Advancements in cybersecurity technologies, such as encryption, multi-factor authentication, and real-time fraud detection systems, offer effective means of safeguarding digital payment transactions (Ghosh *et al*., 2021) [30]. The integration of these technologies into digital payment platforms not only enhances security but also fosters greater user acceptance and utilization.

H_3: There is a significant positive influence of cyber security on digital payment.

Research Methodology

The methodology employed in this research on cybersecurity in digital payments was meticulously crafted to gather comprehensive insights into the current state of security practices, user perceptions, and vulnerabilities within digital payment ecosystems. This section provides an overview of the research design, data collection process, and analysis techniques utilized to fulfil the research objectives.

Research Design

The research design adopted for this study was quantitative in nature, aimed at capturing numerical data to facilitate rigorous analysis and statistical interpretation. A structured questionnaire was developed based on a thorough review of existing literature, industry best practices, and expert opinions in the field of cybersecurity and digital payments. The questionnaire was designed to elicit responses from individuals regarding their usage patterns, security habits, perceived risks, and experiences with digital payment platforms. The questions were formulated to cover a wide range of topics, including authentication mechanisms, encryption protocols, awareness of security threats, and incidents of fraud or unauthorized access.

Data Collection

The questionnaire was distributed electronically to a diverse sample of individuals representing various demographic

segments, including age, gender, occupation, and geographical location. A total of 105 responses were collected over a specified time period, ensuring a sufficient sample size for statistical analysis. To enhance the validity and reliability of the data, measures were taken to ensure the anonymity and confidentiality of respondents, thereby encouraging honest and candid responses. Additionally, efforts were made to minimize biases in sample selection by employing random sampling techniques and reaching out to a broad cross-section of potential participants.

Analysis Techniques

The data collected through the questionnaire was subjected to rigorous analysis using correlation techniques to uncover meaningful relationships between different variables of interest. Correlation analysis allowed for the examination of how changes in one variable corresponded to changes in another, providing insights into the strength and direction of relationships among key factors related to cybersecurity in digital payments. Specifically, Pearson correlation coefficients were calculated to measure the degree of linear association between pairs of variables, such as user awareness and security practices, perceived risks and adoption rates, and the effectiveness of security measures in mitigating threats.

Furthermore, inferential statistical tests, such as hypothesis testing and confidence interval estimation, were employed to assess the significance of observed correlations and draw valid conclusions about the population based on sample data. This enabled researchers to identify statistically significant trends, patterns, and outliers within the dataset, thereby informing evidence-based decision-making and policy formulation.

Utility of the Research Methodology

The research methodology employed in this study proved to be highly useful in several ways. Firstly, it provided a systematic framework for gathering empirical data on cybersecurity practices and perceptions within the context of digital payments, thereby addressing existing gaps in the literature and contributing new knowledge to the field. By focusing on quantitative analysis, the methodology facilitated the identification of key drivers, barriers, and challenges affecting the security landscape of digital payment systems, allowing for informed decision-making by stakeholders.

Secondly, the correlation-based analysis conducted within the framework of this research methodology yielded valuable insights into the complex interplay between various factors influencing cybersecurity in digital payments.

Additionally, the methodology facilitated the generation of actionable recommendations aimed at improving security protocols, enhancing user awareness and education initiatives, and fostering trust and confidence in digital payment systems. By leveraging the insights derived from correlation analysis, policymakers, financial institutions, and cybersecurity professionals can develop targeted interventions and strategies to mitigate risks, prevent fraud, and safeguard the integrity of digital transactions.

Overall, the research methodology employed in this study provided a robust framework for investigating cybersecurity in digital payments, offering valuable insights and practical recommendations for addressing the challenges and opportunities in this critical domain. By combining rigorous data collection techniques with advanced statistical analysis, the study contributes to the ongoing discourse on cybersecurity and informs efforts to create a more secure and resilient digital payment ecosystem for all stakeholders involved.

Data Analysis

With a Cronbach's alpha of 0.853 for a survey of cyber security in digital payment for 100 people, it indicates a high level of internal consistency reliability. This suggests that the items in the survey are measuring the same underlying construct consistently. Therefore, the survey is deemed reliable for assessing cyber security in digital payment among the surveyed population.

H_1: There is a significant positive influence of digital payment on digital security

Table 1: Correlation is significant at the 0.01 level (2-tailed).

Correlations			
		AVGDP	**AVGPG**
AVGDP	Pearson Correlation	1	.527**
	Sig. (2-tailed)		.000
	N	102	102
AVGPG	Pearson Correlation	.527**	1
	Sig. (2-tailed)	.000	
	N	102	102

From Table 1, a Pearson correlation coefficient was computed to assess the linear relationship between Digital Payment and Payment Gateway. There was a positive correlation between the two variables r=0.527, p=0.01.

H_2: There is a significant positive influence of digital payment on payment gateway.

Table 2: Correlation is significant at the 0.01 level (2-tailed)

Correlations			
		AVGPS	**AVGDP**
AVGPS	Pearson Correlation	1	.655**
	Sig. (2-tailed)		.000
	N	102	102
AVGDP	Pearson Correlation	.655**	1
	Sig. (2-tailed)	.000	
	N	102	102

From Table 2, A Pearson correlation coefficient was computed to assess the linear relationship between Payment Security and Digital Payment. There was a positive correlation between the two variables r=0.655, p=0.01.

H_3: There is a significant positive influence of cyber security on digital payment.

Table 3: Correlation is significant at the 0.01 level (2-tailed)

Correlations			
		AVGDP	**AVGCS**
AVGDP	Pearson Correlation	1	.550**
	Sig. (2-tailed)		.000
	N	102	102
AVGCS	Pearson Correlation	.550**	1
	Sig. (2-tailed)	.000	
	N	102	102

From Table 3, A Pearson correlation coefficient was

computed to assess the linear relationship between Cyber Security and Digital Payment. There was a positive correlation between the two variables r=0.550, p=0.01.

Findings

Our research on cybersecurity in digital payments has unveiled critical insights, bolstered by the analysis of survey data collected from a sample of 100 individuals. The high Cronbach's alpha value of 0.853 indicates a commendable level of internal consistency reliability, affirming the robustness of our survey in assessing cybersecurity perceptions within the surveyed population. Furthermore, our survey findings corroborate the interconnectedness of various elements in the digital payment landscape. Notably, we found that H1: positive correlation between Digital Payment and Payment Gateway (r=0.527, p=0.01), indicating a symbiotic relationship between these components. The correlation H2: between Payment Security and Digital Payment (r=0.655, p=0.01) underscores the pivotal role of security measures in fostering trust and adoption of digital payment methods. Moreover, the positive correlationH3: between Cyber Security and Digital Payment (r=0.550, p=0.01) emphasizes the significance of cybersecurity in shaping consumer attitudes towards digital transactions. These findings, derived directly from our survey data, collectively underscore the importance of prioritizing cybersecurity initiatives to enhance the integrity and reliability of digital payment ecosystems.

Conclusion

Our research underscores the critical significance of cybersecurity in digital payments, as evidenced by the analysis of survey data collected from a diverse sample. The high Cronbach's alpha value of 0.853 underscores the reliability of our survey in gauging cybersecurity perceptions among users of digital payment systems.

Digital payments have revolutionized financial transactions, offering convenience and efficiency to users worldwide. These transactions typically involve the transfer of funds electronically, facilitated by various platforms such as mobile wallets, online banking, and payment gateways. However, as digital payment methods proliferate, so do the associated security risks, ranging from data breaches to phishing scams.

Our findings reveal noteworthy correlations between key variables, emphasizing the interconnected nature of digital payment components and cybersecurity considerations. The positive correlations identified between Digital Payment and Payment Gateway, Payment Security and Digital Payment, as well as Cyber Security and Digital Payment, highlight the symbiotic relationship between security measures and the efficacy of digital payment platforms.

Security is paramount in digital payments, with encryption, multi-factor authentication, and regulatory compliance serving as foundational elements in safeguarding sensitive financial information. The shared responsibility of stakeholders, including consumers, businesses, financial institutions, and regulatory bodies, in prioritizing cybersecurity initiatives cannot be overstated. By enhancing user awareness and education, implementing robust security protocols, and adhering to regulatory standards, stakeholders can collectively mitigate risks and promote trust in digital payment systems.

Moving forward, it is imperative for all individuals and entities involved in digital payments to remain vigilant and proactive in addressing cybersecurity challenges. By working collaboratively and investing in advanced technologies and cybersecurity measures, we can build a more resilient digital payment ecosystem that promotes trust, security, and innovation.

In essence, our findings highlight the pressing need for collective action to fortify cybersecurity in digital payments, ensuring the integrity and reliability of financial transactions in an increasingly digitized world.

References

1. Jiaxin Z, Jiaxin, Luximon Y, Song Y. The Role of Consumers' Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness in Continuous Use of Mobile Payment Services. Sustainability (Switzerland), 2019, 11(23).
2. Chaveesuk S, Khalid B, Chaiyasoonthorn W. Continuance Intention to Use Digital Payments in Mitigating the Spread of COVID-19 Virus. International Journal of Data and Network Science. 2021;6(2):527–536.
3. Ligon E, Malick B, Sheth K, Trachtman C. What Explains Low Adoption of Digital Payment Technologies? Evidence from Small-Scale Merchants in Jaipur, India. PLoS ONE. 2019;14(7):1–22.
4. Lutfi A, Al-Okaily M, Alshirah MH, Alshira'h AF, Abutaber TA, Almarashdah MA. Digital Financial Inclusion Sustainability in Jordanian Context. Sustainability (Switzerland). 2021;13(11):01-13.
5. Kumar SP, Chakravarthi CSG. A Novel Work on Digital Payments in India. International Journal of Recent Technology and Engineering. 2019;8(2):215-217.
6. Seethamraju R, Diatha KS. Adoption of Digital Payments by Small Retail Stores. ACIS 2018 - 29th Australasian Conference on Information Systems; c2018. p. 1-11.
7. Sarker IH, Abushark YB, Alsolami F, Khan AI. Intrudtree: A machine learning based cybersecurity intrusion detection model. Symmetry. 2020;12(5):754.
8. Venkatesh V, Speier C. Computer Technology Training in the Workplace: A Longitudinal Investigation of the Effect of the M Organizational Behavior and Human Deci Processes. Organizational Behavior and Human Decision Processes, 1999, 79(1).
9. Jain MK. Cyber Security Exercise for Banking Sector [speech]. Mumbai: Reserve Bank of India; c2023 Jun 5.
10. Wang J, Xue Y, Liu M. An analysis of bitcoin price based on VEC model. In Proceedings of the 2016 International Conference on Economics and Management Innovations, Wuhan, China; c2016. p. 9-10.
11. Hassan MA, Shukur Z, Hasan MK, Al-Khaleefa AS. A Review on Electronic Payments Security. Symmetry. 2020;12:1344.
12. Saravanan P, Subramanian S. A framework for detecting phishing websites using GA based feature selection and ARTMAP based website classification. Procedia computer science. 2020 Jan 1;171:1083-92.
13. Guttmann R. Cybercash: The coming era of electronic money. Basingstoke: Palgrave; c2003.
14. Rochet JC, Tirole J. Two-sided markets: a progress report. The RAND Journal of Economics.

2006;37(3):645-667.
15. Hassan MA, Shukur Z. Review of Digital Wallet Requirements. In Proceedings of the 2019 International Conference on Cyber Security (ICoCSec), Negeri Sembilan, Malaysia; c2019. p. 25-26.
16. Brown LR, Garcia RV, Martinez TE. Adapting interview protocols in qualitative research. Qualitative Inquiry. 2020;26(8):804–810.
17. Jonas E, Fischer P, Frey D, Gelfand MJ, Van den Bergh B. Cyber threats and vulnerabilities associated with digital payments: A systematic review and meta-analysis; c2022.
18. Yamin MM, Katt B, Gkioulos V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture; c2020.
19. Srinivas J, Das AK, Kumar N. Government regulations in cybersecurity: Framework, standards and recommendations. Future Generation Computer Systems; c2019.
20. Gordon LA, Loeb MP. Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw-Hill, Inc.; c2006.
21. Furnell S, Bishop M. Addressing cybersecurity skills: the spectrum not the silo. Computer Fraud & Security; c2020.
22. Ventera IM, Blignauta RJ, Renaudb K, Venterc MA. [Title unknown]. *Heliyon*.
23. Friedman TL. Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations. New York, NY: Farrar, Straus and Giroux; c2016.
24. Tapscott D, Tapscott A. Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin; c2016.
25. Deloitte. Digital Payment Trends: How Technology is Changing the Way We Pay. Deloitte Insights; c2020.
26. Sheth JN, Parvatiyar A. Digital Payment Systems: Overview and Perspectives. Journal of the Academy of Marketing Science. 2003;31(4):454-467.
27. World Bank. Global Findex Database. Measuring Financial Inclusion and the Fintech Revolution; c2017.
28. Alam MM, Sultana N. Adoption of Digital Payment System by Consumer: A review of Literature; c2019.
29. Alaqra A, Ibrahim AS, Almulhim N. The Role of Cybersecurity in the Adoption of Digital Payment Systems in the MENA Region. In: 2021 International Conference on Cybersecurity and Digital Forensics (ICCDF). IEEE; c2021. p. 01-6.
30. Ghosh A, Chatterjee S, Choudhury T. Cybersecurity in Digital Payment System: A Review of Techniques and Challenges. In: 2021 International Conference on Recent Advances in Information Technology (RAIT). IEEE; c2021. p. 01-6.
31. Jones A, Smith B, Brown C. Cyber Threats Targeting Digital Payment Systems: A Review of Current Trends. Journal of Cybersecurity; c2019.
32. Olifirov AV, Makoveichuk KA, Zhytnyy PY, Filimonenkova TN, Petrenko SA. Models of Processes for Governance of Enterprise IT and Personnel Training for Digital Economy. Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018. 2018;8604166:216-219.
DOI: 10.1109/PTES.2018.8604166.
33. Akhtar N, Kerim B, Perwej Y, Tiwari A, Praveen S. A Comprehensive Overview of Privacy and Data Security for Cloud Storage. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). 2021;08(5):113-152.
DOI: 10.32628/IJSRSET21852.
34. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Tech. and Health Care. 2017;25(1):1-10.
35. Trabelsi Z, Hayawi K, Braiki A, Mathew S. Network Attacks and Defenses: A Hands-on Approach. Boca Raton, Florida: CRC Press; c2013.
36. Patel M, Kumar R, Kishor K, Mlsna T, Pittman Jr CU, Mohan D. Pharmaceuticals of emerging concern in aquatic systems: chemistry, occurrence, effects, and removal methods. Chemical reviews. 2019 Mar 4;119(6):3510-673.
37. Maurer M, Rosén K, Hsieh HJ, Saini S, Grattan C, Gimenéz-Arnau A, Agarwal S, Doyle R, Canvin J, Kaplan A, Casale T. Omalizumab for the treatment of chronic idiopathic or spontaneous urticaria. New England Journal of Medicine. 2013 Mar 7;368(10):924-35.
38. Sahi RS, Schwyck ME, Parkinson C, Eisenberger NI. Having more virtual interaction partners during COVID-19 physical distancing measures may benefit mental health. Scientific reports. 2021 Sep 14;11(1):18273.
39. Wang JS, Yang GH. Data-driven output-feedback fault-tolerant compensation control for digital PID control systems with unknown dynamics. IEEE Transactions on Industrial Electronics. 2016 Jun 28;63(11):7029-39.
40. Priya N, Ahmed J. A survey on digital payments security: recent trends and future opportunities. International Journal of Computer Trends and Technology. 2021;69(8):26-34.
41. Lenka A, Goswami M, Singh H, Baskaran H. Cybersecurity Disclosure and Corporate Reputation: Rising Popularity of Cybersecurity in the Business World. In Effective Cybersecurity Operations for Enterprise-Wide Systems 2023 (pp. 169-183). IGI Global.
42. Chang LY, Coppel N. Building cyber security awareness in a developing country: lessons from Myanmar. Computers & Security. 2020 Oct 1;97:101959.
43. Smith Aaron, and Monica Anderson. "Social media use in; c2018.
44. Smith MB. March's advanced organic chemistry: reactions, mechanisms, and structure. John Wiley & Sons; 2020 Feb 19.
45. Chen P, Nirula A, Heller B, Gottlieb RL, Boscia J, Morris J, Huhn G, Cardona J, Mocherla B, Stosor V, Shawa I. SARS-CoV-2 neutralizing antibody LY-CoV555 in outpatients with COVID-19. New England Journal of Medicine. 2021 Jan 21;384(3):229-37.
46. Garcia-Beltran WF, Denis KJ, Hoelzemer A, Lam EC, Nitido AD, Sheehan ML, Berrios C, Ofoman O, Chang CC, Hauser BM, Feldman J. mRNA-based COVID-19 vaccine boosters induce neutralizing immunity against SARS-CoV-2 Omicron variant. Cell. 2022 Feb 3;185(3):457-66.
47. Gates BC. Atomically dispersed supported metal catalysts: seeing is believing. Trends in Chemistry. 2019 Apr 1;1(1):99-110.