SemantJournals

American Journal of Technology Advancement 2997-9382, Vol 01, No. 04, 2024

Article

Third-Party Risk Management in API-Driven Ecosystems: Continuous Vendor Security Practices and Emerging Challenges

Afsara Tasnim Shama

System Engineer, Department of ITSM NOC, Wipro IT Service Limited, Bangladesh

Email: afsaratasnim.shama@wipro.com

Abstract: Background: APIs are crucial for the digital transformation process due to the integration capabilities provided by them. Nevertheless, greater dependence on outside services has increased the number of potential cybersecurity threats, which makes the problem of third-party risk management one of the top priorities in organizations. The purpose of this study is to identify current continuous vendor security approaches and security challenges that arise in the environment of APIs. Methods: Quantitative cross-sectional research method was applied in the current study. Online questionnaire survey was administered to the US professionals, where 185 questionnaires were distributed, and 165 valid responses were received. Results: The highest mean was obtained in Third Party Risk Management Effectiveness (4.15), while Real Time API Monitoring received the second highest mean (4.12). Real Time API Monitoring also received the highest positive response (74.5%) showing its significance in the process of continuous security management. Limited Vendor Transparency (18.2%) became the main challenge in terms of third-party security risks. Correlation analysis showed the presence of strong positive correlations among all variables studied; the highest correlation was obtained for Real Time API Monitoring and Third-Party Risk Management Effectiveness (r = 0.756), which proves that more monitoring leads to better risk management. Conclusion: The results show the significance of vendor continuous security practices, real-time API monitoring and compliance management in the process of third-party risk management.

Keywords: Third-party risk management, API security, Vendor security, Continuous monitoring, Cybersecurity governance

1. Introduction

Application Programming Interfaces have revolutionized the world of computing by allowing seamless integration, interoperability, and exchange of data between different software applications, cloud services, mobile applications, and enterprise information systems [1]. With rapid digital transformation taking place in many industries, the use of APIs has become an important aspect of integration of third party services and delivery of new digital products [2]. Banking, healthcare, e-commerce, manufacturing, telecoms, and even government institutions have come to rely on third party providers offering specific services via API-based architecture [3]. While these integrations bring benefits to their respective organizations in terms of increased efficiency, scalability, and agility, they increase the attack surface at the same time, thus becoming one of the biggest risks of modern businesses [4]. Organizations' reliance on external vendors and APIs has led to an entirely different approach to cybersecurity. In addition to internal controls, the cybersecurity of an organization now depends on the cybersecurity of its vendors and how their respective systems are integrated via APIs

[5]. A single vulnerability in one vendor's systems may lead to serious consequences for many organizations connected to them [6]. Third-party risk management has therefore been identified as a core element of enterprise cybersecurity governance [7]. Firms are now moving from vendor security assessments to security management that involves real-time monitoring, automated risk assessment, continuous compliance checking, and proactive threat detection all through the vendor life cycle [8], [9].

While considerable advancements have been made in the field of cybersecurity technologies, managing third-party risks in API-driven environments is still a challenging task [10]. Organizations are confronted with the problem of lack of visibility in terms of the security controls in place at vendors, poor implementation of authentication and authorization processes, delays in deploying security patches and continuous monitoring of API activities [11]. Cybersecurity attacks are becoming increasingly sophisticated and challenging including software supply chain attacks, ransomware campaigns, and API abuse techniques among others. In addition, organizations are required to implement new governance strategies that enable them to continuously assess the security posture of their vendors in order to comply with regulations and standards [12]. Whereas past studies have considered the subjects of API security, cybersecurity governance, software supply chain security, and vendor risk management separately, there is little empirical research on the relationship between continuous vendor security practices and new security threats, as well as their collective impact on the effectiveness of third-party risk management in the case of API usage. Specifically, very little focus has been placed on the collective effect of continuous vendor security practices, vendor compliance management, real-time monitoring of APIs, automatic risk assessment, and new third-party security risks on enhancing cybersecurity in organizations [13]. This research gap needs to be addressed because good third-party risk management entails both aspects.

Therefore, this research explores third party risk management within API-based ecosystems based on data obtained through an online survey of 165 individuals in the United States. In particular, the research aims to measure the impact of Continuous Vendor Security Practices, Vendor Compliance Management, Real Time API Monitoring, Automated Risk Assessment, and Emerging Third Party Security Challenges on Third Party Risk Management Effectiveness. With empirical analysis on such vital factors, the research seeks to contribute to the existing cybersecurity literature by giving practical information on vendor governance, API security, real-time monitoring, and other essential areas of third party risk management.

2. Materials and Methods

2.1 Study Design and Participants

The research utilized a quantitative approach by employing a cross-sectional survey method to investigate third-party risk management within API-enabled environments, focusing on continual vendor security and contemporary security issues. The study was carried out via an online survey administered to professionals from the United States having practical experience with API security, cybersecurity governance, and third-party risk management. The qualified candidates for the research were cybersecurity professionals, software developers, IT managers, security consultants, and academic researchers [14]. Purposive and convenience sampling methods were employed to identify suitable participants with relevant expertise. The survey was distributed using the social media platform, LinkedIn, cybersecurity professional groups, cybersecurity forums, and professional networks from the United States. 185 surveys were distributed, with 165 complete surveys forming part of the data analysis, hence providing an 89.2% response rate.

2.2 Survey Instrument and Data Collection

The data was collected through a structured online questionnaire that was developed based on previous research on cyber security governance, API security, and third party risk management. The questionnaire had two sections. In the first section, the demographic information was collected. This involved collecting information such as gender, age, education qualification, professional experience, occupation, organization, type and degree of API utilization [15]. The second section involved assessing six constructs which include: Continuous Vendor Security Practices, Vendor Compliance

Management, Real Time API Monitoring, Automated Risk Assessment, Emerging Third Party Security Challenges, and Third Party Risk Management Effectiveness. Several items were used for the measurement of each construct and this was done through a five point Likert scale. This is rated from Strongly Disagree (1) to Strongly Agree (5) [16], [17].

2.3 Data Analysis

Data collection for the study was subjected to IBM SPSS Statistics Version 26 based on the conventional quantitative research methods [18]. The use of descriptive statistics, which include frequencies, percentages, means, variances, skewness, and kurtosis, was undertaken to provide a summary of the respondents' demographics and to assess the distribution of the study variables [19]. The study constructs' relationship was determined through Pearson correlation analysis. Multi-collinearity diagnosis using the variance inflation factor (VIF) and tolerance values was carried out prior to the estimation of the regression analysis model to ensure that the predictor variables were relatively independent [20]. Multiple regression analysis was applied to assess the influence of Continuous Vendor Security Practices, Vendor Compliance Management, Real Time API Monitoring, Automated Risk Assessment, and Emerging Third Party Security Challenges on Third Party Risk Management Effectiveness [21].

3. Results

3.1 Demographic Characteristics of the Respondents

Table 1. Demographic Characteristics of the Respondents

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	102	61.8
	Female	63	38.2
Age Group (Years)	20–29	38	23.0
	30–39	59	35.8
	40–49	43	26.1
	50 years and above	25	15.2
Educational Qualification	Bachelor's Degree	40	24.2
	Master's Degree	77	46.7
	Doctoral Degree	34	20.6
	Professional Certification	14	8.5
Professional Experience	Less than 5 years	28	17.0
	5–10 years	56	33.9
	11–15 years	46	27.9
	More than 15 years	35	21.2
Primary Occupation	Cybersecurity Professional	48	29.1
	Software Developer	40	24.2
	Information Technology Manager	32	19.4
	Security Consultant	24	14.5
	Academic Researcher	21	12.7
Organization Type	Large Enterprise	62	37.6
	Small and Medium Enterprise	44	26.7

Variable	Category	Frequency (n)	Percentage (%)
	Government Organization	27	16.4
	Technology Service Provider	21	12.7
	Academic Institution	11	6.7
Level of API Usage	Extensive	71	43.0
	Moderate	59	35.8
	Limited	35	21.2

The demographic attributes of the 165 sampled individuals show that the study has a well-diversified and professionally experienced sample to examine third-party risk management within API-driven environments as shown in Table 1. Male individuals made up 61.8% of the sampled population while females made up 38.2%. The largest portion of the sampled individuals was in the age range of 30 – 39 years (35.8%) followed by 40 - 49 years (26.1%), thus indicating that the sample is largely populated by mid-career individuals. Almost half of the respondents had a master's degree (46.7%), implying a highly-educated workforce. In terms of work experience, 33.9% had between 5 and 10 years and 27.9% had 11 to 15 years, thus showing that the sample had plenty of industry experience. Cybersecurity experts were the most common occupations among the respondents (29.1%) followed by software developers (24.2%). Furthermore, 37.6% of the individuals worked in large organizations and 43.0% reported heavy usage of APIs.

3.2 Descriptive Statistics of the Study Variables

Table 2. Descriptive Statistics of the Study Variables

Study Variable	Mean	SD	Variance	Skewness	Kurtosis
Continuous Vendor Security Practices	4.08	0.73	0.533	-0.68	0.47
Vendor Compliance Management	3.96	0.77	0.593	-0.52	0.21
Real Time API Monitoring	4.12	0.69	0.476	-0.81	0.74
Automated Risk Assessment	3.91	0.81	0.656	-0.45	-0.12
Emerging Third Party Security Challenges	3.87	0.75	0.563	-0.37	-0.28
Third Party Risk Management Effectiveness	4.15	0.71	0.504	-0.73	0.58

The findings from the descriptive statistics were consistently positive perceptions about all study variables concerning third-party risk management in API-driven ecosystem as seen in Table 2. Third Party Risk Management Effectiveness had the highest mean (4.15) which was indicative of the respondents' positive perception regarding the effectiveness of existing risk management strategies. Real Time API Monitoring came second (4.12) showing the importance of real time monitoring for security. Third Party Security Practices (4.08) were also highly positively perceived which indicated that there is significant need for proactive security practices. Similarly, Vendor Compliance Management (3.96) and Automated Risk Assessment (3.91) were both highly positively perceived. Even though Emerging Third Party Security Challenges was the variable with the lowest mean (3.87), it is an indication of increasing importance of emerging challenges in cyber security.

3.3 Responses to Continuous Vendor Security Practices

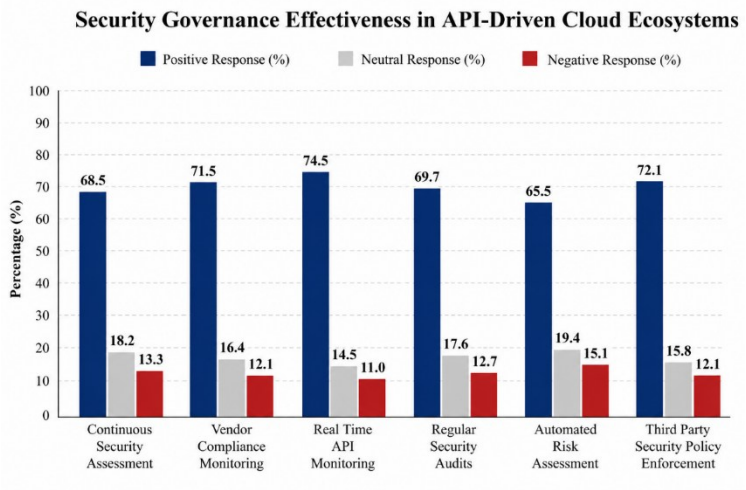

Figure 1. Responses to Continuous Vendor Security Practices

The perceptions of continuous vendor security measures in the ecosystem powered by API as shows in Figure 1. The number of positive answers exceeded the number of negative answers in each aspect of security. The respondents showed high support of the continuous vendor security programs. In this context, Real Time API Monitoring received the largest number of positive answers (74.5%), stressing its importance in identifying and reacting to any threats related to security. The respondents highly agreed on the issues of Third Party Security Policy Enforcement (72.1%) and Vendor Compliance Monitoring (71.5%). Regular Security Audits (69.7%) and Continuous Security Assessment (68.5%) were also considered necessary for ensuring vendor security. Despite the fact that Automated Risk Assessment received the smallest number of positive answers (65.5%), this measure was still positively assessed by the majority of respondents. Neutral answers ranged from 14.5% to 19.4%, and negative answers were rather low (11.0%–15.1%).

3.4 Distribution of Third Party Security Challenges

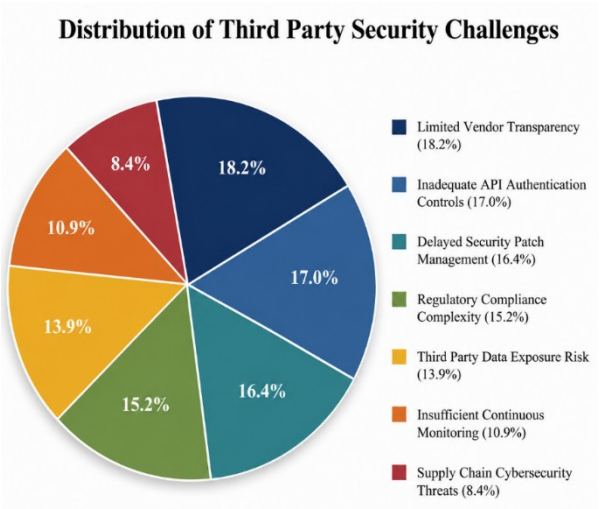

Figure 2. Distribution of Third Party Security Challenges

The distribution of the main third-party security problems reported by the participants in this study as shown in Figure 2. The most prevalent problem was Limited Vendor Transparency, which was reported by 18.2% of the participants and indicates that there is a lack of adequate transparency on the part of the vendors in relation to their security procedures. Inadequate API Authentication Controls (17.0%) and Delayed Security Patch Management (16.4%) were two other significant

problems that require attention from businesses, given the importance of proper authentication and fast patch management. Regulatory Compliance Complexity was reported by 15.2%, showing the difficulty involved in ensuring compliance with regulations in API-based systems. Third Party Data Exposure Risk comprised 13.9% of the reported problems and showed that organizations are concerned about the exposure of data and privacy in third parties.

3.5 Third Party Risk Management Practices in API-Driven Ecosystems

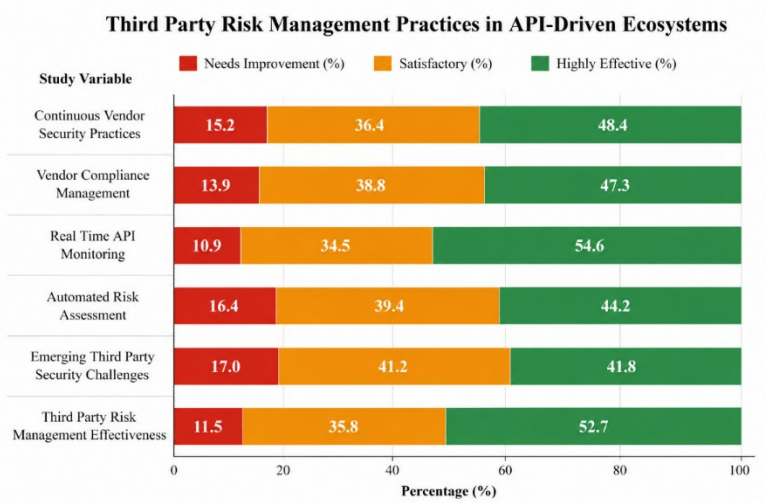

Figure 3. Third Party Risk Management Practices in API-Driven Ecosystems

The assessment of the important third-party risk management practices in the ecosystem of APIs as presents in Figure 3. According to the results, there are positive perceptions about all study variables, where the majority of respondents consider the practices to be highly effective or satisfactory. Real Time API Monitoring was evaluated as the most positively rated practice for being highly effective (54.6%). It is important to stress the importance of this factor for real-time monitoring of threats. Third Party Risk Management Effectiveness was assessed as highly effective (52.7%). This result shows that the respondents believe in effectiveness of their organizations' risk management programs. Continuous Vendor Security Practices (48.4%) and Vendor Compliance Management (47.3%) were rated by the respondents as highly effective too. The Automated Risk Assessment had 44.2% of highly effective responses and the Emerging Third Party Security Challenges had the largest satisfactory responses (41.2%).

3.6 Pearson Correlation Matrix of the Study Variables

Table 3. Pearson Correlation Matrix of the Study Variables

Variable	CVSP	VCM	RTM	ARA	ETSC	TPRME
CVSP	1					
VCM	0.641	1				
RTM	0.682	0.593	1			
ARA	0.574	0.621	0.668	1		
ETSC	0.486	0.518	0.557	0.601	1	
TPRME	0.731	0.684	0.756	0.703	0.589	1

CVSP, Continuous Vendor Security Practices; VCM, Vendor Compliance Management; RTM, Real Time API Monitoring; ARA, Automated Risk Assessment; ETSC, Emerging Third Party Security Challenges; TPRME, Third Party Risk Management Effectiveness.

Pearson correlation analysis for the research variables are presented in Table 3. All correlations were positive, suggesting that an increase in one element of the third party risk management process was connected to the improvement in the other aspects. The highest correlation coefficient was noted between the Real Time API Monitoring and Third Party Risk Management Effectiveness (r = 0.756), followed by the Continuous Vendor Security Practices and Third Party Risk Management Effectiveness (r = 0.731). Automated Risk Assessment variable had a positive correlation of r = 0.703 with Third Party Risk Management Effectiveness, whereas the Vendor Compliance Management had a strong correlation of r = 0.684. The moderate positive relationships were found between other variables, with the values from 0.486 to 0.682. Given the fact that all coefficients were below 0.80, it can be assumed that there is no multi-collinearity in this case.

4. Discussion

The present research is an empirical study on the risk management practices among respondents regarding continuous vendor security, compliance management, monitoring, automated risk assessment, and new security challenges within API-driven ecosystems. According to the demographic results, the survey collected opinions of experienced participants, with 43.0% of them reporting that they use a lot of APIs, and 37.6% representing large companies. It means that the survey reflected the experience of organizations that have already faced some challenges associated with API management, and, thus, it can be used as a basis for further research [22]. Descriptive statistics show that, on average, respondents viewed third-party risk management practices positively [23]. In terms of all research variables, the highest mean was obtained by Third Party Risk Management Effectiveness (4.15), which means that many organizations implement appropriate governance mechanisms in order to mitigate the risks related to the vendors' cybersecurity. Moreover, the variable of Real Time API Monitoring obtained a high mean value (4.12) that reflects its significance in continuous identification of any abnormalities, detection of security events, and decrease of the response time. It shows that continuous monitoring became a basic part of the organization's cybersecurity strategy [24].

The assessment of vendor security practices continuously is another important element which supports the above findings. 74.5% of the survey participants indicated positive perceptions towards Real Time API Monitoring, 72.1% of them were satisfied with Third Party Security Policy Enforcement and 71.5% with Vendor Compliance Monitoring. Hence, these findings clearly point to the recognition of organizations of the necessity of continuous monitoring, policy enforcement and compliance verification as integral parts of vendor risk management process [25]. Even though the percentage of positive perceptions towards Automated Risk Assessment was the smallest (65.5%), the majority of the survey participants recognized that automated risk assessment helps in identifying vulnerabilities and assessing security risks effectively. It may be inferred that even though the organizations are recognizing the importance of automation, they may be facing issues with the use of advanced analytical techniques and capabilities in integrating them [26]. However, along with the positive perceptions of the organizations, there were also security challenges identified through this study. Limited Vendor Transparency (18.2%) was identified as the highest occurring challenge, followed by Inadequate API Authentication Controls (17.0%) and Delayed Security Patch Management (16.4%). These vulnerabilities can create opportunities for breaches and attacks on unauthorized access and supply chain. It is clear that it is necessary to have better vendor governance frameworks, security requirements standardization and monitoring during the whole period of vendor’s activity [27], [28]

Correlation analysis also supports the suggested research framework by proving the positive associations between all considered variables [29]. The highest correlation between the factors was found between Real Time API Monitoring and Third Party Risk Management Effectiveness (r = 0.756) as well as between Continuous Vendor Security Practices and Third Party Risk Management Effectiveness (r = 0.731). It proves that companies that use continuous monitoring and security practices are likely to have effective third party risk management results. Moreover, all correlation values were less than 0.80 which means the lack of serious multicollinearity in the proposed model.

It means that the combination of continuous monitoring, vendor compliance management, risk assessment automation and security governance is very helpful for the organization.

5. Conclusion

The study shows that effective risk management of third-party risks within the API ecosystem is contingent on consistent vendor security measures, API monitoring, compliance management, and risk assessment. Positive trends in organization preparedness are noted while at the same time the difficulties pertaining to vendor openness, authentication measures, and patch management are highlighted. Strong positive correlations between all variables used in this study prove the efficiency of risk management in case of integrated security governance.

REFERENCES

[1] A. Brown, J. Fishenden, and M. Thompson, "API economy, ecosystems and engagement models," in Palgrave Macmillan UK eBooks, pp. 225–236, 2014, doi: 10.1057/9781137443649_13.

[2] S. Dalmolen, H. Moonen, and J. Van Hillegersberg, "Building a supply chain ecosystem: How the Enterprise Connectivity Interface (ECI) will enable and support interorganisational collaboration," Lecture Notes in Business Information Processing, pp. 228–239, 2015, doi: 10.1007/978-3-319-26739-5_13.

[3] D. Ahlers, L. W. M. Wienhofen, S. A. Petersen, and M. Anvaari, "A smart city ecosystem enabling open innovation," Communications in Computer and Information Science, pp. 109–122, 2019, doi: 10.1007/978-3-030-22482-0_9.

[4] S. K. Shivakumar, "Digital workplace development," in Apress eBooks, pp. 77–108, 2019, doi: 10.1007/978-1-4842-5512-4_4.

[5] A. Loukiala, J. Joutsenlahti, M. Raatikainen, T. Mikkonen, and T. Lehtonen, "Migrating from a centralized data warehouse to a decentralized data platform architecture," Lecture Notes in Computer Science, pp. 36–48, 2021, doi: 10.1007/978-3-030-91452-3_3.

[6] C. Tselios and G. Tsolis, "A survey on software tools and architectures for deploying multimedia-aware cloud applications," Lecture Notes in Computer Science, pp. 168–180, 2016, doi: 10.1007/978-3-319-29919-8_13.

[7] S. K. Shivakumar, "Modern web platform performance principles," in Apress eBooks, pp. 105–143, 2020, doi: 10.1007/978-1-4842-6528-4_5.

[8] P. Raj and A. Raman, "The distinct trends and transitions in the information technology (IT) space," in Computer Communications and Networks, pp. 1–12, 2018, doi: 10.1007/978-3-319-78637-7_1.

[9] A. Portier, H. Carter, and C. Lever, "Security in plain TXT," Lecture Notes in Computer Science, pp. 374–395, 2019, doi: 10.1007/978-3-030-22038-9_18.

[10] İ. Met, D. Kabukçu, G. Uzunoğulları, Ü. Soyalp, and T. Dakdevir, "Transformation of business model in finance sector with artificial intelligence and robotic process automation," in Contributions to Management Science, pp. 3–29, 2019, doi: 10.1007/978-3-030-29739-8_1.

[11] E. Bertin, N. Crespi, and T. Magedanz, "Evolution of telecommunication services," Lecture Notes in Computer Science, 2013, doi: 10.1007/978-3-642-41569-2.

[12] B. Nicoletti, "Partnerships in Banking 5.0," in Palgrave Studies in Financial Services Technology, pp. 359–368, 2021, doi: 10.1007/978-3-030-75871-4_11.

[13] M. T. Jakóbczyk, "Cloud-native architecture," in Apress eBooks, pp. 487–551, 2020, doi: 10.1007/978-1-4842-5506-3_9.

[14] S. Furnell, P. Fischer, and A. Finch, "Can't get the staff? The growing need for cyber-security skills," Computer Fraud & Security, vol. 2017, no. 2, pp. 5–10, 2017, doi: 10.1016/S1361-3723(17)30013-1.

[15] J. H. Cheung, D. K. Burns, R. R. Sinclair, and M. Sliter, "Amazon Mechanical Turk in organizational psychology: An evaluation and practical recommendations," Journal of Business and Psychology, vol. 32, no. 4, pp. 347–361, 2016, doi: 10.1007/s10869-016-9458-5.

[16] M. P. Robillard and R. DeLine, "A field study of API learning obstacles," Empirical Software Engineering, vol. 16, no. 6, pp. 703–732, 2010, doi: 10.1007/s10664-010-9150-8.

[17] C. Cheng, H. Yao, and T. Wu, "Applying data mining techniques to analyze the causes of major occupational accidents in the petrochemical industry," Journal of Loss Prevention in the Process Industries, vol. 26, no. 6, pp.

1269–1278, 2013, doi: 10.1016/j.jlp.2013.07.002.

[18] T. Dagget, A. Molla, and T. Belachew, "Job related stress among nurses working in Jimma Zone public hospitals, South West Ethiopia: A cross sectional study," BMC Nursing, vol. 15, no. 1, Art. no. 39, 2016, doi: 10.1186/s12912-016-0158-2.

[19] M. Sarstedt and E. Mooi, "Descriptive statistics," in Springer Texts in Business and Economics, pp. 91–150, 2018, doi: 10.1007/978-3-662-56707-4_5.

[20] D. Yang and M. Li, "Evolutionary approaches and the construction of technology-driven regulations," Emerging Markets Finance and Trade, vol. 54, no. 14, pp. 3256–3271, 2018, doi: 10.1080/1540496X.2018.1496422.

[21] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," Future Generation Computer Systems, vol. 56, pp. 719–733, 2015, doi: 10.1016/j.future.2015.09.003.

[22] K. D. Mandl et al., "The Genomics Research and Innovation Network: Creating an interoperable, federated, genomics learning system," Genetics in Medicine, vol. 22, no. 2, pp. 371–380, 2019, doi: 10.1038/s41436-019-0646-3.

[23] S. Preibisch, "Real-life API examples," in Apress eBooks, pp. 159–169, 2018, doi: 10.1007/978-1-4842-4140-0_9.

[24] E. Varga, "Modular design," in Apress eBooks, pp. 17–43, 2016, doi: 10.1007/978-1-4842-2196-9_2.

[25] V. Pizurica and P. Vandaele, "A cloud-based Bayesian smart agent architecture for Internet-of-Things applications," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 42–47, 2015, doi: 10.1007/978-3-319-19656-5_6.

[26] P. Daugherty and J. Euchner, "Human + machine: Collaboration in the age of AI," Research-Technology Management, vol. 63, no. 2, pp. 12–17, 2020, doi: 10.1080/08956308.2020.1707001.

[27] L. O. Colombo-Mendoza, R. Valencia-García, R. Colomo-Palacios, and G. Alor-Hernández, "A knowledge-based multi-criteria collaborative filtering approach for discovering services in mobile cloud computing platforms," Journal of Intelligent Information Systems, vol. 54, no. 1, pp. 179–203, 2018, doi: 10.1007/s10844-018-0527-2.

[28] S. Varghese, "Authentication to web apps," in Apress eBooks, pp. 121–140, 2015, doi: 10.1007/978-1-4842-1052-9_7.

[29] S. Ganguly, "QML: Way forward," in Apress eBooks, pp. 461–496, 2021, doi: 10.1007/978-1-4842-7098-1_9.