World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Navigating the path to economic empowerment: overcoming challenges in digital platforms for economic empowerment

Otuma O. Andako *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 20(03), 1503–1521

Publication history: Received on 10 June 2023; revised on 21 December 2023; accepted on 23 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.1450

Abstract

This paper presents a comprehensive survey of the challenges faced by economic empowerment digital platforms. As these online platforms revolutionize the economic landscape, they encounter various hurdles that hinder their potential for fostering financial inclusion and empowerment. Through an extensive analysis of existing literature and empirical studies, this survey identifies and categorizes the key challenges faced by these platforms. The survey reveals that regulatory frameworks pose significant obstacles to economic empowerment digital platforms. Issues such as unclear or outdated regulations, varying legal requirements across jurisdictions, and the need for compliance with consumer protection and data privacy laws hinder platform operations and expansion. Moreover, the absence of standardized regulations often leads to legal uncertainties and challenges in ensuring fair competition. Furthermore, the survey highlights the persistent challenge of trust and reputation management within economic empowerment digital platforms. As these platforms rely heavily on user-generated content and interactions, establishing trust among users becomes critical. Issues such as fraudulent activities, identity verification, and dispute resolution mechanisms emerge as key challenges that platforms must address to maintain user trust and credibility. The survey also addresses the technological challenges faced by economic empowerment digital platforms. Issues such as cybersecurity threats, data breaches, and privacy concerns pose significant risks to both platform operators and users. Platforms must invest in robust security measures and adopt innovative technologies to mitigate these challenges and safeguard user information and transactions. Additionally, the survey examines challenges related to financial inclusion and accessibility. Despite the potential for economic empowerment, certain groups, such as individuals from low-income communities or those lacking digital literacy, may face barriers in accessing and utilizing these platforms. Bridging the digital divide and ensuring equal opportunities for all individuals to participate and benefit from these platforms remains an ongoing challenge. Finally, the survey highlights the need for collaboration and cooperation among stakeholders. Platform operators, policymakers, regulatory bodies, and user communities must engage in constructive dialogue to address the challenges faced by economic empowerment digital platforms effectively. Collaborative efforts can lead to the development of regulatory frameworks, industry standards, and best practices that foster a conducive environment for these platforms to thrive.

Keywords: Digital platform; Economic empowerment; Privacy; Security

1. Introduction

In today's interconnected world, digital technologies have revolutionized various aspects of our lives, including the way we conduct business and interact economically [1]-[3]. One notable development is the rise of economic empowerment digital platforms, whose ecosystems are shown in Figure 1 below. These online platforms harness the power of technology to create opportunities for individuals and businesses, aiming to enhance economic inclusion, financial independence, and overall empowerment. According to [4], economic empowerment digital platforms refer to online

* Corresponding author: Otuma O. Andako.

platforms that aim to enhance economic opportunities and financial inclusion for individuals and businesses. These platforms leverage digital technologies to connect users with various resources, tools, and opportunities to improve their economic status. As explained in [5], economic empowerment digital platforms have emerged as transformative tools in the pursuit of financial stability and growth. They leverage the connectivity and convenience of the internet [6] to bridge gaps, connect users, and provide access to resources that were once limited by geographic boundaries or traditional barriers. These platforms have unlocked new avenues for individuals to showcase their skills, talents, and entrepreneurial endeavors, while simultaneously enabling businesses to tap into a global marketplace [7]-[10]. Through these platforms, individuals can engage in various economic activities such as freelancing, e-commerce, crowdfunding, microfinance, peer-to-peer lending and more. They empower individuals to take control of their financial destinies, offering opportunities to earn income, start or expand businesses, access capital, and develop essential financial management skills.

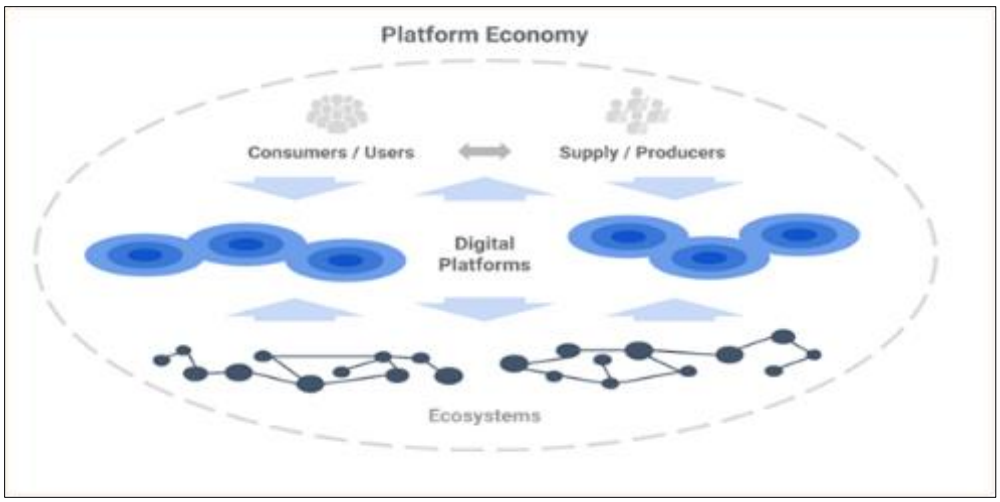

Figure 1 Digital platforms ecosystems

Furthermore, these platforms promote financial inclusion by reaching individuals who may have been previously marginalized or excluded from traditional financial systems [11]. The impact of economic empowerment digital platforms extends beyond individual empowerment. They have the potential to stimulate economic growth and create a more inclusive and sustainable economy. Figure 2 shows the value added chain for digital platforms. By connecting buyers and sellers, fostering entrepreneurship, and facilitating access to financial resources, these platforms contribute to job creation, wealth generation, and the overall advancement of communities.

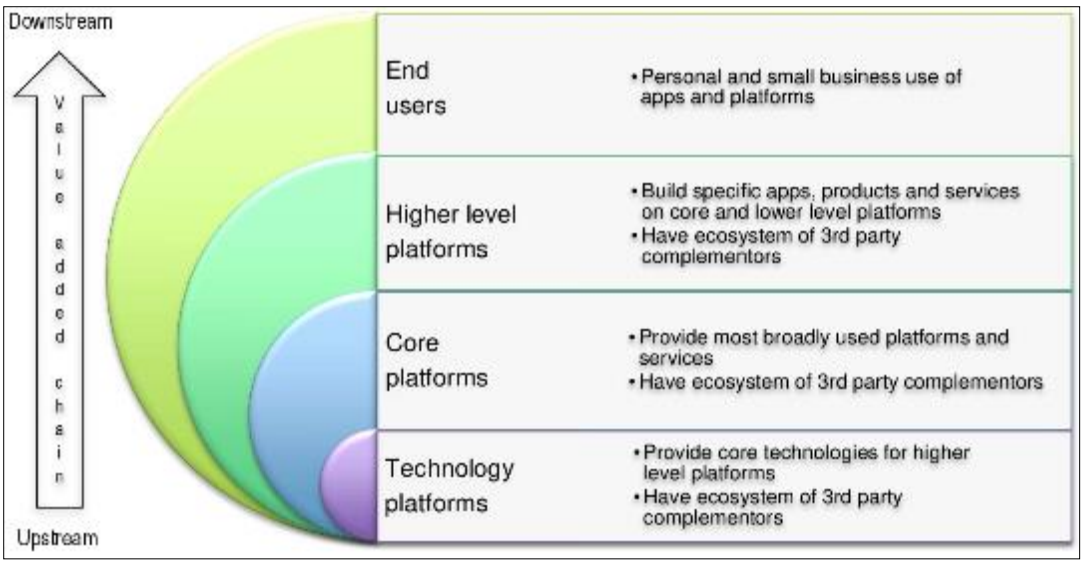

Figure 2 Digital platform value added chain

However, as economic empowerment digital platforms continue to shape our economic landscape, questions regarding regulation, fair competition, data privacy [12], and worker rights also arise. Balancing the benefits and challenges of these platforms requires thoughtful consideration and ongoing dialogue among stakeholders, including governments, platform operators, users, and society as a whole.

1.1. Typical economic empowerment digital platforms

In this era of digital transformation, economic empowerment digital platforms have emerged as powerful catalysts for change. They have revolutionized the way we participate in the economy, offering unprecedented opportunities for individuals and businesses alike. The key enablers for these digital platforms are shown in Figure 3.

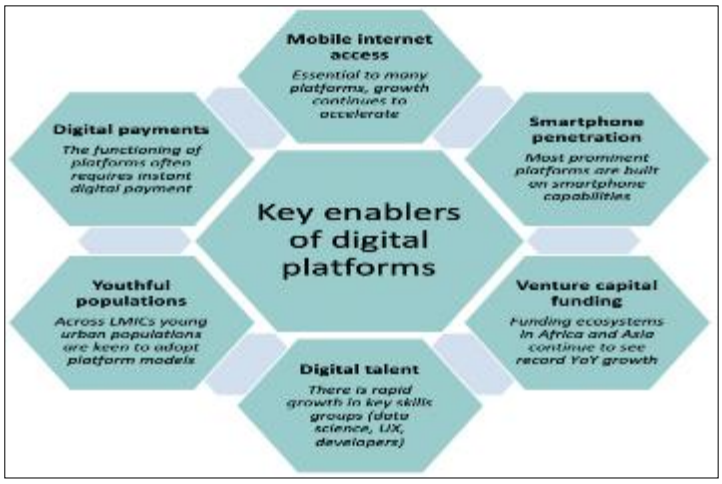

Figure 3 Digital platforms key enablers

By leveraging technology to break down barriers and foster economic inclusion, these platforms are shaping a future where economic empowerment is within reach for all [13]-[15]. The following are examples of economic empowerment digital platforms.

Freelancing Platforms: Platforms such as Upwork, Fiverr, and Freelancer enable individuals to offer their skills and services to clients worldwide [16], [17]. They provide opportunities for remote work, allowing individuals to access a global market and earn income based on their expertise.

E-commerce Platforms: Online marketplaces such as Amazon, eBay, and Alibaba empower individuals and small businesses to sell products and reach customers globally [18], [19]. These platforms offer a streamlined process for listing, selling, and delivering goods, expanding market access and facilitating entrepreneurship.

Crowd-funding Platforms: Websites such as Kickstarter, Indiegogo, and GoFundMe provide individuals and entrepreneurs with a platform to raise funds for their projects, businesses, or personal needs [20], [21]. These platforms enable people to leverage the power of the crowd and access capital without traditional financial intermediaries.

Microfinance Platforms: Digital microfinance platforms, such as Kiva and Zidisha, connect borrowers in developing countries with lenders globally [22], [23]. These platforms enable individuals with limited access to traditional financial services to secure loans and start or expand their businesses.

Peer-to-Peer Lending Platforms: Platforms such as LendingClub and Prosper facilitate lending between individuals, bypassing traditional financial institutions [24]. They provide borrowers with access to loans and investors with opportunities to earn interest on their investments.

Financial Management Apps: Apps such as Mint, YNAB (You Need a Budget), and PocketGuard help individuals track their expenses, budget effectively, and manage their finances [25]. These apps empower users to make informed financial decisions and improve their financial well-being.

Job Matching Platforms: Platforms such as LinkedIn, Indeed, and Glassdoor connect job seekers with employers. They provide tools for job searching, networking, and professional development, empowering individuals to find suitable employment opportunities [26].

These platforms contribute to economic empowerment by reducing barriers to entry, expanding market access, and providing individuals with tools and resources to improve their financial situation. Other merits derived from these platforms are depicted in Figure 4 below.

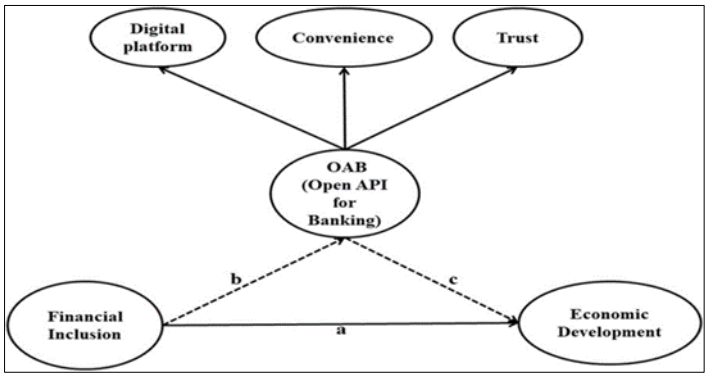

Figure 4 Rationale for digital platforms

By leveraging digital technologies [27], they enable individuals and businesses to participate in the global economy and access economic opportunities that were previously inaccessible. Table 1 discusses some of the examples of these digital platforms.

Table 1 Examples of economic empowerment digital platforms

Platform	Details
Upwork	An online freelancing platform that connects businesses and individuals with freelancers offering a wide range of skills and services [28].
eBay	A popular e-commerce platform that enables individuals and businesses to buy and sell a variety of products in an auction-style or fixed-price format [29].
Kiva	A microfinance platform that allows individuals to lend money to entrepreneurs and small businesses in developing countries to help them start or grow their ventures [30].
Kickstarter	A crowdfunding platform that enables individuals and businesses to raise funds for creative projects, inventions, and entrepreneurial ventures through contributions from the public [31].
LinkedIn	A professional networking platform that connects professionals, job seekers, and businesses, facilitating networking, job searching, and professional development opportunities [32].
Zidisha	A peer-to-peer [33] microfinance platform that connects lenders directly with borrowers in developing countries, enabling them to access affordable loans for business and personal needs [34].
Patreon	A membership platform that allows content creators, such as artists, writers, and musicians, to receive recurring payments from their fans and supporters in exchange for exclusive content or perks [35].
Fiverr	A freelance marketplace that specializes in services provided by freelancers, offering tasks such as graphic design, writing, programming, and marketing [36].
LendingClub	A peer-to-peer lending platform that connects borrowers with individual investors, providing personal loans and small business loans outside of traditional financial institutions [37].
Amazon	A leading e-commerce platform that allows individuals and businesses to sell products globally, leveraging its extensive customer base and fulfillment services [38].

These examples represent a diverse range of economic empowerment digital platforms, each offering unique opportunities for individuals and businesses to access financial resources, expand their reach, and enhance their economic opportunities.

1.2. General challenges of economic empowerment digital platforms

Economic empowerment digital platforms face a range of challenges that impact their effectiveness in promoting financial inclusion and empowerment. These challenges can be categorized into several broad areas as evidenced in Table 2 below.

Table 2 General challenges of economic empowerment digital platforms

Challenge	Description
Regulatory environment	Economic empowerment digital platforms often encounter regulatory challenges, as the legal frameworks and requirements vary across jurisdictions [39]. Unclear or outdated regulations may create uncertainties for platform operators, hindering their operations and expansion. Additionally, compliance with consumer protection laws, data privacy [40] regulations, and taxation requirements can be complex and resource-intensive for platforms to navigate.
Trust and reputation management	Trust is vital for the success of economic empowerment digital platforms. Establishing and maintaining trust among users is crucial, given that these platforms rely on user-generated content, transactions, and interactions [41]-[45]. Challenges such as fraudulent activities, identity verification, and maintaining user privacy can undermine trust. Implementing robust trust and reputation management systems, including effective user authentication, dispute resolution mechanisms, and transparent user reviews, is essential.
Technological infrastructure and security	Economic empowerment digital platforms operate in a rapidly evolving technological landscape, which presents challenges in terms of cybersecurity, data privacy, and platform stability [46]-[50]. Platforms must invest in advanced security measures to protect user information, prevent data breaches, and combat cyber threats. Moreover, they need to adapt to emerging technologies, such as blockchain and encryption, to enhance the security and integrity of transactions and user data.
Financial inclusion and accessibility	While economic empowerment digital platforms have the potential to empower individuals from diverse backgrounds, certain segments of society may face barriers to access and participation [51], [52]. Factors such as limited digital literacy, lack of internet connectivity, or financial constraints can hinder the inclusion of marginalized communities [54], [55]. Platforms need to address these challenges by offering user-friendly interfaces, providing support for digital literacy, and exploring innovative ways to reach underserved populations.
Digital divide and unequal opportunities	Economic empowerment digital platforms may inadvertently perpetuate existing inequalities if access and opportunities are not distributed equitably. The digital divide, characterized by disparities in access to technology and digital skills, can result in uneven participation and benefits [56]-[60]. Platforms should work towards bridging the digital divide by collaborating with governments, nonprofits, and community organizations to provide training, infrastructure, and support to individuals who are at risk of being left behind.
Ethical considerations and algorithmic bias	As economic empowerment digital platforms increasingly rely on algorithms and artificial intelligence for various processes, ethical considerations come to the forefront. Algorithmic bias, where automated decision-making processes exhibit discriminatory outcomes, can lead to unequal opportunities and perpetuate systemic biases [61]-[65]. Platforms must ensure fairness, transparency, and accountability in their algorithms and take steps to mitigate bias and discrimination.

Addressing these challenges requires a collaborative approach involving platform operators, policymakers, regulatory bodies, user communities, and other stakeholders. It involves developing supportive regulatory frameworks, implementing robust security measures, fostering digital literacy, promoting inclusivity, and ensuring ethical practices [66]-[70]. By overcoming these challenges, economic empowerment digital platforms can realize their potential in transforming economies, fostering financial inclusion, and empowering individuals and businesses.

1.3. Security challenges of economic empowerment digital platforms

Security challenges are a critical aspect of economic empowerment digital platforms due to the sensitive nature of financial transactions, user data, and personal information involved. Some key security challenges faced by these platforms are discussed in Table 3.

Table 3 Security challenges of economic empowerment digital platforms

Security issue	Explanation
Data breaches	Economic empowerment digital platforms handle vast amounts of user data, including personal information, financial details, and transaction records [71]-[75]. Data breaches can occur due to vulnerabilities in platform infrastructure, hacking attempts, insider threats, or inadequate security measures. Breaches can lead to unauthorized access to user data, identity theft, financial fraud, and reputational damage.
Cybersecurity threats	Cyberattacks pose a significant challenge to the security of these platforms. Malicious actors may attempt to exploit vulnerabilities, launch Distributed Denial of Service (DDoS) attacks, use phishing techniques, or employ malware to gain unauthorized access, disrupt services, or steal sensitive information [76]-[80]. Ensuring robust cybersecurity measures, such as encryption, multi-factor authentication, intrusion detection systems, and regular security audits, is crucial.
Identity verification	Verifying the identities of users is crucial for maintaining the integrity and trustworthiness of economic empowerment digital platforms. However, identity verification processes can be vulnerable to manipulation and fraud [81]-[85]. Platforms must implement strong identity verification mechanisms, such as document verification, biometrics, and knowledge-based authentication, to ensure that users are who they claim to be.
Payment security	Economic empowerment platforms often involve financial transactions, which require robust payment security measures. The risk of payment fraud, including credit card fraud and unauthorized transactions, must be mitigated through secure payment gateways, encryption of financial data, and compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements [86]-[90].
Privacy concerns	Users expect their personal information to be handled with utmost care and privacy. Economic empowerment platforms must establish and maintain robust privacy policies that comply with relevant data protection regulations [91]-[95]. Adequate data anonymization, consent management, and secure storage and transmission of user data are crucial to address privacy concerns.
Insider threats	Insiders with authorized access to the platform's systems and data can pose a significant security risk. This includes employees, contractors, or third-party service providers. Implementing strict access controls, regular monitoring, and security awareness training for all stakeholders can help mitigate insider threats [96]-[100].
Third-party integration risks	Economic empowerment platforms often integrate with third-party services, APIs, or external platforms. These integrations introduce additional security risks if not thoroughly vetted [101]-[105]. Due diligence should be exercised when selecting and integrating third-party services to ensure that they meet security standards and do not compromise the overall platform's security posture.

Addressing these security challenges requires a multi-layered approach. Economic empowerment digital platforms should implement robust security protocols, conduct regular vulnerability assessments and penetration testing, provide user education on security best practices, and establish incident response plans to mitigate and respond effectively to security incidents [106]-[110]. Collaborating with cybersecurity experts and staying abreast of evolving security threats is essential to protect user data, build trust, and maintain the security of economic empowerment digital platforms.

1.4. Solutions to Security challenges in economic empowerment digital platforms

To address the security challenges faced by economic empowerment digital platforms, several solutions and best practices can be implemented. These measures help enhance the security posture of the platforms and protect user data and transactions. Some of the solutions to these security challenges include the following:

Robust authentication and access controls: Implementing strong authentication mechanisms, such as multi-factor authentication (MFA) or biometrics, adds an extra layer of security to user accounts. Additionally, enforcing granular access controls ensures that users only have access to the data and functionalities they require for their roles, reducing the risk of unauthorized access [111]-[115].

Encryption: Implement end-to-end encryption for sensitive data, both in transit and at rest. This ensures that even if intercepted, the data remains unintelligible to unauthorized individuals [116]-[120]. Encryption should be applied to user data, financial transactions, and communication channels within the platform.

Regular security audits and vulnerability assessments: Conduct periodic security audits and vulnerability assessments to identify and address potential weaknesses in the platform's infrastructure, codebase, and configurations [121]-[125]. This includes conducting penetration testing to simulate attacks and identify areas for improvement.

Strong data protection and privacy measures: Comply with relevant data protection regulations, establish robust privacy policies, and inform users about the collection, use, and protection of their data. Implement data anonymization techniques where appropriate, and obtain user consent for data processing activities [126]-[130].

Secure payment processing: Utilize secure payment gateways and comply with industry standards such as Payment Card Industry Data Security Standard (PCI DSS). Implement fraud detection and prevention measures, such as transaction monitoring and verification processes, to protect against unauthorized payments and financial fraud [131]-[135].

Ongoing security training and awareness: Educate platform users, employees, and stakeholders about security best practices, including password hygiene, recognizing phishing attempts, and the importance of reporting suspicious activities [136]-[140]. Regularly communicate security updates and provide resources to help users protect their accounts and data.

Incident response planning: Develop and regularly update an incident response plan that outlines procedures for identifying, containing, mitigating, and recovering from security incidents [141]-[145]. This plan should include communication protocols, responsibilities, and coordination with relevant stakeholders.

Third-party risk management: Conduct thorough assessments of third-party service providers, vendors, and integration partners to ensure they meet security standards and adhere to best practices. Establish clear contractual obligations and enforce security requirements to mitigate risks associated with third-party integrations [146]-[150].

Proactive monitoring and intrusion detection: Implement robust monitoring systems to detect and respond to potential security breaches promptly. Intrusion detection and prevention systems, log monitoring, and real-time alerts can help identify suspicious activities and take proactive measures to mitigate potential threats [151]-[155].

Collaborative approach: Engage with cybersecurity experts, participate in industry forums, and collaborate with peer organizations to share insights, best practices, and threat intelligence [156]-[160]. Stay updated on emerging security threats, vulnerabilities, and recommended countermeasures.

Through the adoption of these solutions and practices, economic empowerment digital platforms can significantly improve their security posture, protect user data and transactions, and build trust among users [161]-[165]. It is important to continually assess and enhance security measures to adapt to evolving threats and maintain a secure environment for platform users.

1.5. Issues with the current security Solutions

While the solutions provided for addressing security challenges in economic empowerment digital platforms are generally effective, it is important to acknowledge that implementing them may encounter some issues or limitations. Some of these issues are summarized in Table 4.

Table 4 Issues with the current security Solutions

Issue	Description
Emerging threats and evolving technologies	The security landscape is constantly evolving, with new threats and vulnerabilities emerging regularly. Solutions that are effective today may become outdated or insufficient in the face of new and sophisticated attacks [166]-[170]. Keeping pace with evolving technologies and emerging threats requires continuous monitoring, research, and adaptation.
Balancing security and privacy	While strong security measures are essential, they should be balanced with user privacy considerations. Striking the right balance between data protection and usability can be challenging [171]-[175]. Stringent security measures may inadvertently compromise user privacy, leading to concerns about data collection, usage, and transparency.
Human factor and social engineering attacks	Despite technological safeguards, human error and social engineering attacks remain significant challenges. Users can inadvertently disclose sensitive information or fall victim to phishing attempts [176]-[180]. Educating users about security best practices and promoting awareness is critical but may not completely eliminate the risk of human-related security breaches.
Cost and resource constraints	Implementing robust security measures can be costly, especially for smaller or resource-constrained platforms. Investing in advanced security technologies, conducting regular audits, and maintaining a dedicated security team may require significant financial resources [181]-[185]. Platforms with limited budgets may face challenges in implementing comprehensive security solutions.
Complexity of third-party integration	Integrating with third-party services or APIs can introduce security risks. Assessing the security posture of third-party providers, ensuring compatibility with security standards, and maintaining ongoing security audits can be complex [186]-[190]. Platforms need to establish strong partnerships and rigorous vetting processes to mitigate third-party integration risks effectively.
User experience and convenience	Some security measures, such as multi-factor authentication or stringent identity verification, can add friction to the user experience. Striking a balance between security and user convenience is crucial [191]-[195]. If security measures become too burdensome or complex, it may lead to user frustration or abandonment of the platform.
Regulatory compliance	Compliance with various data protection and financial regulations can be a complex and evolving process. Economic empowerment digital platforms must stay up-to-date with regulatory requirements and adapt their security measures accordingly [196]-[199]. Compliance efforts may require significant time, resources, and expertise.

Proper tackling of these issues requires a proactive and holistic approach. Platforms should conduct risk assessments, prioritize security investments based on their specific needs, and strike a balance between usability, privacy, and security [200]-[204]. Collaboration with security experts, leveraging industry best practices, and staying informed about emerging threats are essential for maintaining a robust security posture. Regular evaluation and adaptation of security measures are necessary to address evolving challenges and protect the platform and its users effectively.

2. Conclusion

Economic empowerment digital platforms face a multitude of challenges that can impact their ability to foster financial inclusion and empowerment effectively. These challenges span regulatory, trust and reputation management, technological, accessibility, and security domains. Overcoming these challenges requires a collaborative effort among platform operators, policymakers, regulatory bodies, and user communities. Regulatory frameworks need to be adapted to the dynamic nature of digital platforms, ensuring clarity, fairness, and consistency across jurisdictions. Trust and reputation management systems must be robust, addressing issues like fraud, identity verification, and dispute resolution to maintain user confidence. Technological challenges, including cybersecurity threats and data breaches, call for strong security measures and proactive risk management. Ensuring financial inclusion and accessibility requires bridging the digital divide and addressing the barriers faced by marginalized communities in accessing and utilizing these platforms. Ethical considerations, such as algorithmic bias, need to be addressed to avoid perpetuating

inequalities. Collaboration among stakeholders is crucial to strike a balance between innovation and regulation, protecting the interests of users and society. While the solutions provided to address these challenges are effective, they may encounter issues such as cost constraints, user experience considerations, emerging threats, and the complexity of third-party integrations. Striking the right balance between security, privacy, and usability is a continuous effort that requires ongoing evaluation, adaptation, and collaboration with security experts and industry peers. By actively addressing these challenges, economic empowerment digital platforms can unlock their full potential in transforming economies, promoting financial inclusion, and empowering individuals and businesses. Ultimately, the collective efforts in overcoming these challenges will contribute to a more inclusive and sustainable economic ecosystem, where economic opportunities are accessible to all.

Compliance with ethical standards

Acknowledgement

Special appreciation goes to all colleagues who offered support during the development of this work.

Disclosure of conflict of interest

The author declares that he has no conflict of interest.

References

[1] Deng H, Duan SX, Wibowo S. Digital technology driven knowledge sharing for job performance. Journal of Knowledge Management. 2023 Feb 1;27(2):404-25.

[2] Rusch M, Schöggl JP, Baumgartner RJ. Application of digital technologies for sustainable product management in a circular economy: A review. Business Strategy and the Environment. 2023 Mar;32(3):1159-74.

[3] Holzmann P, Gregori P. The promise of digital technologies for sustainable entrepreneurship: A systematic literature review and research agenda. International Journal of Information Management. 2023 Feb 1;68:102593.

[4] Senyo PK, Gozman D, Karanasios S, Dacre N, Baba M. Moving away from trading on the margins: Economic empowerment of informal businesses through FinTech. Information Systems Journal. 2023 Jan;33(1):154-84.

[5] Luo S, Yimamu N, Li Y, Wu H, Irfan M, Hao Y. Digitalization and sustainable development: How could digital economy development improve green innovation in China?. Business Strategy and the Environment. 2023 May;32(4):1847-71.

[6] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan 4;13(2):691.

[7] Zhao Y, Song Z, Chen J, Dai W. The mediating effect of urbanisation on digital technology policy and economic development: Evidence from China. Journal of Innovation & Knowledge. 2023 Jan 1;8(1):100318.

[8] Li S, Chang G, Zunong R. Does regional digital economy development influence green investment?. Innovation and Green Development. 2023 Sep 1;2(3):100053.

[9] Rohatgi S, Gera N, Nayak K. Has digital banking usage reshaped economic empowerment of urban women?. Journal of Management and Governance. 2023 Apr 17:1-21.

[10] Majeed M, Rashid S. Economic Empowerment of Women Through a Mix of Traditional and Modern Channels: A Case for Women Led Informal Sector Venturing. The International Journal of Community and Social Development. 2023:25166026231173844.

[11] Yao W, Sun Z. The Impact of the Digital Economy on High-Quality Development of Agriculture: A China Case Study. Sustainability. 2023 Mar 25;15(7):5745.

[12] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[13] Tang CS. Innovative technology and operations for alleviating poverty through women's economic empowerment. Production and Operations Management. 2022 Jan;31(1):32-45.

[14] Wang J, Zhang G. Can environmental regulation improve high-quality economic development in China? The mediating effects of digital economy. Sustainability. 2022 Sep 26;14(19):12143.

[15] Yang W, Chen Q, Guo Q, Huang X. Towards sustainable development: How digitalization, technological innovation, and green economic development interact with each other. International Journal of Environmental Research and Public Health. 2022 Sep 27;19(19):12273.

[16] Blaising A, Dabbish L. Managing the Transition to Online Freelance Platforms: Self-Directed Socialization. Proceedings of the ACM on Human-Computer Interaction. 2022 Nov 11;6(CSCW2):1-26.

[17] Alvarez De La Vega JC, Cecchinato ME, Rooksby J. Design Opportunities for Freelancing Platforms: Online Freelancers' Views on a Worker-Centred Design Fiction. In2022 Symposium on Human-Computer Interaction for Work 2022 Jun 8 (pp. 1-19).

[18] Jeong H, Yi Y, Kim D. An innovative e-commerce platform incorporating metaverse to live commerce. International Journal of Innovative Computing, Information and Control. 2022 Feb;18(1):221-9.

[19] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[20] Anglin AH, Courtney C, Allison TH. Venturing for others, subject to role expectations? A role congruity theory approach to social venture crowd funding. Entrepreneurship Theory and Practice. 2022 Mar;46(2):421-48.

[21] Mao Y, Zhao X. Trust me, trust my words: Trustworthiness construction in Chinese online medical crowd-funding discourses. Pragmatics and Society. 2022 Nov 4;13(4):703-24.

[22] Liu A, Urquía-Grande E, López-Sánchez P, Rodríguez-López A. How technology paradoxes and self-efficacy affect the resistance of facial recognition technology in online microfinance platforms: Evidence from China. Technology in Society. 2022 Aug 1;70:102041.

[23] Liu A, Urquía-Grande E, López-Sánchez P, Rodríguez-López Á. Research into microfinance and ICTs: A bibliometric analysis. Evaluation and Program Planning. 2022 Dec 20:102215.

[24] Taleizadeh AA, Safaei AZ, Bhattacharya A, Amjadian A. Online peer-to-peer lending platform and supply chain finance decisions and strategies. Annals of Operations Research. 2022 Aug;315(1):397-427.

[25] Nemeczek F, Weiss D. Insights on Crypto Investors from a German Personal Finance Management App. Journal of Risk and Financial Management. 2023 Apr 18;16(4):248.

[26] Field E, Garlick R, Subramanian N, Vyborny K. Why Don't Jobseekers Search More? Barriers and Returns to Search on a Job Matching Platform.

[27] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InInternational Conference on Internet of Things as a Service 2021 Dec 13 (pp. 3-18). Cham: Springer International Publishing.

[28] Zhang T, Ladhak F, Durmus E, Liang P, McKeown K, Hashimoto TB. Benchmarking large language models for news summarization. arXiv preprint arXiv:2301.13848. 2023 Jan 31.

[29] Hui X, Jin GZ, Liu M. Designing quality certificates: Insights from eBay. National Bureau of Economic Research; 2022 Jan 24.

[30] Schwittay A. Digital mediations of everyday humanitarianism: the case of Kiva. org. Third World Quarterly. 2019 Oct 3;40(10):1921-38.

[31] Jensen LS, Özkil AG. Identifying challenges in crowdfunded product development: a review of Kickstarter projects. Design Science. 2018;4:e18.

[32] Davis J, Wolff HG, Forret ML, Sullivan SE. Networking via LinkedIn: An examination of usage and career benefits. Journal of Vocational Behavior. 2020 Apr 1;118:103396.

[33] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[34] Yartey FN, Birzescu AN. Surveillance of the poor in a socio-financial enclosure: a critical analysis of Zidisha. org. Development in Practice. 2015 Nov 17;25(8):1131-45.

[35] Regner T. Crowdfunding a monthly income: an analysis of the membership platform Patreon. Journal of Cultural Economics. 2021 Mar;45(1):133-42.

[36] Hannák A, Wagner C, Garcia D, Mislove A, Strohmaier M, Wilson C. Bias in online freelance marketplaces: Evidence from taskrabbit and fiverr. InProceedings of the 2017 ACM conference on computer supported cooperative work and social computing 2017 Feb 25 (pp. 1914-1933).

[37] Jagtiani J, Lemieux C. The roles of alternative data and machine learning in fintech lending: evidence from the LendingClub consumer platform. Financial Management. 2019 Dec;48(4):1009-29.

[38] Yang S, Jin W, Yu Y, Hashim KF. Optimized hadoop map reduce system for strong analytics of cloud big product data on amazon web service. Information Processing & Management. 2023 May 1;60(3):103271.

[39] Dredge D, Phi GT, Mahadevan R, Meehan E, Popescu E. Digitalisation in Tourism: In-depth analysis of challenges and opportunities.

[40] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[41] Schmitz AJ. There's an App for That: Developing Online Dispute Resolution to Empower Economic Development. Notre Dame JL Ethics & Pub. Pol'y. 2018;32:1.

[42] Zutshi A, Grilo A. The emergence of digital platforms: A conceptual platform architecture and impact on industrial engineering. Computers & Industrial Engineering. 2019 Oct 1;136:546-55.

[43] Taylor J, Dantu R, Wells T. Promoting Guest Satisfaction: Digital Platforms as a Means to Encourage Economic Development in Hospitality. International Journal of Hospitality & Tourism Administration. 2022 Aug 21:1-30.

[44] Cheng X, Fu S, Sun J, Bilgihan A, Okumus F. An investigation on online reviews in sharing economy driven hospitality platforms: A viewpoint of trust. Tourism Management. 2019 Apr 1;71:366-77.

[45] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[46] Van Dijck J. Governing digital societies: Private platforms, public values. Computer Law & Security Review. 2020 Apr 1;36:105377.

[47] Litvinenko VS. Digital economy as a factor in the technological development of the mineral sector. Natural Resources Research. 2020 Jun;29(3):1521-41.

[48] Salutina TY, Platunina GP, Vasileva IA. Transformation of business technologies into digital platforms and evaluation of the effectiveness of their application. In2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) 2021 Sep 6 (pp. 888-892). IEEE.

[49] Wang W, Xu H, Liu Y. Platform ruralism: Digital platforms and the techno-spatial fix. Geoforum. 2022 May 1;131:12-9.

[50] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[51] Ozili PK. Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review. 2018 Dec 1;18(4):329-40.

[52] Aziz A, Naima U. Rethinking digital financial inclusion: Evidence from Bangladesh. Technology in Society. 2021 Feb 1;64:101509.

[53] Chen W, Li X. Digital inequalities in American disadvantaged urban communities: Access, skills, and expectations for digital inclusion programs. Information, Communication & Society. 2022 Oct 3;25(13):1916-33.

[54] Navaneeth MS, Siddiqui I. How inclusive is online education in India: Lessons from the Pandemic. InSocioeconomic Inclusion During an Era of Online Education 2022 (pp. 135-155). IGI Global.

[55] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432).

[56] Heeks R. From digital divide to digital justice in the global south: conceptualising adverse digital incorporation. arXiv preprint arXiv:2108.09783. 2021 Aug 22.

[57] Schradie J. The great equalizer reproduces inequality: How the digital divide is a class power divide. InRethinking class and social difference 2020 Sep 30 (Vol. 37, pp. 81-101). Emerald Publishing Limited.

[58] Mathrani A, Sarvesh T, Umer R. Digital divide framework: online learning in developing countries during the COVID-19 lockdown. Globalisation, Societies and Education. 2022 Oct 20;20(5):625-40.

[59] Gran AB, Booth P, Bucher T. To be or not to be algorithm aware: a question of a new digital divide?. Information, Communication & Society. 2021 Sep 10;24(12):1779-96.

[60] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InInternational Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2022 May 4 (pp. 16-36). Cham: Springer International Publishing.

[61] Martin K, Shilton K, Smith JE. Business and the ethical implications of technology: Introduction to the symposium. InBusiness and the Ethical Implications of Technology 2022 Nov 10 (pp. 1-11). Cham: Springer Nature Switzerland.

[62] Shin D, Hameleers M, Park YJ, Kim JN, Trielli D, Diakopoulos N, Helberger N, Lewis SC, Westlund O, Baumann S. Countering algorithmic bias and disinformation and effectively harnessing the power of AI in media. Journalism & Mass Communication Quarterly. 2022 Dec;99(4):887-907.

[63] Shin D, Kee KF. Editorial Note for Special Issue on Al and Fake News, Mis (dis) information, and Algorithmic Bias. Journal of Broadcasting & Electronic Media. 2023 Jun 18:1-5.

[64] Marty F, Warin T. The Use of AI by Online Intermediation Platforms: Conciliating Economic Efficiency and Ethical Issues. Delphi. 2019;2:217.

[65] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[66] Bandari V. Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics. 2023 Jan 20;6(1):1-1.

[67] Telo J. Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing. 2023 Feb 27;6(1):31-45.

[68] Telo J. Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis. Sage Science Review of Educational Technology. 2023 Feb 12;6(1):26-38.

[69] Gayathri R, Usharani S, Mahdal M, Vezhavendhan R, Vincent R, Rajesh M, Elangovan M. Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques. Sensors. 2023 Feb 3;23(3):1708.

[70] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[71] Ayaburi EW. Understanding online information disclosure: examination of data breach victimization experience effect. Information Technology & People. 2023 Jan 13;36(1):95-114.

[72] Wang M, Qin Y, Liu J, Li W. Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks. Humanities and Social Sciences Communications. 2023 May 8;10(1):1-5.

[73] Mayer P, Zou Y, Lowens BM, Dyer HA, Le K, Schaub F, Aviv AJ. Awareness, Intention,(In) Action: Individuals' Reactions to Data Breaches. ACM Transactions on Computer-Human Interaction. 2023 Apr 17.

[74] Firoozi M, Ku CH. Corporate accountability during crisis in the digitized era. Accounting, Auditing & Accountability Journal. 2023 Apr 4;36(3):933-64.

[75] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[76] Saleous H, Ismail M, AlDaajeh SH, Madathil N, Alrabaee S, Choo KK, Al-Qirim N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digital Communications and Networks. 2023 Feb 1;9(1):211-22.

[77] Kotsias J, Ahmad A, Scheepers R. Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems. 2023 Jan 2;32(1):35-51.

[78] Johri A, Kumar S. Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Human Behavior and Emerging Technologies. 2023 Jan 12;2023.

[79] Salami Pargoo N, Ilbeigi M. A Scoping Review for Cybersecurity in the Construction Industry. Journal of Management in Engineering. 2023 Mar 1;39(2):03122003.

[80] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[81] Sai BD, Nikhil R, Prasad S, Naik NS. A decentralised KYC based approach for microfinance using blockchain technology. Cyber Security and Applications. 2023 Dec 1;1:100009.

[82] Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023 Jan 20;12(3):546.

[83] Ray PP. Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. Internet of Things and Cyber-Physical Systems. 2023 May 9.

[84] Sasikumar A, Vairavasundaram S, Kotecha K, Indragandhi V, Ravi L, Selvachandran G, Abraham A. Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. Future Generation Computer Systems. 2023 Apr 1;141:16-27.

[85] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[86] Behrendt C, Nguyen QA, Rani U. Social protection systems and the future of work: Ensuring social security for digital platform workers. International Social Security Review. 2019 Jul;72(3):17-41.

[87] Zutshi A, Grilo A, Nodehi T. The value proposition of blockchain technologies and its impact on Digital Platforms. Computers & industrial engineering. 2021 May 1;155:107187.

[88] Chesalina O. Access to social security for digital platform workers in Germany and in Russia: a comparative study. Spanish Labour Law and Employment Relations Journal. 2018 Oct 30;7(1-2):17-28.

[89] Kazan E, Tan CW, Lim ET. Towards a framework of digital platform disruption: A comparative study of centralized & decentralized digital payment providers. ACIS.

[90] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[91] Gal-Or E, Gal-Or R, Penmetsa N. The role of user privacy concerns in shaping competition among platforms. Information Systems Research. 2018 Sep;29(3):698-722.

[92] LeBlanc RJ, Aguilera E, Burriss S, de Roock R, Fassbender W, Monea B, Nichols TP, Pandya JZ, Robinson B, Smith A, Stornaiuolo A. Digital platforms and the ELA classroom. National Council of Teachers of English. 2023.

[93] Garces E, Fanaras D. Antitrust, Privacy, and Digital Platforms' Use of Big Data: A Brief Overview. Competition, Journal of the Antitrust, UCL, and Privacy Section of the California Lawyers Committee. 2018;28(1).

[94] Morimoto M. Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. International Journal of Advertising. 2021 May 21;40(3):431-51.

[95] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[96] Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys & Tutorials. 2018 Feb 1;20(2):1397-417.

[97] Alsowail RA, Al-Shehari T. A multi-tiered framework for insider threat prevention. Electronics. 2021 Apr 22;10(9):1005.

[98] Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. PeerJ Computer Science. 2022 Apr 1;8:e938.

[99] Stafford TF. Platform-dependent computer security complacency: The unrecognized insider threat. IEEE Transactions on Engineering Management. 2021 Mar 9;69(6):3814-25.

[100] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Dec 17;11(24):12040.

[101] Zala K, Thakkar HK, Jadeja R, Singh P, Kotecha K, Shukla M. PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms. IEEE Access. 2022 Aug 11;10:85777-91.

[102] Chan HL, Cheung TT, Choi TM, Sheu JB. Sustainable successes in third-party food delivery operations in the digital platform era. Annals of Operations Research. 2023 Apr 12:1-37.

[103] Fang J, Liu H, Cai Z, Tan CW. Omni-channel retailing on platforms: Disentangling the effects of channel integration and inter-platform function usage difference. Journal of Operations Management. 2023 Mar;69(2):197-216.

[104] Guo W, Straub D, Zhang P, Cai Z. How Trust Leads To Commitment On Microsourcing Platforms: Unraveling The Effects Of Governance And Third-Party Mechanisms On Triadic Microsourcing Relationships. MIS Quarterly. 2021 Sep 1;45(3).

[105] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[106] Abd-El-Atty B, Iliyasu AM, Alaskar H, Abd El-Latif AA. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors. 2020 May 31;20(11):3108.

[107] Masuda Y, Zimmermann A, Shirasaka S, Nakamura O. Internet of robotic things with digital platforms: Digitization of robotics enterprise. InHuman Centred Intelligent Systems: Proceedings of KES-HCIS 2020 Conference 2021 (pp. 381-391). Springer Singapore.

[108] Ansari MT, Agrawal A, Khan RA. DURASec: Durable Security Blueprints for Web-Applications Empowering Digital India Initiative. EAI Endorsed Transactions on Scalable Information Systems. 2022 Jan 13;9(4):e7-.

[109] Pamarthi S, Narmadha R. Adaptive key management-based cryptographic algorithm for privacy preservation in wireless mobile adhoc networks for IoT applications. Wireless Personal Communications. 2022 May;124(1):349-76.

[110] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1;23(4):145-62.

[111] Achar S. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering. 2022 Sep 13;16(9):379-84.

[112] Yu S, Park Y. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. IEEE Internet of Things Journal. 2022 May 2;9(20):20214-28.

[113] Esther C, GB ZS, Tamizhmalar D, Dhinakaran D. Trustworthy Cloud Storage Data Protection based on Blockchain Technology. In2022 International Conference on Edge Computing and Applications (ICECAA) 2022 Oct 13 (pp. 538-543). IEEE.

[114] Salonikias S, Khair M, Mastoras T, Mavridis I. Blockchain-based access control in a globalized healthcare provisioning ecosystem. Electronics. 2022 Aug 25;11(17):2652.

[115] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[116] Deebak BD, Memon FH, Khowaja SA, Dev K, Wang W, Qureshi NM, Su C. A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems. IEEE Internet of Things Journal. 2022 Feb 18;10(8):6652-60.

[117] Hoang TM. A novel design of multiple image encryption using perturbed chaotic map. Multimedia Tools and Applications. 2022 Jul;81(18):26535-89.

[118] Alzoubi HM, Ghazal TM, Hasan MK, Alketbi A, Kamran R, Al-Dmour NA, Islam S. Cyber Security Threats on Digital Banking. In2022 1st International Conference on AI in Cybersecurity (ICAIC) 2022 May 24 (pp. 1-4). IEEE.

[119] Alam A. Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records. InSmart Data Intelligence: Proceedings of ICSMDI 2022 2022 Aug 18 (pp. 307-320). Singapore: Springer Nature Singapore.

[120] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9;2(4):608-13.

[121] Chahal NS, Bali P, Khosla PK. A Proactive Approach to assess web application security through the integration of security tools in a Security Orchestration Platform. Computers & Security. 2022 Nov 1;122:102886.

[122] Popchev I, Radeva I, Velichkova V. Auditing blockchain smart contracts. In2022 International Conference Automatics and Informatics (ICAI) 2022 Oct 6 (pp. 276-281). IEEE.

[123] Rameder H, Di Angelo M, Salzer G. Review of automated vulnerability analysis of smart contracts on Ethereum. Frontiers in Blockchain. 2022 Mar 24;5:814977.

[124] Chahal NS, Abrol P, Khosla PK. Improvisation of Information System Security Posture Through Continuous Vulnerability Assessment. InProceedings of Emerging Trends and Technologies on Intelligent Systems: ETTIS 2022 2022 Nov 16 (pp. 231-250). Singapore: Springer Nature Singapore.

[125] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[126] Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science. 2022 Nov;50(6):1299-323.

[127] Abrardi L, Cambini C. Carpe Data: Protecting online privacy with naive users. Information Economics and Policy. 2022 Sep 1;60:100988.

[128] Farid G, Warraich NF, Iftikhar S. Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science. 2023 Apr 5:01655515231160026.

[129] Calzada I. Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). Smart Cities. 2022 Sep 8;5(3):1129-50.

[130] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InEAI International Conference on Applied Cryptography in Computer and Communications 2022 May 14 (pp. 46-64). Cham: Springer Nature Switzerland.

[131] Siagian H, Tarigan ZJ, Basana SR, Basuki R. The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform (Doctoral dissertation, Petra Christian University).

[132] Kumari A, Devi NC. The Impact of FinTech and Blockchain Technologies on Banking and Financial Services. Technology Innovation Management Review. 2022;12(1/2).

[133] Ben Amor N, Ben Yahia I. Investigating blockchain technology effects on online platforms transactions: Do risk aversion and technophilia matter?. Journal of Internet Commerce. 2022 Jul 3;21(3):271-96.

[134] Kanwal M, Burki U, Ali R, Dahlstrom R. Systematic review of gender differences and similarities in online consumers' shopping behavior. Journal of Consumer Marketing. 2022 Feb 9;39(1):29-43.

[135] Nyangaresi VO. A formally validated authentication algorithm for secure message forwarding in smart home networks. SN Computer Science. 2022 Jul 9;3(5):364.

[136] Koohang A, Sargent CS, Nord JH, Paliszkiewicz J. Internet of Things (IoT): From awareness to continued use. International Journal of Information Management. 2022 Feb 1;62:102442.

[137] Palanisamy R, Norman AA, Mat Kiah ML. BYOD policy compliance: Risks and strategies in organizations. Journal of Computer Information Systems. 2022 Jan 2;62(1):61-72.

[138] Corallo A, Lazoi M, Lezzi M, Luperto A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry. 2022 May 1;137:103614.

[139] Herath TB, Khanna P, Ahmed M. Cybersecurity practices for social media users: a systematic literature review. Journal of Cybersecurity and Privacy. 2022 Jan 20;2(1):1-8.

[140] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[141] Wolf K, Dawson RJ, Mills JP, Blythe P, Morley J. Towards a digital twin for supporting multi-agency incident management in a smart city. Scientific reports. 2022 Sep 28;12(1):16221.

[142] Mouratidis H, Islam S, Santos-Olmo A, Sanchez LE, Ismail UM. Modelling language for cyber security incident handling for critical infrastructures. Computers & Security. 2023 May 1;128:103139.

[143] Angafor GN, Yevseyeva I, Maglaras L. Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. Information & Computer Security. 2023 Mar 2.

[144] Zeitz K, Kay R, Naughton D, Bennett S, Bolton S. Campaign Disaster Response–What Makes It Different. Disaster medicine and public health preparedness. 2023;17:e248.

[145] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[146] Tiwari S, Sharma P, Choi TM, Lim A. Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. Transportation Research Part E: Logistics and Transportation Review. 2023 Feb 1;170:103012.

[147] Zhou H, Wang Q, Wang L, Zhao X, Feng G. Digitalization and third-party logistics performance: exploring the roles of customer collaboration and government support. International Journal of Physical Distribution & Logistics Management. 2023 Jan 12.

[148] Zhou C, Li X, Ren Y, Yu J. How do fairness concern and power structure affect competition between e-platforms and third-party sellers?. IEEE Transactions on Engineering Management. 2023 Apr 12.

[149] Zufferey N, Niksirat KS, Humbert M, Huguenin K. "Revoked just now!" Users' Behaviors toward Fitness-Data Sharing with Third-Party Applications. Proceedings on Privacy Enhancing Technologies. 2023;2023(1):21.

[150] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[151] Wu W, Shen L, Zhao Z, Harish AR, Zhong RY, Huang GQ. Internet of Everything and Digital Twin Enabled Service Platform for Cold Chain Logistics. Journal of Industrial Information Integration. 2023 Jun 1;33:100443.

[152] de Azambuja AJ, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics. 2023 Apr 19;12(8):1920.

[153] Bhandari G, Lyth A, Shalaginov A, Grønli TM. Distributed Deep Neural-Network-Based Middleware for Cyber-Attacks Detection in Smart IoT Ecosystem: A Novel Framework and Performance Evaluation Approach. Electronics. 2023 Jan 6;12(2):298.

[154] TN N, Pramod D. Insider Intrusion Detection Techniques: A State-of-the-Art Review. Journal of Computer Information Systems. 2023 Feb 11:1-8.

[155] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[156] Zainal-Abidin H, Scarles C, Lundberg C. The antecedents of digital collaboration through an enhanced digital platform for destination management: A micro-DMO perspective. Tourism Management. 2023 Jun 1;96:104691.

[157] Gong Y, Li X. Designing boundary resources in digital government platforms for collaborative service innovation. Government Information Quarterly. 2023 Jan 1;40(1):101777.

[158] Reim W, Andersson E, Eckerwall K. Enabling collaboration on digital platforms: a study of digital twins. International Journal of Production Research. 2023 Jun 18;61(12):3926-42.

[159] Mukti IY, Firdausy DR, Aldea A, Iacob ME. Architecting rural smartness: A collaborative platform design for rural digital business ecosystem. The Electronic Journal of Information Systems in Developing Countries. 2023 Jan;89(1):e12236.

[160] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[161] Xu R, Zhang L, Zhao H, Peng Y. Design of network media's digital rights management scheme based on blockchain technology. In2017 IEEE 13th international symposium on autonomous decentralized system (ISADS) 2017 Mar 22 (pp. 128-133). IEEE.

[162] Pisa M, Juden M. Blockchain and economic development: Hype vs. reality. Center for global development policy paper. 2017 Jul;107:150.

[163] Chen Y, Kumara EK, Sivakumar V. Investigation of finance industry on risk awareness model and digital economic growth. Annals of Operations Research. 2021 Oct 29:1-22.

[164] Gadekallu TR, Huynh-The T, Wang W, Yenduri G, Ranaweera P, Pham QV, da Costa DB, Liyanage M. Blockchain for the metaverse: A review. arXiv preprint arXiv:2203.09738. 2022 Mar 18.

[165] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[166] Gitelman LD, Kozhevnikov MV. Adoption of technology platforms in the electric power industry: New opportunities. WIT Trans. Ecol. Environ. 2022 Jul 19;255:23-34.

[167] Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. Journal of computer and system sciences. 2014 Aug 1;80(5):973-93.

[168] Molchanova KM, Trushkina NV, Katerna OK. Digital platforms and their application in the aviation industry. Intellectualization of logistics and Supply Chain Management. 2020(3):83-98.

[169] Buckley RP, Arner DW, Zetzsche DA, Selga E. The dark side of digital financial transformation: The new risks of fintech and the rise of techrisk. UNSW Law Research Paper. 2019 Nov 18(19-89).

[170] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11;2(3):399-406.

[171] Househ M, Grainger R, Petersen C, Bamidis P, Merolli M. Balancing between privacy and patient needs for health information in the age of participatory health and social media: a scoping review. Yearbook of medical informatics. 2018 Aug;27(01):029-36.

[172] Krämer NC, Schäwel J. Mastering the challenge of balancing self-disclosure and privacy in social media. Current opinion in psychology. 2020 Feb 1;31:67-71.

[173] Kuziemsky CE, Gogia SB, Househ M, Petersen C, Basu A. Balancing health information exchange and privacy governance from a patient-centred connected health and telehealth perspective. Yearbook of medical informatics. 2018 Aug;27(01):048-54.

[174] Hacker P. Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. European Law Journal. 2021 May.

[175] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[176] Weber K, Schütz AE, Fertig T, Müller NH. Exploiting the human factor: Social engineering attacks on cryptocurrency users. InLearning and Collaboration Technologies. Human and Technology Ecosystems: 7th International Conference, LCT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22 2020 (pp. 650-668). Springer International Publishing.

[177] Postnikoff B, Goldberg I. Robot social engineering: Attacking human factors with non-human actors. InCompanion of the 2018 ACM/IEEE international conference on human-robot interaction 2018 Mar 1 (pp. 313-314).

[178] Alavi R, Islam S, Mouratidis H, Lee S. Managing Social Engineering Attacks-Considering Human Factors and Security Investment. InHAISA 2015 Jun 3 (pp. 161-171).

[179] Ghafir I, Saleem J, Hammoudeh M, Faour H, Prenosil V, Jaf S, Jabbar S, Baker T. Security threats to critical infrastructure: the human factor. The Journal of Supercomputing. 2018 Oct;74:4986-5002.

[180] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[181] Singh P, Acharya B, Chaurasiya RK. A comparative survey on lightweight block ciphers for resource constrained applications. International Journal of High Performance Systems Architecture. 2019;8(4):250-70.

[182] Gao Y, Su Y, Yang W, Chen S, Nepal S, Ranasinghe DC. Building secure SRAM PUF key generators on resource constrained devices. In2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) 2019 Mar 11 (pp. 912-917). IEEE.

[183] Karimian N, Guo Z, Tehranipoor F, Woodard D, Tehranipoor M, Forte D. Secure and reliable biometric access control for resource-constrained systems and IoT. arXiv preprint arXiv:1803.09710. 2018 Mar 26.

[184] Pei C, Xiao Y, Liang W, Han X. Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks. EURASIP Journal on Wireless Communications and Networking. 2018 Dec;2018:1-8.

[185] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[186] Bialke M, Penndorf P, Wegner T, Bahls T, Havemann C, Piegsa J, Hoffmann W. A workflow-driven approach to integrate generic software modules in a Trusted Third Party. Journal of translational medicine. 2015 Dec;13:1-8.

[187] Eloranta V, Turunen T. Platforms in service-driven manufacturing: Leveraging complexity by connecting, sharing, and integrating. Industrial Marketing Management. 2016 May 1;55:178-86.

[188] Diaconescu A, Frey S, Müller-Schloer C, Pitt J, Tomforde S. Goal-oriented holonics for complex system (self-) integration: Concepts and case studies. In2016 IEEE 10th International Conference on Self-Adaptive and Self-Organizing Systems (SASO) 2016 Sep 12 (pp. 100-109). IEEE.

[189] Muslmani BK, Kazakzeh S, Ayoubi E, Aljawarneh S. Reducing integration complexity of cloud-based ERP systems. InProceedings of the First International Conference on Data Science, E-learning and Information Systems 2018 Oct 1 (pp. 1-6).

[190] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A lightweight hybrid scheme for hiding text messages in colour images using LSB, Lah transform and Chaotic techniques. Journal of Sensor and Actuator Networks. 2022 Oct 17;11(4):66.

[191] Shah Y, Choyi V, Subramanian L. Multi-factor Authentication as a Service. In2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering 2015 Mar 30 (pp. 144-150). IEEE.

[192] Moses S, Rowe DC. Physical security and cybersecurity: Reducing risk by enhancing physical security posture through multi-factor authentication and other techniques. International Journal for Information Security Research (IJISR). 2016 Jun;6(2):667-76.

[193] Bajaj P, Arora R, Khurana M, Mahajan S. Cloud security: the future of data storage. InCyber Security and Digital Forensics: Proceedings of ICCSDF 2021 2022 (pp. 87-98). Springer Singapore.

[194] Ranise S, Sciarretta G, Tomasi A. Enroll, and Authentication Will Follow: eID-Based Enrollment for a Customized, Secure, and Frictionless Authentication Experience. InInternational Symposium on Foundations and Practice of Security 2019 Nov 5 (pp. 156-171). Cham: Springer International Publishing.

[195] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[196] Voigt P, Von dem Bussche A. The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing. 2017 Aug 10;10(3152676):10-5555.

[197] Zetzsche DA, Arner DW, Buckley RP. Decentralized finance (defi). Journal of Financial Regulation. 2020 Sep 30;6:172-203.

[198] Tikkinen-Piri C, Rohunen A, Markkula J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. 2018 Feb 1;34(1):134-53.

[199] Mazurek G, Małagocka K. Perception of privacy and data protection in the context of the development of artificial intelligence. Journal of Management Analytics. 2019 Oct 2;6(4):344-64.

[200] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[201] Taloba AI, Elhadad A, Rayan A, Abd El-Aziz RM, Salem M, Alzahrani AA, Alharithi FS, Park C. A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal. 2023 Feb 15;65:263-74.

[202] Yadav S, Tiwari N. Privacy preserving data sharing method for social media platforms. PloS one. 2023 Jan 20;18(1):e0280182.

[203] Ghazal TM, Hasan MK, Abdullah SN, Bakar KA, Taleb N, Al-Dmour NA, Yafi E, Chauhan R, Alzoubi HM, Alshurideh M. An integrated cloud and blockchain enabled platforms for biomedical research. InThe Effect of Information Technology on Business and Marketing Intelligence Systems 2023 Feb 9 (pp. 2037-2053). Cham: Springer International Publishing.

[204] Wang Z, Yuan C, Li X. Evolutionary Analysis of the Regulation of Data Abuse in Digital Platforms. Systems. 2023 Apr 7;11(4):188.