THE COMPUTERTECH
(An International Peer Review Journal)
VOLUME 7; ISSUE 1(JAN-JUNE); (2021)
WEBSITE: THE COMPUTERTECH

CCPA vs. CPRA: A Deep Dive into Their Impact on Data Privacy and Compliance

Bharath Kishore Gudepu[1], Rebecca Eichler[2]
[1]Senior EDC Developer, State Farm, CityLine Building 1, Richardson, TX, 75085
[2]PRA Group Inc., USA

Abstract

Personal data privacy is a top priority in the digital age, leading to strict legislation like the General Data privacy Regulation (GDPR) and California Consumer Privacy Act (CCPA). This research study examines the relationship between data privacy, legislative frameworks, and the importance of IT audits. The literature study highlights the importance of data privacy in the digital ecosystem, focusing on GDPR and CCPA as relevant benchmarks and evaluating geographic variances in data protection policies. The report outlines the many components of good IT audits, including risk assessment, compliance evaluations, security controls, incident response plans, and rigorous documentation. The study emphasizes the need for vendor and third-party audits to strengthen data protection procedures due to the linked nature of the digital economy. The conclusion emphasizes the importance of a comprehensive approach to data privacy regulation, including ongoing monitoring, adaptation, and proactive risk management. The guidelines encourage firms to invest in developing technology, provide frequent training, and improve collaboration with third parties. This research adds to the discussion on strengthening data security measures, offering significant insights for practitioners, policymakers, and researchers in the ever-changing field of data privacy.

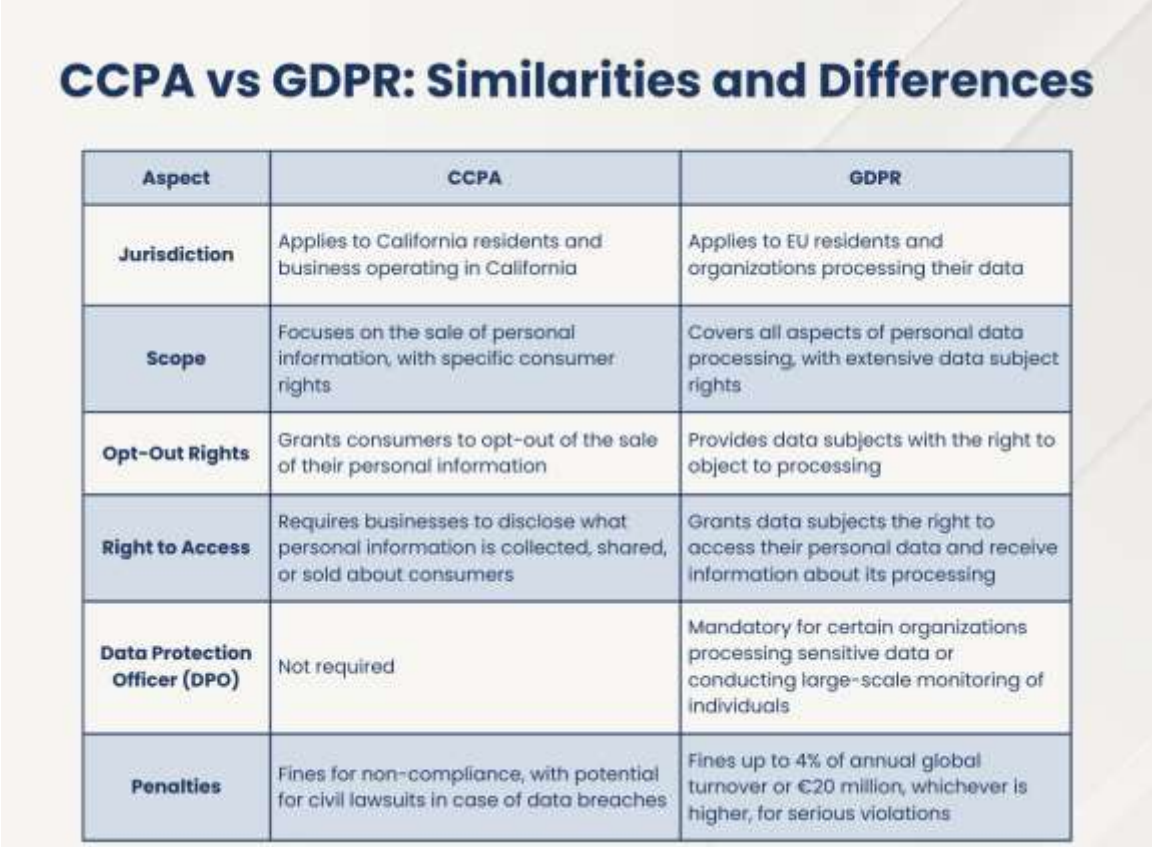
Keywords: CCPA, CPRA, Compliance, Data Privacy, Data Governance, Data Management, Data Quality, Metadata, Data Security, Enterprise Data, Data Discovery, Data Catalog, Regulatory Strategy, GDPR, NYDFS

Introduction

Owing to swift technological advancement, firms increasingly depend on data to facilitate decision-making and secure competitive advantage. To make educated and successful judgments, it is essential to evaluate and ensure the quality of the foundational data. According to a poll by Experian Information Solutions, 83% of respondents indicate that inadequate data quality has adversely affected their business objectives, while 66% assert that it has negatively impacted their company in the past twelve months. A separate research indicates that 84% of CEOs express worry over the quality of the data utilized for decision-making. Moreover, Gartner reports that the average cost repercussions of inadequate data quality are $9.7 million year per firm. It is projected that inadequate data quality incurs an annual cost of $3.1 trillion to the US. Given the current surge of big data characterized by vast quantities of heterogeneous and rapidly evolving information from diverse sources analyzed for decision-making support, the evaluation and assurance of data quality has become increasingly pertinent. The three characteristics of Volume, Velocity, and Variety, commonly referred to as the three Vs of big data, complicate the assurance of data quality,

particularly due to the integration of diverse data sources and the consideration of linked data. Consequently, the repercussions of erroneous judgments are increasingly expensive. This has led to the incorporation of a fourth V (=Veracity), underscoring the significance of data quality within the realm of big data [1-4].

Data quality is defined as "the measure of the concordance between the data representations provided by an information system and the corresponding data in the real world". Data quality is a multi-faceted concept that encompasses several characteristics, including correctness, completeness, consistency, and currency. Each degree of data quality offers a par specific viewpoint on the quality of data representations. Consequently, researchers have established relevant metrics for the quantitative evaluation of these dimensions concerning data views. This study focuses on metrics that evaluate data quality aspects for data views and values stored in information systems. Conversely, measures pertaining to the quality of data methods are not explicitly addressed.



Data quality measures quantify data perspectives, with higher (lower) metric values indicating superior (worse) data quality, and each degree of data quality denoted by a distinct metric value. They are required for two primary reasons. The metric values facilitate data-driven decision-making under uncertain conditions. Robust data quality measurements are necessary to determine the degree to which decision-makers may depend on the underlying data values. Secondly, the metric values provide an economically driven approach to data quality control. Data quality enhancement techniques should be implemented just when the advantages of improved data quality surpass the related expenses. To study the economic efficiency of data quality enhancement

methods, robust data quality metrics are required to evaluate the changes in data quality levels [4-11].

To tackle this research inquiry, we propose five stipulations: the presence of minimum and maximum metric values (R1), the interval scaling of the metric values (R2), the integrity of the configuration parameters and the ascertainment of the metric values (R3), the robust aggregation of the metric values (R4), and the economic viability of the metric (R5).

We examine the current literature and substantiate this collection of needs using a decision-oriented framework. Consequently, our standards facilitate decision-making during uncertainty and promote an economically driven approach to data quality management. Data quality metrics that fail to fulfill standards might result in erroneous decisions and/or financial losses (e.g., due to the lack of assurance in the metric's application efficiency). Furthermore, the outlined standards enable a robust evaluation of data quality, essential for bolstering data governance efforts.

The necessity for such standards is also corroborated by discourse in other study domains, including software engineering. A comprehensive set of criteria for the robust definition of software metrics. The suggested qualities may be utilized by researchers to "validate their new measures" (p. 2) and can be regarded as essential criteria for software metrics. Moreover, within the framework of ISO/IEC standards, the SQuaRE series seeks to "aid those involved in the development and procurement of software products in the specification and assessment of quality requirements". Specifically, ISO/IEC 25020 delineates criteria for the selection of software quality metrics, motivated by the same rationale as previously mentioned.

Qualitative Results (Interviews and Document Analysis)

Key Compliance Challenges

Interviews with Data Protection Officers (DPOs), Chief Compliance Officers (CCOs), and Legal Managers identified many prevalent problems in attaining and sustaining compliance with GDPR and CCPA:

• Cross-Border Compliance: Multinational corporations faced challenges in reconciling GDPR's extraterritorial stipulations with local requirements in various jurisdictions, especially in nations with less rigorous privacy legislation.

• Data Mapping and Inventory: Numerous businesses indicated challenges in precisely mapping data flows and sustaining a thorough inventory of personal data across diverse departments and systems.

• Consumer Rights Management: The data subject rights under GDPR (access, correction, deletion) and the opt-out provisions of CCPA posed obstacles, especially in fulfilling consumer requests promptly. Large firms possessing extensive consumer data encountered challenges in monitoring and addressing requests within mandated times.

• Training and understanding: Although leadership demonstrated considerable understanding, several workers, especially those in non-technical positions, were deficient in training on privacy best practices and data security responsibilities [12-19].

Strategies and Technologies for Compliance

Organizations implemented many solutions to tackle these challenges:

• Centralized Privacy Governance: Numerous big firms have instituted specialized privacy departments or designated a Data Protection Officer (DPO) to guarantee compliance with GDPR and CCPA. Smaller enterprises frequently delegated privacy management to external consultants or service providers.

The implementation of privacy-by-design principles was prevalent, particularly among enterprises creating new goods or services. Businesses used data reduction strategies and assured the incorporation of privacy protections throughout the product development lifecycle.

• Technological Instruments: The utilization of technology was essential for adherence. Automated data mapping tools, encryption technologies, and privacy management platforms (e.g., OneTrust, TrustArc) were frequently utilized to oversee data inventory, monitor consent, and address data subject access requests (DSARs).

Organizational Modifications and Capital Allocation

An examination of internal compliance reports indicated a substantial investment in data security infrastructure.

• Personnel: Organizations employed or educated designated personnel in data privacy, encompassing legal experts, IT security specialists, and compliance officials.

• Policy Revision: Numerous firms updated their privacy policies and terms of service to comply with GDPR and CCPA mandates. Continuous compliance monitoring was established through regular audits and evaluations.

• Data Security Enhancements: To comply with GDPR's security mandates and CCPA's data protection provisions, enterprises have made substantial investments in cybersecurity technology, including encryption, access restrictions, and real-time breach detection systems [20-27].

Quantitative Findings (Survey)

Degree of Compliance

• GDPR Compliance: Among the polled firms, 85% indicated complete or partial compliance with GDPR, with large corporations (over 500 workers) exhibiting greater compliance rates (90%) than SMEs (70%).

• CCPA Compliance: Seventy-eight percent of organizations in California reported either complete or partial compliance with the CCPA. Among enterprises operating outside California yet servicing California residents, 62% reported complete or partial compliance with CCPA rules.

Distribution of Resources

• Compliance Expenditures: Organizations typically incurred yearly costs ranging from $50,000 to $200,000 for compliance-related operations, with bigger enterprises dedicating greater resources to the implementation of compliance programs.

• Technology Investment: 60% of participants reported substantial investment in privacy technology, including automated data inventory and consent management systems. Forty percent of smaller enterprises indicated insufficient money for such technologies, resorting to manual operations or external services instead.

Incidence of Data Breaches and Violations

• Data Breaches: 18% of participants indicated experiencing at least one data breach or security issue concerning personal data in the previous year. Among these breaches, 12% pertained to non-compliance with GDPR or CCPA regulations, underscoring the peril of failing to adhere to these standards.

• Fines and Penalties: 4% of surveyed enterprises faced penalties for non-compliance with data protection regulations. Although most fines were below $100,000, bigger entities claimed penalties over $1 million, especially for infractions concerning data processing or failures in breach notification.

Effects on Reputations

• Consumer Trust: Seventy percent of enterprises reported that adherence to GDPR and CCPA positively influenced customer trust and satisfaction, as consumers exhibited increased confidence in companies that implemented stringent privacy measures.

• Reputational Harm: Sixteen percent of corporations who had a data breach or compliance violation reported reputational harm, with certain enterprises seeing diminished consumer loyalty and a reduction in market share.

Principal Themes and Patterns

Organizational Acumen and Culture

Organizations exhibiting the greatest compliance levels were those that incorporated data privacy into their business ethos. These firms shown robust commitment from senior management, consistently informed staff about data privacy issues, and implemented yearly privacy awareness training.

Inter-Jurisdictional Challenges

The research revealed that multinational corporations, particularly those functioning in both the EU and the US, encountered difficulties in adhering to diverse and occasionally contradictory data privacy regulations. The extraterritorial scope of GDPR necessitated firms to modify their worldwide data management methods, whereas CCPA presented new obstacles in administering consumer rights for residents of California.

Fiscal and Operational Liabilities

The financial repercussions of compliance were particularly pronounced for smaller enterprises, which saw more challenges in allocating requisite resources for compliance initiatives. In contrast, larger organizations have greater resources, enabling them to execute more extensive compliance procedures, such as employing dedicated workers and utilizing specialist privacy management systems.

Results and Discussion

GDPR and CCPA have profoundly influenced company compliance operations, necessitating considerable expenditures in data governance, technology, and human resources. Organizations that proactively embrace privacy-by-design principles and incorporate compliance into their organizational culture encounter more seamless deployment and reduced compliance difficulties. Non-compliance with these standards may lead to significant financial and reputational repercussions, including fines, violations, and erosion of customer trust.

Technological solutions are essential for facilitating compliance, especially in maintaining data inventories, addressing consumer demands, and safeguarding data security. The analysis underscores the necessity for continuous attention and investment in data privacy as a strategic element of corporate governance. These findings highlight the necessity for organizations to comply with GDPR and CCPA while also embracing a long-term, strategic framework for data

privacy, acknowledging it as a catalyst for trust, competitive advantage, and organizational resilience.

This study's results illustrate the substantial influence of data privacy rules such as GDPR and CCPA on company compliance initiatives. Through the analysis of qualitative and quantitative data, we may derive insights regarding organizational responses to these requirements, the problems encountered, and the long-term ramifications of non-compliance. This discourse contextualizes these findings within the wider framework of business compliance, data privacy, and the changing legal environment.

Effects of GDPR and CCPA on Corporate Compliance

The results affirm that GDPR and CCPA have significantly transformed organizational data privacy management. Both legislation have initiated a transition from reactive data protection measures to proactive compliance initiatives. Organizations have progressed beyond basic data security.

Measures for developing comprehensive privacy programs that encompass governance frameworks, personnel training, technological integration, and stringent risk management standards.

A significant conclusion is that larger firms with greater resources are more adept at achieving compliance, mostly because they can commit considerable funds to data privacy programs and invest in specialist technological solutions. For smaller enterprises, the expense of compliance is a significant obstacle, as evidenced by the discovery that 40% of SMEs depend on manual procedures or external services to fulfill compliance obligations. This resource discrepancy indicates that regulatory authorities and legislators ought to implement assistance mechanisms for smaller firms to enable compliance with the more intricate data privacy regulations.

Challenges in Compliance

The research identifies several ongoing obstacles that firms have in attaining complete adherence to GDPR and CCPA. Cross-border compliance continues to be a significant challenge, especially for multinational corporations functioning in jurisdictions with disparate or less rigorous data privacy regulations. The extraterritorial implementation of GDPR introduces complexity for enterprises managing data across numerous countries, necessitating navigation via diverse regulatory frameworks and differing data protection policies.

The implementation of consumer rights, including those specified in the CCPA (right to opt-out) and GDPR (right to access, amend, or delete personal data), remains a significant challenge. The obligation for enterprises to address data subject requests within stringent deadlines exerts strain on businesses, particularly those with extensive data sets and dispersed data storage systems. The findings underscore the necessity of incorporating effective data management systems and procedures to facilitate compliance with these rights, which may be resource-intensive. Furthermore, the intricacy of sustaining exhaustive data inventories and guaranteeing openness in data processing procedures continues to pose a barrier. Organizations must consistently revise their data maps and evaluate their data management policies to comply with the accountability mandates of both GDPR and CCPA [28-36].

Technological Solutions and Privacy by Design

A prominent topic arising from the findings is the essential function of technology in facilitating compliance. The use of privacy-by-design principles represents a significant strategic transformation in several enterprises. By integrating privacy issues into the initial creation of products and services, organizations ensure regulatory compliance while fostering consumer confidence. Technologies such as automated data mapping tools, encryption systems, and privacy management platforms are empowering enterprises to more efficiently monitor, safeguard, and administer personal data.

Nonetheless, dependence on technology has both advantages and hazards. These solutions enable enterprises to comply with data privacy requirements more effectively. Conversely, they need continuous oversight, education, and investment to guarantee that the technology stays compliant with changing regulatory standards. This is particularly pertinent in the realm of AI and machine learning, where automated methods are progressively employed to handle data subject requests and monitor permission. Although these technologies are beneficial, they also elicit concerns around data quality, privacy vulnerabilities, and the possibility of algorithmic inaccuracies if inadequately supervised.

Monetary and Reputational Ramifications of Non-Compliance

The financial and reputational consequences of non-compliance are substantial and cannot be minimized. The research indicates that entities who do not adhere to GDPR and CCPA encounter include direct financial penalties (e.g., fines) and indirect repercussions such as erosion of customer trust, reputational harm, and a decrease in market share. Sixteen percent of firms cited reputational harm following data breaches or non-compliance.

Compliance problems underscore the increasing significance of customer trust in the contemporary data-driven economy. As public knowledge of data privacy rights grows, customers are increasingly inclined to hold corporations liable for the improper management of their personal data. This change in customer expectations indicates that corporations must perceive compliance not just as a legal responsibility but as a strategic commercial benefit. Organizations that actively exhibit their dedication to data security and privacy are more inclined to maintain customer loyalty and appeal to privacy-aware consumers.

Moreover, the expenses associated with non-compliance surpass mere penalties. The enduring harm to a company's brand, customer relations, and market reputation can lead to a diminished competitive edge. This highlights the significance of perceiving data privacy not only as a legislative obligation but as a strategic asset that bolsters confidence and brand equity.

Organizational Culture and Governance

The research emphasizes the essential importance of corporate culture in facilitating effective compliance. Organizations that include privacy into their fundamental principles and governance frameworks typically exhibit more robust compliance processes. The results indicate that organizations with specialized privacy divisions, regular staff training, and strong leadership commitment to data security are more adept at ensuring compliance with GDPR and CCPA.

Particularly, larger corporations have established extensive governance frameworks, with appointed Data Protection Officers (DPOs) and privacy committees to supervise compliance initiatives. Smaller firms frequently lack the necessary resources, hindering their capacity to handle compliance efficiently, especially given the complexity and breadth of the requirements.

The research underscores the necessity for ongoing education and training regarding data protection, since several employees in non-technical positions lack awareness of their responsibilities under GDPR and CCPA. To cultivate a privacy-conscious culture, firms must deliver consistent training and updates on data privacy rules and best practices at all organizational levels.

Worldwide Consequences and Prospective Pathways

As global data privacy standards grow, the report reveals that organizations operating in several countries must remain agile and swiftly react to new legal changes. The growing trend of data localization statutes and the emergence of analogous privacy legislation in several nations indicate that enterprises would encounter heightened difficulty in overseeing cross-border data transfers.

Future study may examine the enduring impacts of GDPR and CCPA on corporate performance, specifically on market share, customer loyalty, and financial outcomes. Moreover, an in-depth examination of how corporations are utilizing new technologies such as blockchain and AI to improve compliance may yield significant insights into the forthcoming generation of privacy solutions.

This study's findings demonstrate that GDPR and CCPA significantly influence business compliance programs, compelling firms to implement more stringent data protection safeguards and reevaluate their strategies around customer data. Although these restrictions have presented considerable hurdles, they have simultaneously provided firms with the chance to cultivate customer trust and distinguish themselves in the market. In the future, organizations must

Continuously adjust to the changing regulatory environment and invest in the technology, procedures, and organizational culture required to maintain compliance.

Conclusion

This report offers a thorough examination of the effects of data privacy rules, namely the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), on company compliance initiatives. Utilizing a mixed-methods approach that integrates qualitative and quantitative data, we have acquired significant insights on organizational responses to these requirements, the problems encountered, and the tactics implemented to assure compliance.

The principal findings demonstrate that GDPR and CCPA have profoundly altered business perspectives on data protection. Large corporations with substantial resources are more equipped to adhere to these requirements, but smaller enterprises encounter heightened difficulties due to the financial and operational burdens of compliance. Despite these obstacles, organizations that actively engage in privacy governance, staff education, and technical solutions are more likely to achieve seamless adoption and sustained success in controlling data privacy concerns.

The research underscores the significance of customer trust and the reputational ramifications of non-compliance. As data privacy concerns increasingly influence consumer decision-making, firms must perceive compliance not only as a legal requirement, but as a strategic opportunity to enhance brand value and sustain customer loyalty. The findings emphasize the necessity of incorporating data privacy into the company culture, supported by explicit governance frameworks and continuous training to guarantee that personnel at all tiers comprehend their responsibilities in upholding compliance.

Technological instruments, like automated data mapping software, consent management platforms, and data encryption systems, are crucial in facilitating compliance initiatives. Nonetheless, dependence on technology necessitates continuous oversight and upgrades to guarantee that these instruments stay efficient and compliant with changing standards. The research suggests that the financial burden of compliance, although onerous for smaller entities, may be alleviated by appropriate investments in privacy infrastructure and smart alliances with third-party service providers. This research highlights the extensive worldwide ramifications of data privacy rules. As privacy legislation progresses, firms must remain flexible and adjust to the changing legal environment. Organizations that prioritize data privacy as an essential business practice will be more adept at adapting to forthcoming legal alterations and sustaining competitive advantages in an increasingly data-centric environment.

GDPR and CCPA have significantly altered corporate compliance procedures, compelling organizations to prioritize data protection in novel manners. To thrive in the changing regulatory landscape, firms must implement a comprehensive strategy to privacy governance that amalgamates legal, technical, and organizational solutions. In the future, enterprises that uphold a robust dedication to data security and customer privacy will not only achieve compliance but also cultivate enduring trust and enhance their market standing.

References:

[1] Pemmasani, P.K. and M. Osaka. (2021) The Future of Smart Cities: Cybersecurity Challenges in Public Infrastructure Management. International Journal of Modern Computing. 4(1): 72-85.

[2] Gonugunta, K.C. and K. Leo. (2018) Oracle Analytics to Predicting Prison Violence. International Journal of Modern Computing. 1(1): 23-31.

[3] Gonugunta, K.C. and K. Leo. (2019) Practical Oracle Cloud for Governments. The Computertech. 34-44.

[4] Malhotra, I., Gopinath, S., Janga, K. C., Greenberg, S., Sharma, S. K., & Tarkovsky, R. (2014). Unpredictable nature of tolvaptan in treatment of hypervolemic hyponatremia: case review on role of vaptans. Case reports in endocrinology, 2014(1), 807054.

[5] Singh, V. K., Mishra, A., Gupta, K. K., Misra, R., & Patel, M. L. (2015). Reduction of microalbuminuria in type-2 diabetes mellitus with angiotensin-converting enzyme inhibitor alone and with cilnidipine. Indian Journal of Nephrology, 25(6), 334-339.

[6] Gonugunta, K.C. and K. Leo. (2019) The Unexplored Territory in Data Ware Housing. The Computertech. 31-39.

[7] Pemmasani, P.K. and M. Osaka. (2019) Red Teaming as a Service (RTaaS): Proactive Defense Strategies for IT Cloud Ecosystems. The Computertech. 24-30.

[8] Karakolias, S. E., & Polyzos, N. M. (2014). The newly established unified healthcare fund (EOPYY): current situation and proposed structural changes, towards an upgraded model of primary health care, in Greece. Health, 2014.
[9] Gonugunta, K.C. (2018) ZDL-Zero Data Loss Appliance–How It Helped DOC in Future-Proofing Data. International Journal of Modern Computing. 1(1): 32-37.
[10] Gonugunta, K.C. (2018) Role of Analytics in Offender Management Systems. The Computertech. 27-36.
[11] Pemmasani, P.K., M. Osaka, and D. Henry. (2021) From Vulnerability to Victory: Enterprise-Scale Security Innovations in Public Health. International Journal of Modern Computing. 4(1): 50-60.
[12] Shilpa, Lalitha, Prakash, A., & Rao, S. (2009). BFHI in a tertiary care hospital: Does being Baby friendly affect lactation success?. The Indian Journal of Pediatrics, 76, 655-657.
[13] Polyzos, N. (2015). Current and future insight into human resources for health in Greece. Open Journal of Social Sciences, 3(05), 5.
[14] Gopinath, S., Janga, K. C., Greenberg, S., & Sharma, S. K. (2013). Tolvaptan in the treatment of acute hyponatremia associated with acute kidney injury. Case reports in nephrology, 2013(1), 801575.
[15] Gonugunta, K.C. (2019) Weblogic and Oracle-Revolutionizing Offender Management System. International Journal of Modern Computing. 2(1): 26-39.
[16] Pasham, S.D. (2018) Dynamic Resource Provisioning in Cloud Environments Using Predictive Analytics. The Computertech. 1-28.
[17] Pasham, S.D. (2019) Energy-Efficient Task Scheduling in Distributed Edge Networks Using Reinforcement Learning. The Computertech. 1-23.
[18] Gonugunta, K.C. (2018) Apply Machine Learning Oracle Analytics–Combined. The Computertech. 37-44.
[19] Pemmasani, P.K. and M. Osaka. (2019) Cloud-Based Health Information Systems: Balancing Accessibility with Cybersecurity Risks. The Computertech. 22-33.
[20] Gonugunta, K.C. (2019) Utilization of Data in Reducing Recidivism in Nevada Prisons. International Journal of Modern Computing. 2(1): 40-49.
[21] Gopinath, S., Giambarberi, L., Patil, S., & Chamberlain, R. S. (2016). Characteristics and survival of patients with eccrine carcinoma: a cohort study. Journal of the American Academy of Dermatology, 75(1), 215-217.
[22] Swarnagowri, B. N., & Gopinath, S. (2013). Ambiguity in diagnosing esthesioneuroblastoma--a case report. Journal of Evolution of Medical and Dental Sciences, 2(43), 8251-8255.
[23] Gonugunta, K.C. (2016) Oracle performance: Automatic Database Diagnostic Monitoring. The Computertech. 1-4.
[24] Gonugunta, K.C. and K. Leo. (2017) Role-Based Access Privileges in a Complex Hierarchical Setup. The Computertech. 25-30.
[25] Pemmasani, P.K., K. Anderson, and S. Falope. (2020) Disaster Recovery in Healthcare: The Role of Hybrid Cloud Solutions for Data Continuity. The Computertech. 50-57.
[26] Pemmasani, P.K. and D. Henry. (2021) Zero Trust Security for Healthcare Networks: A New Standard for Patient Data Protection. The Computertech. 21-27.
[27] Gopinath, S., Ishak, A., Dhawan, N., Poudel, S., Shrestha, P. S., Singh, P., ... & Michel, G. (2022). Characteristics of COVID-19 breakthrough infections among vaccinated individuals and associated risk factors: A systematic review. Tropical medicine and infectious disease, 7(5), 81.
[28] Gonugunta, K.C. and A. Collins. (2021) Data Virtualization and Advancing Data Migration in Mission Critical Environments. The Computertech. 24-33.
[29] Shilpa, Lalitha, Prakash, A., & Rao, S. (2009). BFHI in a tertiary care hospital: Does being Baby friendly affect lactation success?. The Indian Journal of Pediatrics, 76, 655-657.

[30] Gopinath, S., Giambarberi, L., Patil, S., & Chamberlain, R. S. (2016). Characteristics and survival of patients with eccrine carcinoma: a cohort study. Journal of the American Academy of Dermatology, 75(1), 215-217.

[31] Pasham, S.D. (2017) AI-Driven Cloud Cost Optimization for Small and Medium Enterprises (SMEs). The Computertech. 1-24.

[32] Gopinath, S., Janga, K. C., Greenberg, S., & Sharma, S. K. (2013). Tolvaptan in the treatment of acute hyponatremia associated with acute kidney injury. Case reports in nephrology, 2013(1), 801575.

[33] Pemmasani, P.K. and K. Anderson. (2020) Resilient by Design: Integrating Risk Management into Enterprise Healthcare Systems for the Digital Age. International Journal of Modern Computing. 3(1): 1-10.

[34] Pemmasani, P.K., M. Osaka, and D. Henry. (2021) AI-Powered Fraud Detection in Healthcare Systems: A Data-Driven Approach. The Computertech. 18-23.

[35] Gonugunta, K.C. and T. Sotirios. (2020) Data Warehousing-More Than Just a Data Lake. The Computertech. 52-61.

[36] Gonugunta, K.C. and T. Sotirios. (2020) Advanced Oracle Methodologies for Operational Excellence. International Journal of Modern Computing. 3(1): 11-25.